OD OTROS DOCUMENTOS

2022

ICEX España Exportación e Inversiones

Ciberseguridad en Países Bajos

Oficina Económica y Comercial
de la Embajada de España en La Haya

OD OTROS DOCUMENTOS

3 de noviembre de 2022
La Haya

Este estudio ha sido realizado por
Jon Pinies Echeguren

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en La Haya

http://PaisesBajos.oficinascomerciales.es

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

NIPO: 114-22-015-3

Índice

1. Introducción

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 99 % de los hogares 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.

Indicadores del sector de la ciberseguridad en Países Bajos	
Hogares con acceso a Internet en 2021	99 %
Clasificación en el Global Cybersecurity Index (GCI) 2020	16
Exportaciones de bienes TIC (en % s/ bienes manufacturados, 2020)	11,2 %
Importaciones de bienes TIC (en % s/ bienes manufacturados, 2020)	15 %
Altas de contratos de telefonía (por cada 100 personas, 2020)	125
Contratos de telefonía (suscripciones + SIM de prepago) en T1 2022	23,93 millones
Servidores de Internet seguros, 2020	2.387.096
Servidores de Internet seguros por cada millón de habitantes, 2020	136.863
Usuarios que compran a través de Internet (% s/ población total) 2021	80 %
Usuarios de Internet en 2022	16,5 millones
Gasto local en I+D en % PIB, 2020	2,29 % (18.400 MEUR)

Fuente: elaboración propia a partir de datos de Eurostat, ITU, Kepios, ACM, Banco Mundial, ecommerceDB, CBS

2. Características del mercado

2.1. Definición precisa del sector estudiado

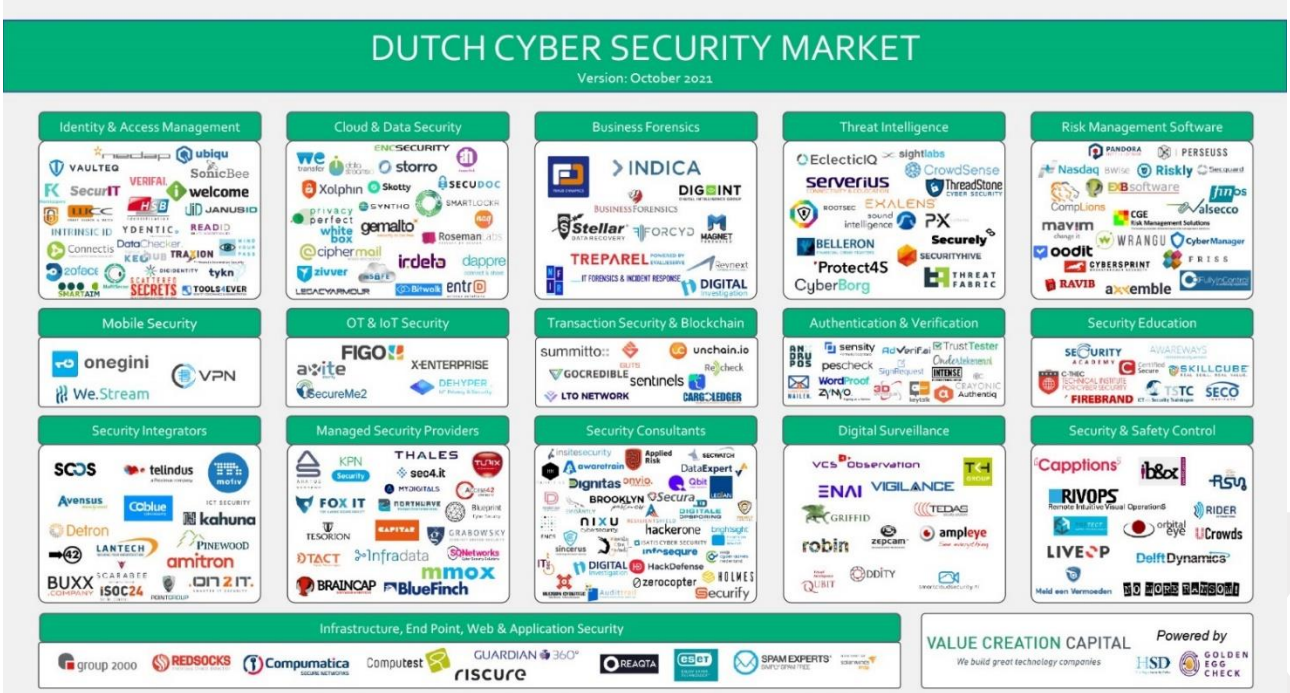
El sector de la ciberseguridad comprende el conjunto de medidas de seguridad susceptibles de ser implementadas para defenderse de los ciberataques. Así, el sector incluye la legislación, políticas, herramientas, tecnologías y acciones que pueden ser utilizadas para proteger los activos informáticos de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

En cuanto a componentes del mercado, el sector de la ciberseguridad puede dividirse en servicios, *software* y *hardware*. Todos los segmentos se encuentran en crecimiento, especialmente los servicios, que abarcan casi dos terceras partes de la industria, y el *software*.

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*
- *Authentication & Verification*
- *Cloud & Data Security*
- *Security Education*
- *Business Forensics*
- *Security Integrators*
- *Threat Intelligence*
- *Managed Security Providers*
- *Risk Management Software*
- *Security Consultants*
- *Mobile Security*
- *Digital Surveillance*
- *OT & IoT Security*
- *Security & Safety Control*
- *Transaction Security & Blockchain*
- *Infrastructure, End Point, Web & Application Security*

EL MERCADO NEERLANDÉS DE LA CIBERSEGURIDAD



Fuente: Value Creation Capital. Octubre de 2021.

2.2. Tamaño del mercado

El mercado TIC neerlandés tiene un volumen de 24.000 MEUR, de los cuales un 10 % corresponden al segmento de la seguridad. El mercado de la ciberseguridad[1] en Países Bajos está creciendo a un ritmo anual de alrededor del 14,5 %. Este elevado crecimiento se explica a través de la dependencia de la economía nacional de la industria tecnológica, y es que los daños anuales en el sector son de 10.000 MEUR[2].

Para apoyar este crecimiento, Países Bajos cuenta con una infraestructura de vanguardia que incluye el Amsterdam Internet Exchange (AMS-IX). AMS-IX es uno de los mayores distribuidores de datos digitales del mundo, lo que contribuye a reforzar la imagen del país como puerta digital de Europa[3].

[1] https://ncsi.ega.ee/country/nl/
[2] Innovation Quarter. *10 reasons why West Holland is the Hotspot for Cyber Security*.
[3] Invest in Holland

La llamada *Triple Helix* que une a empresas privadas, instituciones públicas y universidades permite compartir el conocimiento entre los distintos actores del mercado y avanzar en el desarrollo de soluciones.

Países Bajos alberga el mayor clúster especializado en ciberseguridad de toda Europa, el llamado The Hague Security Delta (HSD), situado en la ciudad de La Haya, y en el cual operan más de 275 empresas del sector privado y público, entre ellas Cisco y Booz Allen Hamilton. La propia organización cataloga Países Bajos como un mercado lo suficientemente grande como para marcar la diferencia, pero lo suficientemente pequeña como para no suponer una amenaza.

También en La Haya es donde se encuentra la sede del Gobierno, además del Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Agencia de Comunicaciones e Información (NCI) de la OTAN, el Foro Global de Ciberexperiencia (GFCE) y el Centro Nacional de Ciberseguridad neerlandés (NCSC). 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, con su universidad politécnica TU/Delft considerada la ciudad universitaria del país por excelencia; Eindhoven, con la universidad politécnica TU/e y 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.

En cuanto a las instituciones del conocimiento, la Universidad de Delft, la Universidad Tecnológica de Eindhoven, la Universidad de Leiden y la Universidad de Twente (UT) son centros punteros que abren nuevos caminos en cuanto a las aplicaciones de seguridad digital. El centro de investigación aplicada TNO, en La Haya, también tiene un fuerte enfoque cibernético.

Atraídos, entre otras razones, por el ecosistema del país, Google y Microsoft ya tienen sede en Países Bajos. De hecho, más de la mitad de las empresas de la lista *Fortune 500* realizan actividades informáticas en el territorio. Por ejemplo, la empresa de ciberdefensa Booz Allen Hamilton protege a las empresas de la lista *Fortune 100* y Thales defiende a los buques de guerra de las amenazas aéreas en su sede de Twente.

El gran desarrollo de estas tecnologías en Países Bajos hace que la demanda de productos/servicios que ofrezcan seguridad en su uso sea elevada. Doce de los catorce cables de Internet transatlánticos que conectan Estados Unidos y Europa pasan por Países Bajos. Además, la penetración y uso de Internet es de los más elevados en Europa.

El comercio electrónico, cuyo pilar fundamental es la seguridad en los pagos y la privacidad de los usuarios, supuso un valor de 30.600 MEUR en 2021[4]. El crecimiento fue de un 15 % respecto a

[4] Statista

2020, representando las ventas *online* un 12,5 % de la industria minorista total. El 86,7 % de la población neerlandesa compró *online* en 2021[5]. 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.

En una encuesta realizada por Deloitte, organizaciones neerlandesas fueron preguntadas por aspectos relacionados con la ciberseguridad. La mayor preocupación de las empresas en el país es proteger los activos vitales de la compañía. De hecho, cuando la ciberseguridad empezó a ganar importancia, las empresas del sector financiero, entre otros, acordaron no competir en esta materia para compartir información y así verse beneficiadas todas.

Las empresas financieras (54 % de los encuestados al menos una vez por trimestre) son las que abordan la ciberseguridad en sus juntas con una mayor frecuencia. Cuanto mayor es el tamaño de la organización, mayor dedicación a la ciberseguridad. Por el otro lado, las empresas públicas todavía no dedican tanto interés a esta cuestión (el 28 % ni si quiera es consciente de la frecuencia).

El 92 % de las empresas declaran poseer una estrategia de ciberseguridad. En cambio, en el sector público (43 %) no son conocedores de la cantidad de recursos que invierten en ciberseguridad. Los sectores de las ciencias de la vida y la salud, y la energía e industria son aquellos donde la inversión en ciberseguridad es mayor[6].

2.3. 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.

2.3.1. Sector público

El Gobierno presentó, en octubre de 2022, la ***Estrategia en ciberseguridad (NLCS) 2022-2028***. La estrategia incluye un plan de acción de medidas concretas para asegurar la seguridad digital de Países Bajos.

Para lograr este objetivo, se va a reforzar el sistema relativo a la seguridad digital. Para ello, el National Cybersecurity Centre, el Digital Trust Centre y el Cyber Security Incident Response Team for Digital Service Providers se fusionarán en una autoridad nacional de ciberseguridad. Además, se introducirán leyes y reglamentos claros para garantizar que se tomen más medidas en las

[5] CBS

[6] Deloitte. *Cyber security in the Netherlands: a responsibility we share*.

organizaciones. El objetivo es también obtener más información sobre las amenazas, para garantizar un aumento de la resiliencia[7].

El presupuesto anual del Gobierno, presentado en septiembre de 2022, dedicará 23 MEUR al National Cybersecurity Centre (NCSC), que asiste a empresas de los sectores denominados "infraestructuras críticas" (analizadas en profundidad en el capítulo 4. Oportunidades del mercado). Las empresas no críticas deben acudir al Digital Trust Centre (DTC) para ser atendidas[8].

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 el plan estratégico en ciberseguridad 2022-2028, diseñado 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[9] 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, RvO, la Cámara de Comercio neerlandesa, NFIA o el

[7] https://securitydelta.nl/nl/nieuws/overzicht/dutch-government-presents-cybersecurity-strategy-nlcs-2022-2028
[8] https://securitydelta.nl/nl/nieuws/overzicht/dutch-government-reserves-millions-for-cybersecurity
[9] The Hague Security Delta

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 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 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.

2.3.2. 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:

[10] https://english.ncsc.nl/topics/national-cybersecurity-agenda

- Bzb Europe
- Infradata
- KMC Solutions
- Provolve IT
- ThreadStone Cyber Security
- YaWorks
- Kpn
- FOX IT
- RedSocks
- PaloAlto
- WeTransfer
- Janus ID
- Onegini
- Thales
- Cisco
- Secure Link
- Group 2000
- Deloitte
- Darktrace

3. 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 de este, 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 los 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 12.º del informe *National Brands Report 2022*[11] en relación con el 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 cuarto puesto, mientras que Países Bajos ocupa el decimosexto[12]. 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. Ejemplo de presencia del sector de la ciberseguridad española en Países Bajos es el caso de **S2Grupo**. La empresa española proveedora de

[11] Brand Directory
[12] ITU

ciberseguridad tiene presencia en Rotterdam, donde refuerza el clúster existente, aporta conocimiento valioso y crea empleo de calidad[13].

[13] https://rotterdampartners.nl/persberichten/red-carpet-dinner-2022/

4. Oportunidades del mercado

Las tendencias en los últimos años en el mercado internacional TIC 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 TIC 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 relacionado con los participantes en el mercado, con grandes compañías internacionales repartiéndose de forma casi oligopolística la cuota total del mercado.

GASTO MUNDIAL EN TIC

En miles de millones de USD

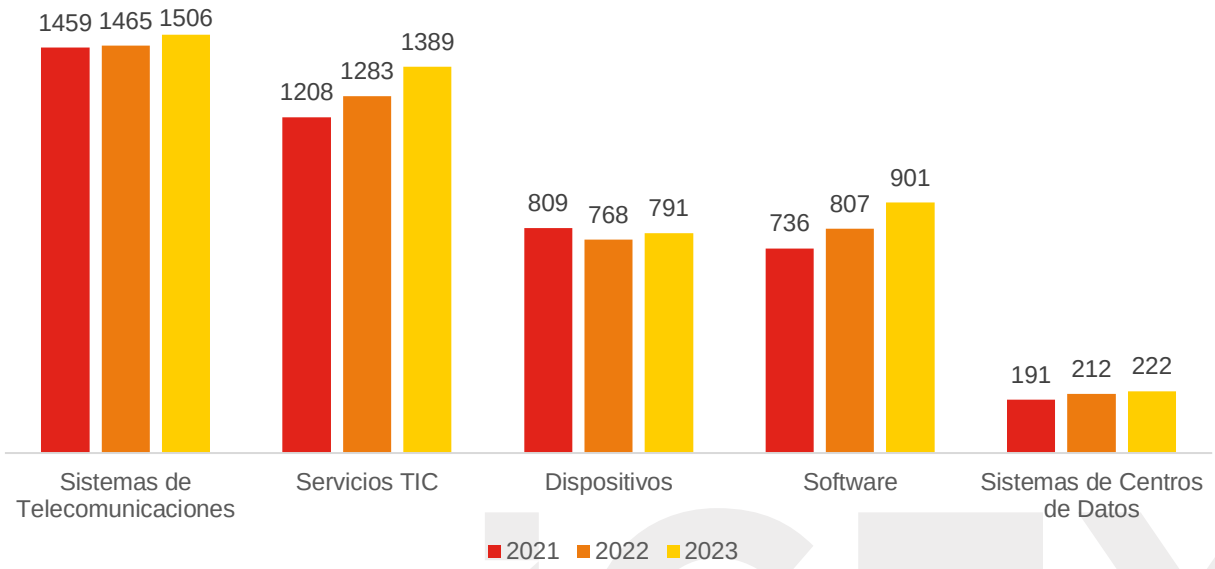
	Gasto 2021	Crecimiento 2021 (%)	Gasto 2022	Crecimiento 2022 (%)	Gasto 2023	Crecimiento 2023 (%)
Sistemas de Centros de Datos	191	6,4	212	11,1	222	4,4
Software	736	14,7	807	9,6	902	11,8
Dispositivos	809	16,0	768	-5,0	791	3,0
Servicios TIC	1.208	12,8	1.283	6,2	1.389	8,3
Servicios de Telecomunicaciones	1.459	2,8	1.465	0,4	1.506	2,8
Total	4.402	10,2	4.535	3,0	4.810	6,1

Fuente: elaboración propia a partir de datos de Gartner. Julio 2022.

De entre las principales partidas de gasto en el sector TIC, 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 TIC, 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 TIC 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 TIC

por año y categorías principales, en miles de millones de USD

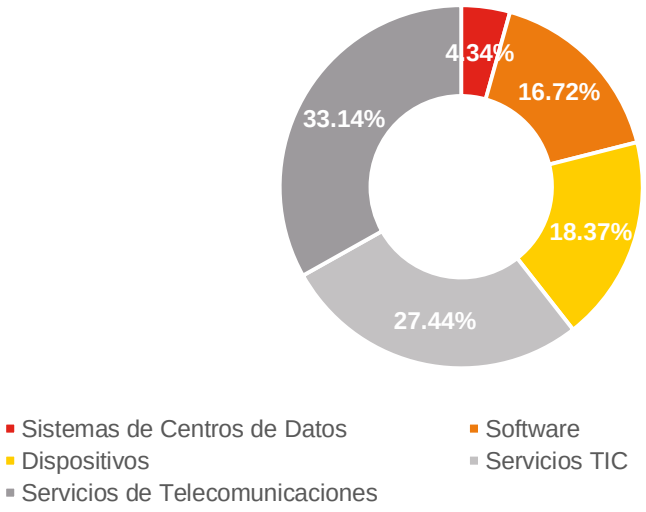


Fuente: elaboración propia a partir de datos de Gartner. Julio 2022.

El *hardware* y los dispositivos siguen siendo una de las mayores partidas de facturación dentro del sector TIC, 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 TIC

En porcentaje por categoría, 2021



Fuente: elaboración propia a partir de datos de Gartner. Julio 2022.

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 existe 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
    - Transporte y distribución nacional de la electricidad
    - Producción, transporte y distribución nacional de gas natural
    - Suministro de petróleo
    - Almacenamiento, producción o procesamiento de materiales nucleares
    - Suministro de agua potable
    - Defensas contra las inundaciones y gestión del agua

- Categoría B

    - Distribución regional de electricidad
    - Distribución regional de gas
    - Internet y servicios de datos
    - Acceso a Internet y tráfico de datos
    - Servicios de voz y mensajería de texto
    - Geolocalización y información horaria de GNSS
    - Gestión del tráfico aéreo
    - Gestión del tráfico marítimo
    - Transporte de personas y bienes en ferrocarril
    - Transporte por carretera
    - Almacenamiento, producción o procesamiento a gran escala de fuentes químicas y petroquímicas
    - Almacenamiento, producción o procesamiento de materiales nucleares
    - Transacciones monetarias de compraventa
    - Transacciones financieras de consumidores
    - Transacciones de alto valor entre bancos
    - Mercado de valores
    - Comunicación con y entre servicios de emergencia
    - Movilización policial
    - Bases de datos de registros personales y de organizaciones
    - Interconectividad entre bases de datos de registros
    - Mensajería electrónica y divulgación de información a los ciudadanos
    - Identificación de ciudadanos y organizaciones
    - Movilización militar

Fuente: elaboración propia a partir de datos del Ministerio de Justicia y Seguridad

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 MEUR. Por ello, la tecnología más vanguardista en términos de ciberseguridad tendrá mayores oportunidades para entrar en un mercado de estas características.

Según la encuesta realizada por Deloitte, las amenazas a la seguridad de las empresas neerlandesas se reparten entre fuga de datos (40 %); *phishing*, *malware* o vulnerabilidades (35 %); y extorsión a la empresa mediante datos (25 %). Un 30 % aseguró que se plantearían pagar en caso de extorsión.

El 63 % de los encuestados pertenecientes a empresas con más de 10.000 empleados declararon que ven oportunidades para contribuir a un sector más resistente y a un ecosistema digital más seguro[14].

[14] Deloitte. *Cyber security in the Netherlands: a responsibility we share*.

5. Claves de acceso al mercado

5.1. 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.

5.2. 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, 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 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.

5.3. Ayudas

- Ayudas en España para la internacionalización
    - ICEX 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 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
  - Comisión Europea a través de ENISA, Agencia de Ciberseguridad de la UE

5.4. Ferias y eventos

- Cyber Security & Cloud Expo

  Próxima edición: Ámsterdam, 26-27 de septiembre de 2023. Formato híbrido.

  Organizado por TechEX, el evento reúne a 5.000 visitantes que tienen la oportunidad de asistir a conferencias de los expertos más relevantes del sector. Se analiza el impacto que tiene la ciberseguridad y la nube en las industrias más importantes.

- ONE Conference

  Última edición: La Haya, 18-19 de octubre de 2022.

  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 para establecer contactos nacionales e internacionales. Tiene como objetivo facilitar el intercambio de conocimientos e ideas dentro de la comunidad internacional de ciberseguridad.

- Benelux Cyber Summit

  Próxima edición: Ámsterdam, octubre de 2023.

  Responsables de departamentos de seguridad de empresas privadas y públicas del Benelux se reúnen para debatir las tendencias y mecanismos de defensa a aplicar.

- TBX

  Última edición: Utrecht, 2-3 de noviembre de 2022.

  Lugar de encuentro para profesionales y directores en el área TIC. Cuenta con más de 75 expositores y pone el foco en el impacto de las nuevas tecnologías en el mundo de la empresa.

- Digital Experience

  Última edición: Utrecht, 5 de octubre de 2022. Formato híbrido.

  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.

- Webwinkel Vakdagen

  Próxima edición: Utrecht, 29-30 de marzo de 2023.

  Con más de 10.000 visitantes en su última edición, es la feria más grande del Benelux sobre comercio electrónico.

6. Información adicional

- Cyber Security Council

  Punto de enlace entre los sectores público y privado, así como los centros de investigación, formado por 18 miembros.

  Turfmarkt 147

  2511 DP Den Haag

  Teléfono: +31 70 751 53 33

  E-mail: info@cybersecurityraad.nl

- National Cyber Security Centre (NCSC)

  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.

  Turfmarkt 147

  2511 DP Den Haag

  Teléfono: (070) 751 55 55

  E-mail: info@ncsc.nl

- National Coordinator for Security and Counterterrorism (NCTV)

  Protege al país contra amenazas que pueda alterar la sociedad. Garantiza la seguridad de las infraestructuras críticas neerlandesas juntamente con sus socios en el Gobierno, la comunidad científica y el sector empresarial.

  Turfmarkt 147

  2511 DP The Hague

  Teléfono: + 31 70 751 50 50

  E-mail: frontoffice-ncc@nctv.minvenj.nl

- The Hague Security Delta (HSD)

  Mayor clúster en materia de ciberseguridad de Europa, donde colaboran empresas, gobiernos e instituciones de investigación.

  Wilhelmina van Pruisenweg 104

  2595 AN Den Haag

  Teléfono: +31 (0)70-2045180

  E-mail: info@securitydelta.nl

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

www.icex.es

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