

Ciberseguridad en Perú

A. CIFRAS CLAVE

El mercado de la ciberseguridad en Perú muestra un entorno en desarrollo, donde la capacidad técnica para proteger sistemas y redes digitales es una prioridad. En 2022, el país registró 15.000 millones de ciberataques, con un aumento significativo del 35 % respecto al año anterior. A pesar de sus esfuerzos por reforzar la seguridad digital, Perú se encuentra en una etapa temprana en comparación con otros países de la región, como queda reflejado en su clasificación en índices internacionales. En pleno proceso de transformación digital, Perú destaca por su compromiso en la cooperación internacional para abordar el crimen informático, resaltando la importancia de fortalecer el marco legal en ciberseguridad.

Datos del mercado en Perú	
Población total de Perú 2022 (habs.)	34.049.588
Usuarios de Internet en Perú (% de población), 2022	75 %
Hogares con acceso a Internet en Perú, 2022	9.221.837
Clasificación de Perú en el Índice Global de Ciberseguridad (GCI), 2020	86 / 165
Clasificación de Perú en el Índice de Conectividad (NRI), 2022	78 / 131
Clasificación de Perú en Índice Global de Innovación (GII), 2023	76 / 132
Número total de ciberataques en Perú, 2022	15.000 M
Ingresos del mercado de ciberseguridad en Perú, 2022	104,7 MEUR

Fuente: [Banco Mundial](#), [Banco Mundial](#), [El Peruano](#), [Global Cybersecurity Index](#), [Network Rediness Index](#), [WIPO](#), [El Comercio](#), Statista.

B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa del sector estudiado

Según el [informe de Estrategia Nacional de Seguridad y Confianza Digital \(ENSC\) 2021-2026](#), publicado por la Presidencia del Consejo de Ministros de Perú, la ciberseguridad se puede definir como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la seguridad digital y es un ámbito del marco de seguridad digital del país. En este sentido, en Perú, el sector de la ciberseguridad se divide en las siguientes categorías: servicios, *software*, *hardware* y seguridad en la nube.

B.2. Tamaño del mercado

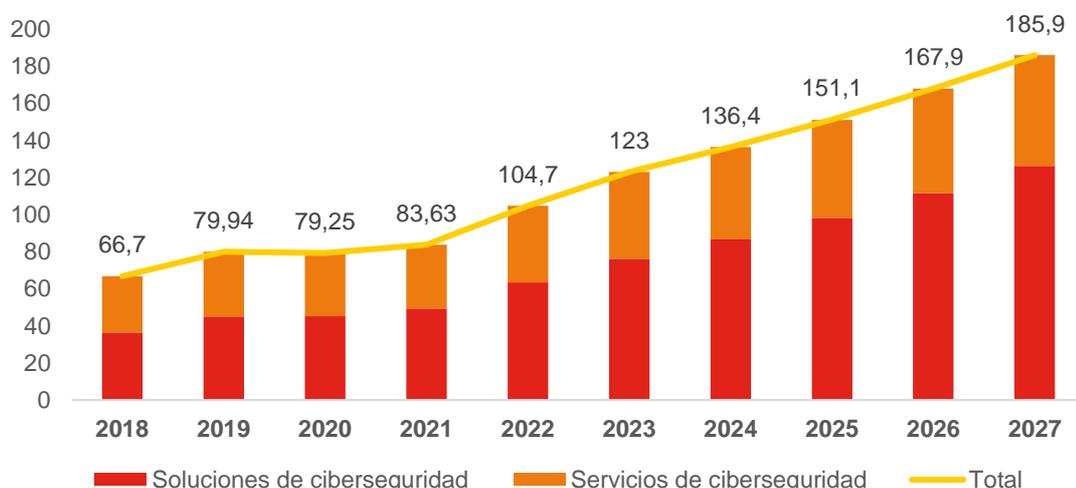
Según el informe anual elaborado por la Unión Internacional de Telecomunicaciones (UIT) que recoge el [Índice Global de Ciberseguridad \(GCI\)](#) de 165 países, Perú ocupa el puesto 86.º y recibe una puntuación (entre 0 y 100) de 55,67 puntos. Haciendo una comparación de los países de la región, Perú se sitúa en el puesto 12.º, siendo Estados Unidos, Canadá y Brasil los primeros en la lista. Perú, según este informe, se considera un **país en desarrollo**, destacando como áreas de fortaleza las medidas legales presentes en el país, y, como áreas de crecimiento, las medidas organizativas y el desarrollo de la capacidad.

Perú se encuentra actualmente en la segunda etapa del [Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones \(CMM\)](#), conocida como la **etapa formativa**. Este modelo, desarrollado por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford, tiene como objetivo evaluar el nivel de madurez de las capacidades de ciberseguridad de un país. Aunque Perú está implementando políticas y organizaciones para el desarrollo de la ciberseguridad, aún se encuentra en un nivel bajo de desarrollo comparado con el nivel regional.

Como se sabe, la ciberseguridad se ha vuelto crucial en la era de la economía digital, ya que la interconexión de productos y servicios en Internet continúa expandiéndose. El ciberdelito, considerado uno de los riesgos más probables que pueden afectar a las organizaciones en la próxima década, se posiciona en el octavo lugar en cuanto a impacto, según el último [informe de riesgos globales del Foro Económico Mundial \(2023\)](#). Esta creciente amenaza ha impulsado a una importante inversión global en ciberseguridad, reflejada en el aumento constante de los ingresos de este sector en los últimos años. En este sentido, en el gráfico siguiente se puede observar la **evolución de estos ingresos en Perú**, para soluciones y servicios de seguridad, no sólo en los últimos cinco años, sino también la estimación de crecimiento prevista para el próximo quinquenio.

INGRESOS POR SEGMENTO DEL MERCADO DE CIBERSEGURIDAD EN PERÚ

Datos en millones de euros



Fuente: Statista, 2022.

Los **sectores más afectados por el cibercrimen** en Latinoamérica son [los sectores de gobierno, minero y de salud](#). Se calcula que el 62 % de los ciberataques se dirigen a entidades relacionadas con estos sectores, siendo Brasil, México y Perú los países más afectados. Por otro lado, en Perú, los [sectores que más demandan servicios de ciberseguridad](#) son: industrial (20 %), financiero (18 %), tecnología (15 %), minería y energía (12 %), *retail* (12 %) y telecomunicaciones (11 %).

En 2022, [Perú alcanzó los quince mil millones de ciberataques](#), experimentando un **aumento del 35 % en intentos de ciberataques, en comparación con el año anterior**. Es más, América Latina y el Caribe hicieron frente a más de 360.000 millones de intentos de ciberataques, siendo México el país más afectado (187.000 millones). Perú, dado el reciente incremento en ciberataques, busca fortalecer su sector de ciberseguridad mediante medidas como la creación del [Centro Nacional de Seguridad Digital \(CNSD\)](#), el cual gestiona, dirige y supervisa la operación, educación, promoción y cooperación de la seguridad digital en el país, a fin de fortalecer la confianza digital.

Los directores de seguridad de la información (CISO) en Perú afrontan desafíos clave, incluyendo presupuestos limitados, fragmentación regulatoria y falta de articulación con otros líderes empresariales. Según una [encuesta de EY Perú](#), el 51 % de los CISO peruanos indicaron que sus empresas experimentaron un aumento en ataques cibernéticos disruptivos desde 2020, y el 63 % de ellos está altamente preocupado por la capacidad de su empresa para gestionar amenazas cibernéticas. La **necesidad de invertir en ciberseguridad y fortalecer la colaboración empresarial** se destaca como crucial para afrontar estos desafíos.

B.3. Principales actores

A **nivel gubernamental**, existen tres figuras relevantes en materia de ciberseguridad:

- [Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros \(SeGDI\)](#): lidera el Sistema Nacional de Transformación Digital al articular al sector público, privado, sociedad civil, academia y ciudadanos en asuntos de gobierno, confianza y transformación digital. Encabeza la implementación y evaluación de la Política Nacional de Transformación Digital. Su estructura incluye la Subsecretaría de Política y Regulación Digital, la Subsecretaría de Tecnologías y Seguridad Digital, y la Subsecretaría de Servicios e Innovación Digital.
- [Centro Nacional de Seguridad Digital \(CNSD\)](#): se encarga de gestionar, dirigir y supervisar las operaciones, educación, promoción y cooperación de la Seguridad Digital en el país, con el objetivo de robustecer la confianza digital. Funcionando como el único punto de contacto nacional, el CNSD facilita las comunicaciones y coordinaciones con otros organismos, centros o equipos, tanto a nivel nacional como internacional, que comparten su misma naturaleza y propósitos. Sumado a esto, administra la [Alerta integrada de seguridad digital](#) con la que se presenta un informe y análisis técnico periódico sobre distintos ataques a la seguridad digital de entidades públicas y empresas privadas.
- [Organismo Supervisor de las Contrataciones del Estado \(OSCE\)](#): supervisa los procesos de contrataciones que realizan las entidades públicas, velando por la aplicación eficiente de la normatividad y el uso óptimo de los recursos públicos.

En cuanto a **organizaciones a nivel privado**, las siguientes son las más relevantes:

- [Cámara de Comercio de Lima \(CCL\)](#): ofrece a sus asociados la posibilidad de constituirse en gremios. Entre ellos cuenta con el [Gremio de las Tecnologías de la Información y de las Comunicaciones](#) con un total de 17 empresas asociadas.
- [Sociedad Nacional de Industrias](#): brinda la opción a sus socios de pertenecer a comités gremiales y cuentan con un Comité de la Industria de las Tecnologías de la Información y de las Comunicaciones (TIC).
- [Asociación Peruana de Productores de Software \(APESOFT\)](#): tiene como objetivo promover la industria nacional del *software*, mejorar la competitividad de sus afiliados y fomentar las exportaciones de programas informáticos peruanos.

Por otro lado, a **nivel empresarial**, destacan dos grupos principales en Perú. Por un lado, los **fabricantes de software y hardware**, como Fortinet, Cisco, Dell, Microsoft o Siemens, los cuales tienen socios locales como **Bafing, Adistec, Softmark** o **Mikrotik** encargados de proveer y distribuir servicios de ciberseguridad en el país.



Por otro lado, se encuentran los **proveedores de servicios de seguridad gestionada (MSS)**, siendo **Telefónica, Neosecure, IBM y Digiware** los principales actores en este campo.

C. LA OFERTA ESPAÑOLA

Si bien es cierto que, en el sector de la ciberseguridad, a nivel global destacan empresas de Canadá, Estados Unidos, Israel y Reino Unido; España es un país comprometido con la ciberseguridad, y ha experimentado un reposicionamiento internacional en cuanto al uso seguro de las TIC. La percepción del sector español de ciberseguridad en Perú es buena, ya que es un país que destaca debido a la labor del [Centro Criptológico Nacional \(CCN\)](#), adscrito al Centro Nacional de Inteligencia (CNI), y del [Instituto Nacional de Ciberseguridad \(INCIBE\)](#).

En cuanto a formación y legislación, España se presenta como un país de referencia en este sector, gracias al INCIBE y a las Leyes de Protección de datos y de Infraestructuras Críticas. Cabe resaltar que, en muchas ocasiones, las leyes aprobadas en Perú en esta, y otras materias, presentan un gran parecido formal con la legislación española.

En lo referente a las empresas españolas de ciberseguridad en Perú, hay que mencionar que estas operan en diferentes ámbitos de actividad del sector, especializándose, a su vez, en nichos de negocio específicos. Así pues, cabe mencionar a [Ayesa](#), [Bit4id](#), [Cypher \(Prosegur\)](#), [Entelgy](#), [InDenova](#), [Indra \(Minsait\)](#), y [Telefónica Tech Cyber Security & Cloud](#), entre otras.

D. OPORTUNIDADES DEL MERCADO

A nivel global, según la "[Worldwide Security Spending Guide](#)" de IDC, se proyecta que la inversión total en servicios de ciberseguridad alcance aproximadamente los 184 MUSD para el año 2024. Las áreas de mayor enfoque de estas inversiones se esperan en los sectores financiero, de manufactura y obtención de recursos, el sector público y las telecomunicaciones.

En 2022, el informe [X-Force Threat Intelligence Index de IBM Security](#) reveló un aumento significativo de ciberataques en América Latina, con países como Brasil, Chile, Colombia, México y Perú entre los más afectados. El **ransomware** fue la táctica más utilizada, y representó el 32 % de los ataques en la región, con América Latina de líder mundial en esta categoría. Aunque a nivel global los incidentes de *ransomware* disminuyeron, en Latinoamérica aumentaron ligeramente. En materia de [tecnologías que plantean mayores riesgos](#), el *ranking* latinoamericano y mundial lo lideran: **nube a escala, Internet de las cosas (IoT), Inteligencia Artificial/Machine Learning, computación cuántica y metaverso**.

Perú se encuentra actualmente inmerso en un **proceso de transformación digital**, tanto en el ámbito público como en el privado. Esta transición hacia lo digital ha abierto nuevas oportunidades, pero también ha llevado consigo la aparición de actividades delictivas relacionadas con el uso de la tecnología, como el incremento en delitos informáticos y fraudes. En el sector público, los **Objetivos Estratégicos** del Documento de Trabajo de la [Estrategia de Seguridad y Confianza Digital 2021-2026](#), presentados por el CNSD, son los siguientes:

1. Seguridad de las Infraestructuras y Servicios Digitales
2. Capacidades de respuestas ante incidentes de Seguridad Digital
3. Cultura, innovación y formación
4. Protección empresarial y social
5. Seguridad del ciberespacio

Por otro lado, según el [informe de International Data Corporation \(IDC\)](#), las predicciones más destacables y comunes para la región de Latinoamérica para los próximos años son las siguientes:

- **Enfoque en Seguridad:** Con más inversión en seguridad (más del 35 % de los presupuestos de TI), hay una alta demanda de soluciones de ciberseguridad para proteger sistemas y datos.

- **Tecnologías Tech-by-wire y Seguridad:** La adopción de inteligencia artificial en decisiones corporativas implica la necesidad de soluciones de ciberseguridad más avanzadas que integren IA para detectar y responder a amenazas.
- **Brecha de Habilidades en Ciberseguridad:** La rápida evolución tecnológica genera una demanda creciente de profesionales en ciberseguridad, abriendo oportunidades para programas de formación especializados.
- **Soberanía de Datos y Seguridad:** Garantizar la seguridad de los datos según las leyes locales ofrece oportunidades para proveedores de soluciones de almacenamiento y gestión de datos con acento en la seguridad.
- **Modelo As-a-Service y Seguridad:** A pesar de los desafíos, el modelo *As-a-Service* puede ser una puerta de entrada para proveedores de seguridad cibernética que ofrecen servicios de seguridad externos.
- **Experiencia Incluida en Servicios de Seguridad:** Ofrecer conocimientos especializados en ciberseguridad como parte de los servicios *As-a-Service* representa una ventaja competitiva para los proveedores de seguridad.

Estas oportunidades destacan la **creciente demanda de soluciones y profesionales en ciberseguridad** debido a la mayor inversión y preocupación por la protección de sistemas, datos y la necesidad de adaptarse a tecnologías emergentes. Todos estos puntos suponen áreas de oportunidad para España y sus empresas, ya que Perú está comprometido con la colaboración internacional para el desarrollo de la transformación digital del país.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

Una empresa especializada en ciberseguridad busca acceder a los activos críticos de sus clientes, lo cual exige un nivel adicional de confianza. En este contexto, la colaboración con un **socio local** fiable, que facilite contactos y clientes, resulta crucial. La prestación de servicios se puede enfocar en la gestión desde la matriz extranjera mediante Servicios SOC (Centro de Operaciones de Seguridad), encargados del monitoreo y administración remota de la infraestructura de seguridad del cliente.

El equipo táctico necesario para los servicios de ciberseguridad generalmente se importa de países tecnológicamente avanzados, mientras que el *hardware* proporcionado al cliente puede adquirirse en Perú, siempre que sea de naturaleza simple. En casos en los que la gestión remota no sea factible, se puede recurrir a distribuidores y prestadores de servicios informáticos locales, tales como integradores de informática, proveedores de servicios gestionados de seguridad, empresas consultoras y otros minoristas de ciberseguridad.

En el caso de los **clientes públicos**, la contratación con el Estado peruano, por ejemplo, para brindar servicios de ciberseguridad a la Administración, implica superar un proceso de licitación supervisado por el OSCE. Este organismo no sólo administra el [Registro Nacional de Proveedores \(RNP\)](#) y resuelve consultas, sino que también aplica sanciones y designa árbitros en casos de controversias. Para ser parte del proceso como participante, postor, contratista o subcontratista del Estado, es necesario estar registrado en el RNP. El registro tiene una validez anual.

E.2. Legislación aplicable y otros requisitos

E.2.1. Legislación aplicable

La legislación en el ámbito de las nuevas tecnologías experimenta cambios constantes para abordar los desafíos y necesidades emergentes. Por esta razón, se aconseja a los empresarios contar con la asesoría de despachos especializados para establecer con precisión, desde el inicio, el marco legislativo aplicable. En el caso de la ciberseguridad en Perú, aún está en **proceso de desarrollo**. A continuación, se mencionan las leyes más significativas para este sector:

- [Ley de Delitos Informáticos](#) (Ley n.º 30096 de 2013): Busca prevenir y sancionar conductas ilícitas en sistemas y datos informáticos mediante tecnologías de la información.
- [Seguridad Digital y Datos Abiertos y Datos Espaciales para los Ciudadanos](#) (Decreto Supremo n.º 050-2018-PCM): Dispone la formulación de un Plan de Transición al Protocolo IPV6.

- [Ley de Gobierno Digital](#) (Decreto Legislativo n.º 1412): Establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico.
- [Ley de Ciberdefensa](#) (Ley n.º 30999 de 2019): Establece el marco de la ciberdefensa del Perú, regulando las operaciones militares en y a través del ciberespacio, responsabilidad de los órganos ejecutores del Ministerio de Defensa.
- [Ley de Firmas y Certificados Digitales](#) (Ley n.º 27269 de 2000 – PCM): Regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que una firma manuscrita u otra similar que implique manifestación de voluntad.
- [Reglamento de la Ley de Gobierno Digital](#) (Decreto Supremo n.º 029-2021 – PCM): Establece disposiciones sobre las condiciones, requisitos y uso de tecnologías y medios electrónicos en los procedimientos administrativos llevados a cabo por entidades públicas.

Asimismo, desde 2019, **Perú forma parte del [Convenio de Budapest](#)**, aprobado por el Comité de Ministros del Consejo de Europa el 8 de noviembre de 2001. El Convenio de Budapest, que promueve la cooperación internacional en la lucha contra el crimen informático mediante la armonización de leyes y el mejoramiento de técnicas, ha logrado dar un impulso al marco legal de Perú.

E.2.2. Aduanas

Internamiento de equipos¹

- El permiso de internamiento para equipos de telecomunicaciones en Perú puede ser temporal o indefinido. El trámite se realiza electrónicamente a través de la [Ventanilla Única de Comercio Exterior \(VUCE\)](#), con un plazo de atención de cinco días hábiles. Los solicitantes deben tener RUC (Registro Único de Contribuyente, equivalente al NIF español) y Clave Sol, y proporcionar detalles del equipo y documentos como factura y ficha técnica.
- Aquellos que soliciten el permiso deben tener registro de la casa comercializadora, concesión única de servicios públicos de telecomunicaciones, autorización de servicios privados o de radiodifusión, o registro para servicios de valor añadido, a menos que el equipo sea para uso privado, en cuyo caso se permite un máximo de cinco unidades por viaje o envío.
- Los permisos temporales duran hasta 12 meses y no necesitan certificado de homologación, pero sólo se otorgan para pruebas, exhibiciones, emergencias o eventos específicos.

Otros requisitos

- Si el valor de la mercancía importada es inferior a 2.000 USD, el mismo importador podrá presentar en la aduana la factura comercial, el documento de transporte, el seguro y el permiso de internamiento. En caso de que la mercancía supere este valor deberá hacerse a través de un agente de aduanas.
- Una persona física puede importar mercancía por valor máximo de 3.000 USD al año, pudiendo realizarse un total de tres importaciones. Si desea superar ese valor deberá constituirse como persona jurídica y disponer de RUC.

E.2.3. Aspectos tributarios

En relación con el ámbito de la ciberseguridad y la prestación de servicios, es importante mencionar que aún **no existe un Convenio de Doble Imposición Internacional** entre España y Perú. En el contexto de las empresas con sede en España que proporcionan servicios transfronterizos a clientes en Perú, la ley impone un impuesto sobre la renta del 30 % o del 15 %, dependiendo del tipo de servicio ofrecido. Para información más detallada acerca del tipo impositivo de los servicios transfronterizos se recomienda leer el apartado 5.3 de la [Guía País 2023 de Perú](#).

¹ Para conocer más sobre el procedimiento, véase el [portal web del Ministerio de Transportes y Comunicaciones](#).

E.3. Ayudas

E.3.1. Ayudas en España

- **Programas de apoyo a la internacionalización de ICEX**
- **Centro para el Desarrollo Tecnológico Industrial (CDTI):** Proyectos de Cooperación Tecnológica Internacional en I+D+I (PCTI), liderados por empresas, abarcan tanto iniciativas a nivel multilateral, como IBEROEKA, como acuerdos unilaterales. Estos proyectos resaltan el valor añadido de la innovación a nivel internacional. Además, permiten una expansión significativa del impacto de sus productos, procesos y servicios en los mercados globales.
- El **Plan Estratégico 2021-2025 del INCIBE:** fortalece la industria española de ciberseguridad, facilitando la internacionalización de empresas en un sector global y competitivo. Acompaña a las empresas en su expansión a nuevos mercados, mejorando su posición internacional según su fase de internacionalización.

E.3.2. Ayudas en Perú

- El **Programa Nacional de Innovación para la Competitividad y Productividad (ProInnovate)**, del Ministerio de la Producción, cuyos recursos se adjudican a través de concursos de alcance nacional, para el cofinanciamiento no reembolsable de proyectos de I+D+i+e. Estas subvenciones van dirigidas a empresas domiciliadas en Perú o a asociaciones empresariales entre una empresa peruana y una extranjera.
- El **Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC)** financia proyectos de desarrollo de nuevos productos o servicios u otras innovaciones tecnológicas, cuyos resultados puedan aplicarse industrialmente o incorporarse en el mercado.

E.4. Ferias

FERIA	DESCRIPCIÓN	ÚLTIMA EDICIÓN
E-Summit Perú Ecommerce	CCL organiza el <i>e-Summit PERÚ ECOMMERCE</i> , con el propósito de continuar impulsando el desarrollo del comercio digital.	6-7 de septiembre de 2023, Lima
Congreso CyberSecurity Bank & Government	Organizado por MTICS Producciones. Recoge las tendencias, estrategias y herramientas relacionado con la seguridad de la información a nivel Gobierno, Financiero y Bancario.	11 de junio de 2023, Lima
F5 Cyberprotector Summit	F5 organiza un evento para abordar las últimas tendencias en ciberseguridad, destacando protección, automatización y visibilidad.	16 de febrero de 2023, Lima
SEGURINFO	Principal congreso anual de seguridad de la información.	7 de noviembre de 2023, Lima
ASIS LATAM 2023	ASIS Latam reúne a profesionales de la industria de seguridad. Organiza diversas actividades a lo largo del año, <i>workshops</i> , foros y encuentros empresariales en el ámbito de la ciberseguridad.	26-27 de octubre de 2023, Lima

F. INFORMACIÓN ADICIONAL

Para más información acerca de Perú, se puede acudir a la [Guía País. Perú 2023](#), disponible en la página web oficial de ICEX España Exportación e Inversiones. Este documento recoge información general del país, así como el marco para la actividad comercial y para la inversión.

G. CONTACTO

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

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

Jorge Basadre, 405
San Isidro
Lima 15073 – Perú
Teléfono: +51 1 442-1788 / 89 / 90
Email: lima@comercio.mineco.es
<http://Peru.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) 97 100 99 a
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.

AUTORA
María Vargas Martín

Oficina Económica y Comercial
de España en Lima
lima@comercio.mineco.es
Fecha: 01/12/2023

NIPO: 114-23-013-7

www.icex.es



FICHAS SECTOR PERÚ



ICEX España
Exportación
e Inversiones