EM ESTUDIOS DE MERCADO

2018

ICEX España Exportación e Inversiones

El mercado de ciberseguridad en Arabia Saudí

Oficina Económica y Comercial
de la Embajada de España en Riad

EM ESTUDIOS DE MERCADO

01 de Junio de 2018
Riad

Este estudio ha sido realizado por
Manuel Gómez Betanzos

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en Riad.

Editado por ICEX España Exportación e Inversiones, E.P.E., M.P.

NIPO: 060-18-042-8

Índice

1. Resumen ejecutivo

En este estudio de mercado se presentan datos e información del mercado de la ciberseguridad en Arabia Saudí. El estudio se divide en varios apartados en los cuáles se analizan los distintos componentes que tienen influencia sobre el sector. Se analiza la composición de la oferta y la demanda, los factores que afectan al establecimiento de los precios y a las preferencias de los consumidores, los canales de distribución y las principales barreras a la exportación, tanto arancelarias como no arancelarias. Por último se ofrecen las perspectivas de crecimiento del mercado y las principales oportunidades de negocio de las que se pueden aprovechar las empresas españolas, además de ofrecer información práctica sobre el país y las formas de hacer negocios.

El sector de la ciberseguridad ha sido declarado de interés prioritario para el desarrollo de la economía del país de acuerdo a los objetivos establecidos en el plan de desarrollo *Vision 2030*. Actualmente se encuentra muy fragmentado en términos de estructurales ya que no está muy claro cuáles son los organismos competentes ni las reglas a seguir debido a la insipiencia del sector. Lo que queda claro es que siendo el mercado más grande de la península Arábica, los altos niveles de crecimiento de la penetración de internet y el desarrollo del comercio electrónico, conllevan una gran necesidad de servicios de ciberseguridad a empresas e instituciones.

La oferta está mayoritariamente copada por las empresas estadounidenses debido a su consideración como líderes en el sector y a los acuerdos establecidos entre ambos países para fomentar la exportaciones americanas de ciberseguridad, todo ello en un marco de estrecha colaboración como resultado de la alianza existente entre ambos países.

La implantación de empresas extranjeras suele producirse de dos maneras, las multinacionales desarrollan alianzas con socios locales para copar grandes segmentos del mercado, mientras que las PYMES suelen acceder a nichos más pequeños de mercado mayoritariamente por medio de licitaciones públicas.

En cuanto a la demanda, se han localizado las principales necesidades de las empresas e instituciones gubernamentales. Arabia Saudí es uno de los países que mayor número de ataques cibernéticos reciben del mundo, por lo tanto existe una latente preocupación por protegerse por parte de las organizaciones que actúan en el país. Atendiendo a encuestas realizadas se han determinado que la demanda por parte de dichas organizaciones se concentra en soluciones de encriptado, copias de seguridad, monitorización de amenazas y firewalls.

Respecto al estableciemiento de precios, se debe considerar la falta de infraestructura logística para desarrollar los servicios de ciberseguridad por parte de las empresas. Estas condiciones pueden suponer hasta un 50% de incremento del precio por dichos servicios en comparación con el país de procedencia.

El producto español, pese a no estar muy extendido, tiene una alta percepción debido a la asociación con la *marca Europa,* lo que supone unos estándares de calidad occidentales que aquí son bien considerados. Por otra parte, las excelentes relaciones existentes entre España y Arabia Saudí, plasmadas en la relación de amistad entre ambas monarquías, suponen un plus para la aceptación de nuestros productos y servicios, en un país en el que las relaciones personales priman, y donde la monarquía es plenipotenciaria y altamente respetada.

En cuanto a los canales de distribución, al tratarse de servicios destinados a empresas, la manera de entrar en contacto con posibles clientes suele ser a través de eventos profesionales, ferias, alianzas con socios locales o licitaciones.

Por otro lado no existen prácticamente barreras de acceso al mercado específicas para el sector. Actualmente el sector se encuentra en proceso de estructuración y pese a que existe un órgano competente, no existe un marco regulatorio específico en materia cibernética al que atenerse. Las empresas interesadas en exportar a Arabia Saudí deberán seguir las pautas marcadas para cualquier otro producto o servicio.

Las perspectivas del mercado son muy atractivas, se trata de uno de los mercados de mayor crecimiento en el ámbito de la ciberseguridad. Las previsiones son que este incremento del mercado se mantenga e incluso aumente considerablemente a medida que se desarrolla el sector privado, concentrándose el crecimiento sobre todo en las regiones norte y central donde discurre la mayor parte de la actividad económica del país. Los campos gubernamentales y de defensa son en los que mayor expansión se prevé.

El sector, desde el punto de vista de las oportunidades comerciales que presenta, se puede subdividir en tres grandes campos; usuarios privados, empresarial e institucional, y por último en el campo educativo.

2. Definición del sector

2.1. Introducción

El sector de la ciberseguridad se trata de uno de los sectores de mayor importancia y crecimiento en la región de la Península Arábica, siguiendo la tendencia global.

Dentro de este sector se engloban todas aquellas actividades que buscan proteger de ataques y accesos no autorizados la integridad de la información digital que se encuentra en sistemas interconectados de computadoras, redes, programas y datos.

La ciberseguridad es uno de los campos que mayor impacto tiene sobre el devenir económico de los países y de los individuos, y cuya trascendencia sólo irá en aumento debido a la dirección en la que se dirige el mundo globalizado moderno.

La interconexión de todos los elementos que intervienen en la actividad económica de las empresas y en la actividad de los gobiernos, depara una necesidad de seguridad al respecto que se ve acrecentada por el aumento de los ataques tanto de individuos o grupos organizados, así como de entidades gubernamentales que buscan obtener a cambio una recompensa en forma de ventaja estratégica o económica.

Dichos ataques cibernéticos pueden acarrear graves problemas en las estructuras operativas de los países; desplome de los sistemas de infraestructuras básicas, sustracción de datos de gran valor, etc. la imaginación de estos delincuentes cibernéticos es el techo. De esta manera no solamente hace falta estar protegido frente a las amenazas ya existentes, sino también anticiparse a futuras nuevas maneras de incurrir en daños en este sentido. Es por ello que se trata de un sector que no solamente tiene que estar a la vanguardia de los desarrollos dentro del campo, sino ir más allá de lo que es conocido.

El objeto de este estudio será analizar el estado del sector en Arabia Saudí, y proveer de información de calidad que sea de utilidad para las empresas que buscan oportunidades en este mercado.

2.2. Morfología del sector

Es necesario mencionar primero que Arabia Saudí no se encuentra a la vanguardia de las posibilidades que ofrece el sector, y que por lo tanto se trata de un mercado con grandes oportunidades para las empresas.

Las intenciones del gobierno de promover la participación del sector privado y atraer inversión extranjera de acuerdo a los objetivos del proyecto *Vision 2030*[1] pueden verse comprometidas por la inseguridad en el ámbito cibernético. Los continuos ataques que sufre el país son un elemento disuasorio en este sentido. Esta situación cobró mayor urgencia en 2012, cuando Saudi Aramco recibió un ataque conocido como "Shamoom" que corrompió miles de hard-drives, impidió el acceso al email de los empleados, destruyó información y afectó al 75% de la infraestructura informática de la empresa. Esto se consideró como un ataque directo contra el reino, puesto que la empresa es el motor del país y representa cerca del 80% de los ingresos del país[2].

Esto supuso que se pusiera de manifiesto la necesidad de progresar en la seguridad cibernética, dando lugar a la creación de la la "*National Information Security Strategy" (NISS*). Esto supone el primer borrador dirigido a establecer un marco nacional de protección cibernética. Sin embargo la mayor parte de empresas e instituciones desarrollan sus propios procesos y medidas de protección. Por otro lado, este borrador no toca aspectos importantes como la protección a infraestructuras críticas (CIP), una de las mayores vulnerabilidades del país.

Por otro lado, en cuanto al sector financiero, es la *SAMA (Saudi Arabian Monetary Authority)*[3] quien ha elaborado un marco regulatorio para salvaguardar la seguridad de los sectores de banca, seguros y entidades de crédito.

Este sector de la ciberseguridad, se encuentra muy fragmentado en cuanto a que no existe una estrategia clara y común a la que atenerse, quizá debido a la reciente adopción de interés en el sector. Esto queda reflejado en el conocido como *"Cyber Readiness Index (CRI) 2.0*", que sirve para evaluar el nivel de preparación frente a riesgos de seguridad cibernética basado en siete elementos; estrategia nacional, respuesta ante incidentes, crimen electrónico y cumplimiento de la ley, intercambio de información, en versión en I+D, diplomacia y comercio, defensa y respuesta ante crisis.

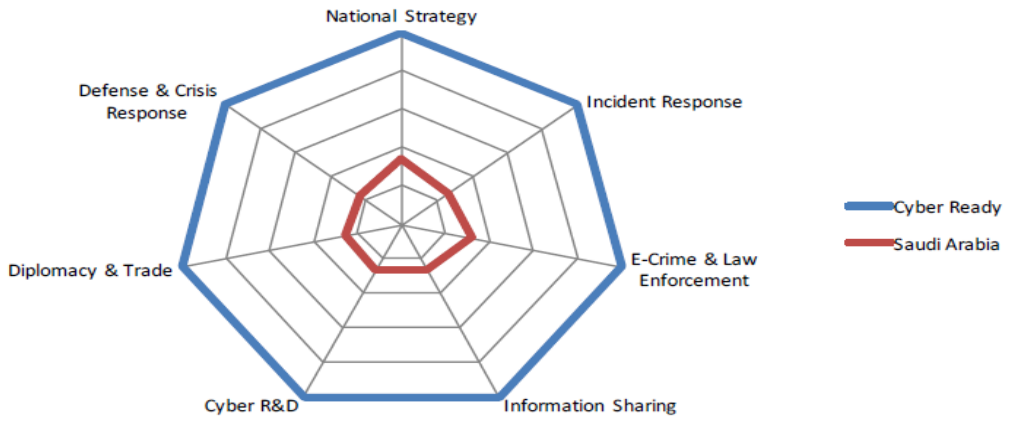
Los resultados quedan reflejados en la siguiente tabla. Como se puede apreciar, el país se encuentra todavía muy lejos del nivel esperado para poder ser considerados como preparados en términos de seguridad en la red.

[1] http://vision2030.gov.sa/en

[2] https://oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom%E2%80%99s-cybersecurity-readiness

[3] www.sama.gov.sa

GRÁFICO 1: CYBER READINESS INDEX ARABIA SAUDÍ.



Kingdom of Saudi Arabia Cyber Readiness Assessment (2017).

Fuente: Belfer Center.

Es por ello que en 2017 el Rey Salman estableció por medio de un decreto real la creación de la "*Presidency of State Security*", una nueva agencia de seguridad nacional responsable de contra-terrorismo e inteligencia doméstica, y la cual integrará entre otras instituciones, al Centro de Ciber-Seguridad Nacional, que dejará de depender del Ministerio del Interior para ser dependiente de Presidencia. Esto supone un esfuerzo por centralizar los esfuerzos en ciberseguridad bajo una única autoridad competente que reporte directamente al rey y al príncipe heredero, y eliminar así la fragmentación existente y que impide la elaboración e implementación de una estrategia nacional eficaz.

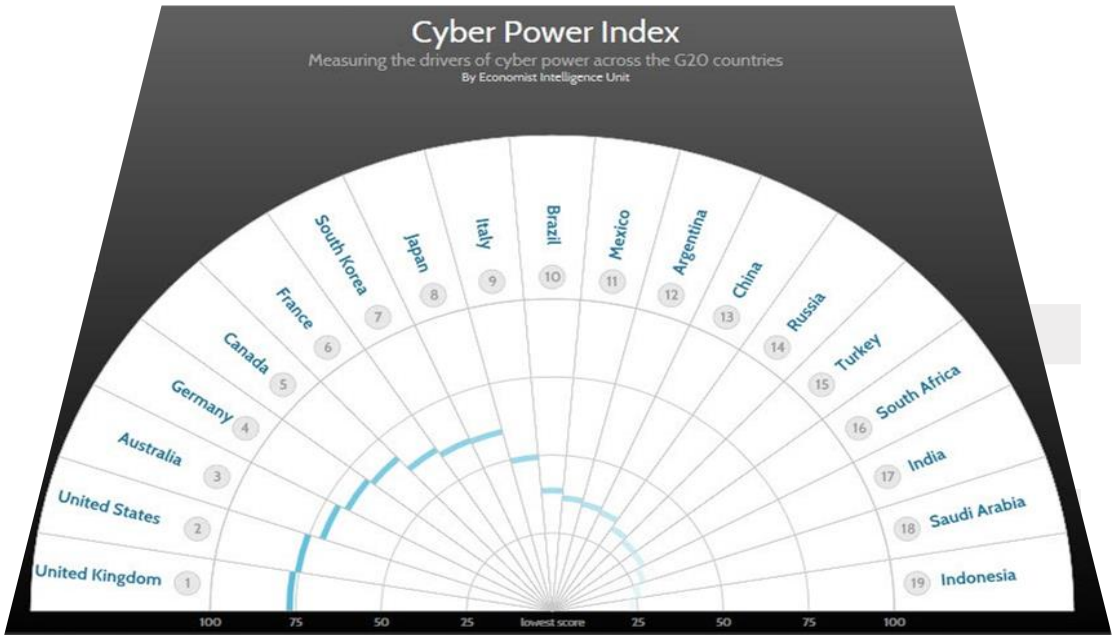
Para lograr afrontar estos objetivos establecidos con solidez (en ambos ámbitos) se reconoce la necesidad de contar con la colaboración del sector privado si se quieren lograr con eficacia. Por ello se espera un crecimiento robusto del mercado de ciberseguridad en Arabia Saudí hasta el año 2022 impulsado por el incremento de los usuarios de internet así como por tener una de las mayores tasas de ataques cibernéticos en los sectores de energía y petroquímica, sectores que componen la columna vertebral de la economía del país.

Actualmente se está produciendo un rápido incremento de usuarios de internet, alcanzando los 14.7 millones de usuarios a día de hoy[4]. Al mismo tiempo se está produciendo también un gran crecimiento industrial en múltiples sectores, muchos de ellos incorporándose al mundo online, entre ellos el financiero, estatal, comercial y educación. Este incremento acelerado de la conectividad en el mundo online está haciendo que el país sea foco de ataques maliciosos.

[4] http://cces-kacst-mit.org/project/cyber-security-initiative

Arabia Saudí se encuentra clasificada actualmente en la posición 12 entre los países que más ataques cibernéticos reciben, representando el 1.81% de todos los ataques a nivel global, siendo además el país que más "spam" recibe del mundo con un ratio de 83.3%. Además se encuentra clasificada en la posición 18 de 19 en el *Cyber Power Index*, indicador que mide la capacidad de los países del G20 para hacer frente a ataques cibernéticos y de construir una la infraestructura digital segura necesaria para una economía productiva.

GRÁFICO 2: CYBER POWER INDEX ARABIA SAUDÍ.



Fuente: Global System for Sustainable Development.

Todo esto pone de manifiesto la necesidad de avanzar en la seguridad cibernética para proporcionar una situación de seguridad que permita a las empresas y entidades gubernamentales desarrollarse y que genere un clima favorable a la inversión extranjera.

Es imprescindible para el devenir económico del país alcanzar una situación de seguridad cibernética para poder alcanzar los ambiciosos objetivos establecidos dentro del plan de desarrollo "*Vision 2030*".

2.3. Segmentación

Los riesgos cibernéticos se pueden clasificar en tres áreas principales:

- Ciber-crimen: actividades llevadas a cabo por individuos o grupos criminales que buscan sustraer información, dinero o causar trastornos por medio de la sustracción de información

de tarjetas de crédito, propiedad intelectual o interrupción de las operaciones de páginas webs.

- Ciber-guerra: actividades de sabotaje o espionaje por parte de una nación con la intención de causar trastornos o sustraer información crítica.
- Cyber-terrorismo: actividades por parte de organizaciones terroristas a través del ciberespacio.

El mercado se puede segmentar atendiendo a distintos criterios que quedan reflejados en los cuadros inferiores:

Por Tipo de Seguridad	Por Solución	Por Servicio	Por Sectores
• Redes • Contenidos • Inalámbrica • Aplicaciones • Nube • End-point	• Identidad y gestión de accesos • Riesgo y gestión de conformidad • Encriptado • Prevención de pérdida de información • Fire2wall • Antivirus y malware • Gestión de amenzas • Detección y prevención de intrusiones • Gestión de la información	• Consultoría • Diseño e integración • Asesoría en risegos y amenzas • Administración de servicios de seguridad • Formación	• Bancario y Financiero • IT & Telecoms. • Defensa • Energía • Sanitario • Retail

Debido a la complejidad y profundidad del sector, y con el fin de facilitar el seguimiento del estudio y la realización del mismo desde un punto de vista comercial en vez de técnico, se segmentará en 2 vertientes muy amplias según el destinatario final de los productos o servicios:

- Usuarios: se refiere a todos aquellos individuos con acceso a internet y que pueden requerir productos de software que protejan sus equipos y redes.

- Empresarial e institucional: se incluyen todas aquellas organizaciones privadas o gubernamentales que requieran soluciones de ciberseguridad personalizados a medida de protección de sus redes, sistemas e información interna.

3. Oferta – Análisis de competidores

La campaña del gobierno para coordinar y construir un sistema cibernético seguro apoyándose en el sector privado genera gran cantidad de oportunidades para las empresas extranjeras debido a la insipiencia del sector y a la escasa experiencia y envergadura de las empresas locales.

Destacan sobre todo los campos de vigilancia electrónica, sistemas de comunicaciones avanzados, equipos de detección electrónica, alarmas ante ciberataques, y sistemas de prevención de intrusiones y biometría.

Entre las empresas extranjeras actualmente activas en el país, se pueden clasificaren dos grupos; grandes multinacionales, y PYMES en busca de capturar nichos de mercado. Las empresas de nacionalidad americana son las más activas debido a su liderazgo en el sector y gracias al énfasis puesto por la administración de los EEUU en potenciar las exportaciones de estas empresas a Arabia Saudí, uno de sus principales socios comerciales y políticos.

Actualmente las grandes multinacionales dedicadas a este sector están desarrollando asociaciones con entidades gubernamentales y empresas privadas, para ir desarrollando sistemas capaces de afrontar y cubrir las amenazas y necesidades existentes.

Es el caso de la campaña de e-government[5] que se está llevando a cabo en el reino por medio de la cual se pretende coordinar la construcción de bases de datos electrónicas para desarrollar la digitalización de las instituciones gubernamentales. Entre los potenciales socios de mayor envergadura se encuentran:

- *Saudi Electronic data Interchange*[6], quien supervisa las transacciones de entidades gubernamentales.

- *E-Government Service Bus Programme*[7], entidad encargad de centralizar las bases de datos gubernamentales.

[5] https://www.yesser.gov.sa/EN/MechanismsandRegulations/strategy/Documents/the_2nd_egovernment_action_plan_ENG.pdf

[6] https://www.fasah.sa/trade/sau/corp/index.htm

[7] https://www.yesser.gov.sa/EN/BuildingBlocks/Pages/government_service_bus.aspx

- *Tabadul*[8], entidad responsable del mercado de valores saudita, quien maneja la inversión pública en infraestructura informática.

Entre las multinacionales destacan aquellas dedicadas a la defensa como Lockheed Martin, Raytheoon, BAE Systems y Finmeccanica, o aquellas focalizadas hacia infraestructura informática como Microsoft, Genetec, Symantec, IBM, Cisco Systems, Trend Micro Inc., Palo Alto Netrworks, McAfee, Trustwave Holdings, RSA Security o Fortinet.

Uno de las asociaciones más importantes en materia de ciberseguridad se ha producido entre los gigantes IBM y Mobily, que juntos han creado el *Global Security Operations Centre* (SOC). Situado dentro del centro de datos de Mobily, emplea la infraestructura de servicios de seguridad de IBM para analizar más de 15 mil millones de eventos de seguridad diarios en más de 140 países, además de gestionar la seguridad cibernética de ciertos ministerios como el Ministerio de Educación[9].

Por otro lado, empresas de menor tamaño como AirPatrol Corporation, DataLocker, FireEye o Glimmerglass Optical Solutions han entrado al mercado tratando de abarcar nichos más asequibles como sistemas de almacenamiento seguro en la nube, programas diseñados para adquirir información proveniente de señales electrónicas y ópticas, así como sistemas supervisión del uso de tablets, smartphones, pc's y demás dispositivos móviles.

En cuanto al panorama de empresas locales de ciberseguridad, es necesario destacar que no existen grandes empresas saudíes, sino que en su mayoría se tratan de asociaciones entre empresas extranjeras que buscan establecerse mediante socios. Por lo tanto respecto a las empresas puramente saudíes destacan las siguientes:

- Saudi Advanced Technologies Ltd.
- AFNAM Information Technology
- AEC Advanced Electronics Company
- Safe Decision Co.

[8] http://www.etabadul.com/

[9] https://oxfordbusinessgroup.com/analysis/front-lines-enhancing-kingdom%E2%80%99s-cybersecurity-readiness

4. Demanda

Existe una gran demanda de productos y servicios de ciberseguridad ya que es imprescindible para alcanzar una digitalización de la economía de forma segura, lo cual es necesario para alcanzar los objetivos de crecimiento del sector privado propuestos dentro de la "Vision 2030".

La existencia de esta demanda creciente se refleja en el desarrollo del sector durante los últimos años. Este desarrollo queda reflejado en números en el cuadro inferior, donde se puede apreciar el incremento del gasto, ingresos y número de establecimientos por parte de las organizaciones atendiendo a datos ofrecidos por el *General Authority of Statistics*[10].

TABLA 1: CIFRAS SECTOR CIBERSEGURIDAD ARABIA SAUDÍ.

Sector de Tecnologías de la Información y Comunicaciones				
	Ingresos	Gastos	Establecimientos	
Actividades de consultoría y administración de infraestructuras	29.185	16.440	24	2016
Otros servicios de IT y ordenadores	138.695	77.438	157	
Procesamiento de datos, hosting y actividades relacionadas	24.047	16.838	122	
Actividades de consultoría y administración de infraestructuras	28.189	15.807	23	2015
Otros servicios de IT y ordenadores	139.133	79.758	153	
Procesamiento de datos, hosting y actividades relacionadas	21.992	15.996	115	
Actividades de consultoría y administración de infraestructuras	26.771	14.977	19	2014
Otros servicios de IT y ordenadores	133.674	75.441	133	
Procesamiento de datos, hosting y actividades relacionadas	20.750	15.038	100	
Actividades de consultoría y administración de infraestructuras	25.019	13.783	16	2013
Otros servicios de IT y ordenadores	128.532	72.540	120	
Procesamiento de datos, hosting y actividades relacionadas	19.952	14.459	90	
Actividades de consultoría y administración de infraestructuras	24.772	13.647	16	2012
Otros servicios de IT y ordenadores	126.242	71.117	117	
Procesamiento de datos, hosting y actividades relacionadas	19.186	13.771	85	

Fuente: General Authority for Statistics.

La interconexión de nuevas aplicaciones a la red aumenta para lograr esta digitalización de la economía, y por tanto también la exposición a amenazas.

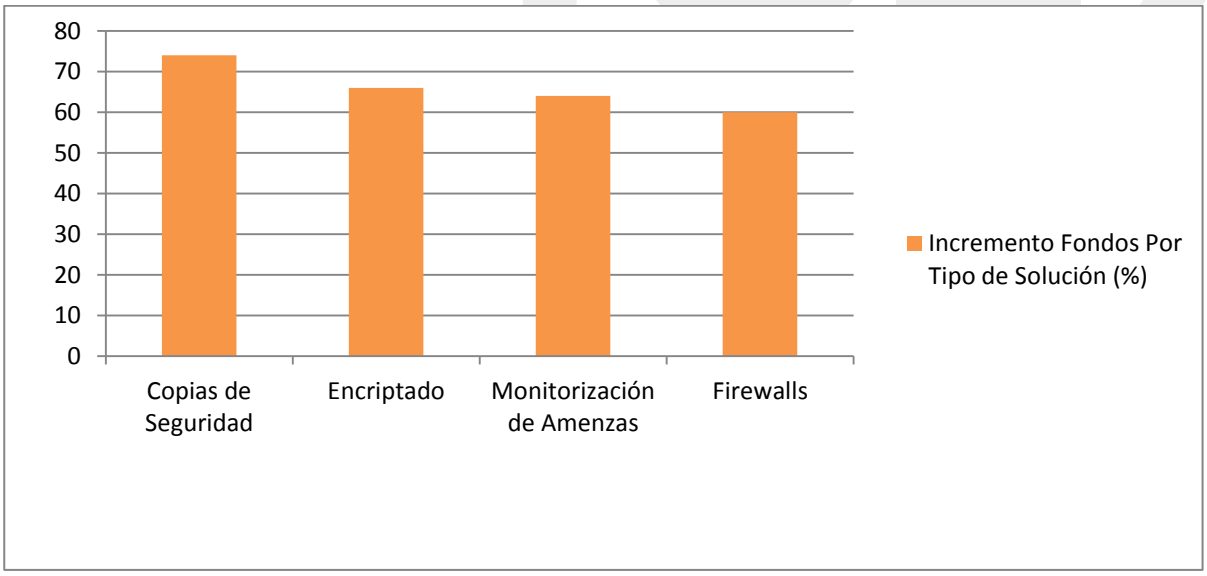
[10] https://www.stats.gov.sa/en

Atendiendo a encuestas realizadas entre profesionales del sector IT por parte VMware[11] (uno de los líderes mundiales en el sector), dos de cada tres altos mandos consideran la ciberseguridad como su prioridad. Esto se debe al elevado número de ataques recibidos por empresas en Arabia Saudí, lo cual deja patente la preocupación en este sentido por parte de las organizaciones. Casi la mitad (46%) de las organizaciones en Arabia Saudí esperan ser atacadas cibernéticamente, lo cual representa una cantidad tres veces superior al miedo existente contra estas amenazas en otras partes del mundo como Europa, África, y el resto de Oriente Medio, donde sólo el 16% comparten esta preocupación.

Debido a esta latente preocupación, los fondos destinados hacia soluciones de ciberseguridad por parte de las organizaciones van en aumento. Arabia Saudí es uno de los países donde mayor inversión se está realizando en el sector de la ciberseguridad donde se espera que el mercado alcance los 3 mil millones de euros en 2019, creciendo a un ritmo del 14.5% interanual según cifras ofrecidas por el centro de Ciberseguridad Nacional.

De nuevo atendiendo a encuestas realizadas por VMware, dos tercios (64%) de las organizaciones empresariales en Arabia saudí consideran la ciberseguridad como su prioridad dentro del campo de IT, incrementando los fondos destinados a copias de seguridad en un 74%, encriptado en un 66%, monitorización de amenazas en un 64% y en firewalls un 60%.

GRÁFICO 2: FONDOS DESTINADOS POR EMPRESAS POR TIPO DE SOLUCIÓN.



Fuente: Intersec Saudi Arabia.

[11] https://www.vmware.com/

5. Precios

Debido a las características de los servicios de ciberseguridad, es muy difícil establecer un precio indicativo que sea comprensivo. Estos servicios son desarrollados a medida de las necesidades de las empresas o instituciones que lo solicitan, y pueden comprender distintas combinaciones de soluciones de ciberseguridad.

Además debido a la opacidad de las empresas del sector en cuanto a los precios de sus servicios, no se ha podido obtener una lista de precios detallada de las distintas soluciones de ciberseguridad existentes.

Por lo tanto para lograr establecer una noción de precios hay que tener en cuenta que debido a las dificultades para implementar sus soluciones de ciberseguridad, las empresas deben proporcionar los servicios adyacentes necesarios para el desarrollo de dichas soluciones.

Por servicios adyacentes se entienden todos aquellos necesarios para que la solución de ciberseguridad sea operativa, es decir, la infraestructura necesaria para que sea posible implementar sus soluciones debe ser establecida en su mayor parte por la empresa exportadora. Esto puede suponer un incremento del precio final en un 25-50%[12] del precio en sus respectivos países.

[12] Información proporcionada por la empresa Invisible Bits.

6. Percepción del producto español

Actualmente solamente existe una empresa española presente en el mercado de Arabia Saudí que se encuentra establecida mediante su filial *Invisible Bits*[13]. Su implantación se ha producido por medio de un acuerdo de coinversión con una empresa local que debido a sus características es confidencial.

Sin embargo la empresa nos incidió en que los productos y servicios de ciberseguridad españoles son percibidos altamente debido a dos circunstancias principales: la buena relación entre ambos países y la asociación de los productos españoles con la *marca Europa*.

Por un lado la asociación con la *marca Europa* con la que vienen acompañados los productos y servicios nacionales, actúa como validación de que se tratan de productos y servicios occidentales y de calidad.

Por otro lado la buena relación existente entre ambos países, ejemplificada sobre todo en la relación de amistad entre ambas monarquías es importante en un país en donde las relaciones de negocios se basan en gran medida en conocimiento mutuo y la confianza. Es importante entender la concepción existente en el país sobre la monarquía, rango que viene concedido por dios a los monarcas y sus familiares, y por ende es en cierta medida divino. Por lo tanto esta excelente relación entre las monarquías genera un clima de aceptación en los negocios, que además cobra mayor importancia en un país en el que el tejido empresarial está controlado mayoritariamente por holdings empresariales propiedad de los jeques familiares cercanos a la familia Al-Saud.

[13] https://www.invisiblebits.com/es/

7. Canales de distribución

La distribución en este sector se enfoca desde dos perspectivas, atendiendo al destinatario final:

- Usuarios individuales
- Empresa e instituciones

Usuarios Individuales

Estos productos o soluciones de ciberseguridad suelen ser genéricos tales como antivirus, firewalls o sistemas de encriptado simples que los usuarios instalan en sus equipos para protegerse de ataques de virus, spams, etc.

Estos productos o soluciones se distribuyen por medio de grandes almacenes o a través de portales de internet de las propias empresas que los venden.

Empresas e Instituciones

Estas soluciones de ciberseguridad son normalmente desarrolladas a medida partiendo de un software base. Estas pueden ser desde sistemas de almacenamiento de datos de forma segura, sistemas de transmisión de datos de forma segura, programas de formación en ciberseguridad orientado a empresas o al ámbito institucional, etc.

La manera de entrar en contacto con posibles clientes para este tipo de empresas suele ser a través de eventos profesionales, ferias, alianzas con socios locales o licitaciones.

También se incluyen en este campo las oportunidades dentro del espectro formativo. Es necesario contar con una masa laboral cualificada que permita cubrir la creciente demanda de empleos en el sector. Es por ello que se necesitan programas formativos y educativos que sean accesibles a la población nacional saudí a través de universidades o centros especializados de educación superior.

Estas oportunidades deben ser buscadas a través de la asistencia a ferias especializadas, eventos profesionales o por medio de alianzas con instituciones educativas.

8. Acceso al mercado – Barreras

Actualmente el sector se encuentra en proceso de estructuración y pese a que existe un órgano competente, no existe un marco regulatorio específico en materia cibernética al que atenerse. Las empresas interesadas en exportar a Arabia Saudí deberán seguir las pautas marcadas para cualquier otro producto o servicio.

8.1 Barreras Arancelarias

Actualmente se ha implementado en Arabia Saudí un 5% de IVA. Este IVA es aplicable a este sector, tanto para los productos de ciberseguridad tales como software antivirus, como para los servicios de ciberseguridad prestados a empresas e instituciones. El registro de la empresa debe hacerse en la *General Authority for Zakat & Tax (GAZT)*[14].

8.2 Barreras No Arancelarias

En el caso de una implantación, la empresa debe estar registrada en el Registro Comercial cuyo órgano competente es *Sagia*. La inversión extranjera puede efectuarse en empresas de propiedad de nacionales saudíes y de inversores extranjeros o en empresas propiedad únicamente de inversores extranjeros, aunque lo más recomendable es implantarse de la mano de un socio local que sea conocedor del mercado.

Las licitaciones públicas se rigen bajo la Ley de Licitación y Contratación Pública[15], y cada organismo gubernamental es responsable de la contratación con cargo a su propio presupuesto. Las empresas extranjeras no deben estar domiciliadas en Arabia Saudí para contratar con el Estado o sus instituciones, pero si deben conseguir una licencia comercial temporal a través de

[14] https://www.gazt.gov.sa/en

[15] *https://www.nazaha.gov.sa/.../GovernmentTendersAndProcureme...*

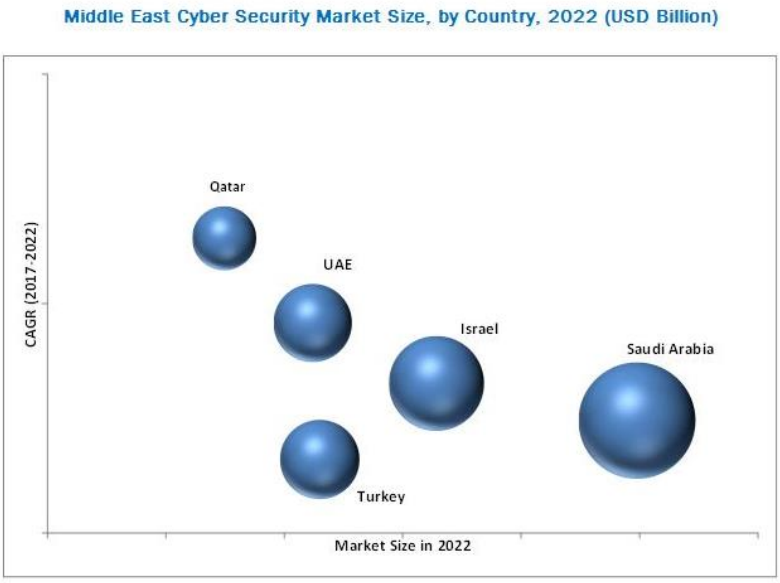
Sagia, con la cual podrán operar hasta un año, tras el cual deberán obtener la licencia comercial permanente.

En cuanto a la regulación de cobros y pagos al exterior, existe libertad de cambios.

9. Perspectivas del sector

En Oriente Medio se espera un gran crecimiento del mercado, desde los 9,75 mil millones de euros en 2017 hasta cerca de 19 mil millones de euros en 2022, lo que supone una tasa anual compuesta de crecimiento (CAGR) del 14,2% desde el año 2017 hasta el 2022[16]. Este crecimiento será liderado por Arabia Saudí, país que considera objetivo primordial crear un ámbito de seguridad que permita el desarrollo económico propuesto en su plan de crecimiento "*Vision 2030*", tal y como se puede apreciar en el gráfico inferior.

GRÁFICO 3: TAMAÑO MERCADO CIBERNÉTICO ORIENTE MEDIO.



Fuente: Markets and Markets.

Arabia Saudí es uno de los países donde mayor inversión se está realizando en el sector de la ciberseguridad donde se espera que el mercado alcance los 3 mil millones de euros en 2019 desde los 1.3 mil millones de 2013, creciendo a un ritmo del 14,5% interanual según cifras ofrecidas por el Centro de Ciberseguridad Nacional.

[16] https://www.marketsandmarkets.com/PressReleases/middle-east-cyber-security.asp

Las previsiones son que este incremento del mercado se mantenga e incluso aumente considerablemente a medida que se desarrolla el sector privado, concentrándose el crecimiento sobre todo en las regiones norte y central donde discurre la mayor parte de la actividad económica del país.

GRÁFICO 4: TAMAÑO MERCADO CIBERNÉTICO ARABIA SAUDÍ.

Fuente: Techsci Research.

Dentro del sector, los campos gubernamentales y de defensa son en los que mayor expansión se prevé en todo Oriente Medio, siendo el propulsor de esta tendencia Arabia Saudí donde las aspiraciones de convertirse en el eje dominante de la zona conllevan una inversión sustancial en este ámbito.

El crecimiento del sector estará impulsado también debido el incremento de la urbanización y de los ciberataques en el sector energético, el cual es el motor de la economía de todo el país y el que debe proporcionar los fondos necesarios para las grandes inversiones que se quieren llevar a cabo desde las instituciones estatales para desarrollar el país.

10. Oportunidades

El sector, desde el punto de vista de las oportunidades comerciales que presenta, se puede subdividir en tres grandes campos:

- Usuarios privados
- Empresarial e Institucional
- Educativo

Usuarios Privados

El rápido incremento de la conectividad de los hogares junto con el escaso nivel de seguridad que existe en el país en términos cibernéticos, hace que estos se conviertan en blanco fácil para ataques maliciosos que buscan sustraer información privada de los usuarios.

Aquí se presentan oportunidades comerciales para productos de protección de sistemas domésticos contra ataques, conocidos como “antivirus”. Estos productos no son muy complejos técnicamente y tienen un mercado muy amplio que cubrir. Si bien es cierto que suelen estar cubiertos por los grandes nombres dentro del mundo cibernético y que son enormemente reconocidos.

Empresarial e Institucional

En este campo es donde se presentan las mayores oportunidades, en los servicios de protección de sistemas e información de las empresas. Para las organizaciones es fundamental contar con sistemas que garanticen la seguridad de sus datos internos y de los datos de sus clientes, y que eviten intentos de sabotajes de sus actividades operativas.

Dentro de este campo se pueden distinguir cinco sub-campos:

- *Sectores críticos*: el sector energético se considera de interés nacional por su importancia como columna vertebral de la economía del país. También se considera el sector sanitario como un foco principal de ataques.

- *Agencias gubernamentales*: imprescindible que la información entre las distintas agencias gubernamentales sea fluida y no esté comprometida.

- *Defensa*: la inversión en el sector está creciendo en gran medida y adquiere gran importancia debido a la lucha contra el ciber-terrorismo.

- *Mercado Financiero*: La seguridad y resiliencia de estos mercados son claves para garantizar el flujo de capitales hacia el país que permitan la financiación privada.

- *E-commerce*: el comercio electrónico es uno de los campos que augura un mayor crecimiento futuro y que necesita de ser seguro y estable.

Las empresas pueden dirigir sus esfuerzos a cubrir las numerosas licitaciones que necesitan ser cubiertas en estos campos y que son publicadas en el portal oficial de la administración *Monafasat*[17]. Esta opción resulta de mayor interés para PYMES que busquen entrar al mercado cubriendo oportunidades específicas, en vez de acudir a asociaciones con socios locales.

Entre los potenciales socios de mayor envergadura se encuentran:

- *Saudi Electronic data Interchange*, quien supervisa las transacciones de entidades gubernamentales.

- *E-Government Service Bus Programme*, entidad encargad de centralizar las bases de datos gubernamentales.

- *Tabadul*, entidad responsable del mercado de valores saudita, quien maneja la inversión pública en infraestructura informática.

Educativo

Por último, es necesario crear una infraestructura de talento entre la población del país que pueda convertirse en la fuerza laboral necesaria para sostener el sector. Es por ello que existen oportunidades dentro de la educación a nivel superior o de formación profesional que capacite a los jóvenes profesionales.

[17] https://monafasat.etimad.sa/

TABLA 2: CIFRAS EMPELADOS SECTOR CIBERNÉTICO.

Sector de Tecnologías de la Información y Comunicaciones				
	Empleados			
	Total	No-Saudí	Saudí	
Actividades de consultoría y administración de infraestructuras	372	251	121	2016
Otros servicios de IT y ordenadores	2.015	1.371	644	
Procesamiento de datos, hosting y actividades relacionadas	874	605	269	
Actividades de consultoría y administración de infraestructuras	358	244	114	2015
Otros servicios de IT y ordenadores	1.966	1.337	629	
Procesamiento de datos, hosting y actividades relacionadas	824	571	253	
Actividades de consultoría y administración de infraestructuras	344	235	109	2014
Otros servicios de IT y ordenadores	1.909	1.298	611	
Procesamiento de datos, hosting y actividades relacionadas	790	554	236	
Actividades de consultoría y administración de infraestructuras	320	219	101	2013
Otros servicios de IT y ordenadores	1.826	1.241	585	
Procesamiento de datos, hosting y actividades relacionadas	753	531	222	
Actividades de consultoría y administración de infraestructuras	320	219	101	2012
Otros servicios de IT y ordenadores	1.781	1.210	571	
Procesamiento de datos, hosting y actividades relacionadas	710	501	209	

Fuente: General Authority for Statistics.

En la tabla superior queda reflejada la evolución de la fuerza laboral del sector en cuestión desde el año 2012 hasta el año 2016. Se observa un incremento del número de empleados en todos los campos del sector año tras año, lo cual indica una demanda creciente que ha de ser cubierta.

Otro resultado significativo es el hecho de que el número de empleados no-saudíes es bastante más elevado que el de los empleados nacionales. Teniendo en cuenta que durante este año 2018 se espera una fuga de expatriados del país debido a cambios regulatorios en el mercado laboral que buscan fomentar la introducción en el mismo de fuerza laboral autóctona, se intuye que existe una oportunidad en el campo educativo para formar a nacionales saudís que puedan cubrir ese vacío laboral que se creará.

11. Información práctica

- Las principales ferias y congresos del sector son:
  - Intersec Saudi Arabia, Yeda 14-16 Abril 2019
  - Innovative Security Summit, Riad 7 de Mayo de 2018
- Las principales publicaciones del sector son:
  - Security Middle East, The Magazine for Security and safety professionals
- Los organismos públicos relevantes son:
  - National Cyber Security Center https://www.moi.gov.sa/wps/portal/ncsc/
  - Ministry of Interior (MOI) https://www.moi.gov.sa
  - Ministry of Communications & Information technology https://www.mcit.gov.sa
  - Presidency of State Security/ Royal Court
- Recomendaciones para el exportador y cultura empresarial:

  Desde la Oficina Económica y Comercial de España en Riad se ofrecen las siguientes recomendaciones a los exportadores españoles interesados en comerciar sus productos en el mercado saudí:

  - Incluso presentando un producto funcional y de calidad, es extremadamente difícil negociar en la cultura árabe si no es perseverante y, sobre todo, si no se realizan negociaciones personalmente ya que valoran conocer a los representantes de las empresas, más incluso que la calidad o el precio de las productos o la experiencia y reputación de la empresa. Por tanto, la visita al país es muy recomendable.

- La colaboración con un socio local, también es recomendable puesto que el conocimiento del mercado y los contactos son fundamentales. Además el conocimiento del idioma local aporta valor añadido.

- Debe tener paciencia, concédase tiempo. Es muy probable que necesite hacer varias visitas al país hasta que pueda lograr su objetivo. En muchas ocasiones, la separación entre actividades públicas y privadas es difusa. Téngalo en cuenta a la hora de plantearse la elección de un agente o representante en el país.

- Como se ha mencionado anteriormente, la relación personal es fundamental. Si esta es buena, con el tiempo su cliente/socio depositará en usted una confianza abrumadora.

12. Anexos

- Oficina económica y Comercial de España en Riad: www.oficinascomerciales.es
- Ministry of Interior (MOI): https://www.moi.gov.sa
- Saudi Arabia General Investement Authority: https://sagia.gov.sa
- Ministry of Finance: https://www.mof.gov.sa
- Ministry of Communications and Information Technology: https://www.mcit.gov.sa
- Presidency of State Security/Royal Court
- National Cybersecurity Center: https://www.moi.gov.sa/wps/portal/ncsc/
- Saudi Arabian Monetary Authority (SAMA): www.sama.gov.sa
- Riyadh Chamber of Commerce: www.riyadhchamber.com
- Cámara de Comercio de España: www.camara.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

www.icex.es

EM

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

ICEX España Exportación e Inversiones