EM ESTUDIO DE MERCADO

2021

ICEX España Exportación e Inversiones

El mercado de la ciberseguridad en Bélgica

Oficina Económica y Comercial
de la Embajada de España en Bruselas

EM ESTUDIO DE MERCADO

15 de diciembre de 2021
Bruselas

Este estudio ha sido realizado por
Dorleta Velázquez González del Herrero

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

http://belgica.oficinascomerciales.es

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

NIPO: 114-21-009-9

Índice

1. Resumen ejecutivo

Este informe presenta un estudio de mercado de un sector clave en Bélgica: la ciberseguridad. El objetivo es analizar la situación actual del sector y, más específicamente, las oportunidades de negocio existentes para empresas españolas que consideren introducirse en el sector de la ciberseguridad en Bélgica.

Definición de sector de la ciberseguridad

La Unión Internacional de Telecomunicaciones (UIT)[1] define la ciberseguridad[2] como «el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno».

La concienciación en el campo de la ciberseguridad es cada vez mayor, la responsabilidad de la seguridad de la red no solo recae en los gobiernos, sino también en las empresas y usuarios[3].

La Estrategia de ciberseguridad belga 2021-2025

La Estrategia de ciberseguridad belga 2.0 (2021-2025), publicada por el Centro de Ciberseguridad de Bélgica (CCB), busca posicionar a Bélgica como uno de los países menos vulnerables de Europa en el entorno cibernético en 2025. Bélgica aboga por un ciberespacio abierto, libre y seguro.

En el contexto actual, con el reciente aumento exponencial de los ataques al entorno cibernético, la Evaluación Nacional de Riesgos de Bélgica 2018-2023 del Centro de crisis Nacional, considera al sector cibernético como uno de los principales focos de riesgo de los próximos años. Dentro de riesgos cibernéticos, la criminalidad cibernética (ciberdelitos) y el hacktivismo se identifican como los mayores riesgos y son considerados riesgos prioritarios nacionales.[4]

Ecosistema de la ciberseguridad belga

Bélgica, además de ser un país con 30.528 km^2, 11,5 millones de habitantes y un PIB de 476.000 millones de euros, con sus respectivas necesidades para particulares, administraciones y empresas, acoge a organismos internacionales, entre los que destacan la OTAN o la Comisión Europea, que tienen su sede principal en el territorio.

[1] Organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación.
[2] Recomendación UIT-T X.12054 , Resolución 181 (Guadalajara/2010) http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx
[3] Spanish Cibersecurity Companies Catalogue 2020 Edition_INCIBE
[4] Centre de crise National (2019). Evaluation des risques nationaux: cyber.

Sector público

El sector público belga tiene una estructura gubernamental compleja que no facilita una política de ciberseguridad coordinada para los departamentos gubernamentales.

El Centro de Ciberseguridad de Bélgica (CCB) es el eje central de la ciberseguridad belga. La seguridad y la ciberseguridad son asuntos federales y se tratan a nivel nacional. Sin embargo, existen instituciones públicas tanto regionales como nacionales, que tienen un impacto directo sobre la ciberseguridad y que están vinculadas al sector.

Desde distintos organismos de gobierno del país se coordina la seguridad estatal, su asociación público-privada, los Proveedores de Servicios de Internet, otros sectores del Gobierno y otras organizaciones. Asimismo, consolidan a las empresas belgas a través de servicios e información, y brindan valor agregado a través de *think tanks*, intentan identificar nuevas tendencias y nuevos desafíos, y ofrecen soluciones innovadoras.

Sector privado

El sector privado es un actor clave en el ciberespacio. Su experiencia y la innovación tecnológica que llevan a cabo en la ciberseguridad, son cruciales para permitir que los organismos públicos respondan eficazmente a las amenazas cibernéticas.

El mercado de la ciberseguridad local es pequeño pero maduro, pudiendo encontrar que, algunos de los mayores competidores del mercado se quedan con hasta el 90 % de la cuota de mercado. No hay muchas nuevas grandes empresas, las nuevas empresas tienden a ser pequeñas y muy especializadas. Proximus y Telenet tienden a comprar pequeñas empresas que tienen éxito.

Organismos internacionales

Bélgica es el hogar de muchas instituciones internacionales, entre las que se encuentran la Comisión Europea y la OTAN (Organización del Tratado del Atlántico Norte). Son numerosas las licitaciones en materia de ciberseguridad licitadas por estos organismos La ciberseguridad es un campo transversal en la mayoría de las licitaciones del campo de la informática.

Demanda

Las empresas y los organismos públicos son cada vez más conscientes de esta necesidad y trabajan para mejorar las vulnerabilidades de sus sistemas. El porcentaje de empresas que utiliza cualquier medida de ciberseguridad alcanza ya el 74 % en Bélgica (por debajo de la media de la Unión Europea que se sitúa en el 77 %).

El número de ataques cibernéticos se ha multiplicado en los últimos años. Se ha pasado, en el ámbito de los ataques contra la ciberseguridad, de 47.740 ataques en 2016 a 100.412 ataques en 2020 (o lo que es lo mismo, un incremento del 110 % en los últimos 5 años).

El 50% de las organizaciones belgas no tiene una estrategia de ciberseguridad activa: muchas empresas todavía no tienen desarrollado su sistema de TI. Asimismo, **las consecuencias de un incidente suelen ser graves**: el 92 % de las empresas que ya habían experimentado un ciberincidente están muy preocupadas por ser víctimas por segunda vez. De las empresas que no han sido atacadas, el 18 % no están preocupadas en absoluto.

España, líder mundial en ciberseguridad

En la última versión del Índice Global de Ciberseguridad (IGC), publicado por la Unión Internacional de Telecomunicaciones (UTI) en 2020, España se coloca a la cabeza mundial en ciberseguridad[5], como **cuarta potencia internacional en ciberseguridad y segunda a nivel de la Unión Europea**. Bélgica ocupa la decimonovena posición en el ranking.

Las empresas españolas que han tenido contacto con el sector de la ciberseguridad belga prefieren entrar en el mercado belga a través de licitaciones, especialmente de organismos internacionales. Algunas de estas empresas utilizan filiales belgas para su entrada en el mercado.

Perspectivas del sector

El futuro de la ciberseguridad en Bélgica de los próximos años viene marcado por los seis objetivos estratégicos que recoge la Estrategia de ciberseguridad belga 2.0 (2021-2025) para responder a los desarrollos tecnológicos y satisfacer la gran necesidad de proteger a la población, los sectores público y privado y los sectores vitales: Fortalecer el entorno digital y aumentar la confianza en éste – Preparar a usuarios y administradores de los ordenadores y redes – Proteger a las organizaciones de interés vital de todas las amenazas cibernéticas – Responder a las amenazas cibernéticas – Mejorar las colaboraciones público-privadas y académicas – Claro compromiso internacional

Oportunidades

En relación con los objetivos de la Estrategia de ciberseguridad belga 2.0 (2021-2025) se establecen 3 **prioridades de ciberseguridad** para Bélgica:

- Sensibilización y formación de los empleados.
- Inversión en tecnología.
- Desarrollo de una estrategia de ciberseguridad:

En este contexto, se encuentran las siguientes oportunidades para las empresas de ciberseguridad en Bélgica:

[5] DSN (2021). España, a la cabeza mundial en Ciberseguridad.

Empresas conscientes de la importancia de la ciberseguridad

Digitalización COVID-19 y trabajo remoto

Internet de las cosas (IdC) y nuevas generaciones de redes fijas y móviles (5G).

Servicios de administrador: centros de operaciones de seguridad

Seguridad humana:
(i) *phishing*
(ii) educación
(iii) ciberseguridad centrada en las personas

La nube y los problemas de seguridad

Machine learning (aprendizaje automático)

2. Definición del sector

La Unión Internacional de Telecomunicaciones (UIT)[6] define la ciberseguridad[7] como «el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, servicios/aplicaciones, sistemas de comunicaciones, comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno.

Las propiedades de seguridad incluyen una o más de las siguientes:

- **disponibilidad**;
- **integridad**, que puede incluir la autenticidad y el no repudio;
- y **confidencialidad**.»

Las perturbaciones generadas en los sistemas y las pérdidas derivadas de la amenaza a la información digital y red de comunicaciones son de naturaleza muy diversa. En muchas ocasiones los ataques son difíciles de cuantificar y, a veces, van más allá del mero valor monetario.

El Observatorio Nacional de Tecnología y Sociedad (ONTSI), en colaboración con el Instituto Nacional de Ciberseguridad de España (INCIBE), realizó una «Caracterización del subsector y el mercado de la ciberseguridad». En este estudio, se catalogan como críticos, dentro del sector de la ciberseguridad, los incidentes que pueden causar degradación de los servicios para un gran número de usuarios, implicar una grave violación de la seguridad de la información, afectar a la integridad física de las personas, causar importantes pérdidas económicas, ocasionar daños irreversibles a los recursos de la organización, incurrir en delitos y/o sanciones reglamentarias u ocasionar un daño muy grave en la imagen de la organización[8].

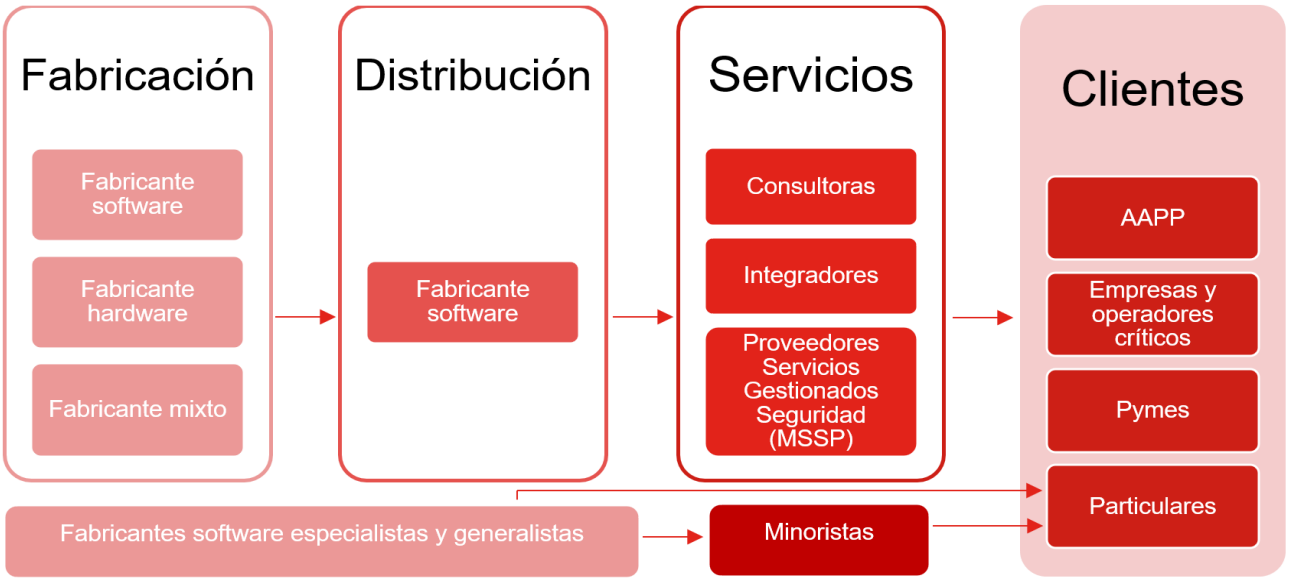
En este contexto, resulta primordial tanto para los gobiernos como para las empresas implementar y desarrollar una metodología que sirva para combatir los desafíos que surgen como consecuencia de estos peligros.

[6] Organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación.
[7] Recomendación UIT-T X.12054 , Resolución 181 (Guadalajara/2010) http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx
[8] ONTSI-INCIBE (2015). Caracterización del subsector y el mercado de la ciberseguridad.

2.1. Cadena de valor de la ciberseguridad

La concienciación en el campo de la ciberseguridad es cada vez mayor, la responsabilidad de la seguridad de la red no solo recae en los gobiernos, sino también en las empresas y usuarios[9].

CADENA DE VALOR DE LA CIBERSEGURIDAD



Fuente: ONTSI-INCIBE (2015). Caracterización del subsector y el mercado de la ciberseguridad.

En cuanto a la clasificación de los productos de seguridad se diferencian los siguientes tipos:

TIPOS DE SOLUCIONES DE CIBERSEGURIDAD

Soluciones de prevención	• Anti-malware • Anti-fraude • Soluciones de prevención de fugas de información • Protección de las comunicaciones • Seguridad en dispositivos móviles
Soluciones de control	• Auditoría técnica • Soluciones de certificación • Soluciones de cumplimiento legal • Soluciones de control de acceso y autentificación
Soluciones de mitigación	• Soluciones de contingencia y continuidad • Soluciones de inteligencia de seguridad

Fuente: ONTSI-INCIBE (2015). Caracterización del subsector y el mercado de la ciberseguridad.

[9] Spanish Cibersecurity Companies Catalogue 2020 Edition_INCIBE

2.2. Mapa mundial de la ciberseguridad

El Índice Global de Ciberseguridad (IGC)[10], publicado por la Unión Internacional de Telecomunicaciones (UIT), mide y evalúa el compromiso local de los países con la ciberseguridad a través de 5 pilares que conformarán su puntuación general:

PILARES DEL ÍNDICE GLOBAL DE CIBERSEGURIDAD

Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de capacidades	Medidas de cooperación
Legislación para la homogeneización de las buenas prácticas en ciberseguridad y la lucha contra ataques cibernéticos nacionales e internacionales. Evaluación: número de instituciones y marcos legales existentes en el sector.	Organismo nacional que imponga medidas mínimas de ciberseguridad y mecanismos para una lucha efectiva contra los ciberataques. Evaluación: número de mecanismos del país para enfrentar a los ciberataques.	Organizaciones y agencias que implementen estrategias nacionales de ciberseguridad. Evaluación: número de instituciones y estrategias nacionales relacionadas con la ciberseguridad.	Concienciación ciudadana y formación y promoción de expertos en ciberseguridad a nivel nacional. Evaluación: número de programas públicos de ciberseguridad: I+D+i, educativos y formación profesional y expertos certificados.	Cooperación nacional e internacional entre países y/o entidades para una lucha más eficaz contra ataques cibernéticos. Evaluación: número de colaboraciones y programas de cooperación suscritos.

COMPROMISOS GLOBALES DE INDICADORES ESPECÍFICOS POR PILAR

	Medición de las leyes y regulaciones sobre ciberdelito y ciberseguridad	**Medidas legales**	
		167	Países con algún tipo de legislación sobre ciberseguridad
		133	Normativa de protección de datos
		97	Regulaciones de infraestructura crítica
	Medición de la implementación de capacidades técnicas a través de agencias nacionales y sectoriales	**Medidas técnicas**	
		131	Equipos de Respuesta ante Emergencias Informáticas (CSIRT[11]) activos
		104	Compromisos en Equipos de Respuesta ante Emergencias Informáticas regionales
		101	Mecanismos de denuncia para la protección infantil *online*
	Medición de las estrategias y organizaciones nacionales implementando la ciberseguridad	**Medidas organizativas**	
		127	Estrategias nacionales de ciberseguridad
		136	Agencias de ciberseguridad
		86	Estrategias e iniciativas de protección infantil *online* comunicadas
	Medición de campañas de concienciación, formación, educación e incentivos de desarrollo de capacidades en ciberseguridad	**Desarrollo de capacidades**	
		142	Países que llevan a cabo iniciativas de concienciación cibernética
		94	Países con programas de I + D en ciberseguridad
		98	Países que informaron tener industrias nacionales de ciberseguridad
	Medición de las asociaciones entre agencias, empresas y países	**Medidas de cooperación**	
		166	Países involucrados en asociaciones público-privadas de ciberseguridad
		90	Países con acuerdos bilaterales de ciberseguridad
		112	Países con acuerdos multilaterales de ciberseguridad

Fuente: UIT (2020). Global Cybersecurity Index 2020.

[10] UIT (2020). Global Cybersecurity Index 2020.

[11] Computer Security Incident Response Team (CSIRT).

En este ranking, Bélgica tiene una puntuación de 96,25 sobre un total de 100 puntos. Se posiciona como el 26º país del mundo en compromiso con la seguridad, por detrás de países como Estados Unidos, Reino Unido, Singapur, España, Rusia, Japón, Francia, India, Luxemburgo o Holanda, entre otros. Tomando los países de la UE-28[12], Bélgica se sitúa en la décima posición.

RANKING DEL ÍNDICE GLOBAL DE CIBERSEGURIDAD EN LA UE-28 EN 2020

País UE-28	Puntuación	Ranking
Reino Unido	99,54	1
Estonia	99,48	2
España	98,52	3
Lituania	97,93	4
Francia	97,60	5
Luxemburgo	97,41	6
Alemania	97,41	7
Portugal	97,32	7
Letonia	97,28	8
Países Bajos	97,05	9
Bélgica	96,25	10
Italia	96,13	11
Finlandia	95,78	12
Grecia	93,98	13

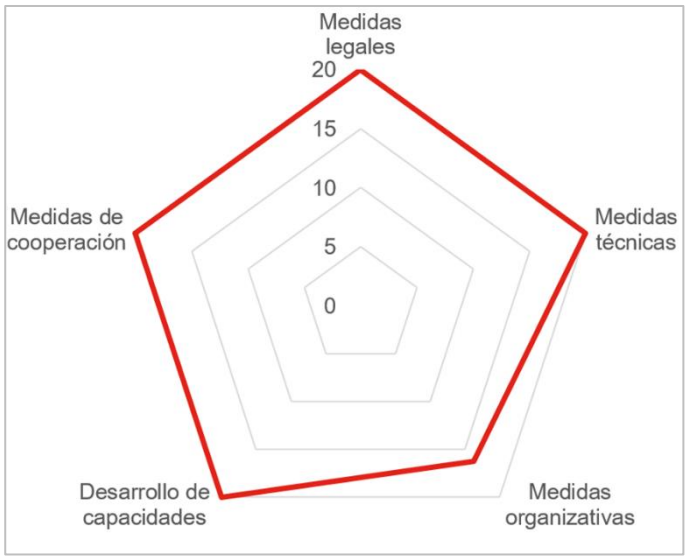
País UE-28	Puntuación	Ranking
Austria	93,89	14
Polonia	93,89	15
Dinamarca	92,60	16
Croacia	92,53	17
Eslovaquia	92,36	18
Hungría	91,28	19
Chipre	88,82	20
Suecia	86,97	21
Irlanda	85,86	22
Malta	83,65	23
Rumania	76,28	24
Eslovenia	74,93	25
República Checa	74,37	26
Bulgaria	67,38	27

Fuente: Elaboración propia a partir de datos de UIT (2020). Global Cybersecurity Index 2020.

Dentro de la región europea destaca el desempeño de Bélgica:

DESEMPEÑO DE BÉLGICA EL ÍNDICE GLOBAL DE CIBERSEGURIDAD EN 2020

Puntuación total y por pilar



Nivel de desarrollo:
País Desarrollado

Área(s) de fortaleza relativa
Jurídica, técnica, Medidas de cooperación, Desarrollo de Capacidades

Área(s) de crecimiento potencial
Medidas organizativas

Puntuación total	96,25
Medidas legales	20,00
Medidas técnicas	20,00
Medidas organizativas	16,25
Desarrollo de capacidades	20,00
Medidas de cooperación	20,00

Fuente: UIT (2020). Global Cybersecurity Index 2020.

[12] Para la comparativa de los datos respecto a la media de la UE, se van a tomar los datos UE28 que incluyen a Reino Unido.

2.3. La Estrategia de ciberseguridad belga 2021-2025[13]

Bélgica busca posicionarse, en 2025, como uno de los países menos vulnerables de Europa en el entorno cibernético. Una de las principales acciones para el cumplimiento de este objetivo ha sido el desarrollo de la Estrategia de ciberseguridad belga 2.0 (2021-2025), publicada por el Centro de Ciberseguridad de Bélgica (CCB) en mayo de 2021. Este documento establece una versión actualizada[14] de la Estrategia de Ciberseguridad Nacional de Bélgica.

El objetivo de esta Estrategia Nacional de Ciberseguridad es salvaguardar las capacidades de los servicios, bienes, personas y capital a través de las fronteras.

2.3.1. Importancia estratégica – Evaluación de riesgos

Bélgica aboga por un ciberespacio abierto, libre y seguro. Sin embargo, en los últimos años los ataques al entorno cibernético han aumentado exponencialmente. La Evaluación Nacional de Riesgos de Bélgica 2018-2023 del Centro de crisis Nacional, considera al sector cibernético como uno de los principales focos de riesgo de los próximos años. Dentro de riesgos cibernéticos, la criminalidad cibernética (ciberdelitos) y el hacktivismo se identifican como los mayores riesgos y son considerados riesgos prioritarios nacionales.[15]

Como ejemplo de las posibles consecuencias de un ataque cibernético de este tipo, podemos analizar lo ocurrido en 2017 con el *ransomware* WannaCry. El *malware* se extendió, en muy poco tiempo, a más de 150 países y supuso la interrupción de numerosas actividades comerciales, convirtiéndose en el incidente cibernético más caro de la historia.

Asimismo, debemos considerar que un nuevo ataque cibernético de estas magnitudes, más si es motivado geopolíticamente, podría tener graves y directas consecuencias en la red de distribución eléctrica, en el sistema bancario o en disponibilidad de todos los servicios *online*, entre otros. Adicionalmente, los ciberataques podrían utilizarse para potenciar un ataque físico generando así una amenaza híbrida que potenciaría los ataques y generaría una atmosfera de caos.

Por último, aquellos eventos con un mayor riesgo de ataque cibernético, como puede ser una cumbre internacional o unas elecciones, requerirán de una evaluación de riesgo específica.

En este contexto, la estrategia define metas nacionales para proteger el paisaje cibernético belga, aun cuando este se halla en constante cambio. Se busca construir y garantizar una seguridad en el ciberespacio, para lo que es esencial la colaboración de todos los actores belgas. Se realizará un enfoque general de la ciberseguridad que implique y responsabilice a todos los actores.

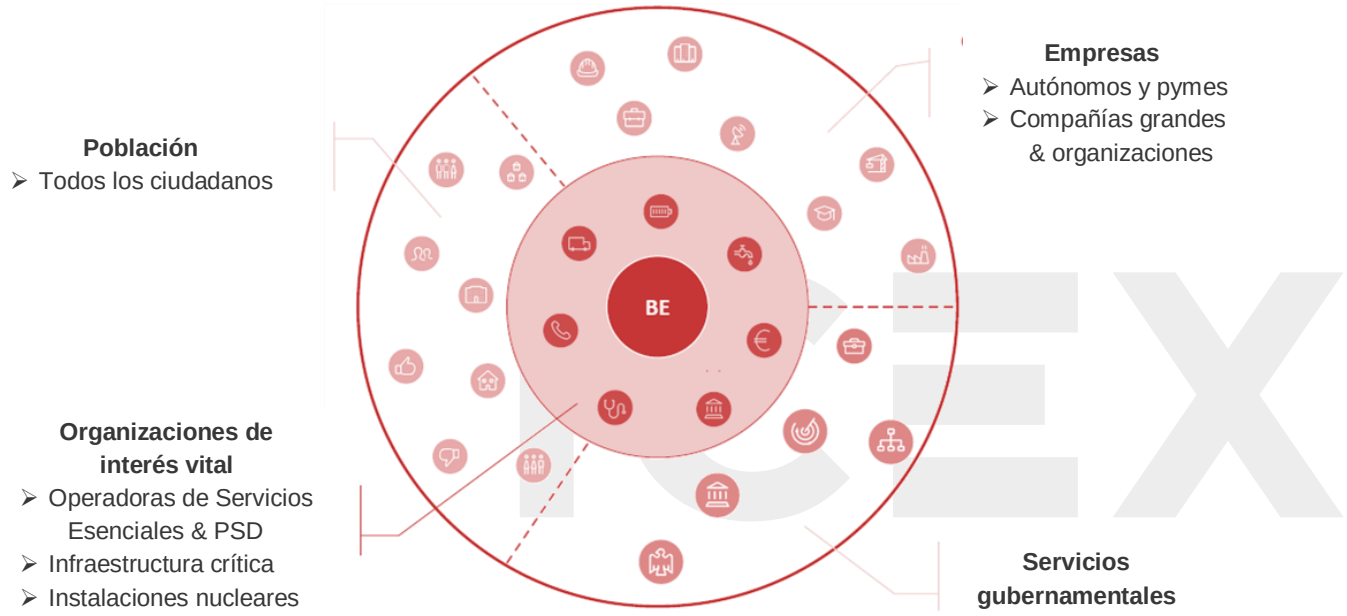
[13] Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).
[14] La primera estrategia de ciberseguridad belga data de 2012.
[15] Centre de crise National (2019). Evaluation des risques nationaux: cyber.

2.3.2. Actores involucrados en la ciberseguridad

Actores de la ciberseguridad belga

La estrategia establece que la ciberseguridad no es únicamente responsabilidad del Gobierno, sino que es un esfuerzo colaborativo al que deben contribuir todas las partes involucradas. Se destaca el papel del esfuerzo global como clave para lograr mejoras en la seguridad general.

PRINCIPALES ACTORES DE LA CIBERSEGURIDAD EN BÉLGICA EN 2021



Población	Los ciudadanos son los principales responsables de proteger sus dispositivos. Esto incluye teléfonos inteligentes, computadoras portátiles, tabletas, pero también las aplicaciones y los datos que contienen. Protegerlos y usarlos de manera adecuada dificulta los ciberataques. Se han creado plataformas como Safeonweb.be y R!SK-iNFO.be para que la población conozca las principales amenazas cibernéticas y se involucre en la seguridad del entorno cibernético.
Empresas	Las empresas[16] juegan un papel importante en la protección de su infraestructura y datos. En este grupo se incluyen instituciones educativas y proveedores de productos de seguridad. Los productos de ciberseguridad (firewalls, análisis de virus, cifrado u otro software y hardware) fortalecen la seguridad de los sistemas de IT y reducen la probabilidad de incidentes. • Invertir en estos productos, apoyar a los proveedores y facilitar su uso a los usuarios. • Desarrollar una certificación de ciberseguridad[17] que a la empresa le permita demostrar que está protegida frente a las ciberamenazas más comunes (ventaja competitiva).
Servicios gubernamentales	Bélgica tiene una estructura gubernamental compleja que no facilita una política de ciberseguridad coordinada. La seguridad y la ciberseguridad son asuntos federales y se tratan a nivel nacional. El Centro de Ciberseguridad de Bélgica (CCB) desarrolla consejos y directrices.
Organizaciones de interés vital	Entidades públicas y privadas que brindan un servicio esencial (los incidentes que le afectan pueden tener un impacto nacional a gran escala.): operadores de infraestructuras críticas y servicios esenciales, proveedores de servicios digitales e instalaciones nucleares[18].

Fuente: Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).

[16] Destacan las pymes con menos de 250 empleados, que constituyen más del 99 % del tejido empresarial belga.
[17] En 2019, la Unión Europea también lanzó un marco de certificación de ciberseguridad en este sentido.
[18] La determinación inicial de quiénes son las Organizaciones de Vital Interés es realizada por las autoridades sectoriales, en consulta con el Centro Nacional de Crisis y el CCB. Pretende ser evolutiva e incluye los sectores de energía, movilidad, telecomunicaciones, finanzas, agua potable, salud pública, proveedores de servicios digitales y gobierno.

Actores amenaza

Es fundamental comprender y monitorear quiénes son los actores de amenazas más importantes. En la Estrategia de ciberseguridad belga 2.0 los siguientes actores son considerados la mayor amenaza para el estado y la población belga: ciberdelincuentes, servicios de inteligencia y militares extranjeros, grupos terroristas y hacktivistas.

PRINCIPALES ACTORES DE LAS AMENAZAS A LA CIBERSEGURIDAD EN BÉLGICA

Servicios de inteligencia y militares extranjeros

Los países tienen muchas armas físicas, un ciberespacio ofensivo e inteligencia con la que infligir daño económico a otros estados, con miras a la inestabilidad política y al debilitamiento de sus defensas.

Terrorismo

Los ciber terroristas utilizan Internet para cometer actos de violencia con el fin de obtener una ventaja política e infundir miedo en la población.

Hacktivismo

El hacktivismo consiste en realizar actividades cibernéticas intencionales con la intención de promover una agenda política, una creencia religiosa o una ideología social

Ciberdelincuencia

El objetivo de los ciberdelincuentes es hacer un mal uso de las computadoras, Internet o las redes para obtener ganancias financieras.

Fuente: Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).

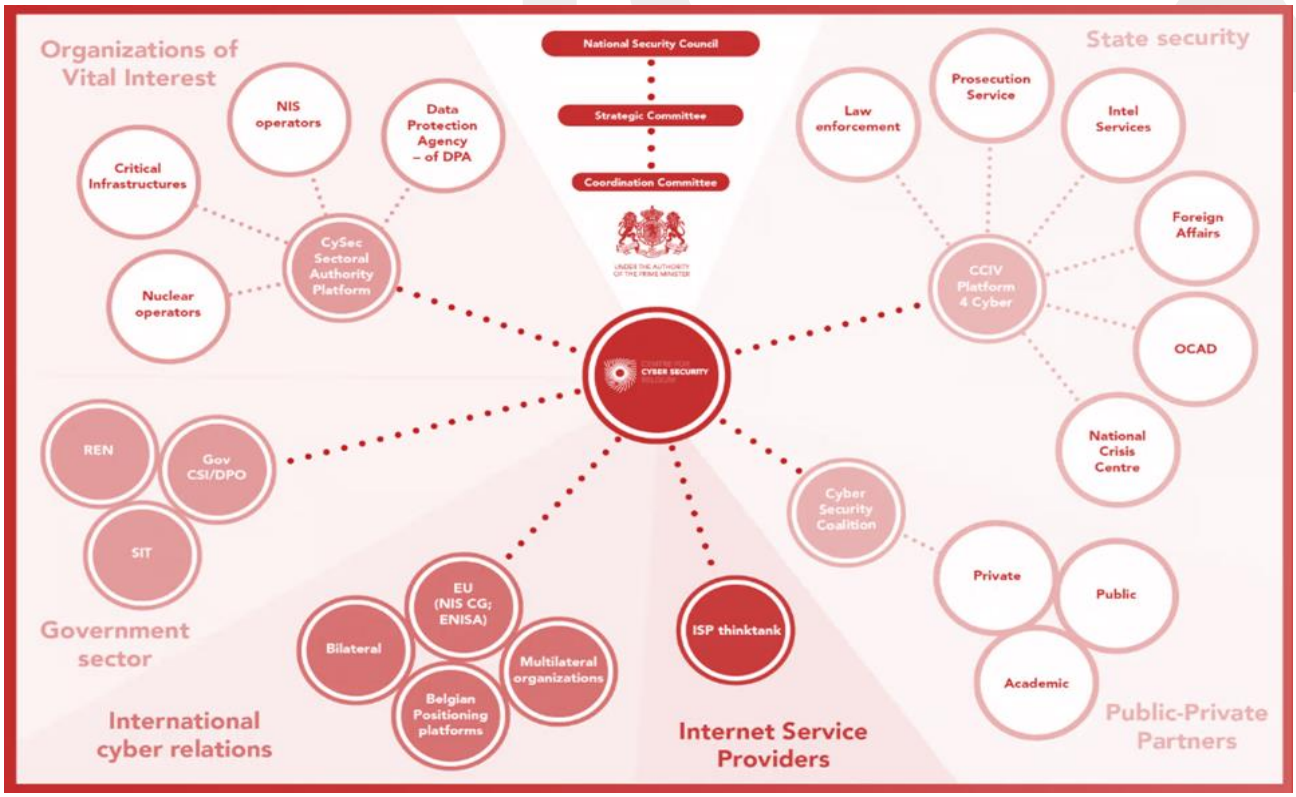
3. Oferta – Análisis de competidores

Como hemos visto en el apartado anterior, el ecosistema de la ciberseguridad belga está compuesto por diversos actores, públicos y privados, que constituyen un mercado en el que conviven particulares, asociaciones, empresas y administraciones, entre otros.

Asimismo, cabe destacar que Bélgica, además de ser un país con 30.528 km^2, 11,5 millones de habitantes y un PIB de 476.000 millones de euros, con sus respectivas necesidades para particulares, administraciones y empresas, acoge a organismos internacionales, entre los que destacan la OTAN o la Comisión Europea, que tienen su sede principal en el territorio.

La colaboración entre los distintos actores es un factor clave para «prevenir, reducir, manejar y monitorear las amenazas e incidentes cibernéticos. El conocimiento sobre ciberseguridad y la evolución de la ciberamenaza se comparte entre las agencias de seguridad relevantes, autoridades públicas y los sectores privado y académico a través de plataformas nuevas o existentes»[19].

MAPA DE LA CIBERSEGURIDAD EN BÉLGICA EN 2021



Fuente: Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).

[19] Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).

3.1. El mercado de la ciberseguridad belga

El tamaño limitado del mercado facilita un gran dinamismo y que todos los actores se conozcan. Las regiones de Flandes y del Brabante Valón son las más dinámicas, mientras que algunas áreas de Valonia, como Charleroi o Luxemburgo, no tienen representatividad en el sector.

En el sector de la ciberseguridad, la escena local está apoyada por una gran cantidad de valor añadido proveniente del Gobierno, lo que lo convierte en uno de los principales actores del país.

De este modo, las instituciones públicas y privadas configuran el mapa de la ciberseguridad belga.

3.1.1. Sector público

Existe un compromiso, plasmado en la Estrategia de ciberseguridad belga 2021-2025, para apoyar, desde el sector público, a los actores públicos y privados en la protección de sus redes.

Este impulso a la ciberseguridad se ha acelerado en los últimos años debido a las medidas que ha ido adoptando, desde el año 2020, el Gobierno belga frente a la crisis sanitaria entre las que destaca el teletrabajo obligatorio para aquellas actividades en las que no sea esencial el contacto.

Bélgica tiene una estructura gubernamental compleja que no facilita una política de ciberseguridad coordinada para los departamentos gubernamentales. En su organización político-administrativa, se divide en tres niveles: el Estado Federal, las Regiones (Flandes, Valonia y Bruselas Capital) y las Comunidades (neerlandófona, francófona y germanófona). El gobierno federal cuenta con servicios horizontales, verticales y programáticos. Las regiones y comunidades tienen ministerios y direcciones. En total hay 7 parlamentos y 3 lenguas oficiales.

La apuesta que realiza el Gobierno belga por la ciberseguridad se gestiona a través del «*Centre for Cybersecurity Belgium* (CCB)». El Centro de Ciberseguridad de Bélgica (CCB) desarrolla consejos y directrices que están disponibles para todos los departamentos gubernamentales. La seguridad y la ciberseguridad son asuntos federales y se tratan a nivel nacional.

El CCB, con nombramiento oficial del Gobierno a través del Consejo de Seguridad Nacional belga, es uno de los principales actores de la cadena de valor de la ciberseguridad en Bélgica.

Con el CCB como eje central de la ciberseguridad belga, desde distintos organismos de gobierno del país se coordina la seguridad estatal, su asociación público-privada, los Proveedores de Servicios de Internet, otros sectores del Gobierno y otras organizaciones. Asimismo, consolidan a las empresas belgas a través de servicios e información, y brindan valor agregado a través de *think tanks*, intentan identificar nuevas tendencias y nuevos desafíos, y ofrecen soluciones innovadoras.

En este apartado se recogen las principales instituciones públicas belgas, tanto regionales como nacionales, que tienen un impacto directo sobre la ciberseguridad o que están vinculadas al sector.

INSTUCIONES PÚBLICAS Y SU ROL EN LA CIBERSEGURIDAD BELGA

Organismos Y Organizaciones Nacionales

Nombre	Información de contacto	Rol en materia de seguridad de la información
CCB	https://ccb.belgium.be/en Centre for Cybersecurity Belgium (CCB) Rue de la Loi 18, 1000, Bruselas +32 2 501 02 11 info@ccb.belgium.be	El Centro de Ciberseguridad de Bélgica (CCB) es la autoridad nacional de ciberseguridad de Bélgica[20]. El CCB supervisa, coordina y monitorea la aplicación de la estrategia belga de ciberseguridad. Mediante un intercambio de información óptimo, las empresas, el gobierno, los proveedores de servicios esenciales y la población pueden protegerse adecuadamente.
NCCN	https://centredecrise.be/fr National Crisis Centre (NCCN) Rue Ducale 53,1000, Bruselas https://centredecrise.be/fr/contact	El Centro de Crisis (NCCN), analiza continuamente los riesgos nacionales clave (incluidos los riesgos cibernéticos), brinda apoyo legal y organizacional a autoridades sectoriales para la identificación de infraestructuras críticas y servicios esenciales y realiza análisis de riesgo sobre cuestiones especiales. El NCCN, junto con el CCB, gestiona la organización y coordinación del Plan de Emergencia Cibernética a nivel nacional (conjuntamente responsables de la gestión de crisis). La NCCN organiza y dirige las comunicaciones en caso de una cibercrisis nacional. El servicio de guardia 24/7 de la NCCN garantiza la disponibilidad de CERT.be, que brinda soporte de primera línea para incidentes y crisis nacionales.
CERT.be	www.cert.be Computer Emergency Response Team (CERT.be) Avenue Louise 231 1050 Bruselas +32 2 790 33 33 cert@cert.be	El Equipo federal de respuesta ante emergencias informáticas, o CERT.be, es el servicio operativo del Centro de seguridad cibernética de Bélgica (CCB). La tarea de CERT.be es detectar, observar y analizar problemas de seguridad en línea e informar a varios grupos objetivo en consecuencia. El CERT.be también aconseja a los ciudadanos y empresas sobre la manera de utilizar internet con total seguridad.
Autoridades sectoriales	https://business.belgium.be/	Las autoridades sectoriales en Bélgica son responsables de la identificación, estandarización e inspecciones de Operadores de Servicios Esenciales: energía, transporte, finanzas, infraestructura digital, atención médica y agua potable, junto con servicios digitales como servicios de computación en la nube, motores de búsqueda en línea y mercados en línea. El CCB y el NCCN tienen un papel asesor importante en esto.
VSSE	https://www.vsse.be/fr Veiligheid van de staat Sûreté de l'état +32 2 205 62 11 info@vsse.be	El servicio de seguridad e inteligencia civil belga (VSSE), es responsable de garantizar la seguridad del país previniendo riesgos de seguridad, asesorando a las autoridades políticas, administrativas, judiciales y militares y recopilar, analizar y procesar datos sobre actividades que puedan amenazar la seguridad o el potencial científico y económico belga. El VSSE se relaciona y recopila información de organismos extranjeros, y comparte la información recibida tanto como sea posible con CERT.be y con otros socios relevantes.
Ministerio de Defensa	https://www.mil.be/ Ministry of Defense (Ministerie van Defensie) Blok 4, Eversestraat 1, 1140 Brussel +32 08 003 33 48	El Ministerio de Defensa está desarrollando una estrategia cibernética, un plan de políticas y las capacidades necesarias para respaldar las operaciones militares y de inteligencia desde y en el dominio cibernética: proteger la infraestructura vital de ciberataques y, si es necesario, llevar a cabo un contraataque.
Servicio Público Federal de Relaciones Exteriores	https://diplomatie.belgium.be/en Service public fédéral Affaires étrangères Rue Petits Carmes 15, 1000 Bruselas +32 2 501 81 11s	Es el punto de contacto internacional a nivel diplomático, (a nivel bilateral y de las organizaciones multilaterales). Ofrece su experiencia en el entorno de una red internacional a las autoridades competentes (CCB), para la observación y análisis de problemas de seguridad online (ciberamenazas, vulnerabilidades en sistemas TIC o ciberincidentes).

[20] Es el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) nacional

NSA	https://www.nvoans.be/en National Security Authority (NSA) Rue des Petits Carmes 15, 1000, Bruselas +32 2 501 45 42 nvo-ans@diplobel.fed.be	La Autoridad de Seguridad Nacional (NSA) es la principal responsable de la tramitación administrativa de las solicitudes y la entrega de los certificados de seguridad (datos más sensibles o información "clasificada"). Desarrollo de productos que puede llevar la seguridad de la información clasificada (pública y privada) en el dominio cibernético al siguiente nivel. Análisis de riesgo, amenazas e impacto de organizaciones vitales y medidas de seguridad de sus sistemas de información.
CUTA	https://cuta.belgium.be/ Coordination Unit for Threat Analysis (CUTA) https://cuta.belgium.be/contact/	La Unidad de Coordinación de Análisis de Amenazas (CUTA) procesa toda la información e inteligencia relevante sobre terrorismo, extremismo y radicalización problemática. En el caso de ciberamenazas (potencialmente) relacionadas con grupos terroristas o extremistas o hacktivistas (ideológicos o religiosos), CUTA puede realizar un análisis de amenazas para el NCCN en cooperación con sus agencias asociadas.
Policía Federal	https://www.police.be/en Federal Police https://www.police.be/__/formulaire-de-contact Rue du Noyer 211, 1000, Bruselas +32 2 743 74 74	Los servicios policiales integrados, en cooperación con sus socios, son responsables de combatir los delitos informáticos. La policía local es el primer punto de contacto para ciudadanos, empresas y agencias gubernamentales. • Unidades Regionales de Delitos Informáticos (RCCU): análisis forense de material TIC: PC, teléfonos inteligentes para todo tipo de delitos del distrito del que forma parte. • Unidad Federal de Delitos Informáticos (FCCU): papel de coordinación de las RCCU y punto de contacto nacional en el enfoque internacional del ciberdelito.
BIPT	https://www.bipt.be/operators Belgian Institute for Postal Services and Telecommunications Ellipse Building C, Boulevard du Roi Albert II 35 box 1, 1030, Bruselas +32 2 226 88 51 88 info@bipt.be	El Instituto Belga de Servicios Postales y Telecomunicaciones (BIPT) supervisa la seguridad de las redes y servicios de comunicaciones de los operadores de telecomunicaciones. Entre otros, monitorea el cumplimiento de los operadores con la legislación (como análisis de riesgos y medidas de seguridad relacionadas), maneja informes de incidentes de seguridad (incluidos los incidentes que constituyen una violación de datos personales, junto con la Autoridad de Protección de Datos), y tiene varios poderes para hacer su trabajo (incluida la emisión de instrucciones vinculantes a un operador). También cuenta con un Equipo de Respuesta a Crisis para estos incidentes. Es también la autoridad sectorial y servicio de inspección para los sectores de comunicaciones electrónicas e infraestructura digital (Puntos de Intercambio de Internet, proveedores de servicios DNS y registros de dominio).
Servicio Público Federal de Economía	https://economie.fgov.be/en Service public fédéral Économie City Atrium C, Rue du Progrès, 50, 1210, Bruselas +32 08 001 20 33 info.eco@economie.fgov.be	El Servicio Público Federal de Economía, pymes, Autónomos y Energía busca crear las condiciones para un funcionamiento competitivo, sostenible y equilibrado del mercado belga. Dada la creciente digitalización de nuestra sociedad y negocios, está involucrado en varias áreas de la ciberseguridad (trabajará con la CCB para incrementar la ciberseguridad de las pymes). Las víctimas de estafas cibernéticas pueden denunciar el fraude en Point de contact: comparte datos relevantes con el CCB y deriva a las víctimas de delitos cibernéticos a la policía.
NBB	www.nbb.be Banque National de Belgique Av. Berlaymont 14, 1000, Bruselas +32 2 221 21 11 info@nbb.be	El banco nacional de Bélgica ha publicado varias directrices detalladas en las que se recoge las medidas de seguridad de los riesgos operativos y servicios de pago para la protección, financieras en materia de seguridad de la información, de los servicios que prestan todas las instituciones financieras.
FEDICT	www.fedict.belgium.be Service Public Fédérale Technologie de l'information et de communication Rue MarieThérese 1, 1000, Bruselas +32 2 212 96 00 info@fedict.belgiuimbe	Servicio Público Federal Tecnológico de la Información y la Comunicación, ha lanzado diversas campañas de concienciación sobre la seguridad en internet y aconseja a numerosas agencias gubernamentales belgas sobre la seguridad de la información.

COMISIÓN DE LA VIDA PRIVADA	www.privacycommission.be Autorité beige pour la protection des données Rue de la Presse 35, 1000, Bruselas +32 2 274 48 78 commission@privacycommission.be	La autoridad belga para la protección de la información tiene como misión esencial velar por que se respete la vida privada. Se trata de un organismo federal belga. La autoridad belga para la protección de la información ha publicado directivas claras sobre cómo gestionar correctamente los incidentes relaticos a la vida privada en el ciber mundo.

Fuente: CCB (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025) y páginas web de cada entidad.

Organismos Y Organizaciones Regionales y Locales

Nombre	Información de contacto	Rol en materia de seguridad de la información
CETIC	https://www.cetic.be/ Centre d'excellence en technologies de l'information et de la communication Av. Jean Mermoz 28, 6041, Charleroi +32 71 159 362 info@cetic.be	El Centro Excelente en Tecnologías de la Información y de la Comunicación (CETIC) es activo en búsqueda / investigación aplicada para el desarrollo de aplicaciones, las tecnologías GRID y los sistemas electrónicos en la región de Valonia. El CETIC es un agente de comunicación que tiene por objeto el traspaso de tecnología entre la investigación universitaria y las industrias.
INFOPOLE	https://clusters.wallonie.be/infopole/fr Business & Learning Center Rue Godefroid, 5-7, 5000, Namur	INFOPOLE Cluster tic, la red valona de profesionales del TIC (empresas, universidades, centros de investigación) de los cuales, cierto número es activo en el dominio de la seguridad de la información.

Fuente: CCB (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025) y páginas web de cada entidad.

3.1.2. Sector privado

El sector privado es un actor clave en el ciberespacio. Su experiencia y la innovación tecnológica que llevan a cabo en la ciberseguridad son cruciales para permitir que los organismos públicos respondan eficazmente a las amenazas cibernéticas.

El mercado de la ciberseguridad local es pequeño pero maduro, pudiendo encontrar que, algunos de los mayores competidores del mercado se quedan con hasta el 90 % de la cuota de mercado. No hay muchas nuevas grandes empresas, las nuevas empresas tienden a ser pequeñas y muy especializadas. Telenet y Proximus tienden a comprar pequeñas empresas que tienen éxito.

ORGANIZACIONES PRIVADAS Y SU ROL EN LA CIBERSEGURIDAD BELGA

Empresas

Empresa	Rol en materia de seguridad de la información
Proximus https://www.proximus.be/en/	Proveedor líder de soluciones y servicios de seguridad, Proximus tiene una amplia cartera para cada tipo de empresa: desde "plug-and-play" hasta soluciones a medida. Proteger su red, dispositivos móviles, datos de la empresa, aplicaciones, definir estrategias de seguridad e implementar soluciones de seguridad, entre otros.
Orange Belgium https://corporate.orange.be/en/social-responsibility/cyber-security-everyone https://orangecyberdefense.com/be/	Uno de los proveedores de servicios de seguridad líder en Europa, y dan soporte a empresas a nivel mundial. Operaciones de seguridad 24/7 en 19 países, monitoreo del estado de TI del cliente en tiempo real y basado en la nube, experiencia e innovación en ciberseguridad y estrecha asociación con proveedores de tecnología líderes en la industria. Habilitación de un espacio digital confiable para empresas: anclaje europeo (con huella global), investigación e inteligencia de amenazas, más de 2500 expertos en ciberseguridad.

Telenet Belgium https://www2.telenet.be/fr/business/sme-le/offre/securite/managed-cybersecurity/	Telenet Business y la consultora de ciberseguridad NVISO han establecido una asociación estratégica para la ciberseguridad. Mientras que Telenet Business se centra en la prevención de la ciberseguridad, NVISO, con sede en Bruselas, está a la vanguardia cuando se trata de responder a las brechas de seguridad y los ciberataques. Las dos empresas se han unido ahora para ofrecer un servicio de ciberseguridad totalmente integrado a empresas de diversas industrias.
Nviso https://www.nviso.eu/	Expertos en seguridad cibernética: servicios de prevención (emulación de adversario, seguridad en la nube, Swift, desarrollo *software*, evaluación de seguridad, riesgo de terceros, conciencia de usuario), detección (evaluaciones de seguridad, compromisos y amenazas, detección y respuesta gestionadas) y respuesta a los ataques cibernéticos (respuesta a incidentes 24/7 y análisis forense digital y *malware*), entre otros.
PriceWaterhouseCoopers Belgium https://www.pwc.be/en/challenges/cyber-security.html	Expertos ciberseguridad y la privacidad (capacidades de protección de datos con especialistas en cibernética y en información) para una sociedad digital segura. Analizan la robustez de los sistemas TI de las empresas para confirmar que dan la protección esperada a la información y están alineados con su estrategia y necesidades de seguridad.
EY Belgium https://www.ey.com/en_be https://www.ey.com/en_gl/cybersecurity	Enfoque proactivo, pragmático y estratégico que considere el riesgo y la seguridad desde el principio (Security by Design). Sus servicios buscan la confianza en los sistemas, diseños y datos para que las organizaciones puedan asumir más riesgos, liderar cambios. Servicios: estrategia de ciberseguridad, riesgo, cumplimiento y resiliencia, protección de datos y privacidad, gestión de identidad y acceso, respuesta y operaciones de seguridad de próxima generación, arquitectura, ingeniería y tecnologías emergentes de ciberseguridad y transformación de la ciberseguridad.
KPMG Belgium https://home.kpmg/be/en/home/__cyber-security.html	Transformación de las necesidades de las empresas en ciberseguridad y en el nuevo entorno de la privacidad (protección de datos de los clientes). Integración de la seguridad cibernética debe integrarse al comienzo de cualquier proceso de innovación o transformación. La integración adecuada en la estrategia de la empresa desde el principio puede ayudarla a convertir su riesgo cibernético en una oportunidad.
Deloitte Belgium https://www2.deloitte.com/be/__cyber-security.html	Servicios diversos de ciberseguridad: gestión de amenazas de seguridad cibernética, ciberseguridad de dispositivos médicos en red y seguridad del paciente (perspectivas de seguridad de la información de la salud), protección de aplicaciones e infraestructura, protección de la información, inteligencia de amenazas de seguridad cibernética, monitoreo de datos, analítica de seguridad y respuesta a incidentes y análisis forense.
IBM Belgium https://www.ibm.com/be-en https://www.ibm.com/security/services	Identificar los riesgos derivados de las nuevas tecnologías y soluciones para controlarlos y aceleración de la innovación. Evaluaciones y estrategias de seguridad líderes en la industria a muchas de las empresas más grandes del mundo, incluidas estrategias críticas como la confianza cero. IBM Security Services puede ampliar el equipo de la empresa, ayudar a detectar y responder a amenazas y unificar su organización en las prioridades de seguridad para acelerar la transformación empresarial.
Thalès Group https://www.thalesgroup.com/en/speakers-bureau/cybersecurity	Líder mundial en protección de datos, cuya experiencia es un factor de diferenciación genuino en todos sus mercados y para todos los proveedores clave cuya transformación digital apoya en el día a día: interconexión extensa de los sistemas de TI, la apertura de las redes, la nube y los objetos conectados, la protección y la seguridad de los datos.
Approach https://www.approach.be/en/	Proveedor de servicios y soluciones de seguridad cibernética (estrategia por capas y basada en riesgos). Prever (evaluaciones y auditorías, pruebas *phishing*, *hackeo* ético), evitar (hoja de ruta de seguridad, ISO 27001, CISO, servicios DPO, conciencia de seguridad, entrenamiento y *coaching*), proteger (SDLC seguro, *software* seguro, cortafuegos, seguridad en la Nube, Office seguro, identidad digital), entre otros. Gestión de identidad y acceso, Firmas Electrónicas), detectar y responder (detección y respuesta gestionadas, inteligencia de amenazas, respuesta a incidentes de seguridad) y recuperar (copias de seguridad seguras, continuidad del negocio, seguro cibernético), entre otros.

HP https://www.hp.com/be-nl/security/endpoint-security-solutions.html	Protección y resistencia completas para sus dispositivos, integradas en hardware (protección robusta para *endpoints* integrada en las impresoras y equipos HP, con niveles de seguridad por debajo, dentro y por encima del sistema operativo, una base segura para una mayor resiliencia), software de seguridad líder *endpoint* (sólida primera línea de defensa - reduce el riesgo de ataque y permite la recuperación remota después de un ataque de *firmware*: *firmware* autorreparable, detección de intrusiones en memoria, aislamiento de amenazas) y servicios de seguridad para empresas de cualquier tamaño (acceso a especialistas en ciberseguridad y potentes herramientas de análisis y refuerzo del equipo informático).
Secutec https://secutec.be/	Soluciones de ciberseguridad para pymes y grandes empresas, bancos (servicios a todos los niveles para asegurar sus operaciones: centros de llamadas cibernéticos subcontratados, monitoreo de tráfico, protección contra phishing, entre otros), empresas de telecomunicaciones (paquete para filtrar contenido malicioso antes de que llegue al cliente final e informes semanales de ciberinteligencia con las últimas amenazas) y gobiernos (protección de las operaciones que brindan servicios cotidianos de misión crítica a la población, asociación con los centros de ciberseguridad del gobierno para una información más actualizada y escrutinio proactivo de los proveedores de infraestructura crítica y alerta sobre las vulnerabilidades a medida que surgen).

Fuente: Elaboración propia a partir de las páginas web de cada entidad.

3.1.3. Universidades

UNIVERSIDADES Y SU ROL EN LA CIBERSEGURIDAD BELGA

Nombre	Información de contacto	Rol en materia de seguridad de la información
CRID	www.unamur.be/droit/crids Centro de Investigación, Derecho y Sociedad Rue de Bruselas 61, 5000, Namur +32 81 72 40 00	El Centro de Investigación en Información, Derecho y Sociedad (Centre de Recherche Information, Droit et Société - CRIDS) tiene su sede en la Universidad de Namur (Bélgica). Este centro de investigación interdisciplinario es miembro del Namur Digital Institute (NADI) y se centra en un amplio espectro de temas relacionados con la sociedad de la información: El CRIDS reagrupa una decena de academias y más de 40 investigadores, quienes, juntos tienen un vasto campo de competencias, desde la historia de la informática, la protección de la vida privada, nuevos modos de gobierno a la producción de bienes culturales comunes, del derecho a las comunicaciones electrónicas, de la protección de los consumidores digitales al cuerpo tecnológico.
ICRI	www.law.kuleuven.be/icri Centre interdisciplinaire pour le droit et les technologies de l'information Sint-Michielsstraat 6, 3000, Leuven +32 16 32 07 90 adminicri@law.kuleuven.be	Es un centro de investigación situadas en la Facultad de Derecho de la Universidad de Lovaina. Ha estado implicado en numerosos proyectos de investigación en materia de seguridad de la información y ha publicado diversos libros blancos sobre el tema. Coordina las actividades del B-CCENTRE.
Solvay Business School	http://www.solvay.edu/ Université Libre de Bruselas Campus du Solbosch Avenue F.O. Roosevelt 42,1050, Bruselas http://www.solvay.edu/contact	(SBS-EM) es una escuela de negocios y la Facultad de Economía y de Gestión de la Universidad libre de Bruselas. SBS organiza Masters o programas de post-graduados en IT Governance e IT Al Dicho and Security

Fuente: Elaboración propia a partir de las páginas web de cada entidad.

3.2. Organismos internacionales

3.2.1. Comisión Europea

La agencia europea encargada de la seguridad de las redes y la información (ENISA) es la respuesta de la Unión Europea frente a los problemas de ciberseguridad de la Unión. El objetivo consiste en hacer del sitio Web de ENISA el *hub* europeo para el intercambio de información, mejorar las prácticas y los conocimientos en el dominio de la seguridad de la información. El CCB representa a Bélgica en los distintos órganos y plataformas de ENISA.

Son numerosas las licitaciones en materia de ciberseguridad licitadas por la Comisión Europea. La ciberseguridad es un campo transversal en la mayoría de licitaciones del campo de la informática[21].

Por ejemplo, recientemente se ha publicado el anuncio de adjudicación de una «Plataforma de servicios centrales para las partes interesadas en la certificación de ciberseguridad de la Unión Europea (CNECT/2020/OP/0069)», por un valor total de 1,6 millones de euros. La beneficiaria de esta licitación ha sido la filial belga de una empresa española.

Para la búsqueda de licitaciones de ciberseguridad publicadas por la Comisión Europea se puede acudir a la web del Suplemento del Diario Oficial de la UE y al portal de Funding & tenders. Pueden encontrar toda la información sobre el funcionamiento y la programación de alertas de este portal en el Estudio publicado por esta oficina en la página web del ICEX: Optimización de la información de licitaciones publicadas en el Diario Oficial de la UE Tenders Electronic Daily (TED).

3.2.2. Asimismo, en la página web del ICEX se encuentra otra herramienta de utilidad para las empresas españolas, el portal de Oportunidades de Negocio. En este portal, previo registro, las empresas españolas pueden consultar todas las oportunidades de Acción Exterior de la Unión Europea (programas, proyectos y licitaciones) que publiquen los organismos públicos. El portal de oportunidades de negocio, permite filtrar por diversos campos como fecha de publicación, sector, organismo contratante, entre otros.OTAN[22]

Las amenazas cibernéticas a la seguridad de la Alianza son complejas, destructivas y coercitivas, y son cada vez más frecuentes. En 2020, el Consejo del Atlántico Norte emitió una «declaración condenando las actividades cibernéticas desestabilizadoras y maliciosas que tienen lugar en el contexto de la pandemia de coronavirus. La declaración expresó la solidaridad de los Aliados y el

[21] Código CPV principal para la búsqueda de licitaciones: 72000000 Servicios TI: consultoría, desarrollo de software, Internet y apoyo
[22] OTAN (2021). Cyberdéfense.

apoyo mutuo para quienes se enfrentan a las consecuencias de estas actividades cibernéticas maliciosas, incluidos los servicios de salud, los hospitales y los institutos de investigación».

En este contexto, la ciberdefensa se ha convertido en una cuestión prioritaria y en un ámbito de operaciones más de defensa colectiva, gestión de crisis y seguridad cooperativa. La mayoría de las crisis y conflictos actuales tienen una dimensión cibernética, mantener una sólida defensa en el ciberespacio permite a la OTAN mejorar sus misiones y operaciones y hacer frente a un panorama de amenazas que cambia rápidamente.

El enfoque principal de la OTAN en la ciberdefensa es proteger sus propias redes (incluidas las operaciones y misiones) y mejorar la resiliencia en toda la Alianza. Asimismo, todos los aliados han hecho grandes esfuerzos para mejorar sus ciberdefensas nacionales.

DESARROLLO DE LA CAPACIDAD DE DEFENSA CIBERNÉTICA DE LA OTAN

Iniciativa	Rol en materia de seguridad de la información
Proceso de Planificación de Defensa	La OTAN define objetivos para la implementación de las capacidades de defensa cibernética nacionales de los países aliados: enfoque común en toda la Alianza y desarrollo de la capacidad de defensa cibernética.
Ejercicio anual de Coalición Cibernética	Integrar consideraciones y elementos de defensa cibernética en todos los ejercicios de la Alianza, incluido Ejercicio de Gestión de Crisis (CMX).
Defensa inteligente: • Plataforma de intercambio de información de *malware* (MISP)[23] • Desarrollo de capacidades de defensa inteligente multinacional (MN CD2)[24]	Permite a los países trabajar juntos para desarrollar y mantener capacidades que no podrían permitirse desarrollar o adquirir solos, y liberar recursos para desarrollar otras capacidades
Otras iniciativas:	• La OTAN ayuda a sus Aliados a desarrollar su experiencia nacional compartiendo información y mejores prácticas y realizando ejercicios de defensa cibernética. • El factor humano juega un papel fundamental en la ciberdefensa. La OTAN continúa mejorando sus capacidades para la educación, el entrenamiento y la formación y los ejercicios de ciberdefensa. • Los países aliados pueden, de forma voluntaria y facilitada por la OTAN, ayudar a los aliados a desarrollar sus defensas cibernéticas.

Fuente: OTAN (2021). Cyberdéfense.

En 2016, se celebró entre la Capacidad de Respuesta a Incidentes Informáticos (NCIRC) de la OTAN y el Equipo de Respuesta a Emergencias Informáticas de la UE (CERT-EU), un «Acuerdo técnico sobre ciberdefensa para ayudar a ambas organizaciones a prevenir y responder mejor a los ciberataques». Este acuerdo «proporciona un marco para intercambiar información y compartir las mejores prácticas entre los equipos de respuesta a emergencias».

Desde entonces, la OTAN y la UE han reforzado su cooperación para hace frente a desafíos comunes en materia de ciberdefensa, en especial las amenazas híbridas y vecindario común más estable y seguro. Intercambian información entre los equipos de respuesta a crisis cibernéticas

[23] Malware Information Sharing Platform (MISP)
[24] Smart Defense Multinational Cyber Defense Capability Development (MN CD2)

(mejores prácticas), formación y capacitación, investigación y ejercicios con resultados tangibles en la lucha contra las amenazas cibernéticas.

La OTAN trabaja también con, entre otros, las Naciones Unidas (ONU) y la Organización para la Seguridad y la Cooperación en Europa (OSCE).

En la Cumbre de Bruselas de 2021, «los Aliados reafirmaron su compromiso de actuar de acuerdo con el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y el derecho internacional de los derechos humanos para promover un ciberespacio **libre**, **abierto**, **pacífico** y **seguro**; y continuar los esfuerzos para **mejorar la estabilidad** y **reducir el riesgo de conflicto**». En esta cumbre, se aprobó una nueva Política Integral de Ciberdefensa que «respalda las tres tareas principales de la OTAN de **defensa colectiva**, **gestión de crisis** y **seguridad cooperativa**, así como su postura general de **disuasión y defensa**. La OTAN debe **disuadir activamente**, **defenderse** y **contrarrestar** todo el espectro de amenazas cibernéticas en **todo momento**, durante tiempos de paz, crisis y conflictos, y **a nivel político, militar y técnico**».

CAPACIDADES DE CIBERSEGURIDAD DE LA OTAN EN BÉLGICA

Nombre	Rol en materia de seguridad de la información
Consejo del Atlántico Norte (NAC)	Proporciona supervisión política de alto nivel sobre todos los aspectos de la implementación de la Política de Defensa Cibernética Integral de la OTAN (implementada por las autoridades políticas, militares y técnicas, así como por los Aliados individuales). El NAC está informado de los principales incidentes cibernéticos y ejerce la autoridad principal en la gestión de crisis relacionadas con la ciberdefensa.
Comité de Ciberdefensa	Subordinado al NAC, es el comité líder para la gobernanza política y la política de ciberdefensa en general.
Consejo de Administración de Defensa Cibernética (CDMB)	A nivel de trabajo, es el responsable de coordinar la defensa cibernética en todos los organismos civiles y militares de la OTAN. Comprende a los líderes políticos, militares, operativos y técnicos de la OTAN con responsabilidades en materia de ciberdefensa.
Capacidad de Respuesta a Incidentes Informáticos (NCIRC)[25]	Responsable de la coordinación de actividades de defensa cibernética dentro de la OTAN, con los países miembros, y el personal de apoyo a la CDMB. Gestiona e informa incidentes y da información sobre incidentes a administradores de seguridad / sistema y usuarios. Tiene un papel clave en la respuesta a cualquier incidente cibernético que afecte a la OTAN. Protege las redes de la OTAN proporcionando apoyo de defensa cibernética centralizado las 24 horas. Se espera que esta capacidad evolucione de forma continua y se mantenga a la par con el entorno tecnológico y de amenazas que cambia rápidamente.
Centro de Operaciones del Ciberespacio	Fortalecer las defensas cibernéticas de la OTAN y ayudar a integrar las ciberdefensas en la planificación y las operaciones a todos los niveles. El Centro proporciona conocimiento de la situación y coordina la actividad operativa en y a través del ciberespacio (apoya a los comandantes militares con conocimiento de la situación para informar las operaciones y misiones). También coordina la actividad operativa el ciberespacio, lo que garantiza la libertad de actuar y hace las operaciones más resistentes a las amenazas cibernéticas.
Asociación Cibernética de la Industria (NICP)[26]	Esta asociación incluye entidades de la OTAN, equipos nacionales de respuesta a emergencias informáticas (CERT) y representantes de la industria de los países miembros. La OTAN y la industria trabajan conjuntamente: actividades de intercambio de información, ejercicios, formación y educación, y proyectos multinacionales de Smart Defense.
Junta de Consulta, Control y Mando (NC3)	Comité principal de consulta sobre los aspectos técnicos y de implementación de la ciberdefensa.

[25] NATO Computer Incident Response Capability (NCIRC).

[26] NATO Industry Cyber Partnership (NICP).

Autoridades Militares (NMA) y Agencia de Información y Comunicaciones (NCIA)	Son los responsables de identificar la declaración de requisitos operativos, adquisición, implementación y operación de las capacidades de defensa cibernética de la OTAN. Asimismo, la NCIA, a través de su Centro Técnico NCIRC, es también responsable de la prestación de servicios técnicos de seguridad cibernética en toda la OTAN.
Transformación de mando aliado (ACT)[27]	Responsable de la planificación y realización del Ejercicio anual de Coalición Cibernética.

Fuente: OTAN (2021). Cyberdéfense.

Un ejemplo de las Oportunidades de Negocio que se están llevando a cabo en la OTAN es el Programa Polaris[28]. Polaris se centra en consolidar la infraestructura de TI de la OTAN para que pueda gestionarse de forma centralizada y en modernizarla para permitir nuevas formas de trabajo.

Paul Howland, Gerente del Programa Polaris en la Agencia NCI, definió el proyecto como «un cambio de juego potencial para la forma en que la OTAN desarrolla e implementa sus servicios operativos en el futuro. Impulsará la innovación y reducirá los costos operativos al garantizar una reutilización mucho mayor de las capacidades»[29].

La fase 1 del proyecto proporcionará servicios de *middleware*[30] sobre los que construir aplicaciones y se prevé que esté terminando a finales de 2021. Este contrato, valorado en 10,4 millones de euros, fue adjudicado a una empresa española en 2019. Dentro del contrato, se proveerán una serie de servicios entre los que se encuentran los servicios de identificación y ciberseguridad.

La ciberseguridad es un campo transversal en la mayoría de los proyectos tecnológicos. En el caso del Programa Polaris, este incluye esfuerzos para mejorar la seguridad particularmente para una plantilla que, en el escenario de teletrabajo actual, es más móvil que nunca.

Para la búsqueda de licitaciones de ciberseguridad publicadas por la OTAN se puede acudir a la web de la Agencia de Comunicaciones e Información de la OTAN (NCI)[31]y de la Agencia de Apoyo y Adquisiciones de la OTAN (NSPA)[32].

Asimismo, igual que en el caso de la Comisión Europea, en el portal de Oportunidades de Negocio también se podrán consultar todas las oportunidades que publiquen las agencias de la OTAN. El portal de oportunidades de negocio permite filtrar, previo registro, por diversos campos como fecha de publicación, sector, organismo contratante, entre otros.

[27] NATO Allied Command Transformation (ACT)
[28] NATO (2021). NATO Platform to lay the foundations for services, apps and agility.
[29] NATO (2021). NATO Platform to lay the foundations for services, apps and agility.
[30] Lógica de intercambio de información entre aplicaciones.
[31] NATO Communications and Information Agency (NCI).
[32] NATO Support and Procurement Agency (NSPA).

4. Demanda

A la hora de invertir en ciberseguridad, la mayor duda entre los demandantes es saber si la inversión que se realice en esta va a ser realmente rentable. El retorno de la inversión es, en muchas ocasiones, opaco y difícil de medir, por lo que genera dudas y escepticismo a la hora de adquirir estas soluciones. No obstante, existe una concienciación cada vez mayor sobre la importancia de la protección de la información. Las empresas y los organismos públicos son cada vez más conscientes de esta necesidad y trabajan para mejorar las vulnerabilidades de sus sistemas.

El porcentaje de empresas que utiliza cualquier medida de ciberseguridad alcanza ya el 74 % en Bélgica (por debajo de la media de la Unión Europea que se sitúa en el 77 %).

RANKING DEL NÚMERO DE EMPRESAS POR PAÍS QUE UTILIZARON CUALQUIER MEDIDA DE SEGURIDAD DE LAS TIC EN LA UE-28 EN 2019

Valor porcentual

Ranking	País UE-28	Valor %	Ranking	País UE-28	Valor %
1	**Finlandia**	91	15	**Bélgica**	74
2	**Letonia**	87	16	**Suecia**	73
3	**República Checa**	86	17	**Bulgaria**	72
4	**Reino Unido**	86	18	**Francia**	70
5	**Irlanda**	85	19	**España**	69
6	**Portugal**	85	20	**Chipre**	68
7	**Alemania**	84	21	**Hungría**	68
8	**Dinamarca**	83	22	**Croacia**	67
9	**Malta**	83	23	**Austria**	66
10	**Italia**	82	24	**Lituania**	66
11	**Eslovaquia**	77	25	**Estonia**	61
Media UE-28		77	26	**Eslovenia**	57
12	**Polonia**	76	27	**Grecia**	55
13	**Países Bajos**	76	28	**Rumania**	53
15	**Luxemburgo**	76			

Fuente: Eurostat (2021). Security policy: measures, risks and staff awareness.

4.1. Delitos cibernéticos

La Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, estableció cuatro delitos principales:

- Acceso ilegal a los sistemas de información: acceso intencionado y sin autorización al conjunto o a una parte de un sistema de información con violación de una medida de seguridad.

- Interferencia ilegal en los sistemas de información: obstaculización o interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización.
- Interferencia ilegal de datos: borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización.
- Interceptación ilegal: la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización.

En Bélgica, el número de ataques cibernéticos se ha multiplicado en los últimos años. Se ha pasado, en el ámbito de los ataques contra la ciberseguridad, de 47.740 ataques en 2016 a 100.412 ataques en 2020 (o lo que es lo mismo, un incremento del 110 % en los últimos 5 años).

En la siguiente tabla se recoge los delitos relacionados con la ciberseguridad en Bélgica.

DELITOS INFORMÁTICOS EN BÉLGICA (2015-2020)

Valor total e incremento porcentual

Criminalidad TIC	2016	2017	2018	2019	2020	Δ 2015-2020
Fraude informático	17.194	17.645	20.210	28.078	34.947	103 %
Hacking	2.367	2.643	3.658	4.162	5.490	132 %
Phishing	219	474	1.316	2.461	7.502	3.326 %
Shouldersurfing	1.097	1.443	1.273	1.460	606	-45 %
Skimming	475	340	263	389	297	-37 %
Ransomware	49	239	185	178	124	153 %
Falsificación informática	764	806	1.255	1.694	3.317	334 %
Sabotaje	508	511	514	492	402	-21 %
Estafa: Fraude por Internet	13.045	14.174	19.257	25.445	36.473	180 %
Fraude con tarjeta de crédito	9.903	9.854	9.503	11.594	9.007	-9 %
Violación de las comunicaciones por particular	67	79	75	71	64	-4 %
Infracción contra la fe pública: falsedad informática	21	25	31	45	60	186 %
Infracción contra la autoridad pública: Denegación de cooperación (TI y telecomunicaciones)	15	18	31	40	103	587 %
Total	**47.740**	**50.268**	**59.589**	**78.128**	**100.412**	**110 %**

Fuente: Police fédérale Belgique (2021). Statistiques policières de criminalité.

4.2. Sectores más afectados

La Directiva (UE) 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (NISD), establece una serie de sectores que de especial protección en materia de ciberseguridad.

Estos sectores los componen los operadores de servicios esenciales (OSE) y los proveedores de servicios digitales (DSP):

- Energía: electricidad (empresas eléctricas, gestores de la red de distribución y gestores de la red de transporte), crudo (operadores de oleoductos de transporte de crudo y operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte) y gas (empresas suministradoras, gestores de la red de distribución, gestores de la red de transporte, gestores de almacenamiento, compañías de gas natural, gestores de instalaciones de refinado y tratamiento de gas natural).
- Transporte: transporte aéreo (compañías aéreas, entidades gestoras de los aeropuertos y operadores de control de la gestión del tráfico que prestan el servicio de control del tránsito aéreo), transporte por ferrocarril (administradores de infraestructuras y empresas ferroviarias), transporte marítimo y fluvial (empresas de transporte marítimo, fluvial y de cabotaje, pasajeros y mercancías, organismos gestores de puertos y operadores de servicios de tráfico de buques) y transporte por carretera (autoridades viarias y operadores de sistemas de transporte inteligente.).
- Banca: entidades de crédito.
- Infraestructura del mercado financiero: gestores de centros de negociación y entidades de contrapartida central (CCP).
- Atención médica: entornos y prestadores de asistencia sanitaria (entre ellos hospitales y clínicas privadas).
- Suministro y distribución de agua potable.
- Infraestructura digital: IXP[33], proveedores de servicios del DNS[34] y registros de nombres de dominio de primer nivel.

En este contexto, cabe destacar que el sector financiero y las empresas biofarmacéuticas son los sectores que más están utilizando la ciberseguridad en Bélgica.

El Banco Nacional de Bélgica (BNB) se ha centrado en «aumentar la resiliencia cibernética mejorando la gestión de riesgos e intensificando el uso de pruebas internas dentro de las empresas para evaluar el nivel de preparación de ciberseguridad»[35].

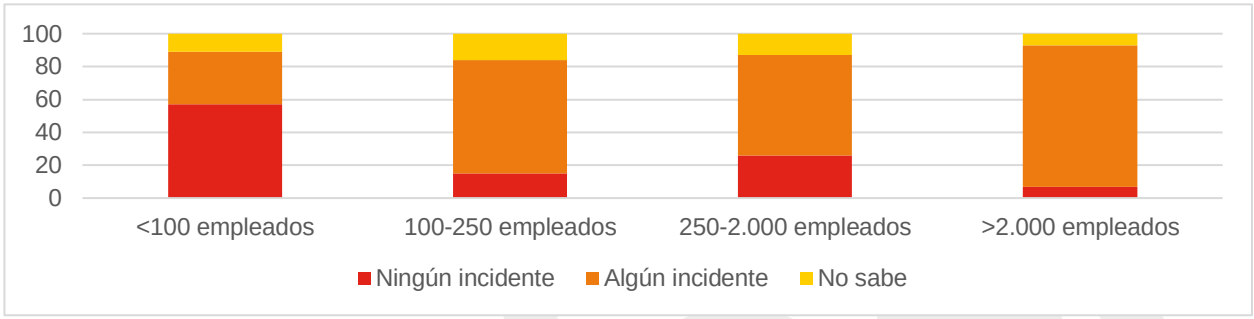
[33] Punto neutro o punto de intercambio de Internet.
[34] Sistema de nombres de dominio.
[35] Ciberseguridad (2021). Normativa de ciberseguridad en Bélgica.

4.3. Estado del arte de la ciberseguridad en Bélgica

En 2020, Proximus publicó el estudio «Cómo gestionan las empresas la ciberseguridad» que extrae una serie de conclusiones principales sobre el sector de la ciberseguridad actual y futuro en Bélgica:

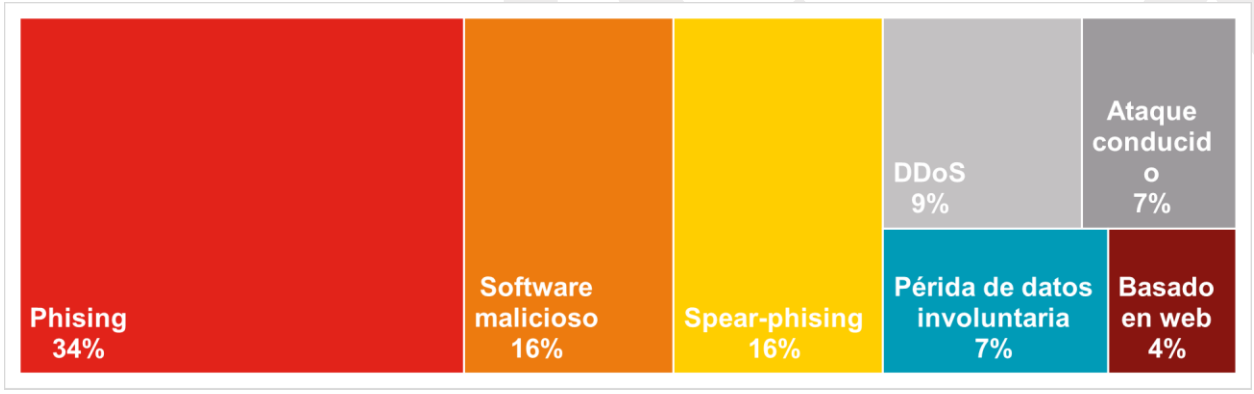
Toda empresa, grande o pequeña, es un objetivo potencial: en 2020 un 54 % de empresas experimentó un incidente, un 34 % no experimentó ningún accidente y un 12 % no sabe.

INCIDENTES DE CIBERSEGURIDAD EN LAS EMPRESAS POR NÚMERO DE EMPLEADOS



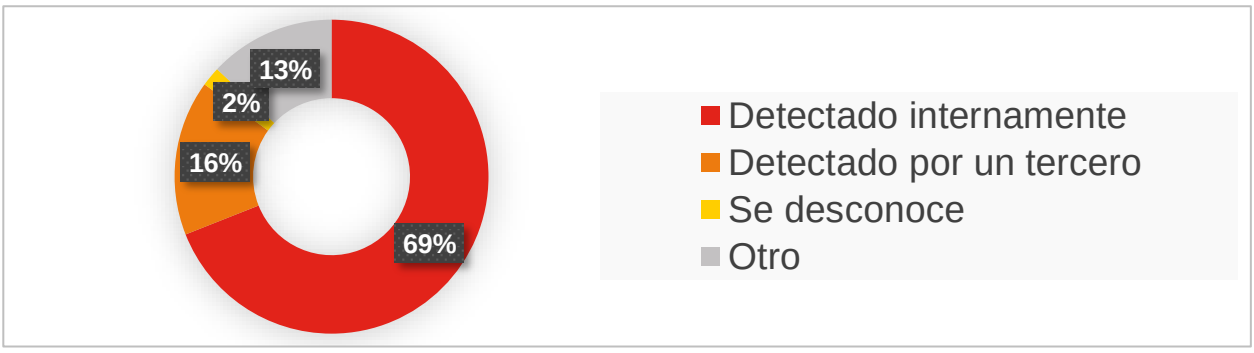
El phishing es el ataque más común: el top 3 de los incidentes de ciberseguridad que afectaron a las empresas en 2020 fueron: *phising* (35 %), *malware* (16 % de los cuales el 52 % fueron un virus y el 33 % *ransomware*) y *spear-phising* (16%).

INCIDENTES DE CIBERSEGURIDAD ESPECÍFICOS EN LAS EMPRESAS



A veces se pasa por alto un incidente: un incidente no siempre se puede identificar instantáneamente. Exige un seguimiento continuo y un análisis del sistema.

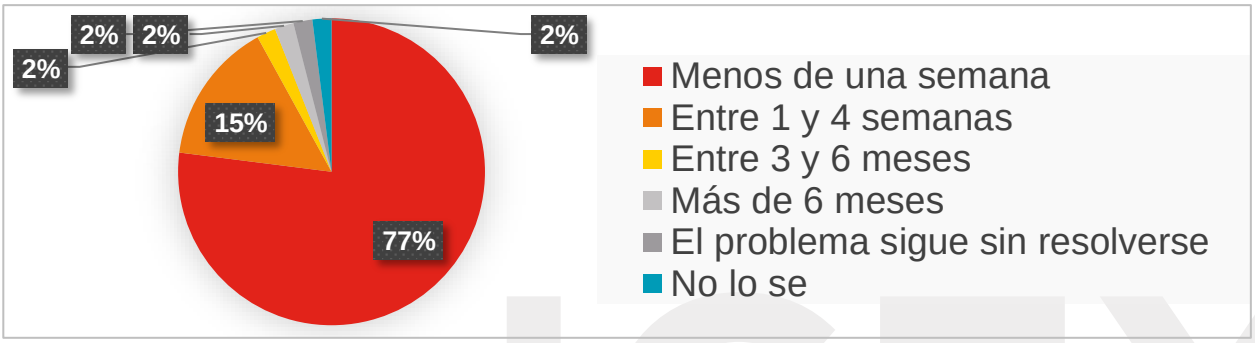
DETENCIÓN DE UN INCIDENTE DE CIBERSEGURIDAD EN LAS EMPRESAS



Las consecuencias de un incidente suelen ser graves: el 92 % de las empresas que ya habían experimentado un ciberincidente están muy preocupadas por ser víctimas por segunda vez. De las empresas que no han sido atacadas, el 18 % no están preocupadas en absoluto.

- 9 % — Desempleo técnico
- 4 % — Pérdida de datos comerciales
- 38 % — Interrupción de la red o del negocio
- 136.000 € — Coste real

TIEMPO TRANSCURRIDO HASTA SITUACIÓN "BAJO CONTROL" TRAS UN INCIDENTE

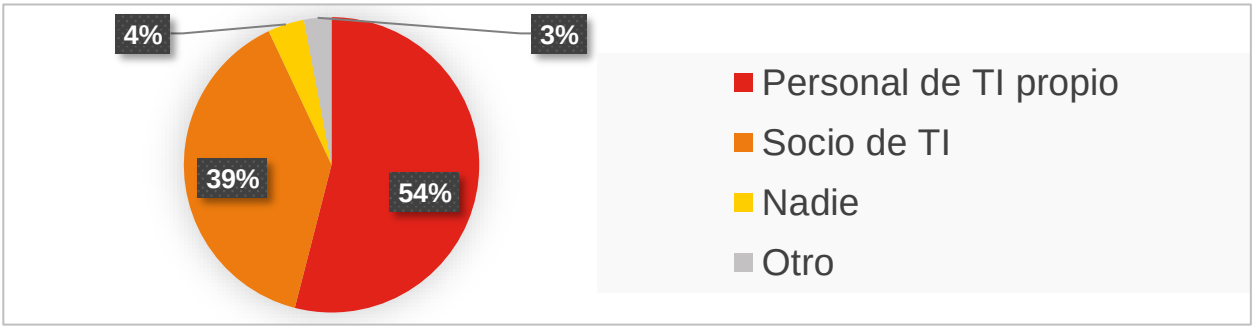


El 50% de las organizaciones belgas no tiene una estrategia de ciberseguridad activa: muchas empresas todavía no tienen desarrollado su sistema de TI.

ESTRATEGIA DE CIBERSEGURIDAD EN LAS EMPRESAS

Existe una escasez de soporte de TI: el 40 % de las empresas no contaba con equipo de ciberseguridad (personal especializado en el departamento de TI). El 22 % de las empresas no tenía ningún empleado de ciberseguridad.

GESTIÓN Y SUPERVISIÓN DE LA INFRAESTRUCTURA DE CIBERSEGURIDAD



Fuente: Proximus (2020). Cómo las empresas gestionan la ciberseguridad.

4.4. Medidas de ciberseguridad en las empresas

Las medidas adoptadas por las empresas en materia de ciberseguridad son muchas y muy variadas, pero destacan el software actualizado (incluidos sistemas operativos), la copia de seguridad de los datos en ubicación separada y la autenticación de contraseña segura.

El Reglamento (UE) 2018/1725, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, exige que los actores que traten datos personales implementen medidas técnicas y organizativas apropiadas (como la seudonimización y el cifrado de datos personales) para garantizar un nivel de seguridad adecuado al riesgo.

En la siguiente tabla, se muestra de manera visual, una comparativa de la adopción de las medidas de seguridad de las TICs por parte de Bélgica, sus países vecinos[36] y España[37].

COMPARATIVA DE LA ADOPCIÓN DE LAS MEDIDAS DE SEGURIDAD DE LAS TICS POR PARTE DE LAS EMPRESAS DE BÉLGICA, PAÍSES VECINOS Y ESPAÑA EN 2019

Valor porcentual

Medidas de seguridad de las TICs	Bélgica	Luxemburgo	Países Bajos	Francia	Alemania	España
Empresas que utilizan cualquier medida de seguridad de las TIC	**94**	**93**	**96**	**94**	**97**	**92**
Software actualizado (incluidos sistemas operativos)	87	87	92	86	**95**	86
Copia de seguridad de los datos en ubicación separada	80	79	86	68	**89**	82
Autenticación de contraseña segura	74	76	76	70	**84**	69
Control de acceso a la red de la empresa (dispositivos y usuarios)	**75**	72	53	69	71	66
Mantenimiento de archivos de registro para su análisis post-incidente	55	50	**64**	43	59	40
VPN (intercambio seguro de datos a través de la red pública)	54	47	**59**	45	56	37
Cifrado de datos, documentos o correos electrónicos	29	39	47	22	**59**	34
Evaluación de riesgos (probabilidad y consecuencias de los incidentes)	43	31	**53**	33	34	28
Pruebas de seguridad de las TIC	47	36	**51**	35	39	32
Documentos sobre medidas, prácticas o procedimientos de seguridad TIC	34	27	42	26	**37**	33
Política de seguridad TIC definida o revisada en los últimos 12 meses	27	22	**32**	18	27	25
Identificación y autenticación biométrica	10	8	-	6	11	**20**
Política de seguridad TIC definida o revisada entre 12 y 24 meses	6	4	**9**	5	7	5
Política de seguridad TIC definida o revisada hace más de 24 meses	2	1	2	2	2	**3**

Fuente: Eurostat (2019). Security policy: measures, risks and staff awareness.

[36] Los países vecinos de Bélgica que se van a analizar son: Luxemburgo, Países Bajos, Francia y Alemania. Se han escogido estos países debido a su interés en relación con el mercado belga por su: posición geográfica cercana y facilidad de comunicación entre ambos mercados, importancia del mercado tanto en valores totales como en valores per cápita y similitudes en los hábitos de consumo.

[37] Asimismo, se incluye España en la comparativa por ser el mercado de origen y, por lo tanto, el que mejor conocen los exportadores.

Las empresas alemanas son las que más medidas de ciberseguridad tienen implementados. Destaca, con respecto a los otros países analizados, el número de empresas alemanas con un software actualizado, copia de seguridad de los datos en ubicación separada y autenticación de contraseña segura, entre otros. Las empresas belgas son las que mayor control de acceso a la red de la empresa (de dispositivos y usuarios) realiza con respecto a los países de su entorno.

Pese a ser un método de ciberseguridad aún no muy implantado en los países analizados, destaca el número de empresas españolas que utilizan identificación y autentificación mediante métodos biométricos, doblando el porcentaje de empresas belgas que poseen esta tecnología.

4.5. Productos y servicios de ciberseguridad en Bélgica

A continuación, se recoge un listado de los 15 productos y servicios de ciberseguridad más demandados en Bélgica.

TOP 15 PRODUCTOS Y SERVICIOS DE CIBERSEGURIDAD (NIVEL 5) EN BÉLGIA EN 2019

Nivel 2	Nivel 3	Nivel 4	Nivel 5	Total (Mill. €)
Infraestructura	Detección de intrusiones	Sistemas automatizados de detección de intrusiones IDS basados en red	Sistemas automatizados de detección de intrusiones IDS basados en red para aplicaciones comerciales	210,09
Infraestructura	Detección de intrusiones	Respuesta automatizada a intrusiones	Aplicaciones comerciales de respuesta automatizada a intrusiones	123,50
Infraestructura	Detección de intrusiones	Sistemas de detección de intrusiones automatizados IDS basados en host	Sistemas de detección de intrusiones automatizados IDS basados en host para aplicaciones comerciales	100,78
Seguridad de la aplicación	Evaluación de vulnerabilidad	Análisis de vulnerabilidad automatizado	Análisis de vulnerabilidad automatizado para aplicaciones comerciales	85,90
Infraestructura	Detección de intrusiones	Sistemas automatizados de detección de intrusiones IDS basados en red	Sistemas de detección de intrusiones automatizados IDS basados en red para organizaciones públicas	84,39
Conciencia situacional	Conciencia situacional de bajo nivel	Evaluación automatizada de daños	Evaluación automatizada de daños para aplicaciones comerciales	71,88
Continuidad del negocio	TI / Informática forense	Forense automatizado	Análisis forense automatizado para investigación especializada	62,85
Infraestructura	Detección de intrusiones	Sistemas automatizados de detección de intrusiones IDS basados en red	Sistemas de detección de intrusiones automatizados IDS basados en red para investigación especializada	57,46
Seguridad de la aplicación	Evaluación de vulnerabilidad	Análisis de vulnerabilidad automatizado	Análisis de vulnerabilidad automatizado para investigación especializada	55.85
Continuidad del negocio	TI / Informática forense	Recuperación de datos forenses	Recuperación de datos forenses para aplicaciones comerciales	51,03
Seguridad de la aplicación	Evaluación de vulnerabilidad	Correlación de alertas automatizada	Aplicaciones comerciales de correlación de alertas automatizada	50,10

Fuente: Publications Office of the European Union (2019). Cybersecurity industry market analysis.

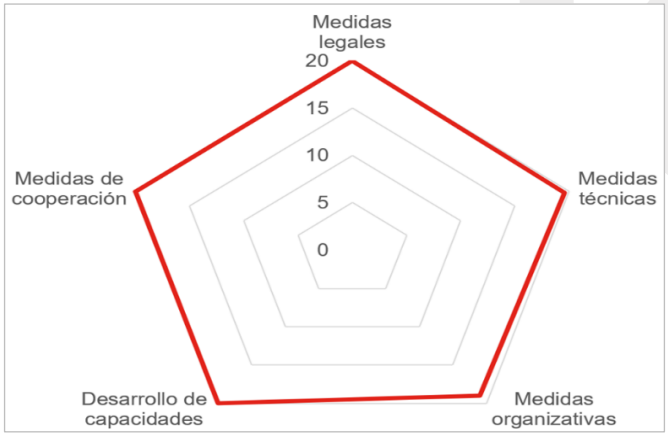
5. Percepción del sector español

En la última versión del Índice Global de Ciberseguridad (IGC), publicado por la Unión Internacional de Telecomunicaciones (UIT) en 2020, España se coloca a la cabeza mundial en ciberseguridad[38], como **cuarta potencia internacional en ciberseguridad y segunda a nivel de la Unión Europea**, solo por detrás de EEUU, Reino Unido, Arabia Saudí y Estonia, e igualada con Corea del Sur y Singapur. España ha ido escalando posiciones en este ranking internacional en los últimos años, escalando 15 puestos en 5 años.

España ha obtenido un total de 98,52 puntos sobre los 100 posibles, lo que es un gran indicativo del compromiso del país con la ciberseguridad.

DESEMPEÑO DE ESPAÑA EL ÍNDICE GLOBAL DE CIBERSEGURIDAD EN 2020

Puntuación total y por pilar



Fuente: UIT (2020). Global Cybersecurity Index 2020.

Nivel de desarrollo:
País Desarrollado

Área(s) de fortaleza relativa
Jurídica, técnica, cooperación, desarrollo de capacidades

Área(s) de crecimiento potencial
Medidas organizativas

Puntuación total	**98,52**
Medidas legales	20,00
Medidas técnicas	19,54
Medidas organizativas	18,98
Desarrollo de capacidades	20,00
Medidas de cooperación	20,00

Destaca el desempeño de España, con respecto a Bélgica en medidas organizativas (medición de las estrategias y organizaciones nacionales implementando la ciberseguridad). El buen posicionamiento del sector de la ciberseguridad en ese pilar podría abrirle las puertas a la realización de proyectos relacionados con el mismo en Bélgica.

Las empresas españolas que han tenido contacto con el sector de la ciberseguridad belga (Airbus, Avascloud, Eptisa, Everis, Idom, Indra, Innotec System, Leap in Value, One Security, S2 Group, Tango 04, Telefónica y TyPSA, entre otras)[39] buscan entrar en el mercado belga a través de licitaciones, especialmente de organismos internacionales. Algunas de estas empresas utilizan filiales belgas para su entrada en el mercado.

[38] DSN (2021). España, a la cabeza mundial en Ciberseguridad.
[39] ICEX (2017). Jornada de ciberseguridad Bélgica.

6. Acceso al mercado – Barreras

A la hora de acceder al mercado de la ciberseguridad belga, no hay barreras directas, las empresas únicamente deben cumplir con los requisitos estándar que se establecen a nivel de la Unión Europea[40] y en la instalación en el país:

6.1. Legislación[41]

- Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, se constituye como el **Reglamento Europeo de Ciberseguridad**. Con el fin de ampliar la respuesta de la UE a los ataques cibernéticos, mejorar la resiliencia cibernética y aumentar la confianza en el Mercado Único Digital, el Reglamento Europeo de Ciberseguridad UE fortalece ENISA, la Agencia de la Unión Europea para la Ciberseguridad[42].
- Reglamento (UE) 2018/1725, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, exige que los actores que traten datos personales implementen medidas técnicas y organizativas apropiadas (como la seudonimización y el cifrado de datos personales) para garantizar un nivel de seguridad adecuado al riesgo.
- Directiva (UE) 2016/1148, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (NISD), regula los estándares de ciberseguridad para infraestructura esencial a nivel de la UE. Bélgica está en proceso de implementar esta directiva.
- Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Sin embargo, cada estado miembro es responsable de la «aplicación operativa y el cumplimiento de estos requisitos y organizar a las autoridades responsables de estas tareas». En Bélgica, el entorno regulatorio, está gestionado por el Center for Cybersecurity in Belgium (CCB), creado hace 7 años, después de varios incidentes relacionados con la ciberseguridad.

[40] Enisa (2021). Cybersecurity Standards and Certification.
[41] Ciberseguridad (2021). Normativa de ciberseguridad en Bélgica.
[42] PAE (2019). La Ley de ciberseguridad de la UE y el marco de certificación de ciberseguridad.

6.2. Certificación en ciberseguridad[43]

El **Reglamento Europeo de Ciberseguridad**, establece un marco armonizado para los certificados de ciberseguridad de la UE para productos, procesos y servicios de TIC que serán válidos en toda la UE (y homogeneizará los mecanismos de certificación actuales basados principalmente en normas ISO).

La certificación requerirá la implementación del principio de seguridad por diseño en productos y servicios de TIC, que serán validados por organismos independientes y acreditados en función de un conjunto definido de criterios y después de los cuales se puede emitir la certificación. El objetivo final del mecanismo de certificación es ayudar a aumentar la protección efectiva contra las violaciones de datos.

6.3. Requisitos para instalarse en Bélgica

6.3.1. Idioma

En su organización político-administrativa, Bélgica se divide en tres niveles:

- El Estado Federal.
- Las Regiones: Flandes, Valonia y Bruselas Capital.
- Las Comunidades: neerlandófona, francófona y germanófona.

En relación con las Regiones (Flandes, Valonia y Bruselas capital), el 58 % de los belgas viven en la región flamenca, el 31 % en la valona y el 11 % en Bruselas. Además, existen grandes diferencias en la densidad de población de cada zona, siendo en Flandes más del doble, 462 habitantes/km^2, que en Valonia, 208 habitantes/km^2. Las principales ciudades del país, de acuerdo con su número de habitantes, son: Bruselas, Amberes, Gante, Charleroi, Lieja, Brujas y Namur.

En relación con las Comunidades (neerlandófona, francófona y germanófona), el sur del país, la población valona es de habla francesa, al norte, la región flamenca, es de habla neerlandesa y Bruselas, aunque mayoritariamente francófona, es oficialmente bilingüe. Finalmente, una pequeña zona al este del país, Eupen, es de habla alemana, aunque sólo representa el 0,7 % de la población.

A la hora de abordar el mercado belga, la empresa española debe considerar el idioma con el que realizar sus comunicaciones. Existe una tendencia a que haya empresas totalmente flamencas o francófonas, pero existen muchas oportunidades para las compañías extranjeras debido a que se trata de un mercado muy abierto.

[43] Ciberseguridad (2021). Normativa de ciberseguridad en Bélgica.

6.3.2. Acceso a líneas de financiación y ayudas

AYUDAS A LA I+D+I

Kit de ciberseguridad https://ccb.belgium.be/fr/actualit%C3%A9/cyber-security-kit-assurez-la-cybers%C3%A9curit%C3%A9-de-votre-entreprise-et-de-votre-personnel
Cheque de ciberseguridad https://www.wallonie.be/fr/demarches/se-faire-accompagner-dans-la-mise-en-place-de-la-politique-de-cybersecurite-de-son-entreprise-de

Fuente: Elaboración propia.

7. Perspectivas del sector

Como hemos dicho anteriormente, nos encontramos ante un panorama de amenazas que cambia rápidamente y frente al cual es muy importante disponer un sistema de defensa cibernético sólido. Los actores de ciberseguridad internacionales cada vez se enfrentan a retos más complejos.

Un ejemplo reciente de amenaza a la ciberseguridad es la Vulnerabilidad Log4Shell, detectada en la librería Log4j2 de Apache Software Foundation (según INCIBE)[44].

Esta vulnerabilidad se origina por la forma en que los mensajes de registro son gestionados por el procesador Log4j, los atacantes podrían diseñar peticiones maliciosas para desencadenar vulnerabilidades de ejecución remota de código.

Esta vulnerabilidad ha afectado a fabricantes de Sistemas de Control Industrial y, actualmente, podría estar explotándose de manera activa. A fecha de publicación de este estudio se desconocen las consecuencias completas de esta vulnerabilidad.

La Estrategia de ciberseguridad belga 2.0 (2021-2025) recoge seis objetivos estratégicos para responder a los desarrollos tecnológicos y satisfacer la gran necesidad de proteger a la población, los sectores público y privado y los sectores vitales. Esta estrategia marcará el futuro de la ciberseguridad en Bélgica de los próximos años:[45]

7.1. Fortalecer el entorno digital y aumentar la confianza en el mismo

7.1.1. Invertir en una infraestructura de red segura

- Creación de una infraestructura de red básica más segura junto con los proveedores de servicios de Internet (ISP).
- Nuevas técnicas de protección para evoluciones tecnológicas: Internet de las cosas (IdC) y nuevas generaciones de redes fijas y móviles (5G).
- Adopción de estándares de Internet más seguros para el intercambio de datos y la validación de identidades y publicaciones (seguridad DNS, enrutamiento seguro, cifrado, etc.).
- Desarrollo de un entorno de prueba ("banco de pruebas") para probar una nueva infraestructura en un entorno confiable, controlado y seguro antes de que sea ampliamente utilizada.

[44] INCIBE (2021). Vulnerabilidad Log4Shell afecta a Sistemas de Control Industrial.
[45] Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025).

7.1.2. Establecimiento de una incubadora cibernética

- Impulso a la innovación en el sector de la ciberseguridad para probar soluciones cibernéticas y modelos comerciales innovadores en un entorno seguro y difundir directrices y mejores prácticas.

7.1.3. Fomentar la experiencia y el conocimiento

- Inversión en Ciberseguridad: investigación y desarrollo (I+D), experiencia y conocimiento.
- Aumento de los conocimientos en ciberseguridad a través de investigaciones de las instituciones educativas y desarrollo y provisión de la formación pertinente.
- Colaboración entre el sector privado e instituciones educativas como universidades y colegios.
- Capacitación de los gerentes de seguridad de las instituciones públicas.
- Formación de la juventud en Ciencia, Tecnología, Ingeniería y Matemáticas para aumentar el número de profesionales: sensibilización e información en escuelas o tutorías.

7.1.4. Certificación de ciberseguridad y etiquetado de productos, servicios y procesos

- Creación de un marco legal, alineado con la Ley de Ciberseguridad de la UE, que permita a las empresas evaluar y certificar la seguridad de los productos, servicios y procesos de TIC.
- Establecimiento de una Autoridad Nacional de Certificación de Ciberseguridad (NCCA): coordinará la experiencia necesaria, autorizará certificados con altos requisitos de seguridad y establecerá una estrecha cooperación con BELAC (la organización de acreditación belga).
- Mecanismo de reconocimiento de ciberseguridad para empresas, especialmente pymes, que deseen demostrar que cumplen requisitos básicos de ciberseguridad, mejores prácticas y políticas (enfoque integrado que combine aspectos de TI, protección física y control del personal).

7.1.5. Fortalecimiento de las habilidades cibernéticas de las agencias de inteligencia y seguridad

- Fortalecimiento de las habilidades cibernéticas de las agencias de inteligencia y seguridad a través del capital humano (rápido crecimiento, capacidades y habilidades).
- Formación técnica de alta calidad a los expertos técnicos en ciberseguridad como motivación y para garantizar suficientes conocimientos técnicos y experiencia.

7.2. Preparar a usuarios y administradores de los ordenadores y redes

- Armar a todos los propietarios de un sistema informático o una red (infraestructura y los sistemas de Internet) de manera adecuada para protegerlos de las amenazas y los ataques cibernéticos.
- Sensibilización a través de los medios de comunicación, de manera integral, para generar confianza con la población y con los medios.

7.2.1. Sensibilizar y participar

- Informar y concienciar a los ciudadanos sobre las amenazas potenciales y sobre cómo protegerse de los riesgos cibernéticos (uso responsable de las medidas técnicas de protección).
- Incremento de iniciativas de participación ciudadana en la seguridad: información sobre amenazas específicas, cómo reconocerlas y cómo protegerse o responder (www.safeonweb.be).
- Campaña anual de sensibilización de la CCB en medios de comunicación (iniciativas europeas).
- Mes Europeo de la Ciberseguridad organizado cada mes de octubre por ENISA.
- Facilitar el contacto entre ciudadanía y prestadores de servicios de calidad en ciberseguridad.
- Incremento en la implementación de campañas de concienciación y sensibilización con impacto directo en la comunidad empresarial: seminarios web, guías o KIT de ciberseguridad.

7.2.2. Informar sobre amenazas y vulnerabilidades

- Análisis permanente y advertencias o alertas por el CCB sobre ciberamenazas o vulnerabilidades importantes (BE-Alert del Centro Nacional de Crisis (NCCN) brindará soporte y enviará alertas).
- Publicación por parte de las empresas y organizaciones de una "Política de divulgación coordinada de vulnerabilidades".
- Los proveedores de servicios de Internet deberán enviar rápidamente las advertencias a sus clientes vulnerables o amenazados.

7.2.3. Pautas y las mejores prácticas de ciberseguridad.

- Estándares internacionales en las políticas de ciberseguridad de las empresas: identificar, planificar y gestión de riesgos, medidas de seguridad y evaluar el uso de ordenadores y redes.

7.3. Proteger a las organizaciones de interés vital de todas las amenazas cibernéticas

- Protección de las organizaciones de interés vital de amenazas cibernéticas cada vez más sofisticadas y en aumento.

7.3.1. Optimizar el intercambio de información y envío de alertas

- Información continua a las organizaciones de interés vital sobre amenazas, vulnerabilidades o incidentes relevantes a través del Sistema de Alerta Temprana (EWS) u otros canales del CCB.
- Creación de una plataforma de consulta entre las autoridades sectoriales (Cyber Security Sector Authorities Platform - CySSAP) para optimizar la gestión de los intercambios de información con Organizaciones de Vital Interés: identificación regulación y seguimiento.

7.3.2. Mejorar la protección de las instituciones internacionales

- Identificación de la Organizaciones Belgas de Vital Interés que apoyan a las instituciones internacionales con sede en Bélgica para brindarles la protección adecuada.
- Diálogo y cooperación con las instituciones internacionales para incrementar la efectividad de la protección y respuesta a los ciberataques.

7.3.3. Ser capaz de manejar incidentes con impacto nacional.

- El Plan Nacional de Emergencias Cibernéticas dará una respuesta rápida y eficaz a los incidentes con impacto nacional a través de una cooperación óptima entre el Equipo Nacional de Respuesta a Emergencias Informáticas (CERT.be) de la CCB, los Servicios Integrados de Policía y el Centro Nacional de Crisis (NCCN), las investigaciones legales se integran de inmediato.

7.3.4. Ejercicios

- Realización de ejercicios regulares (fuerzas de seguridad belgas, otros departamentos gubernamentales y organizaciones de interés vital) para desarrollar resiliencia ante incidentes internacionales y nacionales y probar la efectividad del Plan de Emergencia Cibernética.

7.4. Responder a las amenazas cibernéticas

Inversión en la identificación y respuesta ante el peligro de nuestra población, economía u organizaciones de interés vital frente al aumento del ciberdelito y las amenazas gubernamentales.

7.4.1. Mapeo de las amenazas internacionales

- Seguimiento y evaluación continuos de las ciberamenazas internacionales.
- Identificar las intenciones y capacidades cibernéticas de los "actores" en contra de nuestros intereses esenciales y vitales y se deben monitorear las fuentes potenciales de amenazas.
- Conocer en la mayor medida posible la evolución de sus tácticas, técnicas y procedimientos y evaluar nuestros medios de protección con respecto a ellos.

7.4.2. Perturbar la infraestructura cibernética criminal

- Interrupción de la infraestructura cibernética criminal de la Dark Web: detección y neutralización de infraestructura criminal y sistemas comprometidos, protección de comunicaciones públicas y corporativas y colaboración entre agencias de inteligencia y seguridad (nacional e internacional).

7.4.3. Desarrollar una capacidad represiva adecuada

- Detección, investigación, enjuiciamiento y sanción adecuada del ciberdelito: integración policial y desarrollo de capacidad y experiencia en todos los niveles (local, servicios centrales y federal).
- Identificación, reunión de pruebas y captura de los autores de delitos informáticos.
- Delineación y desmantelación de, la infraestructura criminal, incautación y confiscación de los activos ilegales y procesamiento y condena de los autores de los delitos.
- Coordinación entre todos los países afectados para apresar a los ciberdelincuentes que los ciberdelincuentes operan principalmente en un contexto internacional.
- Sistema judicial y fiscal eficaz en la lucha contra el ciberdelito.

7.4.4. Desarrollar una capacidad de defensa adecuada

- Expansión de las capacidades cibernéticas dentro del Servicio General de Información y Seguridad (ADIV / SGRS) y el Ministerio de Defensa (Plan Estratégico de Defensa).
- Creación de un quinto componente de carácter dual para la protección en caso de crisis híbridas.

7.4.5. Atribución

- Creación de capacidad y coordinación internacional para identificar y atribuir un ciberataque a una persona, grupo o estado en particular (agenda de la OTAN, la UE y la ONU, entre otros).

7.5. Mejorar las colaboraciones público-privadas y académicas

La cooperación entre grupos de interés, nacionales e internacionales, en la prevención, reducción, tratamiento y seguimiento de las ciberamenazas e incidentes, es clave para el éxito.

7.5.1. Promover la coordinación y la colaboración

- Coordinación del CCB de todas las iniciativas de forma centralizada (servicios públicos, sector privado y científico): plataformas nuevas o existentes entre agencias, reuniones periódicas de expertos (compartir información y experiencias y trabajar en red) y diálogo abierto y estructural.

7.5.2. Apoyo a la Cyber Security Coalition

- Cyber Security Coalition (sector público, privado y académico): compartir conocimientos y experiencias, organizar y coordinar iniciativas intersectoriales, concienciar a ciudadanos y organizaciones, creación de conocimiento especializado y asistencia en políticas y regulaciones.

7.6. Un claro compromiso internacional

- Trabajo en estrecha colaboración, con perspectiva holística, de los diversos vectores de cooperación internacional (diplomático, militar, económico, etc.).
- Protección de un entorno cibernético abierto, libre y seguro (gestión legislativa y diplomática).

8. Oportunidades

Como hemos visto en el apartado anterior, la Estrategia de ciberseguridad belga 2.0 (2021-2025) recoge varios objetivos estratégicos transversales para dar respuesta a las nuevas necesidades de ciberseguridad derivadas de los desarrollos tecnológicos y la necesidad de protección del entorno digital.

En este contexto, se pueden observar varias ramas de actuación que se corresponden con cómo las empresas gestionan la ciberseguridad con el objetico de cumplir con esos objetivos. Las acciones concretas para lograr alcanzar esos objetivos podrán generar oportunidades para las empresas españolas en los próximos años.

8.1. Prioridades de ciberseguridad para Bélgica

El análisis de esta situación se establecen 3 **prioridades de ciberseguridad** para Bélgica:

- Sensibilización y formación de los empleados.
- Inversión en tecnología.
- Desarrollo de una estrategia de ciberseguridad:

3 grandes motivaciones para la implementación de medidas de ciberseguridad:

1. Seguridad de la información
2. Prevención de amenazas
3. Cumplimiento de normativa

3 obstáculos principales para la implementación de medidas de ciberseguridad

1. FINANCIERO

La ciberseguridad es un coste enorme para las empresas y rara vez se incluye en el presupuesto. En muchas organizaciones todavía existe la percepción de que la ciberseguridad significa costos enormes y poco o ningún ROI.

2. CULTURA EMPRESARIAL

Si una estrategia no cuenta con el respaldo de la gerencia, los empleados no son conscientes de la importancia de la ciberseguridad y nadie se preocupa por ella.

3. RECURSOS

El entorno de TI, a menudo en las pequeñas empresas, apenas se supervisa o nunca. La falta de conocimiento, capacidad y / o personal es la causa de esto.

Fuente: Proximus (2020). Cómo las empresas gestionan la ciberseguridad.

8.2. Retos y Oportunidades de la ciberseguridad en Bélgica

En una entrevista realizada por esta oficina a Miguel De Bruycker, Director Gerente del Centro de Ciber Seguridad de Bélgica, éste marca los siguientes retos para las empresas de ciberseguridad en Bélgica:

1. La demanda de profesionales cualificados crece rápidamente.
2. La oferta de profesionales cualificados es limitada.
3. Falta de diversidad en la población activa: pocas mujeres, gente que trabaja sin establecer vínculos con el resto de la sociedad.

Asimismo, define una serie de oportunidades para las empresas de ciberseguridad en Bélgica:

1. Hacer que las empresas sean mucho más conscientes de la ciberseguridad en Bélgica - generar confianza. Las empresas aún se muestran reticentes a incorporar herramientas de ciberseguridad en su rutina, hay que aumentar su confianza demostrándoles que estas prácticas les van a aportar un gran valor añadido a corto, medio y largo plazo. Entorno al 40 % de todos los incidentes de seguridad son el resultado del comportamiento humano, por lo tanto, un código de conducta para empleados adquiere una gran importancia.
2. Digitalización COVID-19 y trabajo remoto: la ciberseguridad no se ha posicionado aún como la máxima prioridad, pero debería ocupar una de las primeras posiciones. La digitalización del trabajo remoto supone un gran desafío u oportunidad (como la protección de las infraestructuras de forma preventiva mediante la identificación de vulnerabilidades).
3. IdC y 5G: estas nuevas tendencias ya suponen una nueva evolución tecnológica, las empresas de ciberseguridad deberán facilitar esta transición y generar herramientas y recursos de adaptación y mejora de la seguridad en este contexto.

Asimismo, el experto belga en ciberseguridad centrada en el ser humano de la Universidad Libre de Bruselas, Emmanuel Nicaise opina que las áreas del sector de la ciberseguridad que podrían crecer más en los próximos años son la **nube**, el **machine learning** (aprendizaje automático) y los **servicios de gestión** (administración). En este contexto, enumera una serie de actividades en las que prevé que se den oportunidades de ciberseguridad en un futuro próximo:

1. Servicios de administrador: Centros de operaciones de seguridad. Todo lo que implica reaccionar de forma rápida, automática y eficaz ante las incidencias. Para las pequeñas empresas, es difícil implementarlo por sí solo, por lo que la externalización es necesaria.
2. Seguridad humana: (i) *phishing*, bien abordado, (ii) educación y (iii) ciberseguridad centrada en las personas (su campo de especialización, hacer que la ciberseguridad sea utilizable, porque los controles están disponibles, pero no se utilizan en la práctica).
3. La nube y los problemas de seguridad.
4. *Machine learning* (aprendizaje automático).

9. Información práctica

9.1. Asociaciones

ASOCIACIONES Y FEDERACIONES Y SU ROL EN LA CIBERSEGURIDAD BELGA

Nombre	Información de contacto	Rol en materia de seguridad de la información
AGORIA	www.agoria.be Agoria Diamant Building, Avenue A. Reyers 80, 1030, Bruselas +32 2 706 78 00 Ferdinand.CASIER@agoria.be	La Federación belga de la industria tecnológica, Agoria cuenta entre sus miembros con más de 2000 empresas tecnológicas de la industria manufacturera, digital y telecomunicaciones, de las cuales el 70% son pymes. Agoria tiene alrededor de 200 empleados, ubicados en Bruselas, Amberes, Gante, Lieja y Charleroi. La información que se facilita va dirigida a empresas que quieren integrar aspectos de ciber seguridad en su estrategia comercial.
BELTUG	www.beltug.be Belgian Association of CIOs and Technology Leaders Rue Knaptand 123, 9100, Sin Niklaas +32 3 780 17 30 info@beltug.be	El objetivo de Beltug es derribar las barreras de las empresas al construir su estrategia digital, abordar los desafíos de la organización conectada y cubrir temas como la gestión de activos de software, TI híbrida, seguridad cibernética, IoT, colaboración inteligente, privacidad, blockchain, gestión de datos y mucho más. Organiza mesas redondas y ha publicado varios libros blancos sobre la seguridad de la información. Sus miembros se reúnen y discuten sobre todos los temas ligados a la ciberseguridad.
FEB	www.vbo-feb.be Fédération des Entreprises de Belgique Rue Ravenstein 4, 1000, Bruselas +32 2 525 08 11 info@vbo-feb.be	La FEB Representa a más de 50.000 empresas, 75% del empleo en el sector privado. Es un socio privilegiado de múltiples organismos públicos en un cierto número de programas de acción con el objetivo de proteger la economía nacional. Se ha asociado al ICC Belgium para tomar la iniciativa de editar una guía de ciberseguridad dirigida a todas las empresas belgas.
FEBELIN	www.febelfin.be FEBELFIN Rue d'Arlon 82, 1040, Bruselas +32 (0) 2 507 68 11 info@febelfin.be	La federación belga del sector financiero asiste a 245 instituciones financieras en la lucha contra la cibercriminalidad a través de compartir la información y la cooperación con todos los implicados. Ha lanzado múltiples campañas de sensibilización en materia de seguridad de las operaciones bancarias en Internet.
ICC BELGIUM	www.iccbelgium.be Comité belge de l'international Chamber of Commerce Rue des Sois 8, 1000, Bruselas +32 (0) 2 525 08 44 info@iccwbo.be	Es la organización empresarial más grande del mundo (representa a más de 45 millones de empresas en más de 100 países). Su comisión ICC mundial sobre la economía digital se preocupa de la cibercriminalidad y el desarrollo de directivas ICC orientadas en cuestiones jurisdiccionales con las que están confrontadas empresas mundiales. El ICC combate todos los tipos de criminalidad en relación con el comercio y la ciberseguridad.
ISACA	www.isaca.be ISACA Belgium Rue Royale 109-111 b.5, 1000, Bruselas +32 2 219 24 82 president@isaca.be	Es una asociación internacional de conocimiento sin ánimo lucrativo con más de 800 miembros en Bélgica. La asociación actualmente se enfoca en aseguramiento, seguridad y gobernanza y proporciona certificación mundialmente reconocida en aseguramiento (Auditor de sistemas de información certificado), seguridad (Gerente de seguridad de la información certificado) y gobernanza (Certificado en el gobierno de TI empresarial).
ISPA	www.ispa.be ISPA Rue Montoyer 39B 3,1000, Bruselas +32 2 503 22 65 info@ispa.be	ISPA Belgium reúne la totalidad del ecosistema de la industria de Internet en Bélgica: proveedores de acceso, *hosters*, proveedores de tránsito, centros de datos y plataformas. La asociación traslada la voz de la comunidad de Internet a los responsables políticos y el público en general, para la creación de políticas coherentes, orientadas al futuro y compatibles con la tecnología digital.

L-SEC	www.lsec.be Leaders in Security Kasteelpark 1O, 3001, Heverlee +32 16 32 85 41 info@lsec.be	LSEC es un clúster de seguridad de la información de renombre internacional sin fines de lucro con el objetivo de promover la seguridad de la información y la experiencia en BeNeLux y Europa. Conecta a expertos de la industria de la seguridad, institutos de investigación y universidades, agencias gubernamentales, usuarios finales, organismos de financiación y expertos técnicos que impulsan las agendas de investigación nacionales y europeas. Sus actividades tienen como objetivo concienciar y apoyar la innovación y la competitividad del mercado europeo sobre la seguridad cibernética y promover la visibilidad de sus miembros.

Fuente: Elaboración propia a partir de las páginas web de cada entidad.

9.2. Marco de gobernanza y plataformas de consulta

Cyber Security Coalition Belgium	Reúne periódicamente a expertos en el dominio de las comunidades privada, académica y pública. Esto se hace durante eventos de intercambio de experiencias y en grupos focales para discutir las mejores prácticas, experiencias o iniciativas sobre varios temas (seguridad en la nube, NIS, criptografía, etc.).
Plataforma 4 Cibernética del Comité de Coordinación de Inteligencia y Seguridad (CCIV / CCRS)	Los servicios de inteligencia y seguridad discuten las políticas generales de ciberseguridad.
Plataforma de Autoridad Sectorial de Seguridad Cibernética (CySSAP)	Consulta entre las autoridades supervisoras de las Organizaciones de Vital Interés.
Cybercrime Expertise Network (REN)	Reúne a expertos de los servicios públicos en ciberdelitos, para consultas periódicas (coordina la fiscalía general de Amberes).
Plataforma CSI / DPO (les Conseillers en Sécurité de l'Information / Data Protection Officer)	Reúne a los asesores de seguridad y los oficiales de protección de datos de cada departamento gubernamental. Cada trimestre se organiza una reunión específica sobre cuestiones cibernéticas como parte del Informe trimestral sobre amenazas cibernéticas de CCB / CERT.
SIT (Synergy IT)	Plataforma para compartir conocimiento y consultoría entre gerentes de TI de todos los servicios públicos federales (Servicios Públicos Federales, instituciones públicas de seguridad social e instituciones de servicios públicos). El SIT se reúne mensualmente, con el objetivo de iniciar y dar seguimiento a iniciativas de TI conjuntas, tanto contratos gubernamentales como proyectos, así como proporcionar información técnica sobre iniciativas G-Cloud.
Comisión Económica Interministerial (IEC)	Mecanismo de coordinación técnico-administrativa flexible e independiente que puede ayudar a definir y alinear las posiciones administrativas de las autoridades federales en los ámbitos nacional, europeo e internacionales.

Fuente: CCB (2021) Cybersecurity Strategy Belgium 2.0 (2021-2025) y páginas web de cada entidad.

10. Bibliografía

- Centro de crise National (2019). Evaluation des risques nationaux: cyber. Obtenido de: https://centredecrise.be/fr/documentation/publications/evaluation-des-risques-nationaux-cyber
- Centre for Cyber Security Belgium (2021). Página principal. Obtenido de: https://ccb.belgium.be/en
- Centre for Cyber Security Belgium (2021) Cybersecurity Strategy Belgium 2.0. Obtenido de: https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
- Ciberseguridad (2021). Normativa de ciberseguridad en Bélgica. Obtenido de: https://ciberseguridad.com/normativa/europea/belgica/
- Cybersecurity Coalition (2021). Découvrez nos membres. Obtenido de: https://www.cybersecuritycoalition.be/fr/actualites/
- DSN (2021). España, a la cabeza mundial en Ciberseguridad. https://www.dsn.gob.es/gl/actualidad/sala-prensa/espa%C3%B1a-cabeza-mundial-ciberseguridad
- Enisa (2021). Cybersecurity Standards and Certification. Obtenido de: https://www.enisa.europa.eu/topics/standards
- Eurostat (2019). Security policy: measures, risks and staff awareness. Obtenido de: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en
- Eurostat (2019). Security incidents and consequences. Obtenido de: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en
- IBM (2019). Cyber Resilience in Belgium Action is needed. Obtenido de: https://www.ibm.com/blogs/think/be-en/2019/11/25/cyberresilience-in-belgium/
- ICEX (2017). Jornada de ciberseguridad Bélgica. Obtenido de: https://www.icex.es/icex/es/navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/sectores/servicios/actividades/ACP2017740038.html
- ICEX (2020). Optimización de la información de licitaciones publicadas en el Diario Oficial de la UE Tenders Electronic Daily (TED). Obtenido de: https://www.icex.es/icex/es/navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/paises/__/el-mercado/estudios-informes/DOC2020853801.html?idPais=BE
- INCIBE (2021). Vulnerabilidad Log4Shell afecta a Sistemas de Control Industrial. Obtenido de: https://www.incibe-cert.es/alrta-temprana/avisos-sci/vulnerabilidad-log4shell-afecta-sistemas-control-industrial
- Instituto Nacional de Ciberseguridad (2017). Decálogo ciberseguridad empresas: una guía de aproximación para el empresario. Obtenido de: https://www.incibe.es/protege-tu-empresa/guias/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario

- Instituto Nacional de Ciberseguridad (2021). Glosario de términos de ciberseguridad: una guía de aproximación para el empresário. Obtenido de: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario
- Instituto Nacional de Ciberseguridad (2021). Ransomware: una guía de aproximación para el empresario. Obtenido de: https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario
- NATO (2021). Cyberdéfense. Obtenido de: https://www.nato.int/cps/fr/natohq/topics_78170.htm
- NATO (2021). NATO Platform to lay the foundations for services, apps and agility. Obtenido de: https://www.ncia.nato.int/about-us/newsroom/nato-platform-to-lay-the-foundations-for-services--apps-and-agility.html
- NATO Support and Procurement Agency (2021). Página principal. Obtenido de: https://www.nspa.nato.int
- SPF Économie (2021). Cybersécurité et PME. Obtenido de: https://economie.fgov.be/fr/themes/entreprises/developper-et-gerer-une/cybersecurite-et-pme
- ONTSI-INCIBE (2015). Caracterización del subsector y el mercado de la ciberseguridad. Obtenido de: https://www.ontsi.es/sites/ontsi/files/caracterizacion_del_subsector_y_el_mercado_de_la_ciberseguridad.pdf
- Police fédérale Belgique (2021). Statistiques policières de criminalité. Obtenido de: https://www.stat.policefederale.be/assets/pdf/crimestat/nationaal/rapport_2021_trim1_nat_belgique_fr.pdf
- Portal de la Administración Electrónica (2019). La Ley de ciberseguridad de la UE y el marco de certificación de ciberseguridad. Obtenido de: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Septiembre/Noticia-2019-09-13-Ley-ciberseguridad-UE-marco-certificacion-ciberseguridad.html
- Proximus (2020). Cómo las empresas gestionan la ciberseguridad. Obtenido de: https://cybersecurity.proximus.be/survey2021/research-report-cybersecurity
- Publications Office of the European Union (2019). Cybersecurity industry market analysis. Obtenido de: https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1
- UIT (2020). Global Cybersecurity Index 2020. Obtenido de: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- Velasco, L. y Muñoz, L. (2021). Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea. Observatorio Nacional de Tecnología y Sociedad. Obtenido de: https://www.observaciber.es/sites/observaciber/files/media/documents/indicadoresconfianzadigitalyciberseguridadespa%C3%B1ayue_octubre2021.pdf

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