ICEX España Exportación e Inversiones

FS FICHA SECTOR

PAÍSES BAJOS

Ciberseguridad en Países Bajos

A. CIFRAS CLAVE

Países Bajos es uno de los países con mayor nivel de conectividad del mundo, y punto de acceso a Europa. Cuenta con una infraestructura de comunicaciones muy avanzada, que ha generado una creciente dependencia en los principales sectores económicos y vías de desarrollo del país, haciendo de la ciberseguridad una materia prioritaria en la agenda del Gobierno.

Cabe destacar el alto grado de apertura comercial de Países Bajos, así como su liderazgo en conectividad, su elevado gasto en I+D, y su tejido empresarial altamente terciarizado, con presencia mayoritaria de pymes. El 98 % de la población tiene acceso de banda ancha a Internet, la tasa más elevada de todo el continente europeo. Pese a su pequeño tamaño, el país tiene una elevada densidad demográfica, un clima óptimo para el emprendimiento y un régimen fiscal muy favorable a las empresas internacionales.

Hogares neerlandeses con acceso a Internet, 2019 (%)	**98 %**
Clasificación de Países Bajos en el Global Cybersecurity Index (GCI) 2018	**12/175**
Exportaciones de bienes tecnológicos (en % s/ bienes manufacturados, 2019)	**55,87 %**
Importaciones de bienes tecnológicos (en % s/ bienes manufacturados, 2019)	**15,31 %**
Altas de contratos de telefonía (por cada 100 personas, 2019)	**121**

Servidores de Internet seguros, 2019	**1.733.183**
Servidores de Internet seguros por cada millón de habitantes, 2019	**100.585 (10,06 %)**
Usuarios con acceso a Internet, 2019 (% de la población total)	**98 %**
Usuarios que realizan compras a través de Internet (% sobre población total)	**70 %**
Usuarios de Internet (enero 2020)	**16,2 millones**
Gasto local en I+D en % PIB, 2018	**2,11 % (16,7 M EUR)**

Fuente: Banco Mundial, Eurostat, UNESCO, Trading Economics, Unión Internacional de Telecomunicaciones (UIT).

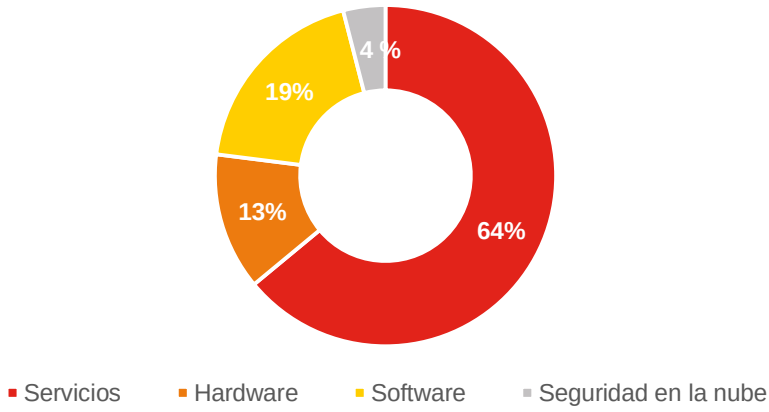
B. CARACTERÍSTICAS DEL MERCADO

B.1. Definición precisa de las actividades / productos del sector estudiado

El sector de la ciberseguridad comprende el conjunto de medidas de seguridad susceptibles de ser implementadas para defenderse de los ciberataques. Así, el sector incluye la legislación, políticas, herramientas, tecnologías y acciones que pueden ser utilizadas para proteger los activos informáticos de las administraciones, empresas y particulares de un país.

De manera más concreta, el sector de la ciberseguridad puede dividirse en **servicios**, ***software***, ***hardware*** y ***cloud security***. El peso de los **servicios** de ciberseguridad en el mundo alcanza prácticamente las dos terceras partes de la industria (IDC, 2018).

EL MERCADO MUNDIAL DE LA CIBERSEGURIDAD
Por tipo de prestación, en porcentaje



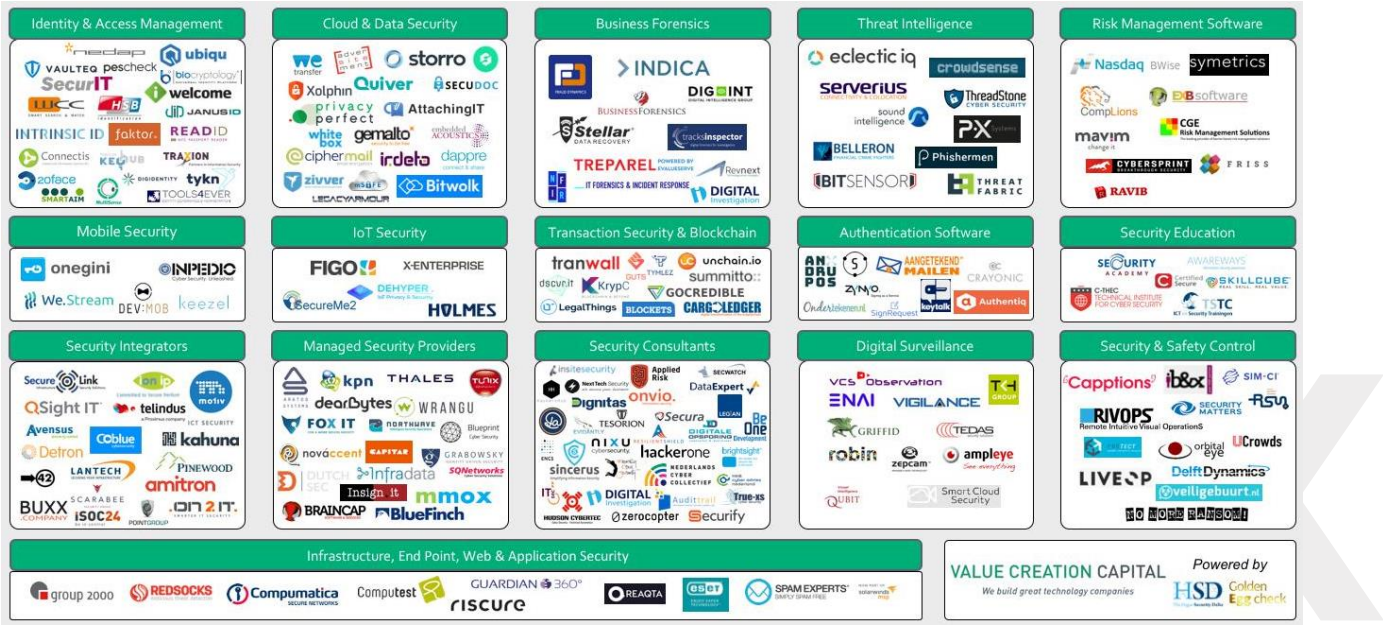
Fuente: IDC, 2018.

Para categorizar el sector en este mercado seguiremos la clasificación de The Hague Security Delta (HSD). En esta clasificación hallaremos un fuerte vínculo entre las áreas de investigación actuales y la aparición de nuevos negocios y aplicaciones futuras.

- Identity & Access Management
- Cloud & Data Security
- Business Forensics
- Threat Intelligence
- Risk Management Software
- Mobile Security

- IoT Security
- Transaction Security & Blockchain
- Authentication Software
- Security Education
- Security Integrators
- Managed Security Providers
- Security Consultants
- Digital Surveillance
- Security & Safety Control
- Infrastructure, End Point, Web & Application Security

EL MERCADO NEERLANDÉS DE LA CIBERSEGURIDAD



Fuente: HSD, junio de 2018.

B.2. Tamaño del mercado

El mercado de la ciberseguridad en Países Bajos está **creciendo a un ritmo anual de alrededor del 14,5 %**. De las 66.000 compañías de TI del país, 3.600 desarrollan actividades en el sector de la ciberseguridad, y más de 2.500 venden productos y servicios de seguridad. El 60 % de todas las empresas del listado Forbes 2000[1] activas en TI tienen operaciones en Países Bajos, incluyendo a los principales actores privados del sector como IBM, Microsoft, Google, Huawei, Oracle o HP.

Países Bajos alberga el mayor clúster especializado en ciberseguridad de toda Europa, el llamado **The Hague Security Delta (HSD)**[2], situado en la ciudad de La Haya, y en el cual operan más de 400 empresas del sector. También en La Haya es donde se encuentra la sede del Gobierno, además del Centro Europeo de Ciberdelincuencia de la UE, la Red Europea de Ciberseguridad, la Agencia de Ciberseguridad de la OTAN, Europol y la Academia de Ciberseguridad. Todas estas entidades han hecho de la región un epicentro para el sector a nivel europeo y mundial. Además de La Haya, existen otras regiones del país especializadas en campos complementarios, como es el caso de Delft, la ciudad universitaria del país por excelencia, Eindhoven, nombrada ciudad más innovadora del mundo por la revista Forbes (2013) o Ámsterdam. Esta última es uno de los principales núcleos de entrada para las empresas de Silicon Valley, lugar de referencia tecnológico a nivel mundial.

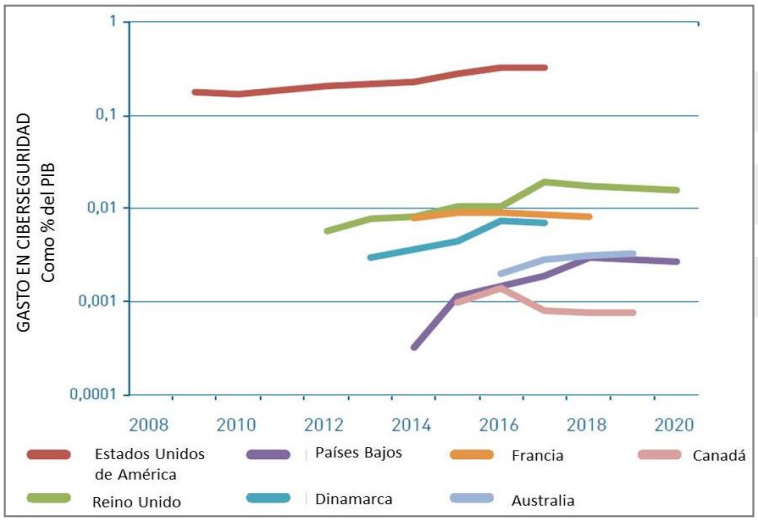
[1] Listado Forbes 2000
[2] The Hague Security Delta

Según INCIBE[3], Países Bajos se sitúa entre los países que mejor aprovechan las oportunidades ofrecidas por las nuevas tecnologías para mejorar el bienestar y el desarrollo. En relación con la disponibilidad de red, Países Bajos cuenta con una puntuación de 5,8 sobre 7 puntos, alcanzando la mayor puntuación en el subíndice de uso individual, que mide la penetración y difusión de las TIC a nivel individual. Además, el **saldo comercial respecto a los productos TIC en Países Bajos es negativo**, dado que las importaciones superan a las exportaciones de productos TIC en un 2,1 %. Sin embargo, las exportaciones de servicios TIC suponen un 34,3 % sobre el total de las exportaciones de servicios; siendo el peso de los servicios TIC en el PIB de un 5 %.

El país cuenta con una gran cantidad de expertos especializados en campos TI, gracias a sus numerosas universidades de ciencias aplicadas. En el curso 2018/2019, hubo más de 105.000 estudiantes matriculados en ciberseguridad. Además, gracias al sistema de "triple hélice", estos profesionales se integran laboralmente en empresas locales que colaboran con las universidades y centros de investigación, con el Gobierno estrechamente apoyando la innovación.

Según datos de SEO Amsterdam Economics, el tamaño del sector de la ciberseguridad es de aproximadamente el **10 % de la facturación del sector de las TIC**. Dicho esto, es difícil medir con precisión este valor para la economía en su conjunto.

GASTO PÚBLICO EN CIBERSEGURIDAD POR PAÍSES



Fuente: The Hague Centre for Strategic Studies.

El comercio electrónico, cuyo pilar fundamental es la seguridad en los pagos y la privacidad de los usuarios, supuso un valor de **23.700 millones de euros en 2018**. El crecimiento fue de un 10 % respecto a 2017, representando las ventas *online* un 9,6 % de la industria minorista total. El 79 % de la población entre los 16 y los 74 años compró *online* en 2018 (CBS 2019). Esto supone un crecimiento proporcional de las tecnologías que propician entornos de compra seguros y entornos de almacenamiento de datos personales de los clientes seguros.

Según Security Boulevard, a principios de diciembre de 2019, los registros por robo de datos alcanzaron los 4.100 millones en el mundo. Según IBM y el Ponemon Institut, las infracciones de datos cuestan a las compañías encuestadas en el informe 150 dólares por registro. El coste de una infracción de datos ha aumentado un 12 % en los últimos 5 años, y ahora cuesta en promedio 3,92 millones de dólares. En Países Bajos, según la Asociación Neerlandesa de Protección de Datos[4], en 2018 hubo 20.881 registros de robo de datos, siendo superior la cifra contando los no reportados.

[3] Ficha internacionalización INCIBE Países Bajos
[4] Dutch DPA

B.3. Principales actores

Dentro del mercado neerlandés de ciberseguridad, podemos distinguir algunos de los principales organismos, entidades y empresas que lideran el crecimiento y desarrollo del sector en representación de sus respectivos segmentos.

B.3.1. Sector público

Según el Centro Nacional de Ciberseguridad neerlandés, el Gobierno tiene marcados, en materia de ciberseguridad, cuatro objetivos fundamentales:

1. **Seguridad**: contrarrestar el cibercrimen y el ciberespionaje, así como prevenir la perturbación social causada por incidentes.
2. **Privacidad *online***: manejar cuidadosa, transparente y legalmente cualquier información proporcionada en línea por los ciudadanos.
3. **Promoción** de la ciberseguridad.
4. **Control**: determinar regulaciones y estándares.

Estos objetivos se llevan a cabo mediante una serie de estrategias, diseñadas en conjunto entre el Gobierno y los actores privados y centros de desarrollo e investigación. El HSD sirve como punto de encuentro para todos ellos, así como de referencia para el resto del sector.

- **The Hague Security Delta**

  Se trata del máximo exponente del sector en este mercado. Está formado por una red de empresas, gobiernos e instituciones de conocimiento que trabajan juntas en soluciones innovadoras de seguridad y desarrollo de conocimiento. En esta red se discuten cuestiones de seguridad y se comparten conocimientos sobre ciberseguridad, seguridad nacional y urbana y protección de infraestructuras críticas. Funciona mediante socios, y su núcleo es el Campus HSD, el centro nacional de innovación para la seguridad situado en La Haya.

  HSD facilita, organiza e inicia el acceso al conocimiento, la innovación, el mercado, el talento y el capital. Los socios[5] de HSD reciben apoyo en materias desde financiación hasta marcos regulatorios y la búsqueda de socios de innovación. Trabaja en estrecha colaboración con socios estratégicos, como Innovation Quarter[6], RVO[7], la Cámara de Comercio neerlandesa[8], NFIA[9] o el Ayuntamiento de La Haya. Forman una red fuerte que ha sido esencial para el crecimiento del clúster.

  De esta manera, HSD aúna en una sola voz a los distintos organismos públicos y privados del sector, centrando el foco de todos ellos en una misma estrategia nacional, y coordinando las acciones hacia la consecución de los objetivos estipulados en la Agenda Nacional de Ciberseguridad (NCSA)[10].

- **Digital Trust Centre**

  De origen público, el DTC[11] tiene la misión de mejorar el intercambio de información y fortalecer la ciberseguridad en sectores y empresas no vitales. El objetivo es crear un ecosistema que proporcione información y perspectivas personalizadas para la acción, principalmente para pequeñas y medianas empresas con menos recursos. Además, ha creado una red nacional de asociaciones de ciberseguridad para compartir información entre las

[5] Listado de socios HSD
[6] Innovation Quarter
[7] Netherlands Enterprise Agency, RVO
[8] Cámara de Comercio neerlandesa
[9] Netherlands Foreign Investment Agency, NFIA
[10] NCSA
[11] Digital Trust Center

partes públicas y privadas de manera más amplia, eficiente y efectiva, al igual que hace HSD. Otras prácticas incluyen la divulgación coordinada de vulnerabilidades y mejoras continuas de las agencias de intercambio de información.

- **ECP**

  Plataforma independiente donde el Gobierno, la comunidad empresarial y las instituciones sociales se unen para intercambiar conocimientos y cooperar para explotar las oportunidades que brinda la sociedad de la información y mitigar las amenazas que surgen en el ecosistema digital. Actúa como portavoz neutral en temas que son importantes para el desarrollo de la sociedad de la información y donde existe la necesidad de un desarrollo público-privado.

B.3.2. Sector privado

Aunque la mayoría de los principales actores del sector privado son socios de HSD y siguen sus líneas de actuación, cabe destacar algunos de los más importantes por su peso en el mercado y su colaboración al desarrollo de este:

- Bzb Europe
- Infradata
- KMC Solutions
- Provolve IT
- ThreadStone Cyber Security
- YaWorks
- Kpn
- WeTransfer
- Quiver
- Janus ID
- Onegini
- Thales
- Cisco

C. LA OFERTA ESPAÑOLA

La oferta española en el mercado se ve determinada por una serie de factores tales como la percepción del producto español en el mismo o el posicionamiento de sus empresas de cara al mercado. Debido al llamado efecto halo (Han, 1989) la imagen país se ve influida por las percepciones del mismo, lo cual afecta de forma directa a la valoración de sus productos en otros países. La relación suele ser proporcional, aumentando el éxito comercial de dichos productos cuanto mejor es la reputación del país emisor. En el caso de Países Bajos, la percepción de la marca española no tiene una connotación negativa, aunque tampoco goza de gran prestigio, principalmente en sectores tecnológicos e industriales, como también le ocurre en el resto de países del mundo. Como consecuencia, resaltar el *made in Spain* no es sinónimo de éxito y no aporta una ventaja competitiva clara a los productos españoles en el mercado neerlandés.

España se sitúa en el puesto 11.º del informe *Nation Brand Report 2019* (Brand Finance, 2019) en lo tocante a valor y percepción de marca. La marca neerlandesa se sitúa en el puesto 13.º, por detrás de la española, aunque su *rating* es mejor (AAA) frente al español (AA) a nivel global.

En materia de ciberseguridad, uno de los medidores de referencia en el sector es el Global Cybersecurity Index, de la Unión Internacional de Telecomunicaciones (UIT). El GCI mide el compromiso de los países en materia de ciberseguridad. España ocupa el séptimo puesto, mientras que Países Bajos ocupa el 12.º Este hecho es significativo y favorece la imagen de las empresas españolas en el mercado, que son percibidas como iguales por los consumidores locales, dado que ambas lideran el *ranking* global en términos de compromiso y ecosistemas propicios a la innovación y el desarrollo del sector.

Otro valor que sirve como referente acerca de la concienciación de un país en la materia es el grado de protección de su tejido empresarial. En este caso, según ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, el *rating* de seguridad de las empresas españolas está por debajo de la media del resto de países europeos, por lo que el compromiso del sector privado no está alineado con el de las instituciones del país.

De todo esto, cabe destacar la falta de claridad y datos sólidos para determinar una percepción clara de la oferta española en el mercado.

D. OPORTUNIDADES DEL MERCADO

Las tendencias en los últimos años en el mercado internacional de TI apuntan a campos en crecimiento constante como el *Cloud Computing* y los servicios de *Software as a Service* (SaaS). Mientras que las partidas que más gasto han supuesto a las empresas en el campo de las TI están relacionadas con servicios de comunicaciones, esta tendencia se ha estancado y ya no crece significativamente. Los servicios de comunicaciones presentan un escenario más estático en lo tocante a participantes en el mercado, con grandes compañías internacionales repartiéndose de forma casi oligopolística la cuota total del mercado.

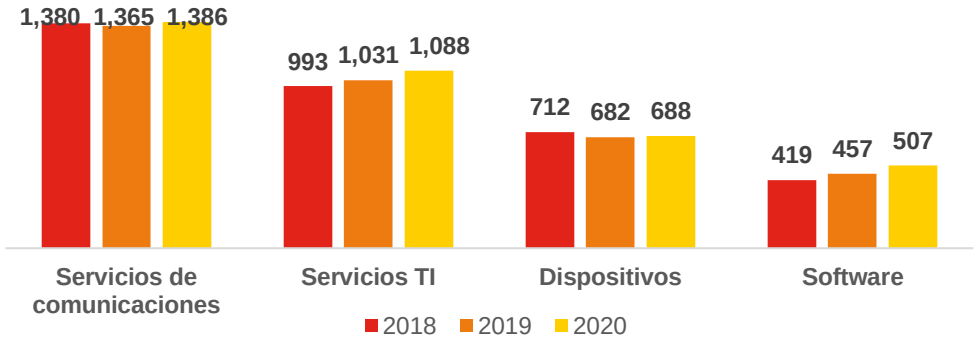
GASTO MUNDIAL EN TI
(en miles de millones de dólares)

	Gasto 2018	Crecimiento 2018 (%)	Gasto 2019	Crecimiento 2019 (%)	Gasto 2020	Crecimiento 2020 (%)
Sistemas de Centros de Datos	210	15,7	203	-3,5	208	2,8
Software	419	13,5	457	9,0	507	10,9
Dispositivos	712	5,9	682	-4,3	688	0,8
Servicios TI	993	6,7	1.031	3,8	1.088	5,5
Servicios de comunicaciones	1.380	-0,1	1.365	-1,0	1.386	1,5
Total	3.716	5,1	3.740	0,6	3.878	3,7

Fuente: Gartner (julio de 2019)[12].

De entre las principales partidas de gasto en el sector TI, cobra cada vez mayor importancia el *software*, que crece de forma regular en los últimos años y aún presenta múltiples vías de innovación y desarrollo de nuevos productos para cubrir necesidades en el mercado. Del mismo modo ocurre con los servicios de TI, entre los cuales se encuentran la implementación de soluciones de *software* o los sistemas de gestión de almacenamiento en la nube. La demanda de estos servicios TI presenta una tendencia que sigue siendo alcista, aunque más irregular en estos últimos años. Sin embargo, se trata de un mercado más extenso y cuya oferta está cada vez menos atomizada, siendo grandes empresas (véase Amazon Web Services, Google o Apple) las que lideran cierto tipo de servicios más demandados como el almacenamiento en la nube, mediante la adquisición de pequeñas empresas que ofrecen tecnologías innovadoras, que integran en su cartera de productos.

TENDENCIAS Y EVOLUCIÓN DEL GASTO EN IT
Por año y categorías principales, en miles de millones de dólares

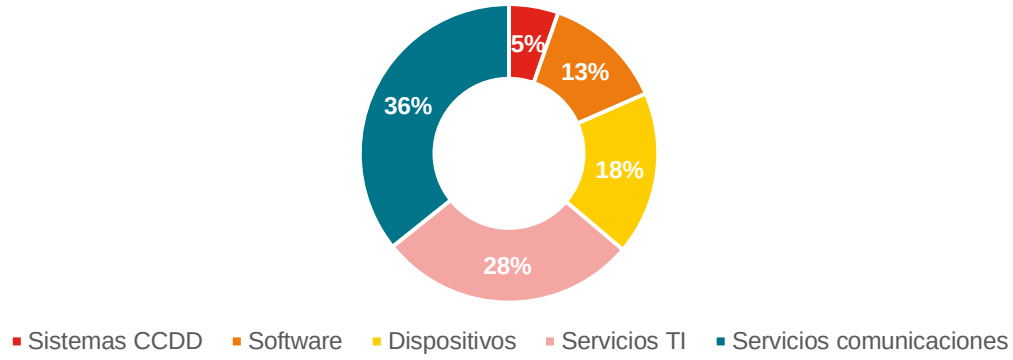


Fuente: elaboración propia a partir de Gartner (julio de 2019).

[12] Gasto Mundial TI (Gartner, 2019)

El *hardware* y los dispositivos siguen siendo una de las mayores partidas de facturación dentro del sector TI, y aunque el nivel de facturación se mantiene estable, es complicado para las empresas obtener el tamaño requerido para competir en este sector, como ocurre en otras partidas.

COMPOSICIÓN DEL GASTO EN TI EN 2020
Por categoría



Fuente: elaboración propia a partir de Gartner (julio de 2019).

Considerando estas tendencias internacionales, las empresas ofertantes de productos relacionados con la ciberseguridad tendrán más facilidad de acceso a los mercados internacionales si se adaptan a ellas y buscan formas de proteger las transacciones de datos o su accesibilidad dentro de estos nuevos sistemas. En el caso de Países Bajos, cabría destacar que existen una serie de infraestructuras críticas o IC, designadas por el Gobierno como tales, y cuya protección es una materia prioritaria. De esta manera, aquellos productos y servicios capaces de asimilar las tendencias del mercado y orientarlas a la aplicación en la protección de dichas infraestructuras tendrán una mayor probabilidad de éxito en el mercado neerlandés.

INFRAESTRUCTURAS CRÍTICAS EN PAÍSES BAJOS, POR CATEGORÍAS

CATEGORÍA A	CATEGORÍA B
• Transporte y distribución nacional de la electricidad • Producción de gas natural • Suministro de petróleo • Almacenamiento, producción o procesamiento de materiales nucleares • Suministro de agua potable • Gestión del agua	• Distribución regional de electricidad y gas • Gestión de vuelos y aviones • Almacenamiento, producción o procesamiento a gran escala de fuentes petroquímicas • Sector financiero (servicios bancarios, transferencias electrónicas entre bancos/usuarios) • Comunicación con y entre servicios de emergencia • Movilización policial • Servicios públicos que dependen de unos sistemas de información fiables y disponibles

Fuente: The Hague Security Delta.

La categoría A se define como aquellas IC cuyo límite se encuentra en uno de estos cuatro impactos: impacto económico (daño o caída del PIB), impacto físico (accidentes, daños), impacto social (subsistencia o problemas emocionales) o efecto dominó. La categoría B incluye umbrales más bajos respecto a los criterios anteriores.

Cabe destacar que, a pesar de los esfuerzos del Gobierno por proteger estás infraestructuras críticas, sigue habiendo un claro margen de mejora dada la continua evolución del mercado. Las innovaciones tecnológicas hacen que las vulnerabilidades sean cambiantes y las medidas contingentes deban estar en constante adaptación. Un ejemplo claro de la vulnerabilidad de las infraestructuras es el caso del ciberataque sufrido por la terminal de la naviera APM en el Puerto de Rotterdam en el año 2017. A pesar de que la infraestructura estaba bien protegida y cumplía con los estándares de protección sobradamente, sufrió un ataque del cual tardó semanas en reponerse, con unos costes que se estiman en cientos de millones de euros. Por ello, la tecnología más vanguardista en términos de ciberseguridad tendrá mayores oportunidades para entrar en un mercado de estas características.

E. CLAVES DE ACCESO AL MERCADO

E.1. Distribución

Los canales de distribución tienen la peculiaridad de estar bien interconectados entre sí, lo que ocurre no sólo a nivel local sino también a escala global. La cooperación y búsqueda de sinergias con socios locales podría ser la forma de entrada más conveniente y puede, a su vez, ofrecer diversas oportunidades a largo plazo.

Los principales canales de distribución de productos de ciberseguridad son los siguientes:

- **Canal directo:** Este tipo de canal no tiene ningún intermediario y, por tanto, el productor o desarrollador desempeña la mayoría de las funciones logísticas tales como la comercialización, envío, almacenaje de producto, cobros y aceptación de riesgos. No es la forma más recomendada de entrada salvo que se trate de una empresa muy grande.

- **Canal indirecto:** De forma indirecta, se podría entrar al mercado bien a través de un distribuidor, bien a través de una transferencia de tecnología o bien a través de alianzas estratégicas. Para el mercado neerlandés, esta última se considera una buena opción, ya que permite establecerse con líderes del mercado a los que se ofrece un valor añadido.

  Como empresas mayoristas y distribuidoras neerlandesas cabe mencionar a **ERPScan** y **Eclectic IQ**, y como empresa líder en desarrollo de *software* y fabricación de *hardware* a **AVG Technologies**, cuya central se encuentra en Ámsterdam.

- **Acceso en grupo:** En caso de que se descarte la opción de entrar como un consorcio de exportación, la opción más viable de entrada en Países Bajos es a través de un clúster de empresas. Países Bajos cuenta con numerosos clústeres industriales que servirían como punto de acceso al tejido empresarial del país. Destaca el ya mencionado **Hague Security Delta**.

E.2. Barreras reglamentarias y no reglamentarias

El nuevo reglamento europeo de ciberseguridad, aprobado por el Consejo Europeo en marzo de 2019, consolida una agencia permanente de ciberseguridad y una certificación común para toda la Unión Europea. Los expertos señalaron este hito como una oportunidad para que España lidere las buenas prácticas en el continente, ya que el ecosistema de certificación español se encuentra entre los mejor valorados de Europa.

El Código Penal neerlandés fue modificado en 2015 para albergar nuevas provisiones en referencia a la lucha contra el cibercrimen, como la implementación de la Directiva de la Unión Europea 2013/40/UE sobre ciberataques[13], sustituyendo a la Decisión Marco 2005/222/JBZ del Consejo Europeo.

En cuanto a los requisitos establecidos por las leyes o políticas, no es necesaria la presentación de un plan de seguridad de la información, sino que está cubierta mayoritariamente por la Decisión del Gobierno sobre Seguridad de la Información Especial de 2013, así como las directrices publicadas por el Centro Nacional e Ciberseguridad. Esta norma requiere la confidencialidad de la información importante relativa al Estado, sus ministerios o aliados. En el artículo 2 se detallan cuatro niveles, según el riesgo de divulgación de información reservada. Además, los

[13] Directiva de la UE 2013/40/UE sobre ciberataques

sistemas de información deben someterse a auditorías de ciberseguridad, aunque no se establece una periodicidad determinada.

Con respecto a la nueva Ley General de Protección de Datos que entró en vigor en enero de 2016, es de obligada notificación la fuga de datos (*Wet meldplicht datalekken*) por parte de los auditores a la autoridad neerlandesa de protección de datos (DPA). Tanto la falta de seguridad como la elusión de las medidas adecuadas son clasificadas como infracción. La mencionada autoridad tiene la potestad de imponer sanciones que pueden alcanzar los 810.000 euros en caso de incumplimiento. Se contemplan además obligaciones especiales de notificación para determinados sectores como el financiero y el de telecomunicaciones, agua y energía y transporte (puerto de Rotterdam, aeropuerto de Schiphol, o control de tráfico aéreo).

Se valorará muy positivamente la encriptación de los datos en el caso de aplicaciones que manejen información de usuarios o clientes. A pesar de que el uso de encriptación puede complicar el trabajo de las agencias de inteligencia y la aplicación penal, el Gobierno ha decidido no imponer medidas restrictivas por ley, dado que se trata de una salvaguarda frente al espionaje y múltiples formas de crimen en la red.

E.3. Ayudas

- Ayudas en España para la internacionalización:

- **ICEX**[14] a través de sus programas de ayuda a la internacionalización.
- Las **Cámaras de Comercio** a través del Plan Cameral de Exportaciones.
- **Instituto de Crédito Oficial** (**ICO**), mediante sus líneas de crédito a la exportación.
- **CDTI.**

- Ayudas en Países Bajos:

  - **Invest In Holland**[15] es la agencia de atracción de inversión extranjera a Países Bajos. Realiza labores similares a las de ICEX Invest In Spain.
  - **HSD** a través de su programa de socios y captación de fondos y capital.

- Ayudas europeas:

  - **Banco Europeo de Inversiones** (**BEI**) financia proyectos de empresas europeas relacionados con los objetivos de crecimiento y desarrollo marcados por la UE. La ciberseguridad es uno de sus objetivos y actualmente el BEI financia proyectos como el de la empresa CS en Francia, a la cual ha financiado con 20 millones de euros.
  - **Comisión Europea** a través de **ENISA**, Agencia de Ciberseguridad de la UE.

E.4. Ferias

- **One Conference 2020**

La Haya, 29-30 de septiembre de 2020.
Promovida por el Ministerio de Asuntos Económicos y Política Climática, el Centro Nacional de Seguridad Cibernética (NCSC-NL) del Ministerio de Justicia y Seguridad y el Ayuntamiento de La Haya, cuenta con la participación tanto del sector público y privado como de representantes del mundo académico, con oportunidades

[14] Programas ICEX
[15] Invest In Holland (https://investinholland.com/)

para establecer contactos nacionales e internacionales. Tiene como objetivo facilitar el intercambio de conocimientos e ideas dentro de la comunidad internacional de ciberseguridad.
https://one-conference.nl/

- **Infosecurity Netherlands**

Utrecht, 28-29 de octubre de 2020.
Lugar de encuentro para profesionales y directores en el área de las TIC, la edición de 2019 registró más de 20 expositores y 1.000 visitantes.
https://www.infosecurity.nl/

- **Digital Experience 2020 (NL)**

Utrecht, 7-8 de octubre de 2020.
Feria anual sobre la lucha contra el fraude y la ciberdelincuencia organizada por DataExpert. Consta de diversas sesiones de transmisión de conocimiento y sobre productos, capacitación y servicios, últimas tendencias y tecnologías.
https://www.dataexpert.nl/en/events/digital-experience-2020/

- **Webwinkel Vakdagen**

Utrecht, 27-28 de enero de 2021
Con 13.643 visitantes en su última edición, es la feria más grande del Benelux sobre comercio electrónico. Además, tiene una sección dedicada exclusivamente a la ciberseguridad aplicada al comercio electrónico.
https://www.webwinkelvakdagen.nl/en

F. INFORMACIÓN ADICIONAL

Organismo	Web y contacto	Rol en materia de ciberseguridad
Cyber Security Council	https://www.cybersecurityraad.nl/index-english.aspx	Punto de enlace entre los sectores público y privado, así como los centros de investigación, formado por 15 miembros.
National Cyber Security Centre (NCSC)	www.ncsc.nl/ Turfmarkt 147 2511 DP The Hague The Netherlands Tel: +31 70 751 55 55 info@ncsc.nl	Integrado en el NCTV del Ministerio de Seguridad y Justicia, el NCSC se encarga de la operativa de los CERT para el Gobierno central en caso de emergencia y de promover el conocimiento y la experiencia en ciberseguridad para el conjunto de la sociedad neerlandesa. Realiza la definición de la estrategia nacional.
National Coordinator for Security and Counterterrorism (NCTV)	https://english.nctv.nl/ P.O. Box 16950 2500 BZ The Hague Tel: + 31 70 751 50 50 info@cyberstability.org	Protege al país contra amenazas que puedan alterar la sociedad. Garantiza la seguridad de las infraestructuras críticas neerlandesas conjuntamente con sus socios en el Gobierno, la comunidad científica y el sector empresarial.
The Hague Security Delta (HSD)	https://www.thehaguesecuritydelta.com/ Tel: +31 70 204 51 80 info@thehaguesecuritydelta.com	Mayor clúster en materia de ciberseguridad de Europa, donde colaboran empresas, gobiernos e instituciones de investigación.

G. CONTACTO

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

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

Burgemeester Patijnlaan 67
2585 BJ La Haya, Países Bajos
Teléfono: (+31 70) 364.31.66
Email: lahaya@comercio.mineco.es
http://Países bajos.oficinascomerciales.es

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

Ventana Global
913 497 100 (L-J 9 a 17 h; V 9 a 15 h)
informacion@icex.es

Para buscar más información sobre mercados exteriores siga el enlace

AUTOR
Miguel Herrera García

Oficina Económica y Comercial
de España en La Haya
lahaya@comercio.mineco.es
Fecha: 28/02/2020

NIPO: 114-20-022-X

www.icex.es

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO · ICEX España Exportación e Inversiones