Estudios de Mercado
RESUMEN EJECUTIVO

El mercado de la ciberseguridad en Australia

Abril 2016

Este estudio ha sido realizado por
Beatriz Jerez del Castillo, bajo la supervisión de la
Oficina Económica y Comercial
de la Embajada de España en Sídney

ICEX España Exportación e Inversiones

"*Si una organización está conectada a la red, entonces es vulnerable*". Con esta frase comienza el informe "*The Australian Cyber Security Centre Threat Report 2015"* apuntando muy certeramente al alcance que el concepto de la ciberseguridad tiene y tendrá aún más en el futuro.

En la era de la información en la que vivimos, los datos y la información han adquirido un valor estratégico. Todos y cada uno de los sectores económicos-sociales del sistema global se han visto afectados por la digitalización: el sector público, la industria y el propio individuo. No es difícil imaginar un horizonte cercano donde el grado de dependencia respecto a estas tecnologías sea equiparable al de nuestros hogares respecto a la electricidad o al agua. Si bien, a medida que las TICs han sido plenamente integradas en las actividades cotidianas de la sociedad y la industria, los riesgos derivados del mundo cibernético se han incrementado en paralelo.

Por su parte, Australia no sólo ha logrado niveles elevados de digitalización, sino que se prevé que distintos factores en este ámbito añadan grados de complejidad a un sistema altamente sofisticado. Conceptos tales como la computación en la nube, el Internet de las cosas, o el *Big Data* crean nuevas posibilidades para los individuos y las empresas. No obstante, aparejadas a dichas posibilidades, aparecen nuevos riesgos y amenazas que deben ser tenidas en consideración. En la nación isleña, dichos conceptos serán apoyados por el despliegue en curso de la *National Broadband Network (NBN)*, que creará un acceso más efectivo y rápido a la red.

Se espera que la creciente demanda que ha apuntalado el desarrollo de la industria en los últimos años siga su ritmo imparable. En particular, un aumento en el número de ciberincidentes, se ha convertido en el catalizador que ha desencadenado importantes inversiones tanto de carácter público como de carácter privado. Todo tipo de organizaciones pueden ser susceptibles a ataques cibernéticos y tendrán que asumir las medidas necesarias para protegerse de los mismos. Aunque en muchas ocasiones dichos ataques no son notificados a las autoridades correspondientes, el Department of Defence estima que en 2012 hasta 5,4 millones de australianos fueron víctimas del cibercrimen con un coste estimado para la economía de A$1.650 millones[1][2].

En este contexto; *IBIS World* -empresa de investigación de mercados especializada en la economía australiana- estima un crecimiento anual medio de los ingresos del sector de un 4,4% para los próximos 5 años, colocando el montante total de la industria en valores cercanos a los A$3.000 millones en 2020-21 (unos 2,010 millones de euros).

Una posible segmentación del mercado distinguiría a cuatro tipos de clientes: el gobierno y los organismos públicos, los operadores de infraestructuras críticas, las empresas (grandes y PYMES) y particulares. Cada uno demandará soluciones de ciberseguridad completamente distintas; desde soluciones integrales que exijan fuertes inversiones en ciberseguridad, demandadas por parte del gobierno o las grandes empresas, hasta soluciones básicas y de precio competitivo, reclamadas por las PYMES y los individuos.

Por otra parte, estamos ante un sector altamente dinámico, donde la dualidad y la fragmentación constituyen dos rasgos característicos del mercado. En este sentido, en la industria australiana de la ciberseguridad encontramos a unas pocas multinacionales de origen extranjero que coexisten

[1] Department of Defence. Australian Cyber Security Centre to be established: Commonwealth of Australia; 2013, http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm

[2] El tipo de cambio utilizado es de1,50 AUD por cada euro. Para información diaria sobre el tipo de cotización entre el dólar australiano y las distintas divisas, puede acceder a la página web del Australian Reserve Bank (ARB), http://www.rba.gov.au/statistics/frequency/exchange-rates.html

junto a un número elevado de pequeñas y medianas empresas. Mientras que las primeras ofrecen soluciones integradas, las segundas se apoyan en una oferta diferenciada y de alto valor añadido para atraer a un cliente de pequeño tamaño, concentrándose en atender las necesidades de los pequeños nichos de mercado.

Hasta 3.000 firmas forman parte de la industria y se suelen localizar en los dos principales estados del país: Nueva Gales del Sur y Victoria (un 70% de las mismas). En concreto, existe una concentración de las empresas de ciberseguridad alrededor de las grandes urbes, especialmente Sídney y Melbourne, puesto que allí es donde se localizarán los principales centros de negocios del país y la mayor parte de sus clientes.

El sector de la ciberseguridad, como el del *software* en general, es un sector altamente globalizado, donde el concepto de frontera nacional ha quedado obsoleto. De este modo, las empresas de ciberseguridad acostumbran a ser muy globales y su producto suele ser fácilmente trasferible a otros mercados, salvo cuando existen restricciones legislativas. El capital extranjero está muy presente, siendo la americana la nacionalidad predominante.

A la hora de entrar a este mercado, la empresa española se enfrenta a un escenario altamente competitivo, donde la competencia aseverada de los gigantes globales de las TICs limitará la posibilidad de lograr los grandes contratos del gobierno o de las grandes compañías. A la hora de acceder a los distintos tipos de cliente, será necesario hacer uso de una estrategia de entrada distinta, diferenciada para cada uno de los segmentos previamente identificados. Mientras que el gobierno y la gran empresa privilegiarán la utilización del método de la licitación, las pequeñas empresas y el usuario final, acudirán al distribuidor de confianza, la tienda digital o la tienda minorista.

Una demanda futura apuntalada por la creciente inversión de las empresas y del gobierno en su presupuesto de ciberseguridad, se combina con un marco político e institucional estable. El convencimiento por parte del Primer Ministro, Malcolm Turnbull, sobre el potencial futuro del sector de la ciberseguridad en Australia, se ha traducido en un generoso apoyo legal y financiero. De este modo, la ciberseguridad se ha incorporado en el marco legal del país, ocupando un papel importante en el nuevo Libro Blanco de Defensa de 2016 (*2016 Defence White Paper*) y obteniendo su propia Estrategia de Ciberseguridad (*Cyber Security Strategy*). La ciberseguridad también ocupa un lugar privilegiado en el marco de la nueva Estrategia de Innovación y Ciencia del gobierno federal (National Innovation and Science Agenda (NISA)), destacándose iniciativas dentro de la misma como el lanzamiento de un Cyber Security Growth Centre (CSCC), el apoyo a DATA 61 o el despliegue de un Digital Marketplace que facilite a las PYMES su participación en el mundo de la adquisición pública de soluciones de TICs.

Entre las oportunidades que se vislumbran en el futuro, destacar la colaboración con las organizaciones punteras de investigación que se alojan en el país. El mercado de la ciberseguridad cambia a una velocidad vertiginosa y se encuentra en crecimiento continuo. Aquellas empresas innovadoras, capaces de explotar una idea diferente y hacerla atractiva para los clientes, encontrarán su hueco en el mercado. La colaboración con los centros punteros de investigación australianos como por ejemplo DATA 61 y DSTO, o las universidades australianas, permitirá desarrollar soluciones novedosas. Además, la naturaleza trasnacional de este fenómeno exige en muchos casos la colaboración internacional.

Las áreas tecnológicas a desarrollar en el futuro son prácticamente ilimitadas. Nuevas amenazas exigirán nuevas soluciones. Si bien, los expertos apuntan hacia tecnologías en áreas emergentes tales como:

- Computación en la nube.
- Internet de las cosas.
- *Big Data*.

Por ejemplo, a medida que más información se almacena en la nube, se hace necesario el establecimiento de nuevos mecanismos que permitan protegerla. Se estima que muchas de las empresas australianas harán uso de soluciones dentro del ámbito de la seguridad de la computación en la nube (*Cloud Computing Security*), fuente potencial de oportunidades para las empresas españolas. El **Internet de las cosas** constituye otro fenómeno a seguir de cerca, y que ha multiplicado el número de posibles vectores de ataque.

El avance del **Big Data** también permitirá desarrollar nuevas soluciones de ciberseguridad. En este ámbito, se hacen necesarias nuevas técnicas que faciliten la separación de la información relevante e irrelevante sobre eventos que en principio parecen desconectados. En paralelo, las organizaciones deberán considerar nuevas áreas como *data analytics o maching learning.*

Por otro lado, la disciplina conocida como **Forense Digital**, aunque relativamente joven, comienza a ganar peso en el marco del sistema judicial público y entre las organizaciones privadas del mundo entero. Nuevas herramientas desarrolladas en el ámbito de los **modelos de gestión de riesgos** también constituye un área de interés para los responsables de la ciberseguridad de la organización.

Hoy en día, los expertos en la materia reconocen que un ataque cibernético complejo y altamente sofisticado es prácticamente imparable. Por ello, las organizaciones deben hacer uso de un nuevo enfoque que maximice la ratio entre el coste y el beneficio de la solución de ciberseguridad adoptada. Dicho de otra forma, dado que el riesgo no puede ser eliminado completamente, lo importante es decidir qué riesgo se está dispuesto a aceptar y construir las defensas de la organización en torno a dicho parámetro. En este ámbito también se está apostando por soluciones integrales, que adoptan un enfoque multicapa. Es decir, las tecnologías para la prevención, la detección y la respuesta a ciberincidentes deben combinarse para garantizar una mejor defensa ante un posible ciberataque.

Otras posibilidades se abren en el campo de la tecnología cuántica de la información o los seguros que garanticen la ciberseguridad. Los datos y la información se han convertido en uno de los activos más importantes de una organización. Es por ello que la contratación de seguros que protejan contra los riesgos de ciberataques se convertirá en una realidad cada vez más extendida en el mundo empresarial y gubernamental.

Las oportunidades son múltiples y evolucionan cada día. El gobierno y la industria australiana son conscientes de ello y se están esforzando por subirse a la ola de oportunidades que supone el sector de la ciberseguridad. España presenta una cantera de empresas innovadoras, que desarrollan soluciones y tecnologías únicas y que están abiertas a la colaboración. Definitivamente, nuestro tejido empresarial tiene el potencial para acceder al mercado australiano. ¿Por qué no capitalizar en esa ola de oportunidades? ¿Qué mejor lugar que Australia para hacer surf?