



OTROS
DOCUMENTOS

2021



Ciberseguridad en Portugal



Oficina Económica y Comercial
de la Embajada de España en Lisboa

Este documento tiene carácter exclusivamente informativo y su contenido no podrá ser invocado en apoyo de ninguna reclamación o recurso.

ICEX España Exportación e Inversiones no asume la responsabilidad de la información, opinión o acción basada en dicho contenido, con independencia de que haya realizado todos los esfuerzos posibles para asegurar la exactitud de la información que contienen sus páginas.

icex



OTROS
DOCUMENTOS

29 de octubre de 2021
Lisboa

Este estudio ha sido realizado por
Agustín Yago Gómez Torremocha

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en Lisboa

<http://Portugal.oficinascomerciales.es>

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

NIPO: 114-21-010-1

Índice

1. Introducción	4
2. Características del mercado	5
2.1. Definición de las actividades / productos del sector estudiado	5
2.2. Tamaño del mercado	7
2.3. Estructura de la industria	8
2.4. Principales empresas del sector	10
2.5. Ataques cibernéticos en Portugal	13
3. La oferta española en Portugal	16
4. Oportunidades del mercado	17
5. Acceso al mercado	19
5.1. Distribución	19
5.2. Barreras y legislación	19
5.3. Ayudas	21
5.4. Tendencias del sector	21
5.5. Ferias	23
6. Información adicional	25
6.1. Organismos relevantes	25
6.2. Fuentes de interés	25

icex



1. Introducción

La pandemia está sirviendo como catalizador del proceso de digitalización, acelerándolo e impulsando las oportunidades en el sector. El teletrabajo y la sofisticación de la ciberdelincuencia suponen un verdadero desafío para la ciberseguridad de las empresas y organizaciones en Portugal. Como en la mayoría de los países desarrollados, en Portugal la ciberseguridad se ha convertido en un elemento clave, volviéndose cada vez más crucial para el éxito económico de toda organización. En la tabla siguiente se presentan los datos más representativos de este sector en Portugal:

Datos del mercado portugués de ciberseguridad	
Población total 2021 (habs.)	10.347.892
Tasa de usuarios de Internet en Portugal 2021	78,3 %
Índice de facilidad para hacer negocios del Banco Mundial, 2020	39 / 190
Clasificación de Portugal en el Global Cybersecurity Index (GCI), 2020	14 / 193
Clasificación de Portugal en el European Cybersecurity Index, ESET 2021	1 / 24
Global Innovation Index 2020	31 / 131
Índice de Alfabetización y Educación en Ciberseguridad	25 / 50
Gasto mundial en ciberseguridad 2021	61.836 MEUR
Valor de mercado¹ de la ciberseguridad en la UE	130.000 MEUR
Gasto en ciberseguridad en Portugal 2019	221,83 MEUR
Tamaño del mercado de las TIC en Portugal, 2019	8.240 MEUR
Exportaciones de servicios TIC de España a Portugal, 2019	685,4 MEUR

Fuente: HCP, Banco Mundial, Red.es, Global Cybersecurity Index, Global Innovation Index, International Finance Corporation, Instituto Nacional de Estadística, Deloitte Cyber Smart Index 2020, Oliver Wyman Consulting, Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (2020), Consejo Europeo, *Information Security and Risk Management Worldwide*, 4Q19 Gartner.

¹ Entendemos por valor de mercado el conjunto de activos (recursos humanos, infraestructuras, patentes, etc.) que lo componen.

2. Características del mercado

2.1. Definición de las actividades / productos del sector estudiado

Según **ENISA** (Agencia de la Unión Europea para la Ciberseguridad), la ciberseguridad comprende todos los aspectos de prevención, predicción, tolerancia, mitigación, extracción, análisis e investigación de los ciberincidentes. Considerando los diferentes tipos de componentes del ciberespacio, la ciberseguridad debe considerar varios atributos: disponibilidad, fiabilidad, seguridad, confidencialidad, integridad, sostenibilidad (para los sistemas tangibles, información y redes), robustez, supervivencia, resiliencia (apoyar el dinamismo del ciberespacio), responsabilidad, autenticidad y no rechazo (apoyar a la seguridad de la información).

El **mercado de la ciberseguridad** engloba todos aquellos productos o servicios destinados a la protección de los sistemas y redes informáticos contra el robo o el daño de su *hardware*, *software* o datos electrónicos, así como contra la interrupción o el desvío de los servicios que presta.

Los Códigos de Actividad asociados a este sector son los siguientes:

CÓDIGOS DE ACTIVIDAD

Aproximación al sector de la ciberseguridad

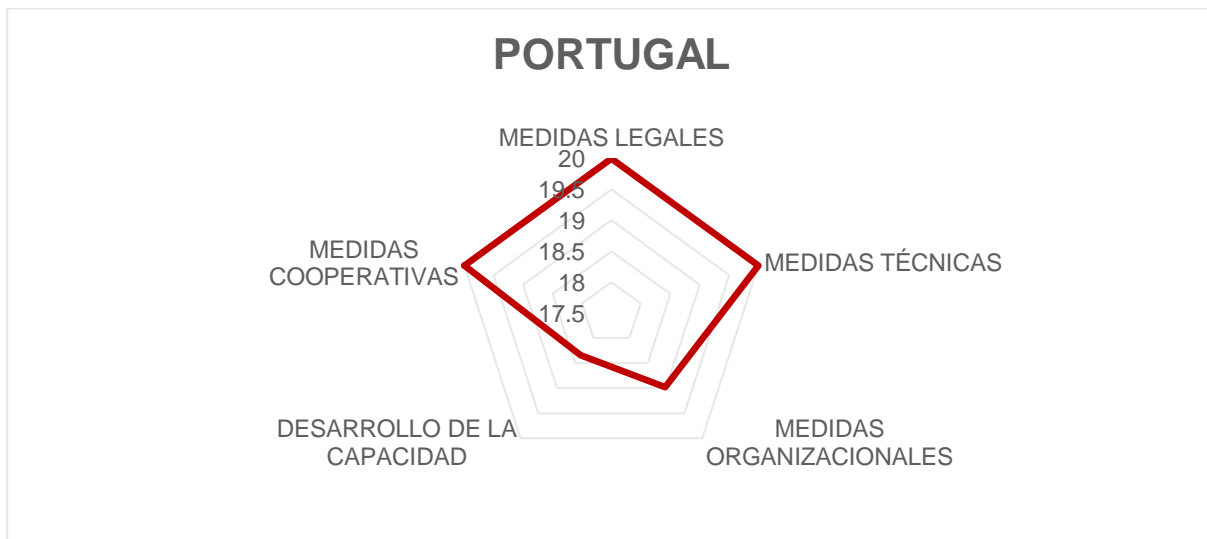
Código	Descripción
62	Programación, consultoría y otras actividades relacionadas con la informática
62010	Actividades de programación informática
62020	Actividades de consultoría informática
62030	Gestión de recursos informáticos
62090	Otros servicios relacionados con la informática y TI

Fuente: Código Actividad SABI.

No existe una delimitación arancelaria categorizada por el Sistema TARIC, ya que este trabajo versa sobre la **prestación de servicios** de ciberseguridad.

El mercado de la ciberseguridad en Portugal presenta los siguientes parámetros, según el Global Cybersecurity Index:

ESTADO DE LA CIBERSEGURIDAD EN PORTUGAL



Fuente: ITU Global Cybersecurity Index v4, 2021, *Security Magazine*.

Entre los aspectos de relativa **fortaleza del mercado luso**, destacan principalmente las medidas legales, técnicas y cooperativas, mientras que las áreas con mayor crecimiento potencial son las medidas organizacionales y el desarrollo de la capacidad.

Portugal se sitúa en el **puesto 14.º en el Índice de Ciberseguridad Global 2020** de la Unión Internacional de Telecomunicaciones (42.º en 2018) y en el octavo lugar en el *ranking* regional europeo (25.º en 2018). El conjunto de iniciativas legislativas, técnicas, organizativas, de desarrollo de capacidades y cooperación que se han definido e implementado con el objetivo de fortalecer el marco de ciberseguridad nacional en los últimos años contribuyó a la mejora de Portugal en este índice. En este sentido, cabe destacar que, según este índice, España ocupa la cuarta posición con 98,52 puntos y el líder es Estados Unidos con una puntuación de 100.

El índice también revela que el país está "muy cerca" de lograr una calificación máxima a través de medidas implementadas a nivel estratégico y organizacional, así como con las medidas de concienciación, capacitación y educación para la ciberseguridad, según indica el Centro Nacional de Ciberseguridad (CNCS).

Según el informe [European Cybersecurity Index](#), publicado este mismo año por la empresa tecnológica ESET, Portugal obtuvo una puntuación en ciberseguridad de 8,21 sobre 10. Así, Portugal encabeza la lista como **la región más cibersegura de Europa**, con un número muy bajo de personas que hayan sido víctimas de *software* malicioso, piratería de redes sociales, fraude

bancario en línea y robo de identidad. Esto, unido a la buena legislación en cinco categorías (estrategia nacional, contenido, privacidad, infraestructura crítica y comercio), propulsan a Portugal a la primera posición del *ranking*.

Por último, Portugal aparece en el centro de la tabla, en el **puesto 25.º entre 50** naciones analizadas, en el [Índice de Alfabetización y Educación en Ciberseguridad](#) de la consultora Oliver Wyman, destacando en materia de educación, pero fallando en la motivación pública.

2.2. Tamaño del mercado

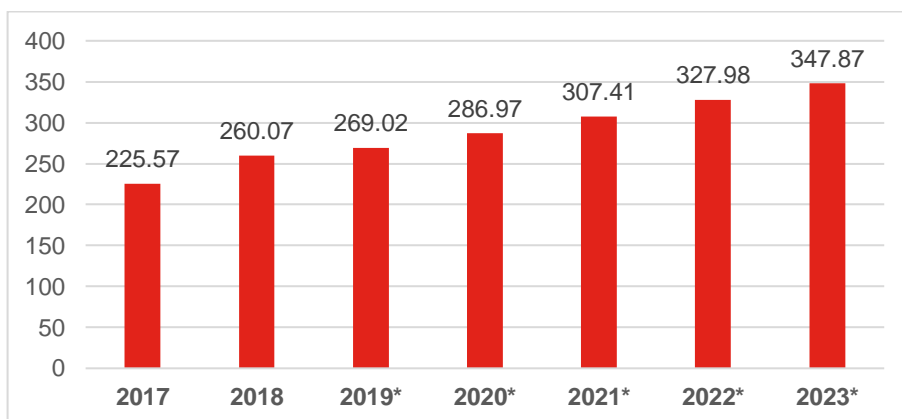
En los veinte primeros puestos del Índice Mundial de Ciberseguridad figuran dieciocho países europeos y el valor del mercado de la ciberseguridad en la Unión Europea se estima en más de 130.000 millones de euros, creciendo a un ritmo aproximado del 17 % anual. Entendemos por valor de mercado el conjunto de activos que lo componen: infraestructuras, recursos humanos, inversión en investigación, etc. Además, la UE cuenta con más de 60.000 empresas de ciberseguridad y más de 660 centros especializados en ciberseguridad.

Según el informe [Information Security and Risk Management Worldwide, 4Q19 de Gartner](#), Portugal ocupa la **40.ª posición en el ranking mundial de gasto** por países en ciberseguridad, con un gasto total de 260,07 millones de USD en 2019, lo que supone una cuota total de mercado a nivel mundial del 0,23 %.

En este mismo informe, Portugal presenta una tasa promedio de **crecimiento anual** en el periodo estudiado 2018-2023, según Gartner: un incremento de **5,99 %** con un aumento del gasto en el periodo estudiado de 123 millones de dólares.

EVOLUCIÓN DEL GASTO EN PORTUGAL EN CIBERSEGURIDAD DE 2017 A 2023*

En MUSD



* Datos estimados.

Fuente: Gartner (2019).

A nivel global, los servicios de ciberseguridad han experimentado un crecimiento medio del 12,4 % en el último año. El segmento del mercado que ha experimentado un mayor incremento ha sido el de servicios de seguridad en la nube.

GASTO MUNDIAL EN CIBERSEGURIDAD POR PAÍSES 2017-2023

En MUSD

MERCADO	2017R	2018R	2019P	2020P	2021P	2022P	2023P	CAGR ² 18-23
Europa Occidental	25.495,50	29.051,83	30.091,06	32.429,99	35.126,20	37.912,79	40.678,69	6,96 %
España	1.376,71	1.594,01	1.651,54	1.770,67	1.905,77	2.043,24	2.179,98	6,46 %
Portugal	225,57	260,07	269,02	286,97	307,41	327,98	347,87	5,99 %
Gasto mundial	101.376,9	112.677,85	120.877,16	131.395,6	143.007,38	155.098,15	167.059,00	8,19 %

Fuente: *Information Security and Risk Management Worldwide, 4Q19* Gartner. INCIBE Analysis.

Según la [consultora IDC](#), para 2022, el **gasto en TIC en Portugal** podría alcanzar los 8.586 millones de euros, lo que corresponde a una tasa de crecimiento anual compuesta del 1,5 % en el periodo 2017-2022.

La nube, *Internet of Things*, *Big Data* y la ciberseguridad son las **tecnologías destacadas**, con tasas de crecimiento anual compuesto superiores al 7 %, un aumento liderado por los sectores de venta detallista, salud, seguros, banca, industria y servicios profesionales.

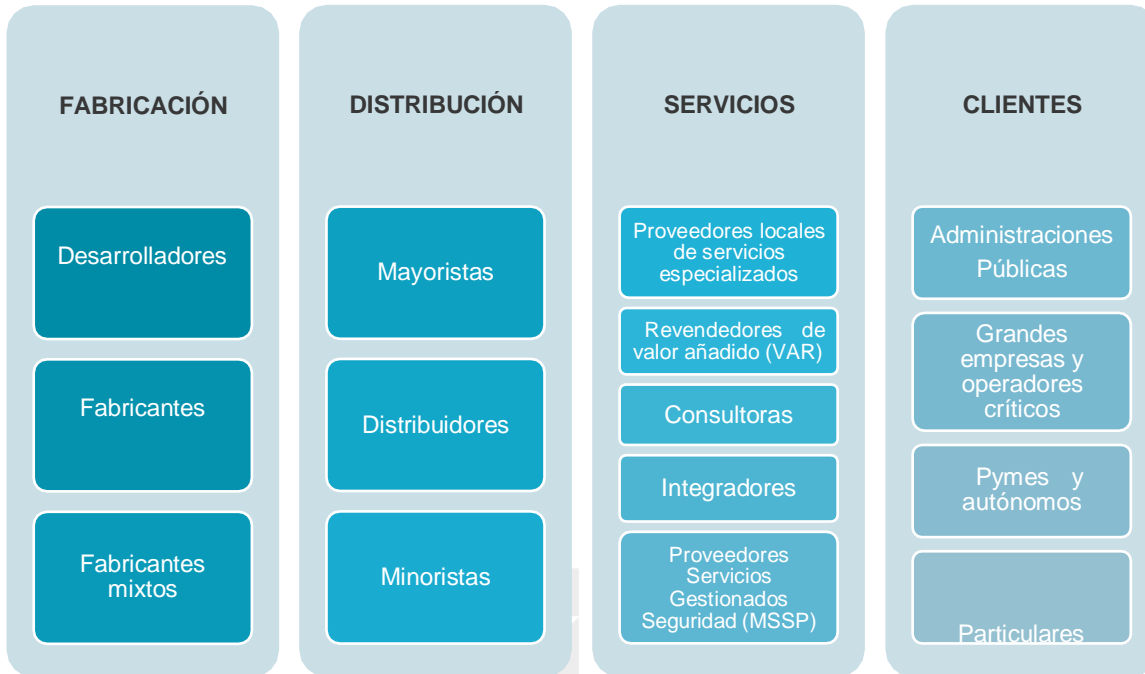
2.3. Estructura de la industria

De acuerdo con los datos más recientes de [INCIBE](#), **en España hay un total de 1.595 empresas dedicadas a la ciberseguridad**. De ellas, 374 se identifican como fabricantes, 439 como distribuidores o mayoristas y 1.524 como integradores o consultores.

Según INCIBE (Instituto Nacional de Ciberseguridad), la estructura de **la cadena de valor de la industria** de ciberseguridad sería:

² Tasa de crecimiento anual compuesta del mercado (CAGR).

CADENA DE VALOR DE LA CIBERSEGURIDAD



Fuente: Instituto Nacional de Ciberseguridad (INCIBE).

De esta forma, los **demandantes de soluciones de ciberseguridad** se pueden clasificar en tres grandes grupos según la complejidad de los tipos de servicios y soluciones que ofertan, quedando estructurados de la siguiente manera:

- **Administraciones Públicas:** las principales amenazas que pueden sufrir son el ciberespionaje y la sustracción, publicación y venta de información sensible a través de Internet. Requieren soluciones de seguridad integral, de ciberinteligencia y ciberdefensa, que contribuyan a la defensa de los organismos públicos locales, regionales y nacionales.
- **Grandes empresas:** su demanda depende del sector en el que opera la empresa, diferenciándose las que pertenecen a sectores catalogados como infraestructuras críticas (instituciones gubernamentales, centrales eléctricas...) que demandan una alta especialización en el sector, en la región o en la tecnología, y las soluciones de seguridad integral.
- **Pymes, autónomos o particulares:** La principal amenaza para este último grupo es el uso, abuso o reventa de información privada que han proporcionado como clientes a organizaciones privadas y los ataques de ciberdelincuencia.

A continuación, con el fin de dimensionar y comprender mejor la estructura de este sector, se presenta el siguiente cuadro en el que se recogen los **gastos mundiales en cada segmento de actividad**. Dentro de estas partidas se integran los servicios de ciberseguridad. En ellos destacan los servicios de seguridad, que suponen el 50 % del total del gasto mundial.

GASTO MUNDIAL EN SEGURIDAD POR SEGMENTO, 2019-2020

En MUSD

Mercado	2019	2020	Crecimiento (%)
Seguridad de aplicaciones	3.095	3.287	6,2
Seguridad en la Nube	439	585	33,3
Seguridad de datos	2.662	2.852	7,2
Gestión de acceso con identidad	9.837	10.409	5,8
Protección de infraestructura	16.520	17.483	5,8
Gestión Integrada de Riesgos	4.555	4.731	3,8
Equipo de seguridad de red	13.387	11.694	-12,6
Otro software de seguridad de la información	2.206	2.273	3,1
Servicios de seguridad	61.979	64.270	3,7
Software de seguridad para el consumidor	6.254	6.235	-0,3
TOTAL	120.934	123.818	2,4

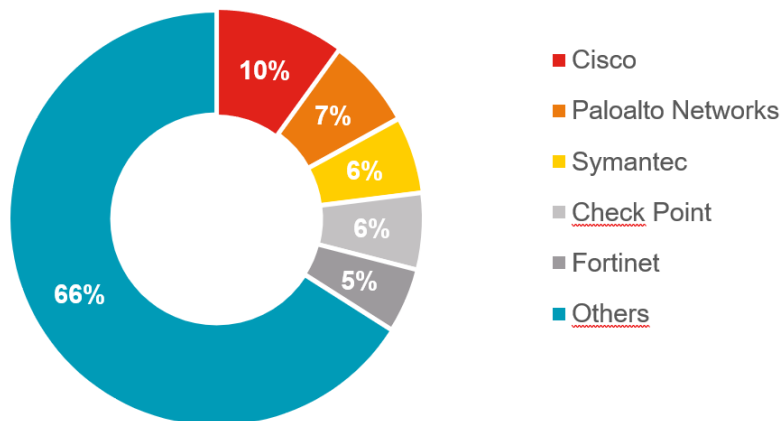
Fuente: KMU Portal (2020).

2.4. Principales empresas del sector

Según [Cybersecurity Ventures](#), se han formado miles de nuevas empresas durante la última década para centrarse en combatir el cibercrimen, que se estima que cueste al mundo 6 billones de dólares anuales en 2021, frente a los 3 billones de dólares de 2015. Se estima que el **coste global anual de la ciberdelincuencia** ascenderá a 10,5 billones de dólares para el 2025.

En cuanto a la **cuota de mercado a nivel mundial**, destacan las siguientes empresas como líderes del sector:

CONCENTRACIÓN DE LA OFERTA DEL MERCADO GLOBAL



Fuente: Statista, 2020.

Respecto a la oferta, muchas de las principales empresas de ciberseguridad del mundo tienen su sede en Estados Unidos. Las empresas reflejadas en el gráfico anterior, salvo Fortinet (Israel), son todas estadounidenses, lo que indica un claro dominio de estas.

La oferta de ciberseguridad en Portugal está marcada por una fuerte presencia internacional:

- **Empresas estadounidenses:** IBM Security, Cisco, SAS Institute
- **Empresas relevantes a nivel europeo:** PwC, Siemens, EY, Deloitte, KPMG
- **Empresas españolas:** SIA, GMV, Panda Cybersecurity

Dentro de las **empresas portuguesas** destaca, por encima de todas, el grupo inversor **Sonae IM**.



Sonae Investment Management ([Sonae IM](#)), grupo inversor portugués propietario de las empresas españolas de ciberseguridad [S21sec](#) (adquirida en 2017) y Nextel (adquirida en 2018), es una empresa líder en servicios y tecnología de ciberseguridad. Con estas operaciones, el grupo se posicionó exclusivamente en el sector de la ciberseguridad (*pure player*), con operaciones en Portugal, España y México.

S21sec es actualmente la mayor empresa de [servicios de ciberseguridad](#) de la península Ibérica, con una dilatada experiencia en el sector que le permite ofrecer una cobertura completa de los riesgos de ciberseguridad en los procesos de negocio de las organizaciones.



Además de estas operaciones, en 2020, Sonae IM decidió crear un nuevo *holding* para consolidar sus inversiones en ciberseguridad. S21sec y [Excellium](#) estarán así juntos en [Maxive Cybersecurity](#). La operación crea uno de los mayores operadores del sector en Europa y Portugal, tanto en términos de negocios, como de trabajadores cualificados y ofrecerá a sus clientes una gama más amplia de servicios, combinando las mejores prácticas y recursos de S21sec y Excellium.

A nivel local, tanto S21sec (España, Portugal y México) como Excellium (Luxemburgo y Bélgica) seguirán operando bajo su estructura de gestión, con un claro enfoque en mantener la posición de liderazgo de ambas empresas en sus mercados locales.

Además de las empresas integrantes del grupo Sonae IM, algunos de los *players* de ciberseguridad más relevantes en el mercado portugués son **empresas españolas**:

SIA  **minsait**

[Indra](#) es una empresa líder en Tecnologías de la Información en España y Latinoamérica. Dispone de una oferta integral de soluciones propias y servicios avanzados desarrollo de soluciones tecnológicas integrales en diversos campos y, a través de su unidad [Minsait](#), da respuesta a los retos que plantea la transformación digital.

Indra adquirió en 2020 a [SIA](#), empresa española especializada en servicios de ciberseguridad. Esta adquisición permitirá la consolidación en el mercado de la península Ibérica. Con esta operación, Indra se convierte en líder en el mercado ibérico de la ciberseguridad, ya que SIA cuenta con una base de clientes diversificada y estable, con más de 10.000 proyectos de seguridad, y es además líder en el mercado español en soluciones de identidad y firma electrónica. SIA contará con más de 1.000 profesionales altamente cualificados y expertos en ciberseguridad.



[Panda Security](#) es una empresa de origen español especializada en la creación de soluciones de seguridad informática. Es una marca con más de 25 años de experiencia en el mercado ibérico. Centrada inicialmente en la creación de un programa antivirus, la compañía ha ampliado sus objetivos expandiendo su línea de negocio hacia los servicios de ciberseguridad avanzada con



tecnologías para la prevención del cibercrimen. Actualmente forma parte del grupo americano [WatchGuard](#).



GMV es un grupo empresarial tecnológico español de capital privado con presencia internacional. Fundado en 1984, ofrece soluciones, servicios y productos en muy diversos sectores (aeronáutica, banca y finanzas, espacio, defensa, sanidad, ciberseguridad). GMV cubre todo el ciclo de vida de la ciberseguridad: identificar, proteger, detectar, responder y recuperar.

2.5. Ataques cibernéticos en Portugal

DATOS SOBRE ATAQUES CIBERNÉTICOS

Variable estudiada	Mercado
22.300 millones de dispositivos en todo el mundo estarán conectados al <i>IoT</i> en 2024	Global
Las pequeñas empresas fueron el objetivo del 43 % de los ciberataques	Global
Los ciberataques en Portugal aumentaron un 79 % en 2020 respecto al año anterior	Portugal
Una cuarta parte de los portugueses (27 %) sufrió un incidente de ciberseguridad en 2020	Portugal
El 74 % de empresas cuentan con políticas de seguridad TIC definidas o revisadas	Portugal
Las denuncias relacionadas con delitos informáticos aumentaron de 193 en 2019 a 544 en 2021	Portugal
Los ataques a la banca se triplicaron en 2020	Portugal
El 43 % del total de incidentes registrados por la plataforma CERT.PT son ataques de <i>phishing</i> y <i>smishing</i>	Portugal
Portugal ocupa el segundo lugar mundial con el 19,73 % del total de ataques de <i>phishing</i>	Portugal

Fuente: Cybint Solutions, "Relatório de Cibersegurança em Portugal – Sociedade", Centro Nacional de Cibersegurança, "Ciberseguridad en Portugal, Riesgos y Conflictos", Kaspersky.

Los ciberataques y la ciberdelincuencia están aumentando en toda Europa, y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro, ya que se espera que 22.300 millones de dispositivos en todo el mundo estén conectados al Internet de las Cosas (IoT) de aquí a 2024.

[Cybint Solutions](#) descubrió que las pequeñas empresas fueron el objetivo del 43 % de los ciberataques recientes a nivel mundial. Los piratas informáticos descubren que muchas pequeñas



empresas no han invertido adecuadamente en seguridad cibernética y quieren explotar sus vulnerabilidades.

La **pandemia de COVID-19** tuvo una influencia innegable en el aumento de actividades ilegales en línea. Se puede explicar por dos razones principalmente: por un lado, el confinamiento social y la adopción de tecnología acelerada digital promovieron una migración al mundo *online*; y, por otro, el mayor uso y necesidad de la esfera digital fomentó el sentido de oportunidad de agentes de amenaza, lo que lleva a la explotación de las vulnerabilidades técnicas más expuestas. Además, según el informe anual [Relatório de Cibersegurança em Portugal – Sociedade](#) de 2020, el CNCS afirma que la delincuencia *online* ha crecido durante los periodos de confinamiento. Con millones de personas usando medios electrónicos para trabajar, los incidentes han aumentado y no es de esperar que su número disminuya nuevamente.

El estudio indica que muchas de las **ciberamenazas continuarán** como consecuencia de la persistencia de la pandemia y de sus efectos y se aprovecharán de las vulnerabilidades provocadas por el trabajo a distancia y por la mayor importancia del ámbito digital y de sectores como la banca y la sanidad en el acceso remoto.

Según el Centro Nacional de Ciberseguridad (CNCS), los **ciberataques en Portugal aumentaron un 79 % en 2020** respecto al año anterior. El CNCS advierte también de que la tendencia empeora y destaca el incremento de los ataques a los bancos.

El año pasado, más de una cuarta parte de los portugueses (27 %) sufrió un **incidente de ciberseguridad**. En las empresas, este valor fue del 8 %. Los datos están contenidos en el informe [Ciberseguridad en Portugal, Riesgos y Conflictos](#), del CNCS publicado en junio de 2020. El riesgo de que una entidad sufra un incidente de ciberseguridad en 2020 aumentó un 94 %, porcentaje que disminuye en 2021, hasta el 86 %.

En Portugal y, según este informe nacional del CNCS, hay menos **empresas con políticas de seguridad TIC** definidas o revisadas (74 %) en comparación con la Unión Europea (76 %). Sin embargo, las organizaciones en Portugal aplican más medidas de seguridad (98 %) que la media europea (93 %).

El número de denuncias relacionadas con **delitos informáticos** también aumentó en Portugal, de 193 en 2019 a 544 en 2021. Al igual que en 2019, en 2020, el fraude informático o de comunicaciones siguió siendo el tipo de delito informático más registrado por las autoridades policiales, representando el 90 % de casos, con un incremento del 22 % respecto al año anterior. Entre los delitos informáticos, el acceso o interceptación ilegítimos es el delito más registrado, representando el 4 % del total de delitos informáticos, con un aumento del 24 % en comparación con el año anterior.



Si se contabilizan los ataques que se aprovechan de vulnerabilidades que permiten a un atacante realizar acciones que no le estarían permitidas, la cifra alcanzó los 1.418 en 2020, lo que supone un aumento del 88 %, acentuando el ritmo de incremento ya observado en años anteriores.

Por sectores, los ataques a la banca alcanzaron los 229 incidentes, convirtiendo a este sector en el segundo más atacado, después del sector público, triplicando sus números en 2020. Así, el CNCS identificó 626 incidentes en sectores no especificados y áreas gubernamentales, por ello, reforzar la protección de las infraestructuras computacionales del Estado es prioritario.

También recibieron ataques las infraestructuras digitales, los proveedores de servicios de Internet y la educación superior. Los sectores de salud, comunicaciones, energía, transporte, banca, suministro y distribución de agua potable, servicios e infraestructuras de mercado son algunos de los identificados como **más vulnerables** a los ciberataques.

El año pasado, entre los incidentes registrados y las denuncias, destacaron los ataques de **phishing** (tipo de fraude financiero en el que los delincuentes defraudan o engañan a las personas por correo electrónico) y **smishing** (*phishing* por SMS), correspondientes al 43 % del total de incidentes registrados por la plataforma [CERT.PT](#). En los informes a la Oficina de Delitos Cibernéticos, se evidencian fraudes en la aplicación [MBWAY](#) y diversas formas de fraude. El factor humano y las técnicas de ingeniería social se señalan como distintivos de esta dinámica, pero también se menciona que, según datos de la Dirección General de Política de Justicia (DGPJ), el fraude informático y comunicacional aumentó un 22 % en 2020.

Por último, según el informe más reciente de [Kaspersky](#), en 2020 se identificaron alrededor de 430 millones de intentos de ataques de *phishing*, con Portugal ocupando el **segundo lugar mundial** con el 19,73 % del total de ataques. Brasil nuevamente lidera la tabla de países con mayor número de víctimas afectadas (19,94 %).

3. La oferta española en Portugal

Según un [informe sectorial de DBK sobre ciberseguridad](#), el mercado español tenía un tamaño de 1.200 millones de euros en 2018, casi cinco veces superior al portugués ese mismo año. Igual que en el mercado luso, la prestación de servicios representa aproximadamente más de dos tercios del valor total (70 %).

Tanto España como Portugal colaboran en la [Agencia Europea de Seguridad de las Redes y de la Información \(ENISA\)](#) y en el consorcio europeo [European Cyber Security Organisation \(ECSO\)](#). Otro de los factores que alinea a ambos países es el papel similar que desarrollan las agencias nacionales de ciberseguridad (CNCS de Portugal e INCIBE en España). INCIBE, además, organiza anualmente el encuentro [ENISE](#) en León con el objetivo de conectar a profesionales del sector con emprendedores y con representantes del mundo académico e investigador a nivel internacional.

Como se ha explicado en el capítulo anterior, destacan los grandes proveedores de ciberseguridad como Indra con [SIA](#) y [Minsait, Panda Security](#) o [GMV Innovating Solutions](#), pero más allá de este tipo de empresas existe un amplio número de pymes que tratan de competir mediante especialización, avances tecnológicos o vía precio. Este hecho pone de manifiesto que la **oferta española se encuentra muy atomizada**, lo que implica que, a menudo, cuando hay alguna pyme que destaca, tiende a ser absorbida por grandes multinacionales americanas, israelíes o asiáticas, como ha ocurrido en el caso de [Panda Security](#), que fue comprada en marzo de 2020 por la empresa estadounidense [WatchGuard](#).

Uno de los medidores de referencia en materia de ciberseguridad es el **Global Cybersecurity Index (GCI)**. En este *ranking* España ocupa el séptimo puesto mundial, mientras que **Portugal se sitúa en el 14.º**. Esta clasificación demuestra la mayor experiencia y *know-how* de las empresas españolas en este sector.

En definitiva, la oferta española cuenta con un buen posicionamiento y reconocimiento en el mercado portugués de ciberseguridad, con empresas líderes en el mercado ibérico.

4. Oportunidades del mercado

El Gobierno de Portugal destinará al menos **130 millones de euros de los Fondos Europeos para potenciar la seguridad** en el uso de los sistemas digitales y de datos. Reforzar la protección de las infraestructuras computacionales del Estado se ha convertido en una de las prioridades del Gobierno luso en el [Plan de Recuperación y Resiliencia](#) (PRR, por sus siglas en portugués). De este total, se invertirán 83 millones en infraestructuras críticas digitales eficientes, seguras y compartidas, con el objetivo de hacer que la red informática del Gobierno sea más resistente. Esta inyección económica a nivel público en el sector puede suponer una muy buena oportunidad para aquellas empresas que estén especializadas en procesos de ciberseguridad con la Administración pública.

El Ejecutivo portugués manifiesta la relevancia que ha tenido el uso de los medios digitales en los servicios públicos tras la llegada de la COVID-19 y justifica así la necesidad de **fortalecer el marco nacional de la ciberseguridad** y la seguridad de los datos, profundizando, de forma estructurada e integrada, en la formación en estos campos y en el uso seguro de los datos.

El informe sobre madurez digital en ciberseguridad elaborado por [Minsait y SIA](#), revela que el 90 % de las empresas no cuenta con profesionales especializados en ciberseguridad, el 82 % no lleva registros actualizados de los activos digitales a proteger, el 73 % no tiene implementada una cultura de ciberseguridad para los empleados y sólo el 55 % cuenta con un centro de operaciones de ciberseguridad para detectar y responder a un ciberataque. El hecho de que **más de la mitad de las empresas portuguesas no cuenten actualmente con una estrategia de ciberseguridad**, supone también una buena oportunidad de entrada al mercado.

Ante este escenario, es fundamental **contar con el apoyo de partners especializados** que ofrezcan una visión integral de los retos que se presentan en un sector hiperprofesionalizado y en constante cambio. En Portugal, según CNCS, las empresas recurren mayoritariamente a proveedores externos para el 75 % de las actividades de ciberseguridad lo que, de nuevo, supone una oportunidad de mercado en el sector. Existe un gran número de empresas que proveen servicios gestionados de ciberseguridad en España, y a medida que esta tendencia se consolide habrá oportunidades para ellas en el mercado luso.

Otro indicador favorable es que el gasto corporativo en ciberseguridad sigue al alza: el 87 % de las organizaciones que participaron en la encuesta global de [Ernst & Young](#) sobre ciberseguridad expresaron la necesidad de **augmentar en un 50 % su presupuesto para ciberseguridad**.

Además, Portugal cuenta con una densa red de **sectores demandantes** de importantes servicios de ciberseguridad: el sector bancario, el sector de seguros y el sector médico/farmacéutico, además de las infraestructuras críticas y las instituciones gubernamentales e internacionales.

A nivel europeo, cabe destacar la creación por parte de [El Basque CyberSecurity Centre \(BCSC\)](#) de un fondo público-privado de inversión en empresas de ciberseguridad. Dicho fondo estará dotado con 1.000 millones de euros y será financiado por el [Banco Europeo de Inversiones \(BEI\)](#) y contará con la colaboración estratégica de la European Cyber Security Organization (ECSO). Su objetivo es impulsar el sector de la ciberseguridad en Europa para reducir su dependencia tecnológica de otras economías mundiales.

Como oportunidades de negocio se han valorado las siguientes tecnologías relacionadas con el sector y con poco recorrido en territorio luso: la **Inteligencia Artificial, Machine Learning, Blockchain e Internet de las Cosas (IoT)**.

Por último, la pandemia de COVID-19 ha afectado a las decisiones de inversión y compra en soluciones de ciberseguridad. Son muchas las organizaciones portuguesas que han implantado nuevas medidas de ciberseguridad en los últimos meses. De hecho, **el 77 % de las empresas afirma haber invertido recientemente en nuevos proyectos de seguridad** por dos razones principales: por un lado, para responder a un incidente cibernético concreto y, por otro, por el riesgo a sufrir una sanción.

SÍNTESIS DE LAS OPORTUNIDADES DE MERCADO EN PORTUGAL

El Gobierno de Portugal destinará al menos 130 millones de euros de los Fondos Europeos para potenciar la seguridad en el uso de los sistemas digitales y de datos.

El 90 % de las empresas no cuenta con profesionales especializados en ciberseguridad.

Creación por parte de El Basque CyberSecurity Centre (BCSC) de un fondo público-privado de inversión en el sector.

Poco recorrido en Portugal de: Inteligencia Artificial, *Machine Learning*, *Blockchain* e Internet de las Cosas.

El gasto corporativo a nivel global en ciberseguridad sigue al alza: el 87 % de las organizaciones lo aumentarán.

Portugal cuenta con una densa red de sectores demandantes de importantes servicios de ciberseguridad.

En Portugal el 77 % de las empresas afirma haber invertido en nuevos proyectos de seguridad recientemente.

Fuente: Plan de Recuperación y Resiliencia, Minsait y SIA, Ernst & Young, Banco Europeo de Inversiones (BEI), Centro Nacional de Cibersegurança, Kaspersky.

5. Acceso al mercado

5.1. Distribución

Los principales canales de distribución y estrategias de entrada al mercado son los siguientes:

- **Mayoristas:** se dedican a la compra de servicios de ciberseguridad y a la venta de estos principalmente a consultoras, integradores y a los proveedores de servicios gestionados de seguridad. Lo habitual es que las soluciones que requieren una adaptación al cliente final sean realizadas por una **integradora o consultora local** portuguesa, lo que supondría la forma más fácil de introducirse en el mercado portugués, completando con soluciones la cartera de productos de las empresas locales.
- **Distribuidores:** venden los productos directamente a empresas de ciberseguridad o a clientes finales. En ocasiones, tanto distribuidores como mayoristas comercializan sus productos a los revendedores de valor añadido.
- **Minoristas:** se trata de tiendas de informática, grandes superficies o pequeñas consultoras orientadas a pymes y particulares.

Otra estrategia habitual de acceso al mercado es establecer asociaciones o alianzas estratégicas con una empresa existente. Es siempre importante favorecer una solución de beneficio mutuo basada en la complementariedad, ya que una dependencia del socio local resta visibilidad y acceso a la información a la empresa, y puede causar problemas a largo plazo.

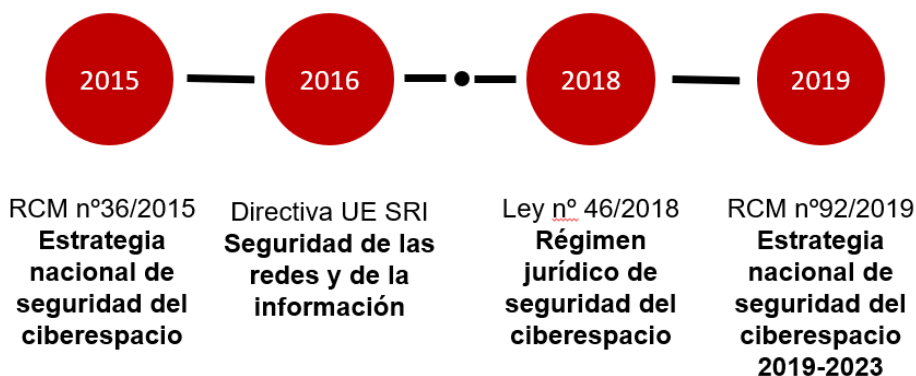
Finalmente, en algunos casos concretos, puede ser recomendable encontrar un socio de representación que tenga contactos con los directores de grandes empresas pertenecientes a los sectores claves mencionados anteriormente para la obtención de grandes proyectos.

5.2. Barreras y legislación

En cuanto a su legislación, el Régimen Legal de Seguridad del Ciberespacio se aplica a las entidades de la Administración Pública, operadores de infraestructura crítica, operadores de servicios esenciales, proveedores de servicios digitales, así como cualquier otra entidad que utilice

redes y sistemas de información. A continuación, se presenta un gráfico en el que se recogen los hitos más relevantes a nivel legislativo³ en Portugal.

ENCUADRAMIENTO CRONOLÓGICO



Fuente: Quadro Nacional de Referência para a Cibersegurança (QNRCS), CNCS, 2020.

La [Ley n.º 46/2018](#), de 13 de agosto, establece el marco legal para la seguridad del ciberespacio, transponiendo la Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas para garantizar un alto nivel común de la seguridad de las redes y los sistemas de información en la Unión Europea. Esta ley exige que la Administración Pública, los Operadores de Infraestructura Crítica, los Operadores de Servicios Esenciales, los Proveedores de Servicios Digitales y cualquier otra entidad que utilice redes y sistemas de información cumplan con los requisitos de seguridad.

Además, el QNRCS cumple con la Estrategia Nacional de Seguridad del Ciberespacio, en su versión actual, aprobada mediante [Resolución del Consejo de Ministros n.º 14 92/2019](#) de mayo. La Estrategia se basa en el compromiso de profundizar la seguridad de las redes y la información, como forma de garantizar la protección y defensa del ciberespacio de interés nacional y promover su uso libre, seguro y eficiente por parte de todos los ciudadanos, empresas y demás entidades públicas y privadas.

Gracias al Reglamento de Ciberseguridad, la UE ha implantado un marco único de [certificación a escala de la UE](#) que generará confianza, aumentará el crecimiento del mercado de la ciberseguridad y facilitará el comercio en toda la UE. Este marco proporcionará un conjunto completo de reglas, requisitos técnicos, normas y procedimientos.

En Portugal, el Gabinete Nacional de Segurança avanza con el proceso de certificación de los sistemas de información y comunicación y ya ha certificado algunos productos y servicios. Ahora

³ La *Resolução do Conselho de Ministros n.º 36/2015* ya ha sido derogada, pero jugó un papel clave en el desarrollo legislativo de este sector.

está preparando la adaptación de la normativa europea para crear un **sello de ciberseguridad** que pretende aportar más confianza al mercado.

Pese a la existencia del marco único de certificación a escala de la UE, en Portugal **no existe** actualmente una **certificación o requisito especial** exigible (como es el caso de España, país firmante del [Acuerdo de Reconocimiento Mutuo de Certificados de Evaluación de la Seguridad en las Tecnologías Informáticas](#)) para poder ofrecer servicios de ciberseguridad, lo que facilita la entrada a este mercado.

El [estándar 25001](#) proporciona requisitos y recomendaciones para gestionar la evaluación y especificación de los requisitos del producto de *software*. La última versión de este estándar es del año 2014.

Además, no se ha identificado ninguna **barrera de entrada** significativa al mercado portugués.

5.3. Ayudas

- **Ayudas en España** para la internacionalización:
 - **ICEX** a través de sus programas de apoyo 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.
 - **Acuerdo ICEX-INCIBE**: INCIBE e ICEX tienen un acuerdo para la promoción del sector de la ciberseguridad español en el extranjero, en el marco del cual se han desarrollado y se desarrollarán actividades que incluyen misiones comerciales directas e inversas.
- **Ayudas europeas**:
 - **Banco Europeo de Inversiones (BEI)** financia proyectos de empresas europeas relacionados con los objetivos de crecimiento y desarrollo marcados por la UE, dentro de los cuales se encuentra la ciberseguridad, comentado en el apartado de oportunidades.
 - **Comisión Europea**, a través de la **European Union Agency For Cybersecurity (ENISA)**, Agencia de Ciberseguridad de la UE.

5.4. Tendencias del sector

[En su informe sectorial sobre ciberseguridad](#), *Fortune* señala las siguientes tendencias en el sector global de la ciberseguridad para el periodo 2020-2027:

- El incremento en popularidad de servicios basados en la **seguridad en la nube** está aumentando también los ciberataques a servidores *cloud*. Esto se debe a la creciente popularidad del uso de dispositivos que no son PC.
- Identifica las soluciones con enfoque **Endpoint Security** como el segmento de mayor crecimiento, a medida que continúa la tendencia a interconectar dispositivos externos de forma cada vez más compleja a redes corporativas.
- La implantación de la **tecnología 5G** en Portugal traerá consigo una nueva serie de vulnerabilidades, además de un incremento en el número de dispositivos *Internet of Things* que las empresas deberán proteger.

Gartner proyecta al cierre de 2021 un gasto mundial de [150,4 miles de millones de USD](#) en seguridad de la información y en tecnología y servicios de gestión de riesgos, con un crecimiento de 12,4 % respecto a 2020.

En la [encuesta](#) de la agenda de CIO (*Chief Information Officer*) de Gartner 2021, la ciberseguridad fue la principal prioridad para los nuevos gastos, con el 61 % de los más de dos mil CIO encuestados aumentando la inversión en seguridad cibernética o de la información en 2021. Los servicios de seguridad que incluyen consultoría, soporte de *hardware*, implementación y servicios subcontratados representan **la mayor categoría de gasto** en 2021, con casi 72.500 millones de USD a nivel global.

Son tales las buenas perspectivas de crecimiento del sector que, según [Cybercrime Magazine](#), se espera que para este año 2021 la industria de la ciberseguridad tenga una tasa de **desempleo del 0 %**, indicador inequívoco de la necesidad de trabajadores cualificados en este ámbito.

En cuanto a su **evolución**, la industria suministra un *input* básico para cualquier proceso de digitalización, lo que se traduce en tasas de crecimiento de cerca de dos dígitos a nivel global según distintos análisis:

Compañía	Crecimiento anual mundial	Período
IDC	9,4 %	2019-2023
Gartner	8,7 %	2018-2019
Statista	9 %	2019-2023
Fortune Business Insights	12 %	2021-2028

Fuente: IDC, 2019, Gartner, 2018, Statista, 2020, Fortune Business Insights, 2021.

De acuerdo con estas previsiones, la más optimista es la de [Fortune Business Insight](#), que proyecta un crecimiento del mercado de la seguridad cibernética de 165,78 billones de dólares en 2021 a 366.100 millones en 2028 a una tasa compuesta anual del 12,0 % durante el período 2021-2028.

Según [Gartner](#), se estima que el gasto de los usuarios finales en el mercado de la seguridad de la información y la gestión de riesgos crecerá a una tasa de crecimiento anual compuesta del 8,7 % desde 2018 hasta 2023 hasta alcanzar los 188,8 billones de dólares en moneda constante.

A nivel europeo, la **Estrategia de Ciberseguridad para la Década Digital**, que la Comisión Europea presentó a finales del año pasado tiene el objetivo de reforzar la resiliencia de Europa frente a las ciber amenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. También cabe destacar que, en diciembre de 2020, el Consejo y el Parlamento Europeo alcanzaron un acuerdo informal sobre una propuesta para crear el **Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad** respaldado por una Red de Centros Nacionales de Coordinación.

También es importante resaltar en el mercado portugués el consorcio de reciente creación **C-Hub: Cybersecurity DIH - Digital Cybersecurity Hub**, que integra el Centro Nacional de Ciberseguridad (CNCS) y otras cinco entidades, cuyo objetivo es convertirse en un **referente nacional y europeo** en la implantación de procesos de transformación digital con foco en las áreas de Ciberseguridad.

Para concluir, las perspectivas para los próximos años son de crecimiento del sector y en Portugal se espera que **la demanda aumente** sobre todo en compañías bancarias, financieras, relacionadas con el sector energético o sanitario, ya que manejan datos sensibles que pueden ser objeto de actividades relacionadas con el cibercrimen.

5.5. Ferias

Destacan las siguientes ferias en el ámbito de la ciberseguridad en Portugal:

- **WEB SUMMIT**: Esta feria de carácter internacional que es considerada el mayor evento tecnológico del mundo. Se celebra anualmente en Lisboa y la próxima edición tendrá lugar entre el 1 y el 4 de noviembre de 2021. Este evento reúne a las personas y empresas que redefinen la industria tecnológica global.
- **BSides Lisbon**: Es la conferencia técnica sobre ciberseguridad más destacada de Portugal. Tiene lugar anualmente en Lisboa y la próxima edición será de carácter presencial del 7 al 8 de abril de 2022. Se abordan los temas de la seguridad, ciberseguridad, seguridad de la información, seguridad operativa, seguridad de datos, protección de datos, etc. El evento se enorgullece de ser una organización sin fines de lucro y con una amplia participación voluntaria de la comunidad local de profesionales de la seguridad informática.
- **C-Days**: La Conferencia Anual de Ciberseguridad C-DAYS, organizada por el Centro Nacional de Ciberseguridad, es un momento decisivo para que tomadores de decisiones, profesionales, investigadores, estudiantes y sociedad civil debatan temas de ciberseguridad desde diferentes puntos de vista: estratégico, operativo y técnico. Tuvo lugar del 14 al 16 de



junio en Oporto y su próxima fecha aún está pendiente de confirmación.

Para más eventos relacionados con la ciberseguridad fuera de Portugal se puede consultar este enlace:

<https://www.csoonline.com/article/3155500/it-careers/the-cso-guide-to-top-security-conferences.html>

ICEX

6. Información adicional

6.1. Organismos relevantes

Entre los organismos más importantes en el ámbito de la ciberseguridad de Portugal, destacan principalmente:

- Centro Nacional de Cibersegurança- [CNCS](#)
- Rede Nacional [CSIRT](#) – Centro Nacional de Cibersegurança
- [APDC](#) – Associação Portuguesa para o Desenvolvimento das Comunicações
- APCIBER – Associação para a Promoção da Cibersegurança e da Proteção de Dados
- [APPD](#) – Associação Portuguesa de Proteção de Dados

Otras entidades asociadas al CNCS:

- ✓ [APAV](#) - Associação Portuguesa de Apoio à Vítima
- ✓ [AP2SI](#) - Associação Portuguesa para a Promoção da Segurança da Informação
- ✓ [Centro de Ciberdefesa](#)
- ✓ [CNPD](#) - Comissão Nacional de Proteção de Dados
- ✓ [DGPDN](#) - Direção-Geral de Política de Defesa Nacional
- ✓ [DGPJ](#) - Direção-Geral da Política de Justiça
- ✓ [Gabinete Cybercrime](#) da Procuradoria-Geral da República
- ✓ [UNC3T](#) - Polícia Judiciária - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
- ✓ [SIS](#) - Serviço de Informações de Segurança
- ✓ [SIED](#) - Serviço de Informações Estratégicas de Defesa

6.2. Fuentes de interés

Las siguientes fuentes resultan de interés para recabar más información sobre el sector:

- Statista: <https://www.statista.com/>
- [The Global Cybersecurity Index \(GCI\)](#) de ITU, Naciones Unidas.
- [Revista Computer World](#), de IDG Portugal.
- [Revista Security Magazine](#), Portugal.
- [Hiscox Cyber Readiness Report 2021](#), Hiscox Group.
- [Quadro Nacional de Referência para a Cibersegurança](#), Centro Nacional de Cibersegurança, 2021.
- [Relatório Anual de Segurança Interna](#), Sistema de Segurança Interna, 2020.
- [Relatório Cibersegurança em Portugal. Riscos e Conflitos](#). Centro Nacional de Cibersegurança, 2021.
- [Security Outcomes Study](#). CISCO, 2020.

ICEX

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



ICEX España
Exportación
e Inversiones