

# Ciberseguridad en Qatar

## A. CIFRAS CLAVE

Qatar vive una transición económica hacia una economía sostenible y digitalizada, donde busca independizarse del *Oil & Gas*. Para ello, se lanzó en 2008 la *Qatar National Vision 2030* (QNV2030), que es el documento que guía las iniciativas del país. A partir de la QNV2030 se crea la Estrategia Nacional de Qatar para la Ciberseguridad en 2014. Este es el primer paso del país para asegurar un espacio seguro para individuos y empresas, con el fin de convertirse en un *hub* tecnológico en la región. En 2021 se creó la Agencia Nacional de Ciberseguridad (NCSA), dando integridad y coordinación a la inversión y gestión institucional en ciberseguridad. La sociedad y la economía de Qatar se encuentran altamente digitalizadas, con una inversión cada vez mayor en ciberseguridad. Esto se traduce en numerosas oportunidades en el sector para las empresas españolas.

Sector de ciberseguridad	2025
Tamaño aproximado del sector ciberseguridad en Qatar	1.450 MUSD
Tasa de crecimiento anual compuesto (CAGR) del sector 2025-2030	8,18 %
Tamaño aproximado del sector ciberseguridad en Qatar en 2029	1.986 MUSD
Porcentaje de empresas que han sufrido un ciberataque en el último año	91 %
Ingresos del mercado de ciberseguridad	142,98 MUSD
Aumento de empresas registradas en 2024 con necesidad de protección <i>online</i> en comparación con el año anterior	230 %
Porcentaje de penetración de la banca <i>online</i> en 2025 en Qatar	37,83 %
Tipos de ciberataque más comunes en Qatar	<i>Phishing</i> , <i>malware</i> y ataque de denegación de servicio (DoS)

## B. CARACTERÍSTICAS DEL MERCADO

### B.1. Definición precisa del sector estudiado

El sector de la ciberseguridad se define como el conjunto de medidas de seguridad susceptibles de ser implementadas para protegerse de los ciberataques. Incluye las tecnologías, acciones, políticas y herramientas que pueden usarse para proteger los activos informáticos propiedad de administraciones, empresas y particulares.

El sector de la ciberseguridad se divide en cuatro subsectores: servicios, *software*, *hardware* y seguridad en la nube. El subsector de servicios es el más grande, ya que representa más de dos tercios del mercado. Le sigue el de *software*, con cerca del 20 %, y luego el de *hardware*, con un 10 %. Por último, está la seguridad en la nube, que, aunque actualmente representa apenas un 3 % del mercado, es el subsector que más ha crecido en los últimos años. Se estima que su crecimiento tendrá una tasa compuesta anual (CAGR) del 15,7 % hasta 2028<sup>1</sup>.

La ciberseguridad es un sector horizontal debido al rápido desarrollo de la economía digital, en la medida en que cada vez más productos y servicios se conectan a Internet. Además, el cibercriminológico supone una amenaza creciente tanto para las personas como para las empresas y las instituciones.

### B.2. Tamaño del mercado

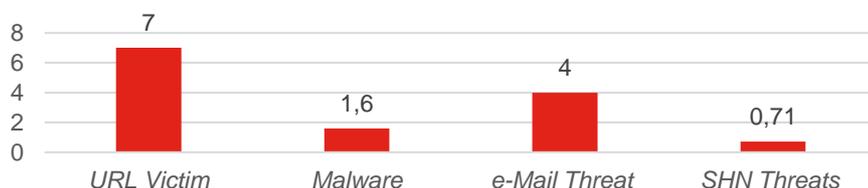
El tamaño del mercado de la ciberseguridad en Qatar se valoró en aproximadamente 1.450 MUSD en 2025. Se espera que crezca a una tasa anual compuesta del 12,6 % durante el período de previsión (2025-2028)<sup>2</sup>. Según el estudio [Qatar Cybersecurity Market Size & Share Analysis - Industry Research Report - Growth Trends](#) el mercado de la ciberseguridad en Qatar no se encuentra muy concentrado, dejando abierta la posibilidad de entrada a nuevos competidores, atraídos por la inversión, tanto institucional como privada, en materia de ciberseguridad.

Eventos como el Mundial de Fútbol de Qatar 2022<sup>3</sup>, la Fórmula 1, el MWC2025 y el [Web Summit 2025](#) exigen al país que aumente sus esfuerzos en ciberseguridad, al abrirse cada vez más a la esfera internacional en un intento por convertirse en un *hub* tecnológico en la región<sup>4</sup>. Se espera que las inversiones digitales de Qatar en tecnologías prioritarias, como la inteligencia artificial o la ciberseguridad, se disparen hasta los 5.700 MUSD en 2026, frente a los 1.650 MUSD de 2022<sup>5</sup>.

Existe una creciente demanda de servicios de ciberseguridad en Qatar, debido a la digitalización de la economía, la mayor concienciación sobre los riesgos cibernéticos, el apoyo del Gobierno a través de la inversión en infraestructura y la creación de un entorno favorable para las empresas de ciberseguridad.<sup>6</sup>

#### NÚMERO DE CIBERATAQUES, POR TIPO, EN QATAR EN 2021

En millones de ataques



Fuente: Trend Micro (<https://www.mordorintelligence.com/industry-reports/qatarcybersecuritymarket>).

<sup>1</sup> [https://www.theinsightpartners.com/es/reports/cloud-security-market?utm\\_source=chatgpt.com](https://www.theinsightpartners.com/es/reports/cloud-security-market?utm_source=chatgpt.com)

<sup>2</sup> <https://www.statista.com/outlook/tmo/cybersecurity/qatar#revenue>

<sup>3</sup> <https://qcdc.org.qa/fifa/cybersecurity-during-the-world-cup-qatar-vows-an-open-and-secure-cyberspace/>

<sup>4</sup> <https://www.trade.gov/market-intelligence/qatar-cybersecurity-sector>

<sup>5</sup> <https://www.invest.qa/en/media-centre/news-and-articles/invest-qatar-and-mcit-launch-smarter-qatar-a-joint-report-on-qatars-digital-transformation-and>

<sup>6</sup> <https://thepeninsulaqatar.com/article/06/05/2023/qatar-positioning-itself-as-global-leader-in-cybersecurity-report>

El número de empresas tecnológicas en Qatar ha aumentado por las necesidades del uso de *Cloud Computing* en el país. Actualmente Qatar posee varios centros de *Cloud*, entre ellos el Google Cloud Platform (GPC)<sup>7</sup> y el Microsoft Azure Qatar<sup>8</sup>, ambos abiertos a mediados de 2022. Se estima en 2.500 MUSD las inversiones públicas por países del CCEAG para 2030<sup>9</sup>.

Se elige Qatar para la ubicación de estos centros por su posición estratégica, sus esfuerzos en energía, atracción de inversión, seguridad y ciberseguridad, así como por su bajo coste de implementación y su alto porcentaje de digitalización, tanto a nivel demográfico como comercial<sup>10</sup>. Esto implica un aumento de demanda de servicios de ciberseguridad en Qatar.

Según el informe de 2023 de Ciberseguridad del Foro Económico Mundial, el liderazgo político en materia de ciberseguridad se acompaña cada vez más de una mayor inversión de los negocios en ciberseguridad. Esto permite un mayor desarrollo y una mayor colaboración entre empresas e instituciones<sup>11</sup>, y esto se refleja también en Qatar.

El esfuerzo gubernamental nace de la *Estrategia Nacional de Ciberseguridad en Qatar*<sup>12</sup>, y de ahí surgió la agencia de Ciberseguridad de Qatar (**NCSA**) en 2021, dando forma al marco legislativo y ubicando una cabeza visible a la que acudir en caso de querer participar en el sector en el entorno gubernamental.

La Estrategia Nacional de Ciberseguridad se basa en cinco pilares:

- Ciberseguridad y Resiliencia en el Ecosistema de Qatar.
- Legislación, Regulación y Aplicación de la Ley por un Ciberespacio Seguro.
- Una Economía Próspera e Innovadora Basada en Datos.
- Cibercultura y Desarrollo del Talento de la Mano de Obra.
- Cooperación Internacional y Alianzas de Confianza.

### B.3. Principales actores

#### • Organismos públicos

- **Ministerio de Comunicación, Información y Tecnología**: es responsable de la política y regulación de la ciberseguridad en Qatar. El Ministerio también es responsable de la coordinación entre los diferentes organismos gubernamentales que trabajan en ciberseguridad.
- **Agencia Nacional de Ciberseguridad (NCSA)**: Esta agencia es responsable de implementar y controlar las necesidades del país en el ámbito de la ciberseguridad, controlando los riesgos y amenazas, poniendo a prueba los mecanismos de protección actuales y reforzando los sistemas para evitar crisis y ataques a infraestructuras estratégicas.
- **Autoridad de Regulación de las Telecomunicaciones (CRA)**: es un organismo independiente que opera bajo la supervisión del Ministerio de Comunicaciones y Tecnología de la Información (MCIT). Es responsable de la regulación de las telecomunicaciones en Qatar. La CRA también es responsable de la seguridad de las redes y sistemas de telecomunicaciones en el país.
- **Q-CERT**: Organización gubernamental responsable de la protección de la infraestructura cibernética de Qatar, se encarga de certificar empresas y procesos en términos de ciberseguridad. Además, publica un boletín

<sup>7</sup> <https://cloud.google.com/about/locations?hl=es>

<sup>8</sup> <https://news.microsoft.com/en-xm/2022/08/31/microsoft-opens-first-global-datacenter-region-in-qatar-bringing-new-opportunities-for-a-cloud-first-economy/>

<sup>9</sup> [https://www.invest.qa/storage/2486/64524f0068629\\_EY\\_Microsoft\\_Cybersecurity\\_Study\\_3523.pdf](https://www.invest.qa/storage/2486/64524f0068629_EY_Microsoft_Cybersecurity_Study_3523.pdf)

<sup>10</sup> <https://www.invest.qa/en/media-and-events/news-and-articles/ipa-qatar-partners-with-microsoft-and-ey-parthenon-to-launch-report-on-qatars-cybersecurity-investment-opportunities>

<sup>11</sup> [https://www3.weforum.org/docs/WEF\\_Global\\_Security\\_Outlook\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf)

<sup>12</sup> [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/Qatar\\_2014\\_national\\_cyber\\_security\\_strategy.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_2014_national_cyber_security_strategy.pdf)

semanal de ciberseguridad, y organiza eventos de formación y capacitación en ciberseguridad. Actualmente forma parte del NCSA.

- [Qatar Cybersecurity Academy](#) (QCS Academy): es una escuela de formación que pertenece al Ministerio de Comunicaciones y Tecnologías de la Información de Qatar (MCIT). Esta ofrece cursos y certificaciones en ciberseguridad en Qatar.
- [Qatar Computing Research Institute](#): En colaboración con [Qatar Foundation](#) y [Hamad Bin Khalifa University](#) trabaja en la aplicación de análisis de datos de datos en tiempo real para la detección de ciberataques.
- **Empresas de ciberseguridad locales**
  - [Cytomate](#): ofrece una amplia gama de servicios, como consultoría, auditoría, formación y desarrollo. Se centra en la protección de empresas y organizaciones frente a las ciberamenazas.
  - [MEEZA](#): es una empresa de TI que ofrece una amplia gama de servicios de ciberseguridad, como consultoría, evaluación, implementación y servicios gestionados. Está especializada en proteger a las empresas y organizaciones de Qatar ante las ciberamenazas.
  - [SecureLink Middle East](#): es una empresa global de ciberseguridad que ofrece una amplia gama de servicios, como consultoría, evaluación, implantación y servicios gestionados. Tiene una fuerte presencia en la región y ofrece diversas soluciones de ciberseguridad a empresas y organizaciones del país.
  - [Barikat Cyber Security](#): es una empresa privada de ciberseguridad que ofrece una amplia gama de servicios, como consultoría, evaluación, implementación y servicios gestionados.
  - [Dicotech](#): es una empresa privada de TI que ofrece una amplia gama de servicios, como consultoría, evaluación e implementación de ciberseguridad. También ofrece otros servicios de TI, como integración de sistemas, seguridad de redes y computación en la nube.
  - [Malomatia](#): es una empresa privada de TI que ofrece una amplia gama de servicios, como consultoría, evaluación e implementación de ciberseguridad. También ofrece otros servicios de TI, como integración de sistemas, seguridad de redes y computación en nube.
  - [Mannai](#): es una de las mayores empresas privadas de Qatar, con una fuerte presencia en el sector tecnológico y de ciberseguridad, además de sus actividades en automoción, energía y comercio.
  - [HIT Services](#): es un integrador de sistemas y consultoría local de Qatar dedicado a crear valor afrontando los retos emergentes de la seguridad digital. Sus servicios abarcan varios sectores verticales, como la administración pública, la banca y los servicios financieros, la tecnología y los medios de comunicación, el petróleo y la energía, las aerolíneas, el comercio electrónico y el comercio minorista.
- **Empresas de ciberseguridad internacionales con presencia en Qatar**
  - [IBM](#): tiene una fuerte presencia en Qatar y ofrece diversas soluciones de ciberseguridad a empresas y organizaciones del país. Entre sus servicios se incluyen IBM Security X-Force, QRadar, SOAR, MaaS360 y Cloud Pak for Security. Además, IBM ha llevado a cabo numerosas colaboraciones con el Gobierno catari, incluyendo proyectos con el Centro Nacional de Ciberseguridad, programas de concienciación y educación, así como el desarrollo de sistemas de protección para entidades gubernamentales.
  - [Microsoft](#): colabora con el Gobierno de Qatar en desarrollar la estrategia nacional de ciberseguridad. También invierte en programas de educación y formación en ciberseguridad en Qatar para ayudar a desarrollar las habilidades de los profesionales de la ciberseguridad en el país.
  - [Cisco](#): ofrece una amplia gama de soluciones y servicios para ayudar a las empresas y organizaciones de Qatar a proteger sus datos y sistemas de los ciberataques. En 2022, Cisco colaboró con el Gobierno de Qatar

para implementar una solución de ciberseguridad de red para proteger la infraestructura crítica del país y en 2023, lanzó un programa de formación en ciberseguridad para mujeres en Qatar.

- **Atos:** es una empresa global de TI que ofrece una amplia gama de servicios de ciberseguridad, incluyendo consultoría, evaluación, implementación y servicios gestionados. En Qatar ofrece formación y certificación en ciberseguridad a los profesionales del país y ha desarrollado una solución de ciberseguridad específica para Qatar, llamada Atos Cyber Defence for Qatar (ACDQ).
- **Big 4:** en Qatar las grandes empresas de auditoría y consultoría también están trabajando en ciberseguridad, concretamente, destacan las participaciones de **EY** y **Deloitte** en desarrollo de estrategias de ciberseguridad e integración entre organizaciones e instituciones.

### C. LA OFERTA ESPAÑOLA

El sector español de la ciberseguridad está experimentando un crecimiento significativo, impulsado por el aumento de la digitalización y la conectividad en el país. Según Mordor Intelligence, el mercado de ciberseguridad de España se estima en 2.270 MUSD en 2024 y se espera que alcance los 3.210 MUSD para 2029, creciendo a una CAGR del 7,16 % durante el período de pronóstico. La ciberseguridad, tanto para la protección de instituciones y gobiernos, como de empresas es una prioridad en España<sup>13</sup>.

Según el Índice Global de Ciberseguridad de 2020, elaborado por la **ITU**, **España, está a la cabeza en ciberseguridad**, ocupando el cuarto puesto del mundo en ciberseguridad<sup>14</sup>. Qatar, por su parte, se encuentra en el puesto 27.º del *ranking* y según la Gulf Information Security Expo and Conference, se halla entre los tres países del Golfo con mayor madurez en ciberseguridad, tan sólo por detrás de Arabia Saudí y Emiratos Árabes Unidos. Este índice, que analiza las capacidades de cada país, demuestra en el caso de España su dilatada experiencia en el sector, albergando unas capacidades legales, de cooperación y una *know-how* inmejorables.

Esto posiciona a España como uno de los países más avanzados del mundo en materia de ciberseguridad, y por tanto tiene una capacidad técnica más que probada que se puede exportar, aportando soluciones a países con menor nivel técnico, como pueden ser los de la región MENA, que presentan necesidades similares a las que se atienden en España, es decir, protección de instituciones y estructuras estratégicas<sup>15</sup>.

#### DESARROLLO DEL SISTEMA DE CIBERSEGURIDAD EN ESPAÑA, ATENDIENDO A LAS CINCO ÁREAS PRINCIPALES DEL SECTOR

Puntuación sobre 20

Medidas legales	Medidas técnicas	Medidas organizacionales	Desarrollo de capacidades	Medidas de cooperación
20	20	20	19,74	20

Fuente: International Telecommunications Union, Global Cybersecurity Index v4, 2024.<sup>16</sup>

El sector en España está formado por una amplia gama de empresas, desde pequeñas empresas especializadas en ciberseguridad hasta grandes empresas multinacionales<sup>17</sup>. Las empresas españolas ofrecen una amplia gama de soluciones y servicios en múltiples áreas de la ciberseguridad. La experiencia de las empresas españolas, tanto en grandes proyectos como en trabajos a menor escala, es bien conocida en Qatar, donde la imagen de la empresa española es impecable.

<sup>13</sup> <https://www.mordorintelligence.com/es/industry-reports/spain-cybersecurity-market>

<sup>14</sup> <https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/>

<sup>15</sup> <https://assets.kpmg.com/content/dam/kpmg/es/pdf/2022/02/consideraciones-ciberseguridad-2022-kpmg.pdf>

<sup>16</sup> [chrome-extension://efaidnbmnnnibpcajpcqlclefindmkaj/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416\\_1b\\_Global-Cybersecurity-Index-E.pdf](chrome-extension://efaidnbmnnnibpcajpcqlclefindmkaj/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)

<sup>17</sup> <https://kpmg.com/es/es/home/tendencias/2023/02/claves-ciberseguridad-2023.html>

Así, cabe mencionar las siguientes empresas españolas destacadas en el área de la ciberseguridad: [AirON](#), [AlaiSecure](#), [Ayesa](#), [CIC](#), [Cipher](#), [Telefónica Tech Cyber Security & Cloud](#), [Innotec Security](#), [Enigmedia](#), [NTT DATA](#), [GMV](#), [Ikusi](#), [Micronet](#), [Minsait](#) y [SIA](#) (Indra), [MNEMO](#), [One eSecurity](#), [Open Cloud Factory](#), [Proactivanet](#), [S21Sec](#), [S2 Grupo](#), [Sothis](#), [TSK](#) y [Tecnalia](#), entre otras.

## D. OPORTUNIDADES DEL MERCADO

Las oportunidades en el sector de la ciberseguridad en Qatar aparecen, por tanto, en dos vías, que, si bien están cada vez más interconectadas, precisan de distintos enfoques. Por la parte **gubernamental**, se puede comprobar en todas las estrategias e iniciativas institucionales en materia de ciberseguridad la estrecha colaboración entre organismos públicos y empresas, dando lugar a un ambiente realmente favorecedor para la inversión extranjera.

Por la parte **privada**, las empresas cataríes cada vez demandan más soluciones de ciberseguridad, en tanto que se abren a mercados exteriores<sup>18</sup> y cada vez están más digitalizadas. Las empresas en Qatar además de integrarse en un espacio digital conviven con una amplia multiculturalidad y abundancia de datos, lo cual precisa de unas necesidades de ciberseguridad notorias.

### DESARROLLO DEL SISTEMA DE CIBERSEGURIDAD EN QATAR, ATENDIENDO A LAS CINCO ÁREAS PRINCIPALES DEL SECTOR

Puntuación sobre 20

Medidas legales	Medidas técnicas	Medidas organizacionales	Desarrollo de capacidades	Medidas de cooperación
20	20	20	20	20

Fuente: International Telecommunications Union, Global Cybersecurity Index v4, 2024.<sup>19</sup>

Como puede comprobarse en la tabla, a partir de los resultados del [Global Cybersecurity Index](#), Qatar presenta una excelente situación en el sector. Con todo, la realidad es que existen carencias en el ámbito regulatorio. En ocasiones, la legislación resulta ambigua; además, el NCSA tiene competencias algo limitadas en lo que respecta a auditoría, y los estándares ISO/IEC no están integrados directamente en el país, sino que son aplicados con el apoyo de consultoras privadas. Esta situación abre la puerta a la entrada de capital humano y servicios de consultoría en Qatar.

Qatar es un país que goza de buena capacidad económica y que, además, tiene gran predisposición a la mejora, como ya refleja claramente su **Estrategia Nacional de Ciberseguridad 2024-2030**. Esta ofrece grandes oportunidades para las empresas españolas del sector. Qatar demanda servicios de consultoría, auditoría y gestión de riesgos, así como soluciones avanzadas para la protección de infraestructuras críticas.

El desarrollo de un marco regulatorio sólido abre la puerta a empresas especializadas en normativas de ciberseguridad y adaptación a tecnologías emergentes como IA, IoT y *blockchain*. Además, Qatar busca impulsar la investigación y el desarrollo (I+D) en ciberseguridad, promoviendo colaboraciones con centros españoles en proyectos innovadores.

La formación de talento es otra prioridad, con oportunidades para programas de capacitación y certificación de profesionales. En sectores clave como energía e industria, se necesitan soluciones de ciberseguridad industrial (OT/ICS) para proteger infraestructuras críticas. Además, hay una demanda de seguridad de la cadena de suministro, con especial foco en auditorías y certificaciones.

Por último, Qatar apuesta por una mayor cooperación internacional, lo que facilita la creación de alianzas estratégicas con empresas e instituciones españolas. En conjunto, este mercado en expansión representa una excelente oportunidad para España como socio tecnológico y estratégico en ciberseguridad.<sup>20</sup>

<sup>18</sup> [https://tdv.motc.gov.qa/sites/default/files/2020-01/Qatar %20Digital %20Investment %20Opportunities.pdf](https://tdv.motc.gov.qa/sites/default/files/2020-01/Qatar%20Digital%20Investment%20Opportunities.pdf)

<sup>19</sup> [chrome-extension://efaidnbmnnnibpcajpcqlclefindmkaj/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416\\_1b\\_Global-Cybersecurity-Index-E.pdf](chrome-extension://efaidnbmnnnibpcajpcqlclefindmkaj/https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)

<sup>20</sup> [https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9 %20- %20Eng %20OL\\_0.pdf](https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20Eng%20OL_0.pdf)

## E. CLAVES DE ACCESO AL MERCADO

### E.1. Entrada al mercado

Aunque la mayoría de los servicios de seguridad provienen de empresas extranjeras, en Qatar la protección de datos y la ciberseguridad son cuestiones estratégicas. Por ello, se valora especialmente la presencia local de las empresas proveedoras de estos servicios. Esto se refleja en iniciativas como el **In Country Value (ICV)** y en la necesidad de contar con un socio local para acceder a ciertos contratos y licitaciones en el ámbito de la seguridad.

Para facilitar la entrada al mercado, también se han de tener en cuenta las certificaciones que la NCSA exige a empresas para ciertos sectores, como la certificación ISO27001. Cumplir con los estándares fijados por la NCSA permitirá una mejor entrada en el mercado de la ciberseguridad en Qatar.

Para el acceso al mercado de la ciberseguridad, en Qatar es realmente recomendable acudir con un *partner* local que apoye la entrada en el mercado y facilite la instalación y la captación de demanda en el sector. Así las alianzas estratégicas y las *joint ventures* son clave para la internacionalización en este sector del país.

Para acceder al mercado también es recomendable acudir a organismos públicos como [Tasmu Digital Valley](#), donde se potencian el emprendimiento digital en múltiples sectores, y se atiende a una cooperación entre talento nacional y extranjero<sup>21</sup>.

### E.2. Legislación aplicable y otros requisitos

El sector de la ciberseguridad en Qatar se rige principalmente por las siguientes normativas:

- (NCSA Framework) [Booklet\\_NISCF.pdf](#).
- (Qatar Cloud Security Policy) [cs-csps\\_cloud\\_security\\_policy\\_eng\\_v1.3.pdf\(qcert.org\)](#).
- (Qatar 2022 Cyber Security Framework) [National Information Security Compliance Framework – Audit Standard](#).
- (Ley de Protección de Datos Personales) [Law No.13 of 2016\(qcert.org\)](#).
- (Ley de Prevención del Cibercrimen, Ley 14 de 2013) [Qatar Cyber Crime Prevention Law](#).

### E.3. Ayudas

- **Ayudas en España para la internacionalización:** ICEX (a través de sus programas de apoyo a la internacionalización), Cámaras de Comercio (a través del Plan Cameral de Exportaciones), Instituto de Crédito Oficial (ICO) (mediante sus líneas de crédito a la exportación), el Centro para el Desarrollo Tecnológico Industrial (CDTI) y el compromiso de colaboración ICEX - Instituto Nacional de Ciberseguridad (INCIBE).
- **Ayudas europeas:** El Banco Europeo de Inversiones (BEI) financia proyectos de empresas europeas relacionados con los objetivos de crecimiento y desarrollo marcados por la UE, entre los cuales se encuentra la ciberseguridad, y la Comisión Europea, a través de la European Union Agency For Cybersecurity (ENISA), apoya el desarrollo de la industria de ciberseguridad en Europa.

## F. INFORMACIÓN ADICIONAL

- Congreso de Ciberseguridad Cyberx Qatar, el 20 de febrero de 2024 <https://cyberxqatar.com/>.
- Qatar cloud & Cybersecurity Summit 2023, el 13-14 de noviembre <https://www.qccsummit.com/>.
- *Estrategia Nacional de Ciber Seguridad 2024-2030*. [The National Cyber Security Strategy 2024-2030 is launched](#)
- ENISA Agencia de la Unión europea para la Ciberseguridad <https://www.enisa.europa.eu/about-enisa/about/es>
- Instituto Nacional de Ciberseguridad (INCIBE) <https://www.incibe.es/>.

<sup>21</sup> <https://oxfordbusinessgroup.com/reports/qatar/2022-report/economy/digital-drive-both-the-public-and-private-sectors-turn-to-online-solutions-while-the-country-taps-emerging-segments-such-as-e-sports>

## G. CONTACTO

---

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

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

West Bay – Zone 66 – Street 563 – Saha 93 – Villa 9  
Doha - Qatar  
Teléfono: +974 44 835886  
Correo electrónico: [doha@comercio.mineco.es](mailto:doha@comercio.mineco.es)  
<http://Qatar.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 (L-J 9 a 17 h; V 9 a 15 h)  
[informacion@icex.es](mailto: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.

### AUTORES

Sandro Otarashvili Shatirishvili  
Álvaro Martín García

Oficina Económica y Comercial  
de España en Doha

[doha@comercio.mineco.es](mailto:doha@comercio.mineco.es)

Fecha: 27/03/2025

© ICEX España Exportación e Inversiones, E.P.E.

NIPO: 224250231

[www.icex.es](http://www.icex.es)



FICHAS SECTOR QATAR



**ICEX** España  
Exportación  
e Inversiones