ICEX España Exportación e Inversiones

FS FICHA SECTOR

COLOMBIA

Ciberseguridad en Colombia

A. CIFRAS CLAVE

Colombia es uno de los países de Latinoamérica en pleno crecimiento de la transformación digital y penetración de Internet, y, como consecuencia, el nivel de ataques cibernéticos también ha crecido considerablemente. Es el segundo país de la región con más incidentes de ciberseguridad hasta agosto de 2021, con 1,8 millones de ciberataques[1].

A continuación, se exponen los principales indicadores para una primera comprensión del sector de la ciberseguridad en Colombia. Hay que tener en cuenta que la evolución de las tecnologías de la información otorga al sector un carácter estratégico para el país.

Indicadores	2019	2020
Población (habitantes)	50.339.443	50.882.884
Índice de conectividad (NRI)	48,77	46,81
Número de empresas TIC	n. d.	41.419
Gasto en ciencia y tecnología[2] (% del PIB a precios constantes)	3,43 %	3,54 %
Hogares con acceso a Internet (%)	51,9 %	56,5 %
Penetración banda ancha fija y móvil (líneas/100 habs.)	13,81/57,7	15,26/63,6
Posición en el *ranking* mundial de ciberseguridad	79	81
Delitos cibernéticos	19.298	35.184
Participación del sector TIC con respecto al valor agregado nacional	3,7 %	3,8 %

Fuente: Banco Mundial, Networked Readiness Index, DANE, Banco de la República, ENTIC, OCDE, Global Cybersecurity Index 2020, Centro Cibernético Policial de Colombia, DANE

[1] https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

[2] Actividades profesionales, científicas y técnicas y fabricación de aparatos y equipo eléctrico, productos informáticos, electrónicos y ópticos.

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

Según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (en adelante MINTIC), la ciberseguridad se define como el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

El sector de la ciberseguridad se divide en dos categorías principales:

A) DESARROLLO DE *SOFTWARE* Y *HARDWARE*

- Anti Fraude
- Anti *Malware*
- *Firewalls* Industriales
- SIEM (Gestión de eventos e información de ciberseguridad)
- Diseño de Redes y Arquitecturas
- Control de acceso y autenticación
- Cumplimiento legal
- Inteligencia de seguridad
- Prevención de fuga de información
- Protección de las comunicaciones
- Seguridad en dispositivos móviles

B) SERVICIOS

- Auditoría de seguridad, planificación y asesoramiento
- Certificación de normativa
- Planes de Continuidad y/o Contingencia
- Cumplimiento legal
- Formación y concienciación
- Gestión de incidentes
- Implantación de soluciones y sistemas
- Seguridad en la nube
- Consultoría y asesoría
- Soporte y mantenimiento

La situación del sector de la ciberseguridad industrial se puede resumir través de la siguiente matriz DAFO:

Debilidades	Fortalezas
- Falta de certificaciones de tecnología OT, procesos y profesionales - Falta de una regulación específica en ciberseguridad industrial - Ausencia de un catálogo de soluciones y servicios en ciberseguridad industrial - Falta de CERT específicos	- Fomento e impulso desde las administraciones públicas (Industria, Interior y Defensa). - Mayor concienciación, especialmente en infraestructuras industriales críticas - Mayor frecuencia de eventos y foros sobre ciberseguridad industrial
Amenazas	**Oportunidades**
- Normativa lenta - Escasez de profesionales cualificados y especializados - Escasez de herramientas de gestión de riesgos específicos de Ciberseguridad Industrial	- Incremento de la demanda en ciberseguridad para Industria 4.0, Inteligencia Artificial e Internet de las cosas (IoT)

Fuente: Centro de Ciberseguridad Industrial en Colombia

La mayor fortaleza de Colombia es en la aplicación de las capacidades técnicas a través de los organismos nacionales y sectoriales, es decir que tengan equipos de respuesta a incidentes de seguridad (CSIRT) activos, participen en un CSIRT regional y que cuenten con mecanismos de notificación para la protección de la infancia en línea. No obstante, debe mejorar en medidas organizativas y legales: legislación sobre ciberseguridad, normativa de protección de datos y sobre infraestructuras críticas.

B.2. Tamaño del mercado

De acuerdo con el Global Cybersecurity Index 2020, el prestigioso *ranking* de ciberseguridad mundial elaborado por la Unión Internacional de Telecomunicaciones (agencia de las Naciones Unidas), entre los 194 Estados miembros, **Colombia alcanzó el puesto 81.º del mundo y el 4.º de Latinoamérica**, por detrás de Brasil, Uruguay y Chile, empeorando dos puestos a nivel regional con respecto al *ranking* de 2019.

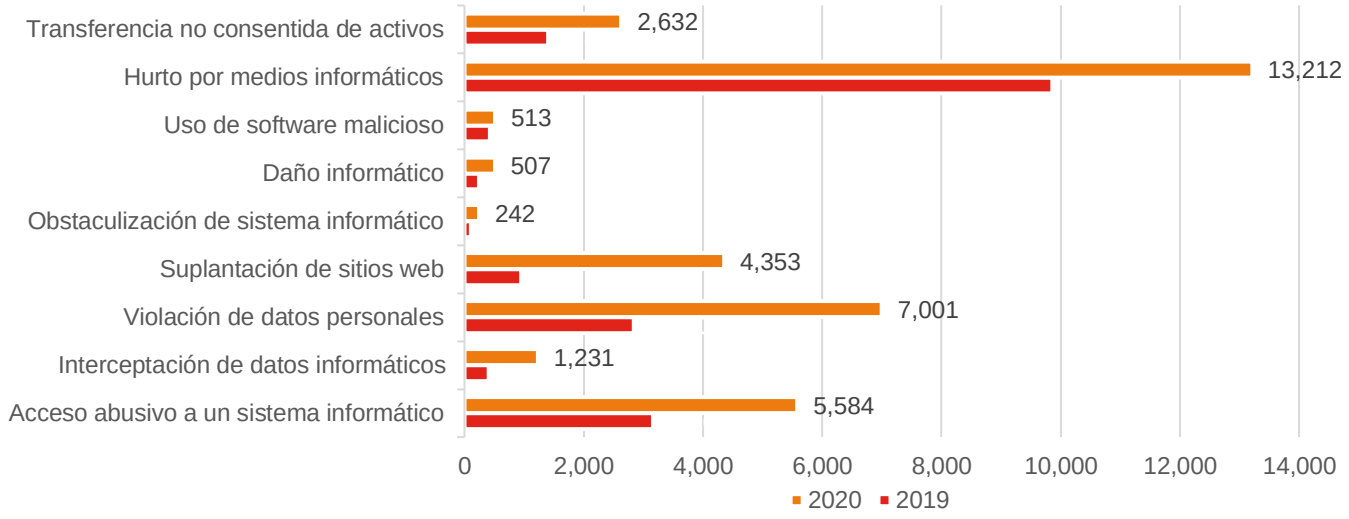
Mientras, según el Ranking Comparitech 2021, Colombia ocupa el puesto 16.º en nivel de en ciberseguridad de 75 países del mundo analizados y **es el país más seguro a nivel digital de Latinoamérica**. De hecho, Colombia destacó como **uno los países con menor índice de usuarios atacados por troyanos de *ransomware* móvil**. Así lo ratifica también el mapa interactivo elaborado por el gigante ruso de la ciberseguridad Kaspersky, para el que Colombia fue uno de los países con menor proporción de usuarios atacados por *malware* móvil durante el primer trimestre de 2021 (2,63 %), el tercero de la región por detrás de Argentina y Perú.

Sin embargo, en Colombia se producen 87 ciberataques por minuto, donde el *phishing* (mensajes fraudulentos) es una de las modalidades de ataque más frecuente, que afectó al 11,09 % de los usuarios atacados entre enero y agosto de 2021, según el informe *Panorama de Amenazas en América Latina 2021*.

Así lo demuestran varios informes, como el Cyber Threat Report 2021, que sitúa a Colombia entre los 10 países del mundo con mayores ataques por *ransomware* (superando los 3,7 millones) y como segundo país de Latinoamérica, por detrás de Brasil. Para el portal de McAfee, **Colombia es el 4.º país del mundo con mayores detecciones maliciosas del mundo**. Concretamente, en lo que va de año 2021 (hasta octubre) ha tenido más de 543.813.

De acuerdo con el Tanque de Análisis y Creatividad de las TIC (TicTac) de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), en 2020 Colombia reportó 32.000 ciberataques; la suplantación de sitios web fue el delito informático con mayor crecimiento, con un 358 %, en comparación con el 2019. Según el Centro Cibernético Policial de Colombia, existe alerta ante el aumento preocupante de los delitos cibernéticos, como demuestra su informe comparativo 2020/2019, donde por ejemplo la violación de datos personales aumentó un 147 %, pasando de 2.840 a 5.794 casos denunciados.

BALANCE DE CIBERCRIMEN 2020



Fuente: Centro Cibernético Policial de Colombia

Datacrédito Experian reveló en su Informe global de *Fraude e Identidad 2021*[3], que Colombia ocupa el tercer lugar, dentro del *top 5* de fraudes, en materia de cibercrimen, generando pérdidas superiores a los 5.285 millones de euros.

Los sectores más afectados son el financiero, salud, educación y gubernamental, aunque todas las industrias pueden ser vulnerables y sufrir costes tanto financieros como reputacionales**.** En 2018, las empresas colombianas invertían un 12 % de su presupuesto de seguridad en ciberataques, en comparación con el 21 % del promedio de la región[4]. Mientras que el gasto en ciberseguridad estimado en 2020 fue de unos 259 millones de euros, un 9 % más que en 2019, representando cerca del 5 % del total de Latinoamérica, cuya cifra supone el 0,10 % del PIB de Colombia en 2020, según datos del Boston Consulting Group (BCG). Para 2021, se proyecta que la inversión en ciberseguridad ascienda aproximadamente a 281 millones de euros, con un porcentaje de crecimiento ligeramente superior al del 8 % estimado para Latinoamérica. De hecho, el 55 % de las empresas colombianas están dispuestas a incrementar el presupuesto que destinan a la ciberseguridad en los próximos tres años[5]. Entre los principales motivos destacaron: el incremento de complejidad de la infraestructura de TI (41,5 %), mejorar el nivel de conocimientos especializados en seguridad (39,6 %) y el aumento de las ganancias (26,4 %).

Según la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria), el presupuesto destinado a la seguridad digital por parte del sector financiero creció un 64 % entre 2019 y 2020, superando los 70 millones de euros[6]. Durante el año pasado, aproximadamente el 41 % del fraude en el sistema financiero se realizó a través de canales digitales, en su mayoría banca móvil (49,83 %), y la ingeniería social por teléfono fue la principal modalidad de ciberataque (78,05 %).

B.3. Principales actores

Colombia cuenta con diversos organismos públicos nacionales que velan por generar un marco legal adecuado, es **miembro tanto de Interpol como de Europol** y ha priorizado su participación en escenarios internacionales para garantizar la progresiva incorporación de la ciberseguridad en todas las estructuras del país. Entre las principales cabe destacar:

- **Grupo de Respuesta a Emergencias Cibernéticas de Colombia** (colCERT), depende del Ministerio de Defensa Nacional, y es el encargado de atender en primer término los incidentes cibernéticos y proteger la infraestructura crítica cibernética nacional (ICCN).
- **Comando de Operaciones Cibernéticas** (SOC-CCOC).
- **Centro Cibernético Policial** (CCP).
- **Equipo de Respuesta a Incidentes de la CCIT** (CSIRT).
- **MinTIC y la Empresa de Telecomunicaciones de Bogotá** (CSIRT-ETB).
- **Comité de Seguridad Digital**, liderado por el Coordinador Nacional de Seguridad Digital, ente máximo para tratar temas intersectoriales de seguridad digital.

Con respecto a las diferentes acciones y políticas públicas por parte del MINTIC, destacan los memorandos de entendimiento firmados con Fortinet para la capacitación, transferencia de conocimiento tecnológico e intercambio de información estratégica sobre amenazas relacionadas con la ciberseguridad y con Asobancaria para la capacitación a 250 administraciones locales y departamentales del país, con el fin de minimizar el nivel de exposición y riesgo ante amenazas o incidentes cibernéticos, cuya afectación ha rondado los 50.000 millones de pesos al año (unos 11,4 millones de euros).

Colombia fue uno de los primeros países del mundo en elaborar leyes específicas en materia de ciberseguridad, con la Ley 1273 de 2009 “Protección de la información y los sistemas de datos”. Asimismo, Colombia fue el primer país de la región en 2011 y, posteriormente en 2016, en aprobar una estrategia nacional de ciberseguridad (NCS,

[3] https://www.semana.com/economia/empresas/articulo/ataques-ciberneticos-en-colombia-han-generado-us-6179-millones-en-perdidas-datacredito-experian/202101/

[4] https://acis.org.co/portal/content/NoticiaDelSector/fortinet-presenta-estudio-sobre-inversiones-en-ciberseguridad-en-colombia

[5] https://latam.kaspersky.com/blog/presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-recortes-por-covid-19/21022/

[6] https://www.portafolio.co/economia/finanzas/bancos-aumentaron-64-gastos-en-ciberseguridad-553594

por sus siglas en inglés), cuyo objetivo general es el de fortalecer las capacidades del Estado para responder a las amenazas en materia de seguridad cibernética y defensa. Además, según el Reporte Ciberseguridad 2020 del BID, Colombia fue el país con mayor desarrollo en seguridad cibernética en las dimensiones "Política y estrategia" y "Cultura y sociedad". Sin embargo, a pesar de los esfuerzos regulatorios del país mediante políticas públicas, leyes estatutarias y otros mecanismos político-legislativos, tanto el sector privado como los ciudadanos aún tienen un amplio margen de mejora en prevención y respuesta ante ciberataques.

Entre las principales leyes y reglamentos nacionales que forman parte de la legislación colombiana se encuentran:

- CONPES 3701 de 2011, Política de Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
- Ley 1341 de 2009, políticas públicas que rigen el sector de las TIC.
- Ley 1621 de 2013, Inteligencia y Contrainteligencia.
- Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia".

Por un lado, en cuanto al sector privado, destacan los siguientes operadores nacionales en destino: Digiware (está en el *top* 5 de empresas de ciberseguridad en Latinoamérica), PSL Corp, Gorilla Logic, Grupo Ouruss, Leanware, MQA, iSy TEk, TICS, Junpack, 2Secure, HeOn Health online, SecPro, Globaltek Security, Grupo Gtd, B-SECURE, Agencia de Marketing Digital, EFEYCE Integrales, Sophos, Schneider Electric.

Por otro lado, también existe una presencia de multinacionales de *hardware* y *software*, servicios de tecnología, consultoras y administradores de seguridad: AWS, Intel, Rockwell, Kaspersky, Paloalto Networks, Cisco Systems, Accenture, Check Point, Phoenix Contact, Siemens, Atos, DeNexus, Getronics, Lumu Technologies, Belden Solutions, eSoft (*partner* oficial de Broadcom), Attivo Networks, NSIT (*partner* de Fortinet), EY, IBM, Deloitte, KPMG, PWC, Thales, NeoSecure, Capgemini, DXC Technology, Dexon Software, VU.

C. LA OFERTA ESPAÑOLA

Según el último Catálogo de Empresas y Soluciones de Ciberseguridad publicado por el Instituto Nacional de Ciberseguridad (INCIBE), existen 1.745 empresas españolas registradas que ofrecen un total de 7.529 soluciones de ciberseguridad.

Entre las siguientes empresas españolas identificadas del sector que operan o tienen interés por Colombia, destacan: AirON, Alai Secure (Seguridad Telco), Ayesa, CIC Consulting Informático, Cipher (división de ciberseguridad de Prosegur), Electronic IDentification, ElevenPaths (Telefónica), Enigmedia, Entelgy Innotec Security, Everis, GMV, Ikusi, Inetum, Micronet, Minsait y Sia (Indra), Mnemo, One eSecurity, Open Cloud Factory, Proactivanet, S21sec, S2Grupo, Seidor, Sothis, Grupo TSK y Tecnalia.

En general, la percepción del sector español de ciberseguridad en el país es buena y en cuanto a colaboración interinstitucional, España es un país de referencia en este sector, gracias a la labor del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), y del INCIBE, que han desarrollado diversos eventos y actividades de formación y de consultoría en materia normativa con la administración colombiana.

D. OPORTUNIDADES DEL MERCADO

Entre las tendencias globales en materia de ciberseguridad para 2021 se han destacado las siguientes:

1. Mayor importancia de la Inteligencia Artificial (IA) y *Machine Learning* (ML).
2. Para 2022 el 35 % de los clientes estará atendido por proveedores de MSS en la nube.
3. Incremento de divisiones políticas y económicas.
4. Interferencia política más sofisticada.
5. Aumento de la brecha de habilidades de ciberseguridad.
6. Aumento del pirateo de datos y robo de vehículos.
7. Vulnerabilidad de los sistemas ICS / SCADA.

8. Crecimiento de ataques a la cadena de suministro.
9. Aumento de las amenazas de la red 5G.

La pandemia ha impulsado y obligado a la transformación digital como alternativa para que las organizaciones continúen operando a distancia. Como consecuencia de ello, los riesgos son cada vez más grandes y el cibercrimen está en auge, por lo que disponer de soluciones de ciberseguridad que permitan estar preparados ante cualquier riesgo es vital. Las principales oportunidades de negocio se presentan en tres ámbitos diferentes:

a) **Servicios de gestión y reporte de incidentes en infraestructuras críticas**: sistemas de defensa, armamento, puertos y aeropuertos, sector energético, telecomunicaciones, agua, etc. Existe un mercado poco explotado y una demanda todavía insatisfecha, provocada por una desconexión entre la seguridad actual y los constantes avances tecnológicos que se presentan en el mercado. Se necesitan mecanismos de análisis, identificación, prevención, investigación y persecución de ciberataques cuyo objetivo sean organismos públicos.
b) **Formación en ciberseguridad**. Existe una acuciante escasez de mano de obra especializada en el sector. Por ello hay que promover y apoyar la I+D+i sobre ciberseguridad, generar conocimientos y soluciones de alto nivel, y desarrollar programas de educación formal (pregrados y posgrados) y no formal (cursos, seminarios, diplomados, etc.) que preparen a los profesionales requeridos para trabajar en ciberseguridad en las diversas organizaciones.
c) Soluciones de seguridad para *e-commerce*. El comercio electrónico creció un 53 % en 2020 y se espera que para 2025 se incremente un 74 %[7]. Los *marketplaces* son conscientes de la importancia de fortalecer la seguridad de sus plataformas digitales y mantener la confianza y privacidad de sus clientes.

Además, con la crisis generada por la COVID-19 han surgido nuevos nichos específicos de demanda de servicios de ciberseguridad en:

- **Sanidad**: protección para dispositivos médicos, historial clínico electrónico, información confidencial, etc.
- **Educación**: *e-learning* y teleformación.
- **Teletrabajo**: plataformas de videoconferencias, servicios en la nube, etc.
- **GovTech**: servicios digitales de las administraciones públicas para la ciudadanía.
- **Sector financiero**: uno de los sectores que más ataques sufre y donde existe un auge de empresas dedicadas a la innovación tecnológica en servicios financieros (*Fintech*).
- **Eventos**: los organizadores deben estar preparados para evitar el colapso de sus eventos virtuales ante ataques cibernéticos.

Por lo tanto, dada la tendencia hacia la digitalización y el uso de herramientas propias de la 4.ª Revolución Industrial, resulta imperativo aplicar medidas preventivas, políticas y acciones de seguridad ante ciberataques tanto en el sector privado como público y la ciudadanía.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

La cadena de valor de la ciberseguridad está compuesta por tres grandes actividades:

- **Fabricación** y desarrollo de los componentes de *software, hardware* y mixtos.
- **Distribución** de productos de ciberseguridad, ya sean empresas **mayoristas** dedicadas a la compra y venta de soluciones a los prestadores de servicios o **minoristas**, puntos de venta de soluciones tales como tiendas de informática, grandes superficies e incluso pequeñas consultoras.
- **Prestación de servicios**, sobre todo de consultoría, que ofrecen servicios de asesoramiento, servicios de seguridad en alojamiento web y SaaS (*Software as a Service*). A su vez, encontramos:

[7] https://www.icex.es/icex/es/navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/paises/navegacion-principal/noticias/comercio-electronico-colombia-new2021890119.html?idPais=CO

- **Integradores**: empresas dedicadas a crear soluciones de ciberseguridad para entornos más complejos, elaborando diagnóstico del problema y las necesidades, diseño e ingeniería de la solución, adaptación al entorno, implementación real y servicio posventa. Normalmente combinan soluciones de diferentes fabricantes y las complementan con soluciones propias.
- **Proveedores de servicios gestionados** (MSSP): ofrecen servicios externalizados de seguridad, incluyendo consultoría, desarrollo, integración, etc.

E.2. Barreras reglamentarias y no reglamentarias

Según el portal de la Secretaría de Estado de Comercio barrerascomerciales.es no existen barreras al comercio e inversión específicas para el sector de la ciberseguridad. No obstante, uno de los obstáculos generales de acceso al mercado colombiano en cualquier sector es el exceso de burocracia del país, sumado a otros factores como:

- **La brecha digital**: el grado de digitalización varia enormemente entre las áreas rurales y urbanas, además de las considerables diferencias entre pymes y grandes empresas.
- **Menor concienciación**: existe una baja concienciación de la ciudadanía colombiana y escaso uso de herramientas de protección y mitigación de riesgos digitales. No obstante, se observa un cambio significativo en los últimos años en Colombia, puesto que en 2017 la ciberseguridad era una preocupación para el 54 % de los CEO y en 2021 lo es ya para el 87 %. Además, dicha preocupación está 9 puntos por encima de la media de la región de acuerdo con la 24.ª Encuesta Global de PWC de CEO 2021.
- **Desconocimiento relativo al reporte de incidentes**, dado que la mayoría de los ciberataques ni siquiera se comunican a las autoridades competentes. Esto se debe a múltiples razones, entre las que destacan el desconocimiento de los procedimientos adecuados, la mala imagen del sistema fiscal colombiano, así como a aspectos relativos a la reputación de la propia empresa que sufre un ciberataque.
- **Aversión a la tecnología extranjera**. Según ProColombia, el 40 % de los mercados en desarrollo exigirán el uso de proveedores locales de ciberseguridad para asegurar el gobierno e infraestructura crítica.

E.3. Ayudas

A modo de interés, el MinTIC lazó en 2021 una convocatoria nacional para capacitar gratuitamente a 540 empleados y directivos del país en seguridad informática mediante el diplomado Habilidades Digitales-Ciberseguridad.

E.4. Ferias

- **2.º Foro Internacional de Pensamiento Estratégico de la Seguridad Empresarial,** del 22 al 24 de noviembre de 2021.
- **Expodefensa 2021,** del 29 noviembre al 1 de diciembre de 2021
- **ANDICOM, Congreso Internacional de TIC,** del 17 al 19 de noviembre de 2021.
- **Meditech**, Feria Internacional de la salud, del 12 al 15 de julio de 2022.
- **Feria Internacional de Seguridad ESS+,** del 24 al 26 de agosto de 2022.

F. INFORMACIÓN ADICIONAL

Los principales organismos colaboradores que tener en cuenta a la hora de internacionalizar una empresa de este sector son los siguientes:

- **PROCOLOMBIA**: http://www.procolombia.co/
- **CAF**: https://www.caf.com/
- **BID**: https://www.iadb.org/es
- **CDTI**: https://www.cdti.es/
- **Invest in Bogotá**: https://es.investinbogota.org/
- **ACI Medellín**: https://www.acimedellin.org/

G. CONTACTO

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

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

Carrera 9A, N.º 99-07, Piso 9 Torre “La Equidad”
Bogotá - Colombia
Teléfono: +57 (1) 5202002
Email: bogota@comercio.mineco.es
http://colombia.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

AUTOR
Omar Reyes Castro

Oficina Económica y Comercial
de España en Bogotá
bogota@comercio.mineco.es
Fecha: 03/11/2021

NIPO: 114-21-012-2