MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

CARACTERIZACIÓN DEL SECTOR INDUSTRIAL DE LA SEGURIDAD Y SU TAXONOMÍA TECNOLÓGICA

Autor: Manuel Mayo Navas

Director: Clara Tébar Losa

Madrid

Julio de 2019

Índice de Documentos

DOCUMENTO I. MEMORIA

DOCUMENTO II. ANEJOS

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Manuel Mayo Navas DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Caracterización del Sector Industrial de la Seguridad y su taxonomía tecnológica, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción

de derechos derivada de las obras objeto de la cesión.

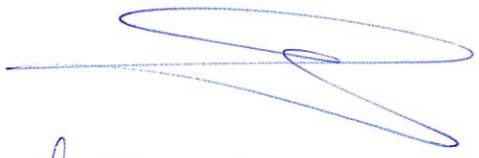
6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 16 de Julio de 2019

ACEPTA



Fdo. Manuel Mayo Navas

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

CARACTERIZACION DEL SECTOR INDUSTRIAL DE SEGURIDAD Y SU TAXONOMÍA TECNOLÓGICA

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico 2018/2019 es de mi autoría, original e inédito y no ha sido presentado con anterioridad a otros efectos. El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.

Fdo.: Manuel Mayo Navas Fecha: 16 / 07 / 19

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Clara Tébar Losa Fecha: 16 / 07 / 2019

MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER

CARACTERIZACIÓN DEL SECTOR INDUSTRIAL DE LA SEGURIDAD Y SU TAXONOMÍA TECNOLÓGICA

Autor: Manuel Mayo Navas

Director: Clara Tébar Losa

Madrid

Julio de 2019

CARACTERIZACIÓN DEL SECTOR INDUSTRIAL DE LA SEGURIDAD Y SU TAXONOMÍA TECNOLÓGICA

Autor: Mayo Navas, Manuel

Director: Tébar Losa, Clara

Entidades Colaboradoras: ICAI – Universidad Pontificia de Comillas

TEDAE

Resumen del Proyecto

El proyecto en cuestión trata sobre la caracterización del Sector Industrial de la Seguridad y la posterior caracterización del mismo. Esto se debe a que es un sector tecnológico amplio y complejo, de reciente separación con respecto al sector de la Defensa. Además, la seguridad, como concepto, ya es en sí misma amplia y compleja. Esto se debe a que abarca distintos aspectos de la sociedad, como pueden ser la seguridad física, la seguridad cibernética, la seguridad económica, la seguridad institucional y política, la seguridad del transporte y la seguridad medioambiental. Además, se debe considerar que, al ser la sociedad heterogénea, la seguridad recae en un gran número de agentes y actores, tanto públicos como privados.

También cabe destacar la amplitud de tecnologías a las que se dedican las distintas empresas pertenecientes al sector, y la transversalidad de las mismas. Estas podrían utilizarse en otros muchos sectores catalogados tradicionalmente como aeronáutica, naval, telecomunicaciones o defensa. Es más, la mayoría de las empresas forman parte del grupo líder en innovación e inversión dentro de sus segmentos de mercado. Es por ello que incrementar la ventaja competitiva y posicionar la industria nacional en una posiciona de fuerza dentro de la competencia internacional fijaría un pilar estratégico que robustecería la economía.

Es por todo ello que se pretende realizar una caracterización y posterior taxonomía del Sector Industrial de la Seguridad. Con ello, se podría definir el ámbito en el que las empresas deben centrar sus esfuerzos, ganando en ventaja competitiva y aprovechando las oportunidades que el mercado actualmente ofrece.

Metodología

El proyecto está dividido en varias partes. En la primera caracteriza y define el Sector Industrial de la Seguridad, además de realizar un breve análisis económico del mismo gracias a los datos proporcionados por la entidad colaborativa TEDAE.

Se concluye que la definición del sector sería el conjunto de empresas, principalmente de carácter tecnológico, dedicadas al desarrollo, mejora y creación de productos y servicios para proveer a las Fuerzas y Cuerpos de seguridad y agentes asociados de todo lo necesario para cumplir con su cometido. Además, se incluirán todas aquellas dedicadas a la innovación e investigación científica, siempre que tengan como fin proveer o mejorar la seguridad de la sociedad.

Después de analizar los distintos segmentos a los que se enfocan las empresas pertenecientes al sector, se observan los datos económicos. Emplean a un gran número de personas, con una facturación superior a 150 millones de euros, siendo el 22% procedente de la exportación, además de reinvertir dichos resultados en innovación en un porcentaje superior al de otros sectores, y para finalizar, tienen una productividad 2,6 veces la media nacional. Se concluye que es un sector sano, en pleno crecimiento y en expansión, enfocado a la tecnología, siempre atractivo para las nuevas inversiones.

En el siguiente apartado se mencionan las distintas fuentes de financiación europeas que podrían ser de interés para las empresas. Se concluye que los programas más importantes de los que podrían beneficiarse son tres: Horizonte 2020, los Fondos Estructurales de Inversión Europeos, y los Fondos Europeos para Inversiones Estratégicas. Todo ellos disponen de fondos enfocados a las nuevas tecnologías, innovación e investigación, incluso programas dedicados específicamente a fomentar el desarrollo de productos y servicios pertenecientes al ámbito de la seguridad.

Posteriormente se realiza un estudio del arte de diferentes taxonomías del sector que se han realizado con anterioridad. Se escogen cinco taxonomías, la mayoría provienen de proyectos realizados por la Comisión Europea, y se realiza una base los mejores aspectos de cada una para utilizarlos en este proyecto.

Ya sentados los cimientos para la creación de la taxonomía, se procede a seleccionar los distintos criterios o niveles de las que dispondrá. Para delimitar la frontera del Sector Industrial se ha optado por escoger las distintas líneas de acción o amenazas identificadas por el DSN. Pero existe un problema, estas líneas de acción disponen de segmentos pertenecientes al sector de la Defensa, por lo que hay que realizar una diferenciación. Para dicha diferenciación, se han ido investigando las distintas competencias de las Fuerzas y Cuerpos de Seguridad y de la Armada y sus distintos cuerpos. Con ellas, y realizando un análisis de las líneas de acción, se ha delimitado la frontera del Sector Industrial de la Seguridad.

El siguiente nivel sería dividir las distintas líneas de acción en fases, ya que habrá productos específicos según la situación en la que se encuentren los distintos FCS al enfrentarse a las amenazas. Se ha optado por las siguientes: Comunicaciones, Detección, Gestión de la Información, Posicionamiento, Evaluación de Riesgos, Conocimiento o Consciencia de la situación, Entrenamiento, Doctrina y operaciones, Respuesta al Incidente.

Por último, se ha realizado una agrupación de todos los productos y servicios en familia tecnológicos según su finalidad común. Esto grupos serían: Inteligencia Artificial y

Apoyo en la toma de decisiones, Biometría, Biotecnología, CBRNE, Comunicaciones, Autentificación Electrónica, Energía, Forense, GIS, Ciencias Humanas, Plataformas Integradas, IT, Seguridad en IT, Materiales, Navegación, Sensores, y Procesamiento de las señales. Con esto quedarían explicados los distintos criterios seguidos para la realización de la taxonomía.

Resultados

El resultado final es una taxonomía formada por tres anillos. Se ha considerado, tras el análisis de las competencias de las distintas Fuerzas y Cuerpos de Seguridad que la líneas de acción que delimitarían la frontera serian: Lucha contra el Terrorismo, Ciberseguridad, Lucha contra el Crimen Organizado, Seguridad Económica, No proliferación de armas de destrucción masiva, Ordenación de flujos migratorios, Contrainteligencia, Seguridad Marítima, Protección de Infraestructuras Criticas, Protección del espacio aéreo ultraterrestre, Seguridad frente a pandemias y Epidemias, y Preservación del Medioambiente. Los anillos que conforman la taxonomía con respecto a los tres niveles descritos anteriormente tendrían la siguiente forma:

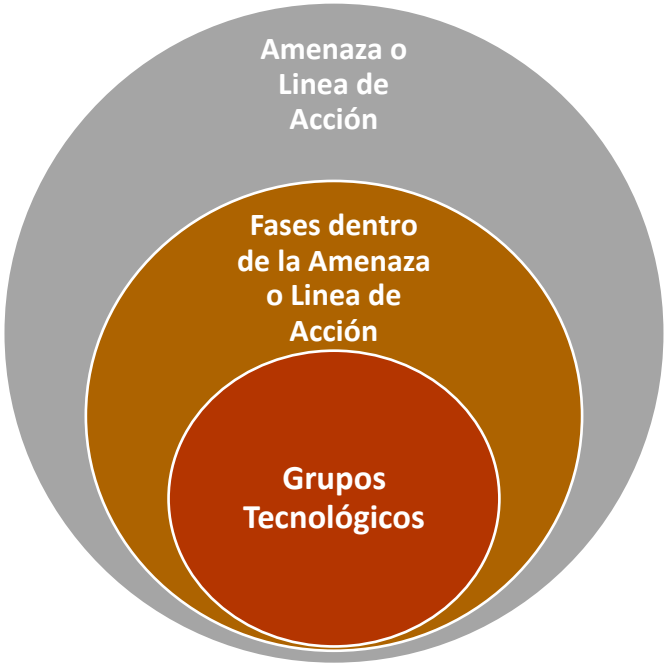


Ilustración: Esquema de la taxonomía

Además, se podría realizar una aplicación de la taxonomía de forma matricial. Para ilustrarlo de forma clara y concisa, se ha realizado un organigrama ejemplo con distintos posibles grupos de la línea de acción Lucha contra el terrorismo. Este organigrama tendría la siguiente forma:

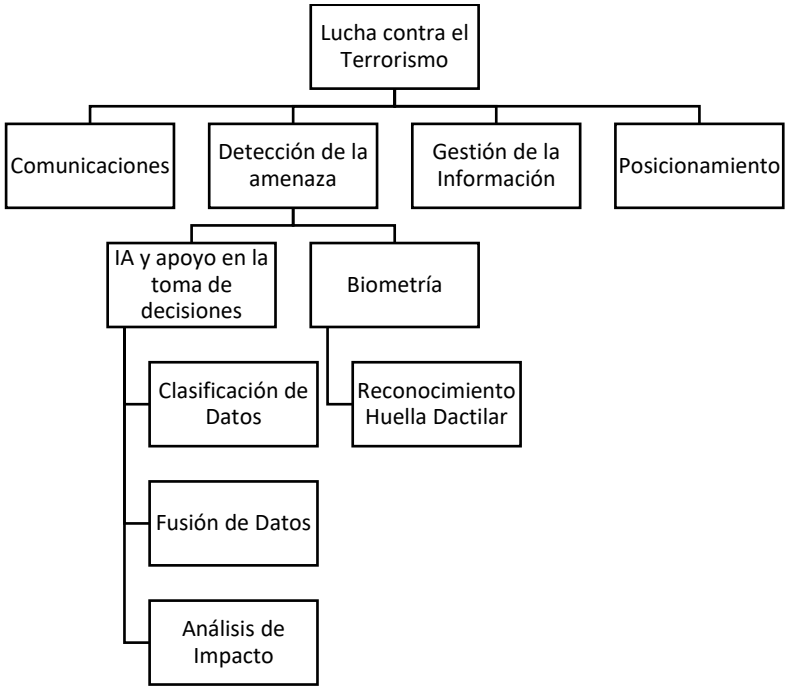


Ilustración: Ejemplo Organigrama de la Taxonomía

Se debe mencionar que esta taxonomía final no es definitiva. Debido al carácter dinámico del sector, esta matriz podría sufrir cambios en el futuro debido a las irrupciones tecnológicas y a los cambios en las competencias de las Fuerzas y Cuerpos de Seguridad. En este proyecto se hace hincapié en que el valor añadido del mismo es la metodología escogida para estructurar el sector industrial objeto del estudio. Esto es, en breves palabras, enfocar las amenazas o líneas a combatir, estudiar las competencias de las distintas FCS a los que irán enfocados los productos y servicios, dividir en sectores estas amenazas, e identificar los grupos tecnológicos útiles para enfrentar a los mismos.

Conclusiones

Se concluye finalmente que este sector industrial es un pilar fundamental dentro de la sociedad. Adquiriendo cada día más importancia debido a la rápida digitalización de la misma, y las nuevas amenazas que están surgiendo. Además, su carácter principalmente tecnológico, de constante innovación y desarrollo hace de él un sector estratégico, activo de gran valor añadido, capaz de robustecer la economía nacional y posicionar el país como referente internacional. Es por ello, y por el carácter difuso ya explicado anteriormente de este sector, que este proyecto aporta valor al futuro de la seguridad nacional. Sentar las bases de la organización de este mejoraría el planteamiento estratégico de las distintas empresas, enfocando sus productos y servicios a los intereses reales de los agentes e instituciones beneficiarios. Además, atraería nuevos fondos y financiación, tanto nacional como internacional, ofreciendo apoyo económico a los proyectos que se están llevando a cabo, y como se ha explicado anteriormente, apoyando la economía nacional y mejorando el futuro de este país.

Referencias

“Estrategia de Seguridad Nacional, Departamento de Seguridad Nacional,” 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf.

“Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional,” 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN%202017.pdf.

“Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional,” 2018. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN2018.pdf.

“Estrategia Anual de Ciberseguridad,” 2019. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf.

“TEDAE,” 2018. [Online]. Available: https://www.tedae.org/es/publicaciones/etiqueta/memorias-de-actividad.

CHARACTERIZATION OF THE INDUSTRIAL SECURITY SECTOR AND ITS TECHNOLOGICAL TAXONOMY

Author: Mayo Navas, Manuel

Director: Tébar Losa, Clara

Collaborating Entities: ICAI - Universidad Pontificia de Comillas

TEDAE

Abstract

Project Summary

The project in question deals with the characterisation of the Industrial Security Sector and its subsequent characterisation. This is due to the fact that it is a broad and complex technological sector, recently separated from the Defence one. Moreover, security, as a concept, is in itself broad and complex. This is because it covers different aspects of society, such as physical security, cyber security, economic security, institutional and political security, transport security and environmental security. In addition, it should be considered that, as a heterogeneous society, security falls on a large number of agents and actors, both public and private.

It is also worth highlighting the breadth of technologies used by the different companies belonging to the sector, and their transversality. These could be used in many other sectors traditionally catalogued as aeronautics, naval, telecommunications or defence. Moreover, most companies are part of the leading group in innovation and investment within their market segments. It is for this reason that increasing the competitive advantage and positioning the national industry in a position of strength within the international competition would establish a strategic pillar that would strengthen the economy.

It is for all these reasons that it is intended to carry out a characterization and subsequent taxonomy of the Industrial Security Sector. This could define the scope in which companies should focus their efforts, gaining competitive advantage and taking advantage of the opportunities that the market currently offers.

Methodology

The project is divided into several parts. In the first part, the Industrial Security Sector is characterized and defined, as well as a brief economic analysis thanks to the data provided by the collaborative entity TEDAE.

It is concluded that the definition of the sector would be the set of companies, mainly of a technological nature, dedicated to the development, improvement and creation of products and services to provide the Security Forces and Corps and associated agents with all that is necessary to fulfil their mission. In addition, all those dedicated to innovation and scientific research will be included, as long as their purpose is to provide or improve the security of society.

After analysing the different segments to which the companies belonging to the sector are focused, the economic data is observed. They employ a large number of people, with a turnover in excess of 150 million euros, 22% of which comes from exports, in addition to reinvesting these results in innovation in a higher percentage than in other sectors, and finally, they have a productivity 2,6 times the national average. It is concluded that it is a healthy sector, in full growth and expansion, focused on technology, always attractive for new investments.

The following section mentions the different sources of European financing that could be of interest to companies. It concludes that the most important programmes from which they could benefit are three: Horizon 2020, the European Structural Investment Funds, and the European Funds for Strategic Investment. All of them have programmes focused on new technologies, innovation and research, even programmes specifically dedicated to promoting the development of products and services in the field of security.

Subsequently, a study of the art of different taxonomies of the sector that have been carried out previously is carried out. Five taxonomies are chosen, most of them come from studies carried out by the European Commission, and a base is made of the best aspects of each one to use them in this project.

Having mentioned the foundations for the creation of the taxonomy, we proceed to select the different criteria or levels available. In order to delimit the border of the Industrial Sector, it was decided to choose the different lines of action or threats identified by the DHS. But there is a problem, these lines of action have segments belonging to the Defence sector, so it is necessary to make a differentiation. For this differentiation, the different competences of the Security Forces and Corps and of the Navy and its different corps have been investigated. With them, and carrying out an analysis of the lines of action, the border of the Industrial Security Sector has been delimited.

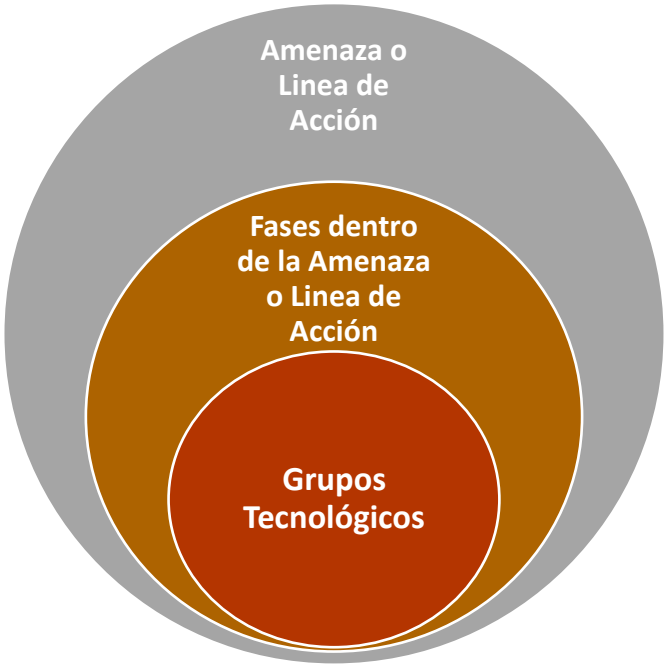
The next level would be to divide the different lines of action into phases, since there will be specific products according to the situation in which the different FCS find themselves when facing threats. The following have been chosen: Communications, Detection, Information Management, Positioning, Risk Assessment, Knowledge or Awareness of the situation, Training, Doctrine and Operations, Incident Response.

Finally, all products and services have been grouped into technological families according to their common purpose. These groups would be: Artificial Intelligence and Decision Support, Biometrics, Biotechnology, CBRNE, Communications, Electronic Authentication, Energy, Forensics, GIS, Human Sciences, Integrated Platforms, IT, IT

Security, Materials, Navigation, Sensors, and Signal Processing. This would explain the different criteria followed for the realization of the taxonomy.

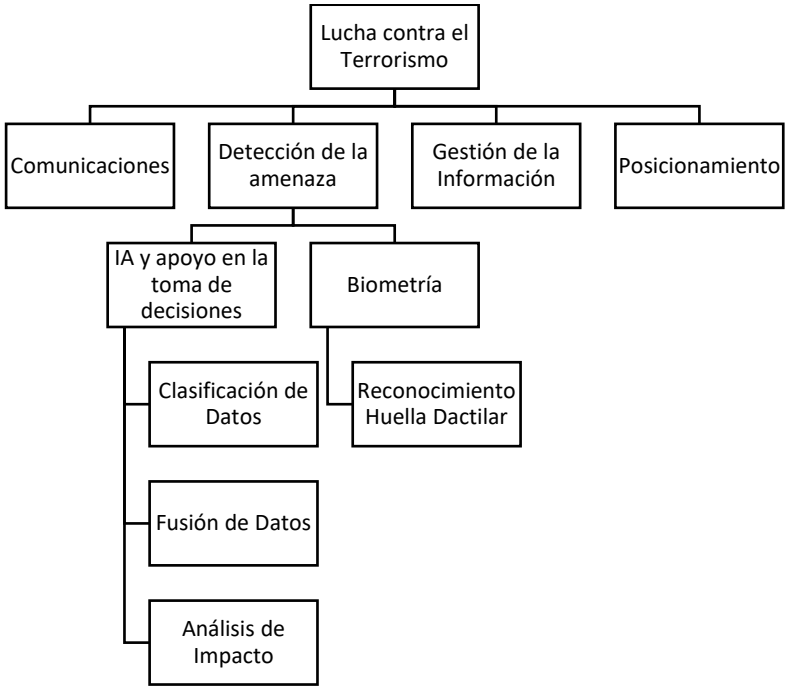
Results

The final result is a taxonomy composed by three rings. It has been considered, after the analysis of the competences of the different Security Forces and Corps, that the lines of action that would delimit the border would be: Fight against Terrorism, Cybersecurity, Fight against Organized Crime, Economic Security, Non-proliferation of weapons of mass destruction, Management of migratory flows, Counterintelligence, Maritime Security, Protection of Critical Infrastructures, Protection of outer airspace, Security against pandemics and epidemics, and Preservation of the Environment. The rings that make up the taxonomy with respect to the three levels described above would have the following form:



Ilustration: Taxonomy scheme

In addition, a matrix application of the taxonomy could be made. To illustrate this concisely, an example organigram has been made with different possible groups of the line of action against terrorism. This organigram would have the following form:



Ilustration: Example Taxonomy Organization Chart

It should be mentioned that this final taxonomy is not definitive. Due to the dynamic nature of the sector, this matrix could undergo changes in the future due to technological breakthroughs and changes in the competences of the Security Forces and Corps. In this project it is emphasized that the added value is the methodology chosen to structure the industrial sector object of the study. This means, in short, focusing on the threats or lines to be combated, studying the competences of the different FCS to which the products and services will be focused, dividing these threats into sectors, and identifying the technological groups useful for dealing with them.

Conclusions

It is finally concluded that this industrial sector is a fundamental pillar within society. Acquiring more importance every day due to the rapid digitalization of it, and the new threats that are emerging. In addition, its mainly technological character, of constant innovation and development makes it a strategic sector, active with great added value, capable of strengthening the national economy and positioning the country as an international reference. It is for this reason, and due to the diffuse nature of this sector already explained above, that this project adds value to the future of national security. Laying the foundations for the organisation of this would improve the strategic approach of the different companies, focusing their products and services on the real interests of the beneficiary agents and institutions. In addition, it would attract new funds and financing, both national and international, offering economic support to the projects that are being carried out, and as explained above, supporting the national economy and improving the future of this country.

References

"Estrategia de Seguridad Nacional, Departamento de Seguridad Nacional," 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf.

"Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional," 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN%202017.pdf.

"Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional," 2018. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN2018.pdf.

"Estrategia Anual de Ciberseguridad," 2019. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf.

"TEDAE," 2018. [Online]. Available: https://www.tedae.org/es/publicaciones/etiqueta/memorias-de-actividad.

Agradecimientos

No son pocas las personas que han interferido en este Trabajo de Final de Máster a lo largo de su elaboración. Personas que me han animado tanto en los momentos de flaqueza como aquellos en los que estaba más motivado. Además, todos aquellos que han aportado sus conocimientos y experiencias para que este proyecto salga adelante. Espero ser capaz, con estas palabras, de agradecer consecuentemente el esfuerzo y dedicación de todas aquellas personas.

Empezando por el ámbito personal, en primer lugar debería agradecer todo el esfuerzo a mis familiares. Tanto por su apoyo económico, emocional y por estar ahí siempre que los he necesitado, en los momentos de fuerte carga de trabajo como en los de celebración. Este proyecto no habría salido adelante sin su ayuda y cariño, por lo que se merecen este primer puesto en la lista de agradecimientos.

En segundo lugar, estarían mis compañeros de Máster y amigos, aquellos que conocí hace poco menos de dos años, en los que he encontrado amistades que duran para toda la vida. Además de su apoyo, me han contagiado su tenacidad y capacidad de trabajo, su ambición y afán de superación, animándome a ser la mejor versión de mí mismo. Estos dos años de formación han sido una etapa muy importante en mi vida, que me ha marcado tanto en el ámbito personal como profesional, y todos ellos son responsables de lo que soy hoy por hoy. También cabe destacar a todos mis amigos que viven en mi ciudad natal, que desde la lejanía, me han seguido apoyando en mi ambición laboral.

Y para finalizar, en el ámbito profesional no son menos las personas a las que debo agradecer su apoyo, ayuda y recursos. En primer lugar, debería agradecer desde la cálida acogida, hasta su apoyo día tras día a todos los trabajadores de TEDAE que han compartido oficina conmigo a lo largo de los seis meses de prácticas realizados. En especial, quiero destacar a la Coordinadora del Polo de Seguridad, que ha sido mi guía en todo este proceso. Y por último agradecer todo su esfuerzo, trabajo y dedicación a mi tutora y COO de la empresa, Clara Tébar, y a mi coordinador y Presidente, Jaime Rábago. También quería agradecer a todas las empresas socias de TEDAE su colaboración y aportación de información para facilitar que este proyecto saliese adelante.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

En este proyecto se procede a realizar la caracterización y posterior taxonomía del sector de la Seguridad. Se pretende delimitar las fronteras del mismo y que ámbitos abarca, pero la seguridad, como concepto, ya es en sí misma amplia y compleja. Entre otros, abarca distintos aspectos de la sociedad:

- Seguridad física. Este aspecto se centra tanto en la protección de los bienes como de las personas a las que pertenecen, al igual que infraestructuras, haciendo especial énfasis en aquella denominadas como críticas. Para ello persiguen toda amenaza o agente que pueda resultar dañino o peligroso para este aspecto, entre los que se encuentran como más comunes el crimen organizado, delitos comunes, tráfico ilegal y terrorismo.

- Seguridad cibernética. Aspecto que se centra en preservar, proteger y garantizar el funcionamiento de los sistemas e infraestructuras telemáticas, haciendo énfasis en la información que contienen. Este aspecto es de creciente importancia en una sociedad cada vez más dependiente de las nuevas tecnologías y donde la digitalización es una realidad en todo ámbito de la sociedad.

- Seguridad económica. Aspecto que queda definido al asegurar y potenciar, de forma sostenible, un modelo de crecimiento económico, luchas contra toda actividad ilícita, disminuir los desequilibrios entre mercados, fomentar la resiliencia de la economía española y potencias su presencia en el extranjero a través del correcto funcionamiento de los agentes y las estructuras económicas.

- Seguridad institucional y política. Con el fondo siempre presente de las leyes, mantener el correcto funcionamiento de la sociedad fomentando la estabilidad de toda estructura política e institución establecida dentro de los marcos de la legalidad.

- Seguridad del transporte. Este aspecto centra su ámbito en garantizar el ordenado transito tanto de personas como de mercancías por todo el territorio nacional y las infraestructuras diseñadas y construidas para el efecto. Dicho flujo debe ser libre, aun teniendo control de acceso y permanencia gracias a sus fronteras.

- Seguridad medioambiental. Este último aspecto queda definido a través de las siguientes premisas. La primera, se debe reparar, evitar y prevenir todo daño humano producido al medioambiente. Además, y enlazado con la premisa anterior, se debe garantizar la pervivencia de la biodiversidad y del ecosistema español minimizando las consecuencias de la actividad humana o las posibles catástrofes naturales que ocurran.

Como queda demostrado en los apartados explicados anteriormente, la seguridad toca y se encuentra presente en todos y cada uno de los ámbitos de la sociedad. El problema

es que esta sociedad, heterogénea, está compuesta por distintos actores, ya sean público o privados, y la seguridad no solo debe recaer en los primeros. Los agentes privados deben implicarse de forma especial debido al creciente peso que tienen en la sociedad, si esta quiere tener unos cimientos firmes y seguros.

Por todo ello, la Industria de la Seguridad se constituye como un importante actor. Ya sea a través de los servicios o productos que proporciona, tiene una gran repercusión tanto en la seguridad de personas, empresas e instituciones. Es más, son los encargados de proporcionar cualquier sistema o equipo que precisen las Fuerzas y Cuerpos de Seguridad del Estado para que puedan cumplir con su cometido a través de sus capacidades operativas.

Uno de los grandes problemas que tiene este sector es la amplitud de ámbitos, su heterogeneidad y transversalidad de tecnologías, debido a que estas podrían entrar dentro de otros muchos sectores catalogados tradicionalmente como telecomunicaciones, naval, aeronáutica, automoción o defensa. Estos mismos productos, modificados o no, desarrollados o adaptados para las especificaciones necesarias, pueden perfectamente cumplir las funciones que se precisan en seguridad, diferenciándose de los servicios, productos y equipos de otros sectores.

En gran parte, todas las empresas dedicadas al Sector de la seguridad pertenecen al grupo líder en innovación e inversión en sus propios segmentos de mercado dentro de la industria. Esto se debe a que sus productos y servicios se desarrollan a través de tecnologías de alto valor añadido. Mantener, fomentar y potenciar esta ventaja competitiva es imprescindible para impulsar unas condiciones de mercado favorables, asegurando el sector Industrial de la Seguridad nacional en el mercado europeo, constituyendo un importante activo estratégico.

Cabe destacar la diferencia entre el Sector Industrial de la Seguridad al que se hace referencia con el mercado de la seguridad tradicional. Este último se centra en los servicio y productos que se venden al público, ya sean sistemas de alama, como de detección e identificación. En este aspecto del mercado de la seguridad, la ventaja competitiva reside en el bajo coste de los productos.

Por todos estos motivos descritos anteriormente, se proponer realizar una taxonomía del Sector Industrial de la Seguridad para definir el ámbito de esfuerzo de todas las empresas que lo componen. Con ello se pretendería potenciar la ventaja competitiva y tecnológica de que se dispone, buscar nuevas oportunidades de negocio y posicionar el sector a nivel europeo, incrementando así la presencia y economía del estado.

2. SECTOR INDUSTRIAL DE LA SEGURIDAD

En este apartado se pretende realizar una caracterización del Sector Industrial de la Seguridad. Para ello, se hará una definición de lo que es el sector, sus características, se comentará sobre los representantes más importantes a nivel nacional, y algunas cifras del sector.

Se definirá el Sector Industrial de la Seguridad como el conjunto de empresas, principalmente de carácter tecnológico, dedicadas al desarrollo, mejora y creación de productos y servicios para proveer a las Fuerzas y Cuerpos de seguridad y agentes asociados de todo lo necesario para cumplir con su cometido. Además, se incluirán todas aquellas dedicadas a la innovación e investigación científica, siempre que tengan como fin proveer o mejorar la seguridad de la sociedad.

Para poder realizar un análisis del sector a nivel nacional, primero se debería centrar el foco en un cierto número de empresas. Hay multitud de empresas de lo que se denomina "seguridad tradicional", pero cuando se habla de empresas tecnológicas el número se ve reducido. Tras un breve estudio del panorama empresarial nacional, se ha decidido optar por estudiar las empresas pertenecientes a TEDAE, Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio. Como es lógico, solo se han escogido aquellas que pertenezcan al polo de Seguridad.

A continuación, se representará la imagen de todas las empresas comentadas anteriormente:

Ilustración 1: Empresas pertenecientes al Polo de Seguridad

Una vez cercado el foco de estudio, se ha hecho una revisión de todos los productos y servicios que ofrecen estas empresas. Para ello, se han ido visitando una a una todas las páginas Web oficiales, estudiado sus catálogos y ofertas, recopilando datos para su posterior análisis. Después del informe realizado, que no se presentará en este proyecto debido a que no es el objeto de este, se ha realizado un breve resumen y agrupación de los mismo.

La gran mayoría de productos y servicios podrían agruparse en distintas líneas de acción o amenazas comunes en todas estas empresas, que es donde el sector está enfocando tanto el esfuerzo económico como el esfuerzo en I+D+i. Estas líneas de acción serían las siguientes:

- Seguridad Marítima y Control de Fronteras
- Protección de Infraestructuras Criticas
- Vigilancia y Seguridad Privada
- RPAs
- Plataformas Integradas
- Ciberseguridad

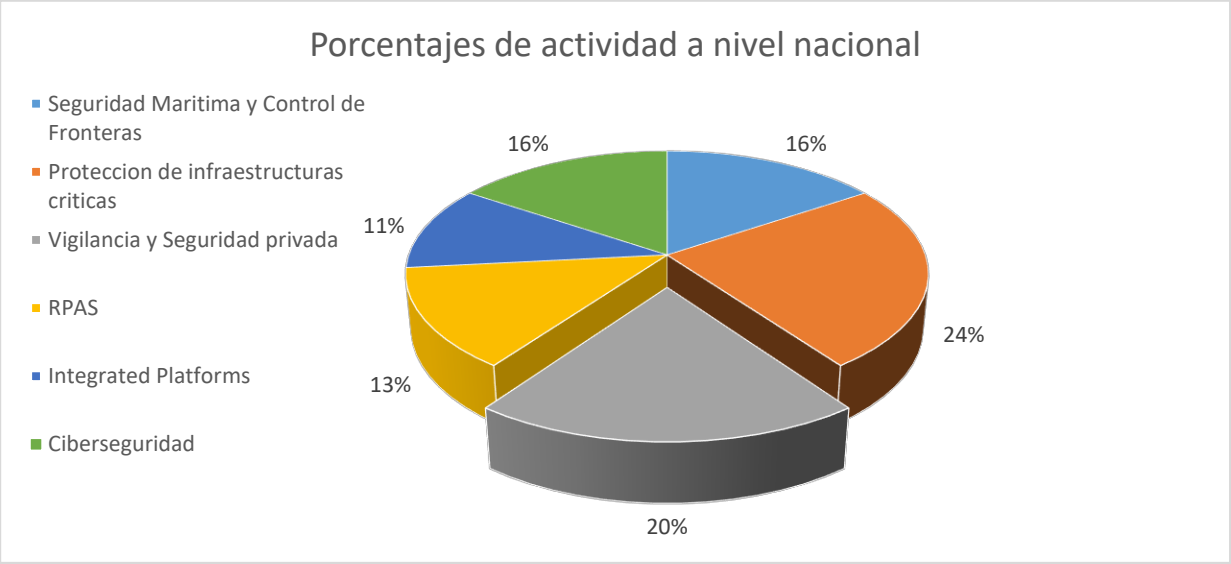


Ilustración 2: Porcentajes de actividad de las empresas

Estos porcentajes están referido a la actividad de las empresas, no a los datos de facturación ni de cuota de mercado. Se puede observar que el 20% de las empresas tiene productos que llamamos de "seguridad tradicional", y que el porcentaje más alto se dedica a la protección de infraestructuras críticas. Cabe destacar que, aunque solo el 11% se dedique a la seguridad marítima y control de fronteras, son las empresas de mayor tamaño y facturación (Navantia), copando casi toda la demanda del mercado. Cabe destacar las nuevas irrupciones dentro del Sector Industrial de la Seguridad que son los RPAS o UAVs y la Ciberseguridad. Ambos productos o servicios son aquellos que están al alza tanto en demanda, como en inversión e innovación. Se hablará específicamente de las cifras de ciberseguridad a continuación.

Para poder realizar un estudio económico del sector industrial de la Seguridad, se precisan cifras y datos de facturación. Debido a la opacidad de las empresas, es muy difícil realizar un examen exhaustivo. Esto se ha solucionado en gran medida gracias a TEDAE, que ha brindado sus datos económicos finales de las empresas asociadas, para así poder realizar un análisis. Estos datos han sido extraídos a través de su Infografía anual del Sector de la Seguridad PONER ANEXO. Cabe destacar que este es el primer año

que se realiza este estudio para el Polo de Seguridad. Después de que las empresas entregasen sus datos económicos a TEDAE, esta asociación realizó un breve estudio y saco las siguientes conclusiones.

- Emplea a 974 personas de forma exclusiva
- Factura 155 millones de euros
- Reinvierte en innovación el 11% de su facturación
- El 22% de su facturación proviene de productos exportados
- La productividad del sector es 2,6 veces la media del sector

Siendo un sector delimitado recientemente, sin estudios previos económicos, todas estas señales indican que es un sector sano, en pleno crecimiento y en expansión, enfocado a la tecnología, siempre atractivo para las nuevas inversiones, y que fomenta la innovación. Innovación en productos con posibles aplicaciones en otros campos, con repercusión directa en la sociedad, de recompensa tangible y reconocimiento público. Es por ello que este sector augura un crecimiento exponencial en los próximos años, sobre todo en sectores como los RPAS y la ciberseguridad, donde España encabeza una gran expansión gracias a lo atractivo del proyecto y al capital que está atrayendo, tanto a nivel nacional como europeo.

3. FUENTES DE FINANCIACIÓN EUROPEAS

En este apartado se realizará un breve estudio sobre las fuentes de financiación de las empresas dentro del Sector Industrial de la Seguridad. Concretamente, se hará un estudio de las fuentes que provengan de la Unión Europea.

Si cualquier empresa del Sector Industrial de la Seguridad buscase financiación, podría hacerlo a través de tres programas diferentes:

- Horizonte 2020
- Fondos Estructurales y de Inversión Europeos
- Fondos Europeos para Inversiones Estratégicas (FEIE)

3.1. HORIZONTE 2020

Es, definitivamente, el programa de innovación, desarrollo e investigación más ambicioso de la Unión Europea con casi 80.000 millones de euros de presupuesto. La finalidad última de este tipo de fondos es mejorar, asegurar y potenciar la competitividad europea a nivel Global.

El objetivo se pretende alcanzar fomentando la inversión en las áreas de investigación, innovación, crecimiento sostenible, inteligente e integrador. Con esto se pretende hacer hincapié en que Europa debe esforzarse en promover el crecimiento económico a través de la creación de tecnología y ciencia competitiva a nivel mundial.

Los tres pilares que rigen este programa son "Ciencia Excelente", "Liderazgo Industrial, y "Retos de la Sociedad". Constituyen los tres paquetes fundamentales, además de otros tantos paquetes con menor presupuesto, en donde se engloban los distintos fondos y recursos, cada cual con distintos requisitos para poder financiar proyectos. A continuación, se realizará un breve resumen de los más relevantes:

- *"Ciencia y Excelencia".* Objetivo es atraer el mejor y nuevo talento, promoviendo el intercambio de ideas y situar a la Unión Europea en una posición de importancia en el ámbito científico. Está compuesto por los siguientes Programas.
    - *"Investigación en las Fronteras del Conocimiento Financiada por el Consejo Europeo de Investigación (CEI)".* Presupuesto de 13.095 millones de euros.
    - *"Acciones Marie Sktodowska-Curie".* Presupuesto de 6.162 millones de euros.
    - *"Tecnologías Futuras y Emergentes".* Presupuesto de 2.696 millones de euros.
    - *"Infraestructuras de talla internacional".* Presupuesto de 2.488 millones de euros.

- *"Liderazgo Industrial*". Con el objeto de establecer colaboraciones público-privadas, este fondo promueve la inversión en toda tecnología de gran potencial y estratégica para que el sector privado apueste por invertir más en investigación y así alcanzar la excelencia en Europa.
    - *"Liderazgo en las tecnologías industriales y de capacitación".* Presupuesto de13.557 millones de euros, de los cuales 3.000 millones de euros fueron específicos para PYMEs.
    - *"Acceso a la financiación de riesgo".* Presupuesto de 2.842 millones de euros.
- *"Retos de la Sociedad".* Este programa está especialmente enfocado para reportar beneficios tangibles para toda la población de los países miembros de la UE. Se han identificado siete aspectos que disponen de prioridad a los que se les ha proporcionado financiación.
    - *"Salud y Bienestar".* Presupuesto de 7.472 millones de euros.
    - *"Seguridad alimentaria y explotación sostenible de recursos biológicos".* Presupuesto de 3.851 millones de euros.
    - *"Energía sostenible".* Presupuesto de 5.931 millones de euros.
    - "Movilidad integrada y ecológica". Presupuesto de 6.339 millones de euros.
    - *"Acción por el clima, medioambiente, eficiencia de los recursos y materias primas".* Presupuesto de 3.081 millones de euros.
    - *"Europa en un mundo cambiante: sociedades inclusivas, innovadoras y reflexivas".* Presupuesto de 1.309 millones de euros.
    - *"Sociedades seguras: proteger la libertad y la seguridad de Europa y sus ciudadanos".* Presupuesto de 1.695 millones de euros.
- *"Difundir la Excelencia y Ampliar la Participación".* Con este presupuesto se pretenden apoyar el trabajo en equipo entre instituciones, establecer relaciones entre centros de investigación, y creación de políticas de apoyo para innovación e investigación. Presupuesto de 816 millones de euros.
- *"Ciencia con y para la sociedad".* Promueve la estrecha colaboración entre sociedad y ciencia para poder atraer y acercar talento a sus filas. Presupuesto de 462 millones de euros.
- *"Investigación en materia nuclear para todos los ciudadanos".* El presupuesto ofrecido por la Unión Europea se centra en financiar toda investigación asociada con la medicina, gestión de residuos radiactivos, usos del material en la industria, aplicaciones en la agricultura, y seguridad. Presupuesto de 1.603 millones de euros.
- *"Instituto Europeo de Innovación y Tecnología (EIT)".* Financiación para promover la integración de la investigación, innovación y enseñanza superior a través del marco de las CCI. Con ello se pretende crear un nuevo estímulo al crecimiento, la innovación, el espíritu emprendedor y la competitividad.

Presupuesto de 2.711 millones de euros.

[20]

A continuación, se presentará un breve resumen gráfico de todos los fondos:

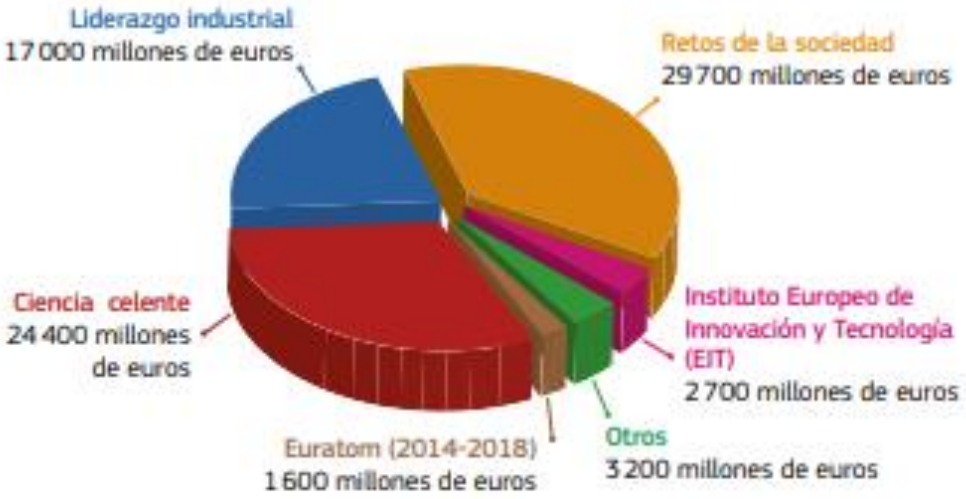


Ilustración 3: Gráfico Resumen H2020. Fuente: Comisión Europea20

El Sector Industrial de la Seguridad podría buscar todo tipo de financiación a través de estos programas. Específicamente, del presupuesto ofrecido a través de "Liderazgo Industrial" y "Ciencia Excelente", ya que cualquier empresa del sector cumpliría con los requisitos exigidos para acceder a los fondos. Cabe destacar que la Unión Europea ha dedicado un programa por completo a la financiación de cualquier proyecto enfocado a la seguridad a través de "Retos de la Sociedad". Es en este donde toda empresa que pretenda conseguir financiación debe enfocarse, ya que el único requisito expuesto es pertenecer al sector, sea cual sea el tipo de industria y si fomenta o no la innovación e investigación.

3.2. FONDOS ESTRUCTURALES DE INVERSION EUROPEOS

A continuación, se presentará uno de los fondos más importantes a nivel europeo, que abarca más de la mitad del presupuesto de la Unión Europea para este tipo de programas, y son los Fondos Estructurales de Inversión Europeos (o fondos EIE). Tanto la Comisión Europea como los países miembros de la UE son responsables de la gestión conjunta de estos programas al apoyo del desarrollo económico.

Gestionados a través de acuerdos de asociación por los propios países miembros, el objeto de estos fondos no es otro que el de fomentar la creación de empleo y crecimiento económico, compatible con el respeto y mantenimiento del medioambiente europeo. El foco de este tipo de financiación se centra en cinco sectores diferentes, los cuales son:

- PYMEs
- Economia hipocarbónica
- Gestión sostenible de los recursos naturales
- Tecnologías Digitales
- Investigación e Innovación

Al ser cinco los sectores en los que se centra la totalidad de los recursos económicos se han creado cinco fondos diferentes en los que se reparte todo el presupuesto, centrando la inversión en cada uno de los temas. Estos fondos tienen los siguientes nombres:

- Fondo Europeo de Desarrollo Regional, o FEDER.

Enfocados a fomentar el desarrollo en las regiones donde haya un desequilibrio frente a otras.

- Fondo Social Europeo, o FSE

Invirtiendo directamente en todo lo referente con el capital humano europeo, pretende apoyar todo proyecto o idea relacionado con la creación de empleo dentro de los países miembros.

- Fondo de Cohesión, o FC

El objeto de este fondo consiste en financiar todo proyecto de medioambiente y transporte, pero con una excepción. Solo ira destinado a aquellos países que dispongan de una renta per capita mejor al 90% en comparación con la media de los países miembros de la Unión Europea. España queda totalmente excluida por este criterio, por lo que este fondo quedará fuera del estudio.

- Fondo Europeo Agrícola de Desarrollo Rural, o Feader

Fondo dedicado exclusivamente a la resolución de problemas e inversión en las zonas rurales de todos los países miembros de la Unión Europea. Sobre todo, centrado en

aquellas empresas dedicados a la ganadería y agricultura, en proyectos como Granjas Ecológicas, bioenergía y biocombustibles.

- Fondo Europeo Marítimo y de Pesca, o FEMP

Enfocado primordialmente a las zonas litorales y comunidades costeras, estos fondos tienen el objeto de diversificar la economía, promover la pesca sostenible, y mejorar la calidad de vida de la población de estos lugares.

Examinando las distintas características de los cinco fondos mencionados hasta ahora, el Sector Industrial de la Seguridad podría verse beneficiado por los dos primeros, tanto los FEDER para el desarrollo regional como los FSE. Ambos comparten objetivos comunes con el desarrollo del sector, por lo que diferentes proyectos que precisen financiación podrían optar y aplicar por dichos recursos.

3.3. FONDOS EUROPEOS PARA INVERSIONES ESTRATEGICAS (FEIE)

Este fondo es uno de los pilares fundamentales en las que se sustenta el programa europeo Plan de Inversiones para Europa. Su acrónimo nunca debe confundirse con el de los Fondos EIE, explicado anteriormente, ya que son programas completamente distintos con recursos independientes. El objeto de este tipo de fondo era paliar la falta de inversión y la total desconfianza de la inversión fruto de la crisis económica mundial sufrida en años anteriores.

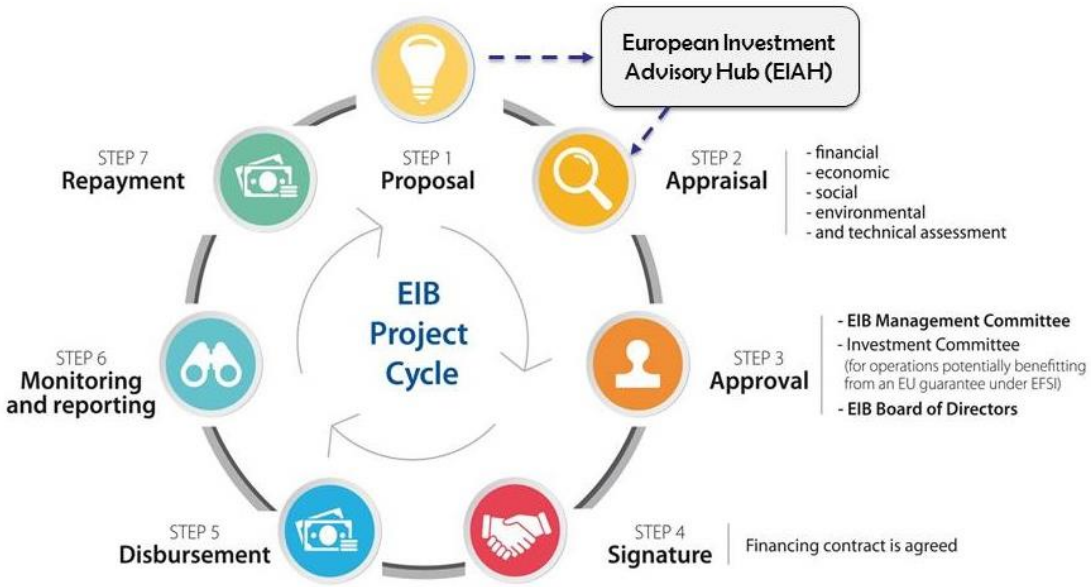


Ilustración 4: Proceso de Petición de Fondo. Fuente: Comisión Europea22

En estrecha colaboración con el socio estratégico de este proyecto, El Grupo del Banco Europeo de Inversiones, o grupo BEI, el fin de este fondo es apoyar y fomentar toda inversión considerada estratégica en sectores clave. Estos pueden ser muy variados:

- Proyectos sociales
- Sanidad
- Educación
- Tecnologías Digitales
- Agricultura
- Medioambiente
- Investigación e Innovación
- Energías Renovables
- Eficiencia Energética
- Infraestructuras
- PYMES

En un principio, el presupuesto de este fondo era de unos 315.000 millones de euros, pero gracias al éxito de este programa, en 2016 se amplió hasta querer alcanzar los 500.000 millones de euros en inversiones de nuevos proyectos para 2020. Actualmente, los porcentajes de inversión por área son los siguientes

Ilustración 5: Porcentaje de Inversión FEIE. Fuente: European Investmen Bank24

Este tipo de fondos funciona de forma distinta, ya que es la UE la que ofrece al Grupo del Banco Europeo de Inversiones cobertura frente a la posible primera perdida. Como consecuencia de esta protección, se financian proyectos con un nivel de riesgo mayor al que normalmente estarían dispuestos a asumir. Sin cuotas, y bajo el riguroso criterio de un Comité de Inversión independiente, la financiación es concedida en función de la demanda.

El sector Industrial de la Seguridad puede verse beneficiado por este tipo de fondos, ya que al ser un sector centrado en las tecnologías, plataformas integradas, y la innovación, entra en su totalidad en el marco de objetivos a financiar. Por ello, toda empresa, ya sea PYME o con un cierto tamaño, debería aprovechar precisamente este tipo de fondo para financiar aquellos proyectos más arriesgados, y consecuentemente de difícil búsqueda de inversión para los mismo, debido al más relajado criterio de aceptación explicado anteriormente.

4. ESTUDIO DEL ESTADO DEL ARTE

A continuación, se realizará un estudio del estado del arte de las posibles taxonomías realizadas anteriormente y por otros organismos del sector de la seguridad. Debido a la importancia del sector, y las grandes oportunidades de negocio que existen, no son poco los que han intentado crear una estructura organizativa. Aun así, todas han sido a petición de organismos, tanto públicos como privados, centrados en un solo ámbito, ya sea el tecnológico o una rama del mismo. Por ello, estas taxonomías no cumplen los requisitos necesarios que se precisan de este proyecto, haciendo palpable la necesidad del desarrollo de una nueva metodología para cumplir con todas las expectativas.

Tras una búsqueda exhaustiva, se han encontrado cinco taxonomías procedentes de fuentes y organismos fiables. Primero, y antes de su análisis, se procederá a la enumeración de las mismas.

Los distintos documentos son:

- *"Taxonomy of Security Product, Systems and Services"*. El acrónimo del proyecto es "CRISP", y su título "Evaluation and Certification Schemes for Security Products".
- "Report on Technology Taxonomy and Mapping". El acrónimo del Proyecto es "PACT", y su título "Public Perception of Security and Privacy: Assesing Knowledge, Collecting Evidence, Translating Research into Action".
- "EDA Technology Taxonomy"
- "STACCATO, Main Conclusions and Recommendations on the European Security Equipment Market (ESEM) and Executive Summary of the Final Study Report"
- "European Technology Watch on Security", Acrónimo del Proyecto "STRAW".

Una vez nombrados todos los documentos, se procederá al análisis de cada uno de ellos para establecer las bases de la taxonomía que se debe realizar en este proyecto.

4.1. CRISP

En la primera taxonomía, de las cinco la mejor base para el estudio que se va a acometer en este proyecto, se pueden encontrar distintas estructuras. Para organizar la taxonomía del sector de la seguridad se realiza una división en tres niveles. En el primer nivel se puede observar las áreas o amenazas delimitadas para el estudio, que son las siguientes:

- Gestión de fronteras
- Infraestructuras críticas (por ejemplo, generación/transmisión de electricidad, gas y agua)
- Sistemas bancarios y financieros
- Centros de preparación para emergencias/Gestión de crisis
- Hogares
- Industria y comercio

- Lugares públicos y semipúblicos, incluyendo entretenimiento, edificios gubernamentales,
- Hospitales, campus, deporte, cultura, lugares de culto, etc.
- Transporte, incluidos la aviación, el transporte marítimo y el transporte ferroviario

Estas siete amenazas fueron elegidas a partir de la síntesis de las áreas identificadas al examinar las categorizaciones de los grandes proveedores de seguridad, todos ellos habiendo hecho una clasificación de los equipos de seguridad en función de la necesidad percibida del cliente.

Por otro lado, el siguiente nivel tiene como aspecto de estudio la tecnología utilizada. Se realizó un breve resumen de donde se extrajeron ocho apartados donde poder proyectar todos los productos disponibles:

- Control de acceso
- Seguridad de activos/cargas
- Seguridad cibernética
- Seguridad de empleados/visitantes/pasajeros
- Prevención de pérdidas
- Seguridad del perímetro/área/edificio
- Seguridad en los puntos de transito
- Concienciación de la situación

Como se puede observar, no hace foco en todas las tecnologías disponibles, ya sean emergentes o disponibles, por lo que se obtiene como resultado una taxonomía restringida con la que poder delimitar todo el sector Industrial de la Seguridad.

En el tercer nivel se analizaron las necesidades o funciones. Como ejemplo del porqué de la necesidad de este tercer nivel se puede utilizar el siguiente. Los sistemas de alarma, que controlan y detectan, también se comunican por medio de señales, visuales o sonoras. Por ello se realiza esta división posterior, que es la siguiente:

- Evaluar
- Autorizar
- Comunicar
- Control
- Crear conciencia de la situación
- Detener
- Identificar
- Recopilación, almacenamiento y gestión de la información para la posterior producción en inteligencia
- Localizar
- Prevenir/proteger
- Rastrear
- Verificar

En el caso de los servicios, la división por niveles, que es el interés de este estudio, es la misma. Por ello no se entrará en detalle en la propia clasificación de los mismo ya que en este proyecto se realizará una propia.

Esta metodología por niveles será en gran medida la base para la creación de la taxonomía final de este proyecto. Esto se debe a que con este sistema se podrá abarcar la totalidad del sector Industrial de la Seguridad. Aun así, se deberá ampliar el foco de estudio de forma considerable ya que los temas tratados en esta taxonomía son insuficientes.

4.2. PACT

En esta segunda taxonomía, también gran ejemplo y base para este proyecto, se podrán observar mejores divisiones por parte de las amenazas y tecnologías. Es, además, también un proyecto con relación a requerimientos de la Unión Europea. El problema de esta metodología es que centra el enfoque en toda la rama que anteriormente se ha descrito como tradicional. Centra y realiza la división de la taxonomía en las tecnologías que se refieren a todos los sistemas de vigilancia y seguridad de perímetro. Si bien es cierto que nombra y estudia todo proyecto de I+D, nueva tendencia e innovaciones, no es suficiente para poder analizar todo el sector industrial de la seguridad. No obstante, será de gran utilidad para la creación de la taxonomía en este proyecto una vez que se centre el estudio en esta rama del sector.

Para la creación de esta taxonomía se han creado siete familias distintas que agrupan todas las formas de vigilancia, en las que se incluyen un total de cuarenta y un grupos de tecnologías diferentes. Estos son:

- Vigilancia visual (que incluye sistemas de seguridad por vídeo/CCTV y almacenamiento, escáner corporal e imágenes corporales aumentadas, vigilancia aérea, vigilancia por satélite/tierra, imágenes personales)
- Vigilancia de datos (que abarca la comunicación de campo cercano, las redes sociales, la red inteligente, la historia clínica electrónica, el phishing y las tecnologías relacionadas, las tecnologías de elaboración de perfiles, las tecnologías de vigilancia basadas en navegadores, las tecnologías de nube para la gestión de datos personales, las tecnologías de ciberdefensa, las tecnologías antimalware y las tecnologías de mejora de la privacidad).
- Vigilancia de las comunicaciones (que incluye escuchas telefónicas, de llamadas, vigilancia de correo electrónico y VoIP)
- Biometría e identificación (que abarca la biometría penal, la biometría civil, las tecnologías para sistemas multibiométricos, las tecnologías para los sistemas de cooperación judicial y policial, las tecnologías para el pasaporte electrónico y eGates, otras tecnologías de autenticación, control de acceso e identidad).
- Sensores (que incluyen tarjetas inteligentes de proximidad, tecnologías de detección de olfato y nariz artificiales/explosivos/armas/drogas, redes de sensores, tecnologías de seguimiento de vehículos, sistemas de seguimiento de personas, análisis de comportamiento, tecnologías hogares inteligentes, tecnologías de detección de aeropuertos/puertos, tecnologías para sistemas de control de fronteras terrestres y marítimas).
- Determinación de la ubicación (que incluye la ubicación del transmisor, etiquetado geográfico, RFID, tecnologías similares de Wi-Fi/Bluetooth) y

- Tecnologías emergentes y futuristas (que incluyen el análisis de las ondas neuronales, el ADN, las tecnologías de detección de intención/ comportamiento anormal, las tecnologías de sistemas de vehículos inteligentes

Después de esta clasificación, se realiza un estudio y descripción de cada una de las tecnologías, además del análisis de sus tendencias y proyectos de I+D. Para el posterior análisis del sector industrial de la seguridad se considera excesiva tal cantidad de información, y como ya se ha dicho anteriormente, el foco debería ser más amplio y abarcar distinto nichos de tecnologías.

4.3. EDA

La tercera taxonomía realiza una división del sector de la seguridad a través de su separación por tecnologías. Realiza una distinción entre tecnologías, la composición de los materiales, al campo al que pertenecen y el fin para el que se utilizan. En ningún momento especifica el fin de estas, ni al ámbito en el que se van a enfocar dichas tecnologías. Por ello, esta taxonomía es perfecta para realizar una estructura teniendo en cuenta el criterio tecnológico, pero en ningún momento especifica el objetivo de las mismas, por lo que quedaría incompleta para definir el sector Industrial de la Seguridad. Además, toca ámbitos y aspectos del sector de la defensa, como se puede ver a continuación en el resumen realizado:

- Materiales Estructurales e Inteligentes y Mecánica Estructural
- Materiales relacionados con la firma
- Tecnología de materiales electrónicos
- Materiales fotónicos/ópticos y tecnología de dispositivos
- Tecnología de dispositivos electrónicos, eléctricos y electromecánicos
- Materiales energéticos y tecnología de plasma
- Materiales Químicos, Biológicos y Médicos
- Tecnologías de la Computación y Técnicas Matemáticas
- Tecnología de Procesamiento de Información y Señal
- Ciencias Humanas
- Entorno operativo Tecnología
- Tecnologías y dispositivos mecánicos, térmicos y de fluidos
- Letalidad y protección de plataformas
- Propulsión y centrales eléctricas
- Tecnologías de diseño para plataformas y armas
- Guerra Electrónica y Tecnologías de Energía Dirigida
- Control de firmas y reducción de firmas
- Sistemas de sensores
- Sistemas de guiado y control de armas y plataformas
- Simuladores, Entrenadores y Ambientes Sintéticos
- Tecnología de Sistemas Integrados
- Comunicaciones y tecnologías relacionadas con la CEI
- Sistemas de protección de personal
- Procesos de fabricación/herramientas de diseño/técnicas

- Análisis de Defensa
- Plataformas integradas
- Armas
- Instalaciones e Instalaciones
- Personal Equipado
- Funciones diversas de defensa y apoyo a las políticas
- Información sobre el espacio de batalla
- Proceso de Negocio

Si bien cierto que escueta, además de tocar ciertos aspectos de otros sectores, se pueden extraer de esta taxonomía ideas y divisiones para la taxonomía que se realizará posteriormente en este proyecto. Aun así, y como ya se ha indicado, se debería centrar y a la vez ampliar el foco en la rama de Seguridad para hacer de esta metodología una estructura factible para el estudio.

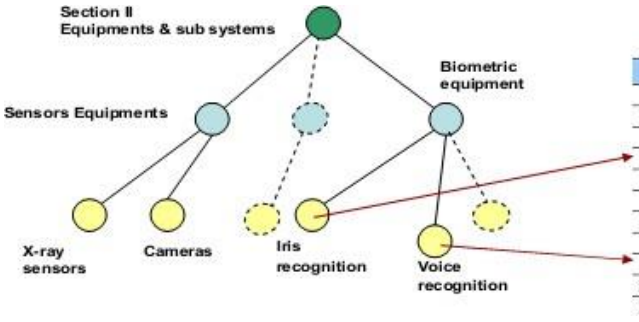
4.4. STACCATO

La cuarta taxonomía crea un mapa de competencias y base de datos, un mapa de los escenarios, una metodología para el estudio de las tecnologías y realiza una distinción entre las áreas en la que los distintos agentes dedicados al sector industrial de la seguridad deben centrar sus productos. El objetivo es ayudar a clarificar la estructura de la industria europea de la seguridad e identificar los potenciales de crecimiento del mercado y el factor de deficiencia de la industria.

STACCATO desarrolla un lenguaje común para la comunidad de seguridad global de actores públicos y privados basado en una taxonomía que tiene en cuenta la taxonomía SeNTRE8 para el mapeo de las competencias europeas. Para la taxonomía del Sector de la Seguridad, que es donde debe centrarse el estudio del estado del arte, se han tenido en cuenta dos premisas para el mapeado de las competencias europeas. La primera, la codificación tecnológica, y en segundo lugar la codificación del producto o servicio. Luego, esta ha sido estructurada en siete niveles distintos, o secciones, que se denominan:

- Componentes y tecnologías
- Equipamientos y subsistemas
- Funciones de los sistemas-servicios
- Diseño y manufacturación
- Plataformas integradas, sistemas, y factores humanos
- Capacidades de misión
- Políticas y apoyo

Por otro lado, crea 3 subcategorías en cada una de las secciones para poder dividir la misma en tecnologías, funciones y necesidades. Como resultado de la metodología se obtiene:



203	Biometric equipment
203-1	Facial recognition
203-2	Fingerprints recognition (digital fingerprints)
203-3	Vein identification
203-4	Iris recognition
203-5	Hand shape recognition
203-6	Retinal patterns recognition
203-7	DNA analysis
203-8	Gait recognition
203-9	Voice recognition
203-10	Signature recognition
203-11	Ear shape recognition

Ilustración 6: Estructura de la Taxonomía STACCATO (1). Fuente: Comisión Europea[14]

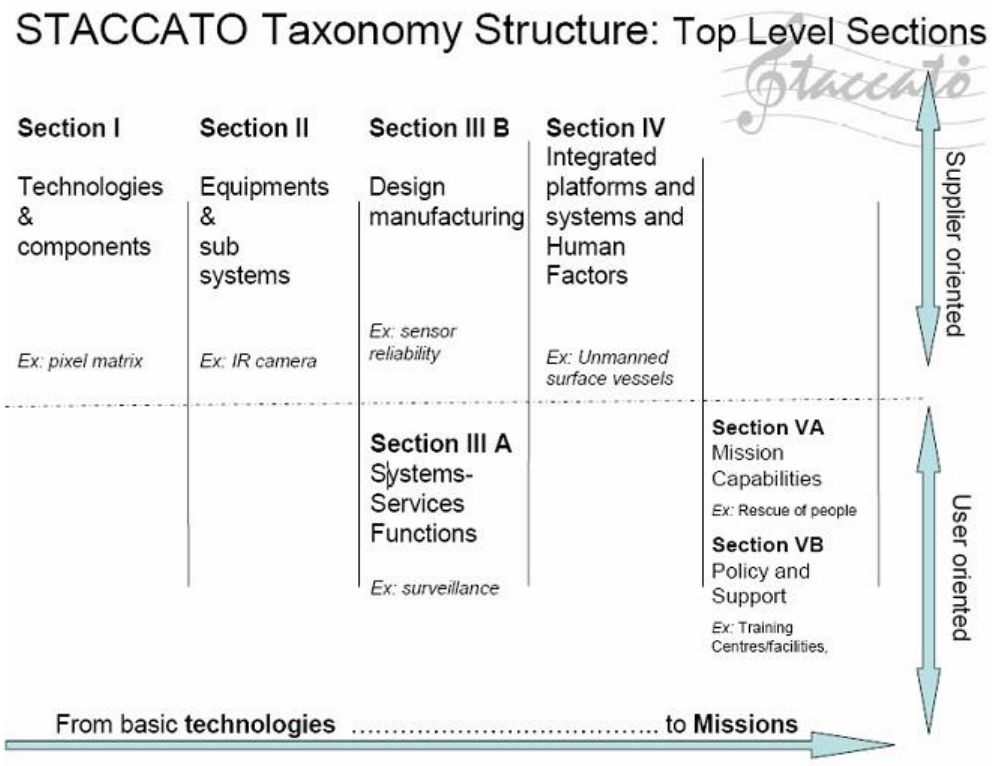


Ilustración 7: Estructura de la Taxonomía STACCATO (2). Fuente: Comisión Europea[14]

Cabe destacar que esta taxonomía es dual-use tanto para las áreas de Seguridad y Defensa. Esto destaca la difícil diferenciación entre ambos sectores debido a la dualidad de funciones y usos de las tecnologías desarrolladas para sus propósitos. Por ello, se puede escoger la metodología como base, pero habrá que trabajar sobre la creación de la frontera o "zonas grises" para separar de forma sistemática los productos de ambos sectores. Este es uno de los motivos por lo que esta metodología es insuficiente para el proyecto que se pretende llevar a cabo, además de abarcar distintas áreas de conocimiento que no son objeto de este estudio.

4.5. STRAW

En quinto y último lugar, en el proyecto STRAW se define una taxonomía de seguridad en la que se aplica un enfoque distinto a los anteriores. Se pretende hacer un mix de algunas de ellas, una metodología para clasificar la seguridad en otras utilizando a su vez las aportaciones del proyecto STACCATO en su forma de estructurarse. Se decidió reorganizar los proyectos anteriores clasificando las tecnologías relevantes.

Este proyecto está impulsado por las necesidades que han ido apareciendo por las partes interesadas. Estos son desde la UE, hasta expertos y proveedores de tecnologías que trabajan en el ámbito de la seguridad. Como entrada, se prefiltró un flujo de documentos de diversas fuentes de acuerdo con criterios que determinaban el nivel de interés para extraer los conceptos pertinentes y organizar esta información en una base de documentos. El mecanismo de filtración era el siguiente:

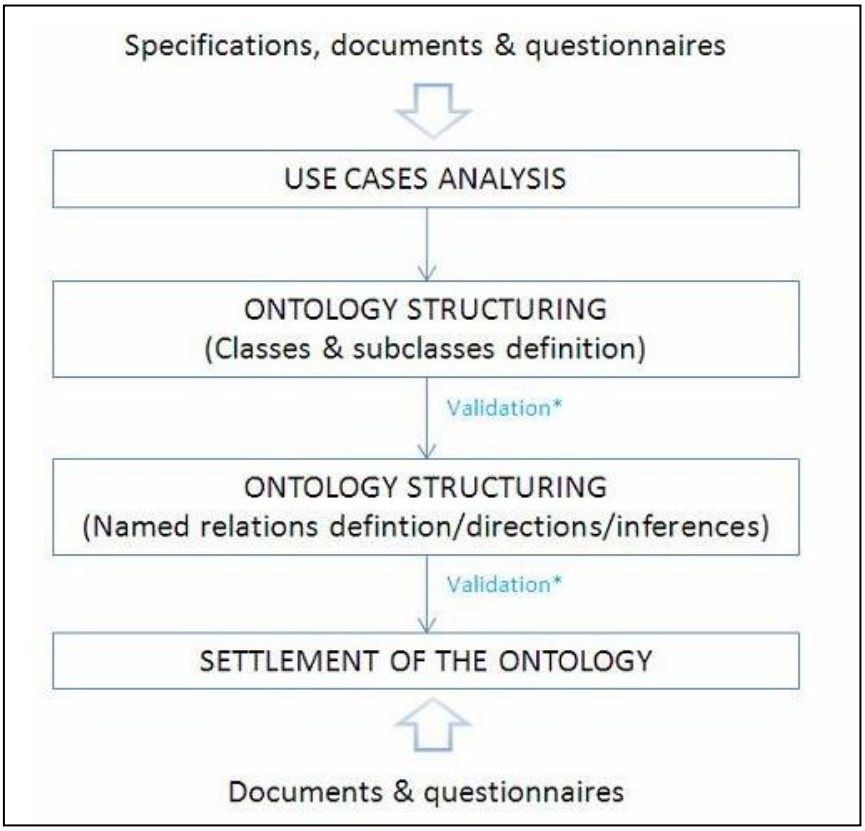


Ilustración 8: Metodología de procesamiento de documentos. Fuente: Comisión Europea[12]

El resultado del mix de taxonomías de STRAW es una nueva estructura compuesta por nomenclaturas de clasificación, criterios de clasificación y conceptos extraídos. El objetivo era que, en última instancia, los expertos pudieran utilizar diversas herramientas de análisis para trabajar con documentos o datos estructurados. Los expertos que consultan esta información pueden ampliar la base de conocimientos operativos añadiendo nuevos conceptos o documentos.

Se define un "árbol de nomenclaturas" para la clasificación según las partidas y para su uso. La clasificación es representativa de un tema o de un concepto y se asigna a cada título de clasificación a un perfil. La estructura de clasificación de la nomenclatura es independiente de la estructura de la base de conocimientos, lo que permite adaptar la disposición a las necesidades específicas de los usuarios.

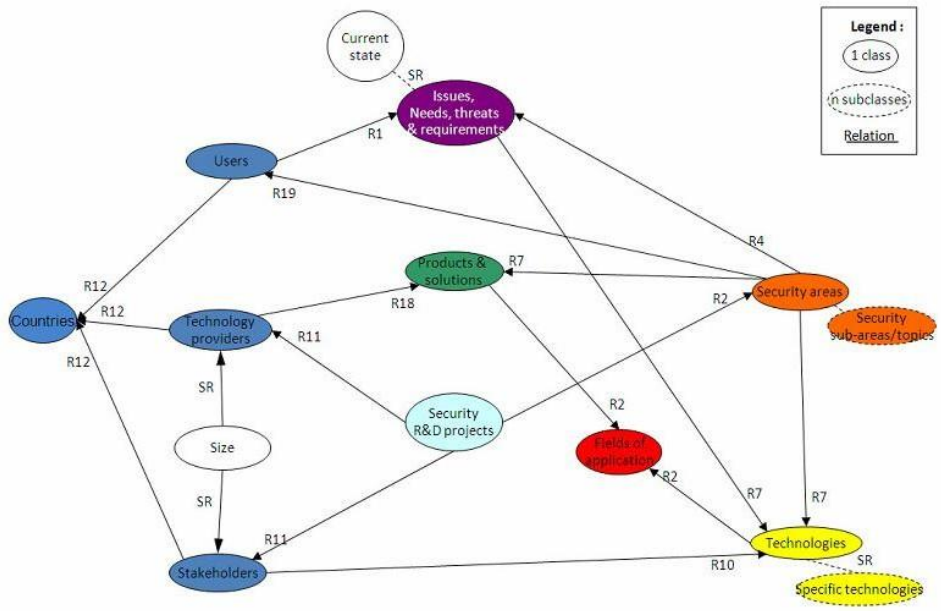


Ilustración 9: Mapa Conceptual de la Taxonomía Straw. Fuente: Comisión Europea[12]

Se definió 9 áreas de seguridad (por ejemplo, asegurar la identificación y el control de bienes y personas, la protección de ciudadanos y bienes, el control y la vigilancia de áreas, la protección de redes, la gestión de crisis, etc.) sobre la base de las "misiones" de STACCATO y 20 subáreas o sub-misiones de seguridad (por ej. Asegurar la gestión y el control de las identidades y los derechos, la lucha contra la delincuencia y la inseguridad, la seguridad del espacio público, la vigilancia de las zonas de riesgo humanitario, la vigilancia del medio ambiente para alertar, la vigilancia epidemiológica, la vigilancia aérea, la vigilancia de las zonas marítimas circundantes, la vigilancia de los costes y de los límites, la protección de los lugares en los que tienen lugar los acontecimientos, etc.). En este tipo de taxonomía cada tecnología pertenece a una misión, y cada misión puede tener subapartados. Una submisión solo puede depender de una misión superior, pero una tecnología puede estar asociada a varias.

Esta metodología para crear una taxonomía se asemeja mucho a la final escogida para este proyecto. Se escogerán como bases la forma de división de los apartados con distintas categorías. Aun así, este análisis sigue siendo insuficiente, además de no estar enfocado a la industria nacional española. Por ello se seguirá como ejemplo y base, pero se actualizará y mejorará en este proyecto.

5. INTRODUCCIÓN A LA TAXONOMÍA

En este apartado de procederá a realizar la taxonomía final del sector Industrial de la Seguridad. El sector Industrial de la Seguridad será el conjunto de empresas, instituciones, organizaciones, agentes y actores que proveen de equipos, materiales y servicios a los Cuerpos y Fuerzas de Seguridad para poder enfrentar las distintas amenazas. Como se ha explicado anteriormente, este sector es amplio y complejo, con fronteras difusas, y para poder aprovechar toda oportunidad de negocio deben esclarecerse las áreas que abarca.

Para poder definir las fronteras de este sector se ha optado por crear una matriz de capacidades y tecnologías. Esta matriz sigue tres criterios para establecer las áreas operativas, y estos son los siguientes:

- Amenazas o Líneas de Acción
- Situación dentro de la amenaza
- Tecnologías

Con respecto al primer criterio, el Departamento de Seguridad Nacional, a través de sus informes anuales, estableció una serie de amenazas o líneas de acción que hacen que peligre el estado de bienestar de los ciudadanos españoles. Las Fuerzas y Cuerpos de Seguridad son los encargados de enfrentarlas y de evitar que estas alteren el orden y la paz de la sociedad. Por ello, y para ayudar a los diferentes actores y agentes a cumplir con su cometido, el sector industrial debe centrarse en crear productos específicos para combatirlas. Es por ello que se ha optado a utilizar este tipo de criterio para la clasificación, debido a que cada amenaza será acometida de forma distinta, precisando de materiales y equipos específicos.

Bajo el criterio de las tecnologías, se han estudiado, con base en otras taxonomías, las distintas familias de productos y subproductos que existen. Se ha elaborado un listado de los mismos y realizado una breve explicación de su fin y sus funciones. Se pretende abarcar bajo este estudio todo tipo de tecnologías que están involucradas dentro del sector de la Seguridad. Cabe destacar, que debido a la naturaleza de las acciones tomadas por los distintos agentes, no todas las tecnologías serán usadas en las distintas amenazas. Además, debido al carácter dinámico del sector, la taxonomía podrá cambiar y distintas tecnologías que no se usaban para enfrentar ciertas amenazas puedan funcionar en un futuro, o que irrumpan nuevas tecnologías. Lo que no cambiaría sería la metodología de clasificación y las fronteras definidas por estos criterios.

Para terminar con el proceso de definición de la taxonomía, queda describir las situaciones dentro de la amenaza. Enfrentarse a cualquier amenaza tiene varias fases, desde su investigación hasta el propio enfrentamiento. Todos y cada uno de esos aspectos precisará de equipos y servicios distintos ya que las tareas a realizar son

específicas según la actividad en la que sen encuentren. Después de analizar las posibles componentes en la metodología de operación de las Fuerzas y Cuerpos de Seguridad, se ha optado por dividir las amenazas en las distintas fases:

- Comunicaciones
- Detección
- Gestión de la Información
- Posicionamiento
- Evaluación de riesgos
- Conocimiento o consciencia de la situación
- Entrenamiento.
- Doctrina y operaciones
- Respuesta al incidente

Con esto quedarían descritos los distintos criterios para crear la matriz y taxonomía del sector Industrial de la Seguridad. A continuación, se realizará un estudio exhaustivo de cada uno de los apartados, entrando en detalle en la clasificación. Aun así, antes de comenzar, queda esclarecer el problema que acarrea utilizar las amenazas descritas por el Departamento de Seguridad como criterio. Estas no son exclusivas de las Fuerzas y Cuerpos de Seguridad, es más, algunas son competencia directa de Defensa, área que queda completamente fuera del estudio de este proyecto. Por ello, se deberá realizar un estudio adicional de las competencias tanto de Defensa como de los CFS para establecer una frontera entre ellos y poder delimitar el sector de la seguridad.

El hecho de que se hayan escogido las competencias como criterio para definir el sector industrial de la seguridad es simple. El concepto de la Seguridad, descrito anteriormente, es amplio y complejo. Por ello, las competencias, definidas claramente por organismos nacionales que ya han estudiado todas las condiciones, es una garantía de éxito en la creación de la taxonomía. Con esto se asegura el sector que todo esfuerzo económico, productos, equipos y servicios que se presten serán única y exclusivamente pertenecientes al ámbito de la seguridad, respaldado en todo momento por las leyes que lo definen.

Con esto finaliza la descripción previa de los distintos criterios que se utilizarán para realizar la taxonomía. En los siguientes apartados se realizará un estudio exhaustivo de todos y cada uno de ellos para así definir las fronteras del sector. Se irá en orden, definiendo primero las competencias de los CFS y las de Defensa para poder definir los límites de las amenazas. Posteriormente se describirá el listado de los grupos tecnológicos, y finalmente las divisiones dentro de las amenazas. Para terminar, habrá un apartado final concluyente donde se cerrará la taxonomía del Sector de la Seguridad, y se propondrá una matriz ejemplar que servirá como base para la industria.

6. DESCRIPCIÓN DE LAS DISTINTAS FUERZAS Y CUERPOS DE SEGURIDAD Y SUS COMPETENCIAS

Debido al carácter único de la composición del territorio nacional, la descripción de los distintos grupos precisa de una breve introducción. España está compuesta por 17 comunidades y dos ciudades autónomas, con una gran cantidad de competencias propias. Por ello, existe una gran diferencia entre los distintos cuerpos, pudiendo realizar una clasificación de los mismos a nivel administrativo. Estos niveles son nacional, autonómico y local, donde cada Administración tiene la posibilidad de insertar su propio cuerpo de seguridad. Además, y siguiendo la Ley Orgánica 2/1986, artículo 2, se componen y definen las Fuerzas y Cuerpos de Seguridad como:

- Todos aquellos cuerpos que dependan del gobierno de la nación quedarán definidos como Fuerzas y Cuerpos de Seguridad del Estado.
- Todos aquellos cuerpos que dependan de las Comunidades Autónomas serán definidos como Cuerpos de Policía dependientes de las mismas.
- En último lugar, quedarán los dependientes a las corporaciones locales.

Por otro lado, existen grupos especiales debido a su actividad y jurisdicción. Estos son:

- Agentes forestales.
- Policía portuaria.
- Servicio de Vigilancia Aduanera.

Estos Cuerpos de Seguridad tienen tareas muy específicas, creados debido a la magnitud de las amenazas que atenazan sus propios sectores. Además, como se verá más adelante, tienen competencias comunes con otros cuerpos.

Una vez realizada una breve presentación de la organización de las fuerzas del orden, se procederá a realizar la clasificación formal y definición de competencias de los mismos. Se comenzará por aquellos menos conocidos y se finalizará por aquellos más importantes a nivel operativo.

6.1. DIRECCIÓN ADJUNTA DE VIGILANCIA ADUANERA (DAVA)

Dependiente de forma orgánica y funcional del Departamento de Aduanas e impuestos, además de pertenecer al Ministerio de Hacienda, es considerado el brazo o cuerpo armado de la Agencia Estatal de Administración Tributaria.

Ilustración 10: Escudo Dirección Adjunta de Vigilancia Aduanera

Sus competencias son claras. No es el objeto de la taxonomía realizar un estudio exhaustivo de las actividades que realiza cada cuerpo, por lo que se centrará en análisis en las áreas de interés, que son:

- Descubrir, perseguir y reprimir todo acto e infracción de contrabando, en todo el territorio y espacio aéreo nacional y las aguas jurisdiccionales.
- Enfrentar todo acto ilícito que tenga relación con el blanqueo de capitales, fraude aduanero y el control de cambios. Además, perseguirá y reprimirá toda economía sumergida, en estrecha colaboración con los actores competentes.
- Dentro de la propia categoría del fraude aduanero y contrabando se encuentra la lucha contra el narcotráfico, de especial mención debido a su importancia.

Es más, según la Ley Orgánica de Represión del Contrabando, se les está permitido realizar labores de abordaje e intercepción en el caso que fuese necesario, ya sea en aguas nacionales o internacionales.

6.2. AUTORIDAD PORTUARIA

Existen 28 autoridades portuarias en España en la actualidad, todas dependientes del Ministerio de Fomento. Merece una mención especial ya que es el cuerpo más antiguo de policía en este país. Aun siendo un Cuerpo de Seguridad, sus labores son básicamente administrativas, con competencias muy similares a las de la Policía Local, que se describirán más adelante.

Debido a la actividad que realizan, que son básicamente operaciones portuarias (atraques, accesos, medio ambiente, control de infracciones), tienen una estrecha relación con la Dirección Adjunta de Vigilancia Aduanera y la Guardia Civil.

6.3. POLICÍA MEDIOAMBIENTAL

Dependientes de las comunidades Autónomas, con la condición de agentes de la autoridad y Policía Administrativa, estos funcionarios públicos tienen una sola función especial. Según el apartado 6º de la Ley de Enjuiciamiento Criminal, Artículo 283, son la policía judicial además de custodios de los bienes de la naturaleza forestal jurídicos.

Ilustración 11: Escudo Policía Medioambiental

Entre sus funciones caben destacar:

- Conforme a la normativa medioambiental administrativa, realizar inspecciones y controles.
- Investigar los delitos y las causas de incendios, con función de policía.
- Investigar los delitos contra la protección de fauna y flora.
- Investigar los delitos sobre la ordenación del territorio.
- Investigar los delitos contra el medio ambiente y los recursos naturales

6.4. POLICÍA LOCAL

Con naturaleza civil, siendo un instituto armado, los Cuerpos de Policía Local de España cumplen las siguientes características. Dependientes de las administraciones a las que pertenezcan, con órgano superior los reglamentos dispuestos por la Comunidades Autónomas, y de las normas impuestas por el ayuntamiento del que dependan. Su régimen estatutario queda definido por la Ley Orgánica 2/86, sección IV, capitulo IV, Título II y por los capítulos II y III, Título I.

Debido al extenso número de cuerpos y las distintas normas que cumplen cada uno de ellos, y debido a las distintas leyes promulgadas en cada una de las Comunidades autónomas, se realizará un estudio y resumen da las competencias comunes a todos, basado en la Ley Orgánica 2/86:

- Responsables de la dirección, ordenanza y señalización del tráfico dentro del casco urbano.
- Responsables de la protección, vigilancia y custodia de las distintas corporaciones y autoridades locales, además de sus instalaciones y edificios.
- De forma ya explicada y redactada en las Leyes, los Cuerpos de policía Local prestarán ayuda en casos de catástrofe, accidente o calamidad pública, en función de los distintos planes dispuestos por protección civil.
- Realizar cualquier actividad de actuación o prevención precisa para enfrentar o evitar cualquier tipo de acto ilícito, siempre dentro de los marcos colaborativos que se hayan establecido entre los distintos Cuerpos y Juntas de Seguridad.
- Establecer un ambiente colaborativo siempre que fuese necesario o posible en la resolución de conflictos privados y domésticos.
- En caso de concentraciones humanas o manifestaciones, y siempre que sean requeridos para ellos, los Cuerpos de Policía Local apoyaran a las distintas Fuerzas y Cuerpos de Seguridad del Estado y policías de las CCOO en las tareas de mantenimiento del orden y vigilancia.

6.5. POLICÍAS AUTONÓMICAS

En este apartado no se realizará un estudio intenso de las competencias de las distintas Policías Autonómicas. Los motivos son simples, hay un gran número de policías autonómicas, todas con competencias distintas entre sí, por lo que no puede obtenerse un resumen común. Pero el principal es, sin duda alguna, que las Policías Autonómicas ejercen distintas competencias exclusivas de los Cuerpos y Fuerzas de Seguridad del Estado que han sido delegadas a las distintas Comunidades autónomas. Son competencias que en algún momento, o simplemente deberían realizar la Guardia Civil y la Policía Nacional. Todas ellas siempre relacionas con tareas referidas al orden público, vigilancia y ordenación de aglomeraciones de personas, seguridad ciudadana, y en algunos casos, el control del tráfico urbano dentro de sus Comunidades autónomas. En los casos que tengan competencias no exclusivas de los Cuerpos y Fuerzas de Seguridad del Estado, serán competencias compartidas con los Cuerpos responsables de las mismas.

Por todo ello no se realizará el resumen de competencias establecido en los apartados anteriores, y se hará hincapié en los próximos apartados donde se describan la Guardia Civil y el Cuerpo Nacional de Policía.

6.6. CUERPO NACIONAL DE POLICÍA

De naturaleza Civil, es considerado como un instituto armado. Es el responsable, según determine el Gobierno, de vigilar todos los núcleos urbanos y las capitales de provincia. Todos aquellos territorios, incluidos mares territoriales, que no entren dentro de este marco serán responsabilidad de la Guardia Civil.

Ilustración 12: Escudo del Cuerpo Nacional de Policía

El Cuerpo Nacional de Policía es amplio y extenso, con una rica historia digna de ser contada, pero que no es objeto de este estudio. Este proyecto se centrará en el estudio de sus competencias, para poder delimitar el sector industrial de la seguridad. Por ello, previo al resumen que ha ido exponiendo de los anteriores grupos, se mencionarán todas las normativas de las que depende este Cuerpo para que toda aquel que lo precise pueda contrastar la información aquí expuesta:

- 27 de Julio, Real Decreto 952/2018.
- 28 de Julio, Ley Orgánica 9/2015.
- 20 de Mayo, Ley Orgánica 4/2010.
- 13 de Marzo, Ley Orgánica 2/1986.

Una vez nombradas todas las Leyes y Reales Decretos por los que se rige, se procederá a presentar las distintas competencias de las que el Cuerpo Nacional de Policía es responsable. Como en los apartados anteriores, no se presentarán el conjunto completo, solo aquellas que ayuden a delimitar las amenazas de las cuales son responsables.

- Perseguir e investigar todo delito que tenga relación con el narcotráfico.
- Responsable de controlar las entradas y salidas, tanto de ciudadanos españoles como de extranjeros, dentro del territorio nacional.
- Responsables de la protección y vigilancia tanto de las instalaciones como edificios públicos que requieran de dicho servicio.
- Responsables del mantenimiento, y posible restablecimiento en caso de necesidad, de la seguridad ciudadana y el orden.
- De forma ya explicada y redactada en las Leyes, el Cuerpo de Policía Nacional prestará ayuda en casos de catástrofe, accidente o calamidad pública, en función de los distintos planes dispuestos por protección civil.
- Investigar, perseguir y enfrentar todo acto ilícito cometido por grupos, agentes o actores terroristas dentro del territorio nacional.
- Desactivar, neutralizar e intervenir cualquier tipo de artefacto explosivo, nuclear, radiológico, biológico o químico.
- Investigar, perseguir y enfrentar todo acto ilícito que utilice las distintas plataformas digitales para llevar a cabo sus actividades. Entre ellos se pueden encontrar los fraudes, estafas, piratería y ataques cibernéticos y pornografía infantil. Además, aplicarán protocolos de ciberseguridad en todas las instituciones públicas que dependan de este Cuerpo.
- Investigar, perseguir y enfrentar todo acto ilícito cometido por los actores y agentes pertenecientes al crimen organizado.
- Ofrecer y participar en tareas de apoyo operativo a través de los Medios Aéreos en misiones humanitarias o misiones de auxilia a la ciudadanía.
- El Cuerpo Nacional de Policía es responsable, según la legislación vigente, de establecer refugio y asilo, de las extradiciones, expulsiones, inmigración e inmigración, y todas sus variables ilícitas. No son competencias exclusivas suyas, es más, tanto la trata de seres humanos como la inmigración ilegal es también responsabilidad de ciertos Cuerpos de Policía Autonómicas y la Guardia Civil.
- Colaborar o prestar auxilia a los distintos cuerpos de policía que pertenezcan a otros países, siempre conforme a las leyes orgánicas que rigen este tipo de misiones, y bajo la coordinación y supervisión de la Secretaria de Estado de Seguridad.

Hasta aquí sería el resumen más claro, conciso y concreto de las capacidades, responsabilidades y competencias del Cuerpo Nacional de Policía que incumbirían para el estudio y delimitación del sector industrial de la Seguridad.

6.7. GUARDIA CIVIL

A diferencia de los distinto grupos ya descritos anteriormente, este instituto armado es de naturaleza militar, aun ejerciendo las funciones de policía. Además, depende directamente tanto del Ministerio de Defensa como del Ministerio de Interior. Es otro cuerpo con una gran historia, pero debido al carácter de este proyecto, no se entrará en materia. Se procederá, como en los anteriores, a describir que leyes rigen las competencias de este Cuerpo dependiente del Estado y cuáles son las mismas.

Ilustración 13: Escudo de la Guardia Civil

Las distintas leyes que rigen a la Guardia Civil son:

- 18 de Julio, Real Decreto 628/2014.
- 28 de Noviembre, Ley 29/2014.
- 27 de Octubre, Real Decreto 1224/2006.
- 18 de Febrero, Real Decreto 179/2005.
- 30 de Diciembre, Real Decreto 2394/2004.
- 19 de Noviembre, Real Decreto 1250/2001.
- 15 de Septiembre, Real Decreto 1429/1997.
- 22 de Junio, Real Decreto 1970/1983.
- 13 de Marzo, Ley Orgánica 2/1986.
- Artículo 104 y 126 de la Constitución.

Una vez descritas las distintas leyes que rigen este Cuerpo, y a las que se podrá remitir en caso de duda, se procederá a realizar el resumen de las competencias relevantes para el estudio de este proyecto.

- De forma ya explicada y redactada en las Leyes, la Guardia Civil prestará ayuda en casos de catástrofe, accidente o calamidad pública, en función de los distintos planes dispuestos por protección civil.

- Responsables de la protección del libre ejercicio de las libertades y derechos, a través de la prevención e investigación de las conductas delictivas, de los ciudadanos.
- Responsables de vigilar, regular, auxiliar y controlar el transporte y tráfico, garantizando la seguridad en toda vía interurbana.
- En lo referente a la Ley en materia de armas y explosivos, la Guardia Civil tiene las siguientes competencias. Debe controlar e inspeccionar toda fabricación y reparación de armas, imitaciones, réplicas y sus piezas fundamentales. Además, deberá controlar su circulación, comer, y adquisición. Es responsable de la prevención, investigación y persecución del tráfico ilícito de armas y explosivos. Finalmente, también debe controlar cualquier movimiento de cartuchería y munición.
- Responsable de la lucha contra cualquier grupo o célula terrorista. Con prioridad en la lucha contra la banda terrorista ETA, operaciones que supongan un grave riesgo o que dispongan de una rápida respuesta, siendo una reserva de carácter especial a completa disposición del Director General para misiones dentro y fuera del territorio nacional, además de una unidad de apoyo para cualquier misión que suponga enfrentarse a material NRBQ.
- Responsables, a través del órgano central del Servicio de Costas y Fronteras, de la lucha contra el contrabando, tráfico de drogas, mercancías ilícitas, redes internacionales de tráficos de sustancias ilegales y personas. Cabe destacar que su área de trabajo son las fronteras nacionales, con especial énfasis en puertos y aeropuertos.
- Responsable de vigilar y controlar toda actividad en el medio subacuático, además de custodiar las costas y realizar el control de la inmigración irregular en las aguas marítimas españolas y las aguas continentales.
- Responsable, a través del SEPRONA, de controlar, preservar y velar por el medioambiente, sus recursos hídricos, además de sus recursos forestales, piscícolas y su riqueza cinegética. En otras palabras, esta al cargo de la protección de la sanidad animal, del agua, suelo y atmosfera y la conservación de las especies que viven en ella, tanto fauna como flora. Investigará y enfrentará cualquier comercio o tráfico ilegal de especies protegidas, pesca irregular, prevención de incendios y cualquier contaminación o vertido efectuado.
- Responsable del mantenimiento, prevención, y si fuese necesario, del restablecimiento de la seguridad pública. Además, deberá proteger y velar por la seguridad de altas personalidades, en colaboración con los distintos cuerpos responsables. Garantizará la seguridad y el orden en eventos donde se congreguen grandes cantidades de personas. Y por último, servirán como unidades de apoyo y refuerzo en servicios y misiones a las distintas Unidades Territoriales.

- En el ámbito de las nuevas tecnologías, en primer lugar, se encargarán de detectar cualquier tipo de delito informático, llamando a los grupos encargados patrullas cibernéticas. En segundo lugar, investigaran cualquier tipo de delincuencia o fraude cometido en el sector de las telecomunicaciones. Y en último lugar, servirán como unidades de apoyo tanto al resto de la Guardia Civil como a los distintos Cuerpos de Seguridad.
- Responsables de la desactivación, neutralización y detección de cualquier tipo de explosivo, ya sea radiactivo, biológico, químico o incendiario. Además, son los responsables de desplegar en el territorio nacional cualquier tipo de Servicio de Desactivación de Explosivos y Defensa TEDAX-NRBQ.
- Responsables de proteger y vigilar todo tipo de redes de servicios públicos, costas, fronteras, aeropuertos, puertos, edificios públicos, penitenciarias e infraestructuras críticas.

Con esto quedaría completamente resumido todas las competencias de la Guardia Civil. Además, se cierra el capítulo de descripción de las Competencias de los Cuerpos y Fuerzas de Seguridad, ya sean dependientes del Estado o no, que formarán la frontera con respecto a las amenazas identificadas por el Departamento de Seguridad Nacional y definirán el sector industrial de la Seguridad. Pero antes, para poder definir dicho sector de forma clara y concisa, se precisa delimitar las diferencias que hay en las zonas grises de estas amenazas con las competencias de Defensa. Para ello, se realizará una breve presentación de los componentes de las Fuerzas Armadas y un resumen de sus competencias. De este modo, se podrá contrastar los ámbitos de actuación y definir completamente el sector de la seguridad.

6.8. FUERZAS ARMADAS

De naturaleza militar, es la organización dependiente del estado responsable de garantizar la independencia y soberanía del Estado, defensora de su integridad territorial y del ordenamiento de la Constitución. Están compuestas por:

- Armada Española.

Su misión fundamental es defender la total integridad del territorio nacional, su ordenamiento constitucional, y garantizar la soberanía e independencia del Estado Español, en el ámbito marítimo.

- Ejército del Aire

Su misión fundamental es defender la total integridad del territorio nacional, su ordenamiento constitucional, y garantizar la soberanía e independencia del Estado Español, en el ámbito aéreo.

- Ejército de Tierra

Su misión fundamental es defender la total integridad del territorio nacional, su ordenamiento constitucional, y garantizar la soberanía e independencia del Estado Español, en el ámbito terrestre.

- Guardia real

Constituida por una representación de todos los componentes de las Fuerzas Armadas Españolas, única y exclusivamente al servicio del Rey. Sus misiones se centran en ofrecer guardia militar, dar escoltar y rendir honores a la familia real, además de a los Jefes de Estado extranjero visitantes cuando se les ordene.

- Cuerpos Comunes de las Fuerzas Armadas Españolas

Son los cuerpos militares que complementan a las unidades ya existentes en los ámbitos no tradicionales. Estos son el cuerpo de Sanidad, Intervención, Jurídico Militar y el de Músicas Militares.

- Unidad Militar de Emergencia

Responsable de las intervenciones en caso de catástrofe, calamidad pública y cualquier otra situación de grave riesgo.

Ilustración 14: Escudo de las Fuerzas Armadas

Una vez descritas las distintas divisiones dentro de las Fuerzas Armadas, se procederá a realizar un estudio de las competencias de las mismas. Para ello, se ha estudiado la Ley Orgánica del 17 de Noviembre, 5/2005, donde quedan descritas las misiones de las Fuerzas Armadas y su control parlamentario. Los artículos que se estudiarán serán el 15 y 16, donde queda perfectamente resumidas las competencias para su posterior contraste con las de los Cuerpos y Fuerzas de Seguridad.

Debido a que cada artículo trata un tema distinto, el artículo 15 trata las Misiones y el artículo 16 trata los Tipos de Operaciones, se hará un breve resumen de cada uno por separado.

El artículo 15 puede resumirse en:

- Las Fuerzas Armadas están autorizas, en el caso que fuese necesario, a preservar la seguridad y bienestar ciudadano en el caso de catástrofe, calamidad, o situación de grave riesgo, siempre bajo el mandato establecido por la legislación vigente.
- Las Fuerzas Armadas velarán por contribuir militarmente, tanto a España como a sus aliados, a mantener o reestablecer, si fuese necesario, la seguridad y defensa, así como mantener la estabilidad, paz y ayuda humanitaria.
- Cualquier grupo de las Fuerzas Armadas puede realizar evacuaciones, siempre y cuando las circunstancias en el país sean de inestabilidad, residentes españoles en el extranjero.
- El principal cometido de las Fuerzas Armadas, según la Constitución (artículo 8.1), es garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional.

El artículo 16 puede resumirse en:

- Las Fuerzas Armadas colaboraran con cualquier tipo de Administración pública,

y siempre bajo la ordenanza establecida por la legislación vigente, en caso de catástrofe, calamidad, o situación de grave riesgo.

- Las Fuerzas Armadas participaran con otros organismos o instituciones, ya sean nacionales o internacionales, siempre que haya necesidad de preservar el bienestar y la seguridad de ciudadanos españoles fuera de sus fronteras.
- Las Fuerzas Armadas podrán llevar a cabo una respuesta militar frente a ataques terroristas que se realicen con el uso de aeronaves.
- Las Fuerzas Armadas apoyaran a las Fuerzas y Cuerpos de Seguridad del Estado, instituciones y organismos en la lucha contra el terrorismo, rescates terrestres, aéreos y marítimos, además de en las tareas de búsqueda y salvamento.
- Las Fuerzas Armadas colaborarán en operaciones de paz y estabilización en países extranjeros. Además, podrán reestablecer la administración, reconstruir su seguridad, y rehabilitar el país, zona o región según los tratados establecidos.
- Las Fuerzas Armadas son responsables de vigilar los espacios marítimos, vigilar el espacio aéreo y el control del espacio aéreo que se encuentre bajo soberanía nacional. Además, son responsables de garantizar la soberanía e independencia de la nación, así como de proteger la vida de sus ciudadanos e intereses.

7. AMENAZAS Y LÍNEAS DE ACCIÓN

En este apartado se definirá la frontera del Sector Industrial de la Seguridad. El resto definirá el sector de forma interna, delimitando las posibles capacidades y productos de forma dinámica y para una imagen del presente en la industria. Pero en lo que a la taxonomía concierne, esta será la aclaración de las zonas grises que se precisa para centrar los esfuerzos de la industria.

Para realizar esta tarea, se ha tomado como base las amenazas y líneas de acción estratégicas identificadas por el Departamento de Seguridad Nacional, organismo encargado de la definición de las estrategias e informes anuales para la Seguridad Nacional.

Las líneas de acción, o amenazas, definidas por el departamento son las siguientes:

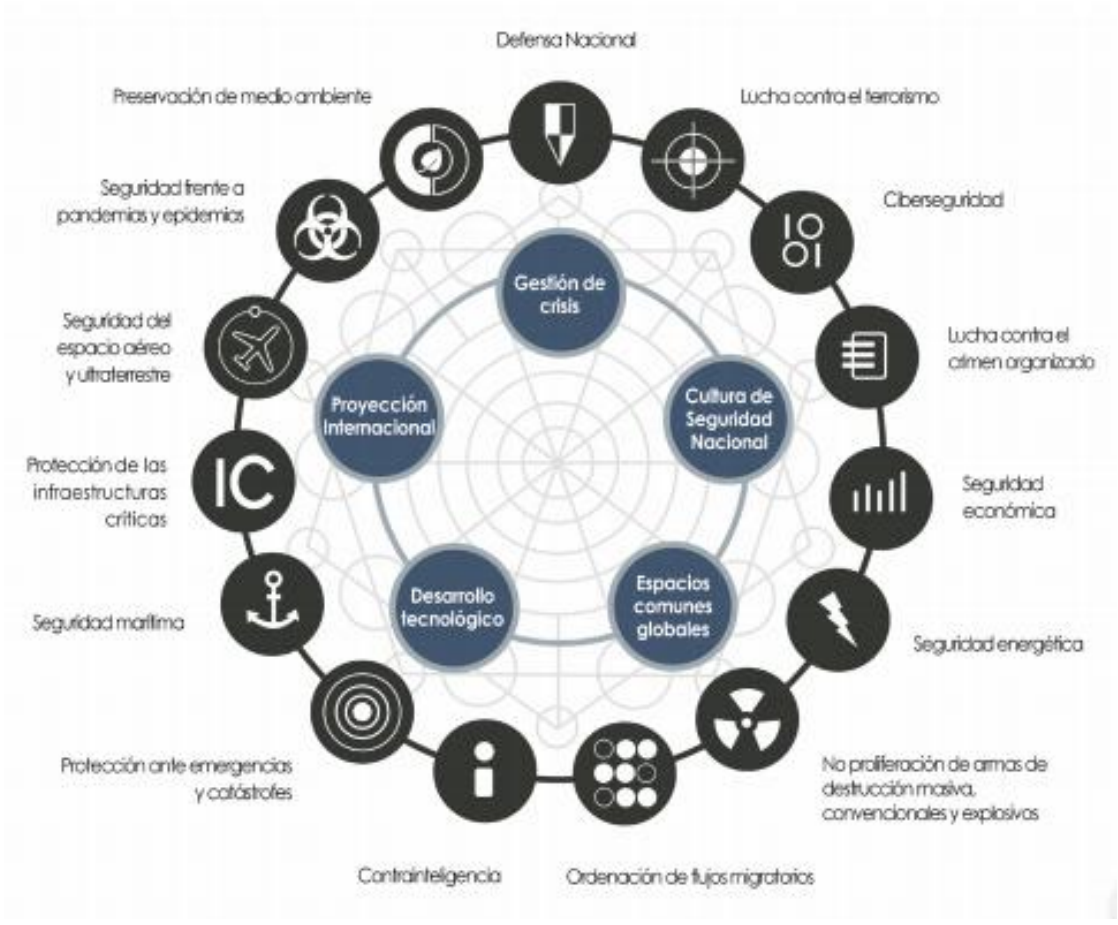


Ilustración 15: Amenazas o Líneas de Acción identificadas por el DSN. Fuente: Departamento de Seguridad Nacional[1]

Aun así, y como se ha dicho anteriormente, estas líneas de acción mezclan competencias tanto de Seguridad como de Defensa. Para definir claramente aquellas pertenecientes solo a las Fuerzas y Cuerpos de Seguridad, deberán analizarse una a una y definir a que sector pertenecen.

Podrá ocurrir que ciertas amenazas tengan tanto competencias de Defensa como de Seguridad. En ese caso, deberá realizarse la división interna y esclarecer que responsabilidades pertenecen a cada organización. Una vez aclaradas las pesquisas necesarias, se procederá a analizar cada una de las líneas de acción.

7.1. DEFENSA NACIONAL

Objetivo:

"Asegurar la defensa de la soberanía e integridad de España y la protección de la población y el territorio frente a cualquier conflicto o amenaza proveniente del ámbito exterior, de forma autónoma o junto a socios y aliados. Asimismo, contribuir a crear un entorno internacional más estable y seguro mediante la proyección de estabilidad y el refuerzo de la cooperación con los socios, particularmente en las áreas de especial interés para España" [1]

Líneas de acción más relevantes:

- Tener la capacidad militar para disuadir cualquier amenaza externa además de mejorar la capacidad autónoma de defensa.
- Las Fuerzas Armadas deben estar dotadas con las suficientes capacidades como para cumplir con los objetivos establecidos por la OTAN.
- Se debe plantear una estrategia industrial nacional de Defensa que fomente el aumento de las capacidades y competitividad a nivel global de la misma.
- Las Fuerzas Armadas son responsables de crear un entorno nacional de seguridad y paz, evitar conflictos, contener las nuevas amenazas en las áreas de interés nacional.

Realizando un análisis claro de esta línea de acción dispuesta por el Departamento de Seguridad Nacional, se llega a la conclusión que no pertenece al sector Industrial de la Seguridad. Es por ello que toda tecnología y actividad dispuesta para cualquiera de las finalidades descritas no será objeto de estudio ni entrará dentro de la taxonomía.

7.2. LUCHA CONTRA EL TERRORISMO

Objetivo:

"Neutralizar la amenaza que representa el terrorismo contra los ciudadanos y los intereses españoles dentro y fuera de las fronteras, reduciendo la vulnerabilidad de la sociedad y haciendo frente a los procesos de radicalización violenta" [1]

En el caso del Terrorismo, el DSN hace cuatro divisiones dentro de las propias líneas de acción según en la fase de la amenaza que se encuentre. A continuación, se presentará un breve resumen de las más relevantes:

- En la fase de Prevención, se pretenden potenciar la implantación del PEN-LCRV, potenciar los mecanismos diseñador para luchar contra la financiación del terrorismo, y reforzar el papel de España en la lucha contra el terrorismo internacional a través de organismos como la OTAN y la UE.
- En la fase de Protección, reforzar las capacidades nacionales contra el terrorismo a nivel nacional, y colaborar con otros países de la UE para mejorar en el control de fronteras.
- En la fase de Persecución, fomentar e incrementar las capacidades de inteligencia e investigación, apostar por la mejora de las tecnologías en los servicios de información e inteligencia para enfrentar las nuevas tácticas terroristas. Además, se deberá fomentar e incrementar las tácticas, técnicas y servicios que eviten el acceso a suministros para cometer los atentados.
- En la fase de Preparación de la respuesta, fomentar la toma de planes y medidas necesarias para asegurar la coordinación de todos los actores, agentes y organismos que deben asumir responsabilidades. Además, dar apoyo y minimizar los daños sufridos por las víctimas de los ataques.

Si se compara los objetivos, competencias con Defensa y competencias con los Cuerpos y Fuerzas de Seguridad, queda patente que esta línea de acción pertenece al sector de la seguridad. Si bien es cierto que con claras excepciones.

Como bien indica el Artículo 16 de la Ley Orgánica del 17 de Noviembre, 5/2005, toda acción terrorista que se lleve a cabo utilizando una aeronave será competencia de las Fuerzas Armadas. Además, en el caso en el que por acción terrorista se declaré la situación de catástrofe, las Fuerzas Armadas podrán apoyar en el restablecimiento de paz. Aun así, sería como apoyo, y disponiendo de las tecnologías y equipos que disponen para sus misiones diarias. Por ello, todo equipo, material o servicio que sirva para enfrentar las amenazas terroristas a través de aeronaves quedarán fuera de sector Industrial de la Seguridad.

Por otro lado, y para el resto de acciones terroristas ocurridas en territorio nacional, toda tecnología, actividad, proceso, o técnica que este enfocada a la creación de

equipos, materiales o servicios cuyo fin sea la lucha contra el terrorismo pertenecerá al Sector de la Seguridad, de los que serán beneficiarios de los FCS.

7.3. CIBERSEGURIDAD

Objetivo:

"Garantizar un uso seguro de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable" [1]

Líneas de acción más relevantes:

- A través del desarrollo tecnológico, aumentar las competencias en recuperación, respuesta, análisis, detección, reacción y prevención frente a toda amenaza cibernética.
- Promover, potenciar, e impulsa todo mecanismo técnico para la seguridad y protección en Sectores Estratégicos, Sectores Públicos, Servicios Esenciales, Sector Empresarial e Infraestructuras Criticas para garantizar fiabilidad en los entornos digitales.
- Fomentar el impulso y desarrollo de la Industria española en el sector de la ciberseguridad para aumentar las capacidades tecnológicas óptimas para enfrentar las amenazas en este sector.
- Contribuir y fomentar la participación de España en la creación de un ciberespacio seguro en un ámbito internacional y de la Unión Europea.

Una vez explicado el objetivo de la Ciberseguridad y resumidas las líneas de acción pertinentes para este proyecto, se procede a analizar si pertenece a la frontera del sector industrial.

Viendo las competencias de todas las Instituciones descritas anteriormente, y contrastando con los objetivos y líneas de acción propuestas por el DSN en lo referente al área de Ciberseguridad, esta recae bajo la responsabilidad de las Fuerzas y Cuerpos de Seguridad del Estado, concretamente Guardia Civil y Policía Nacional. Es por ello que la Ciberseguridad se incluirá como frontera del Sector Industrial de la Seguridad.

7.4. LUCHA CONTRA EL CRIMEN ORGANIZADO

Objetivo:

"Neutralizar las amenazas relacionadas con el crimen organizado mediante estrategias dirigidas a desarticular grupos ya existentes, prevenir la implantación de otros nuevos y contrarrestar su confluencia con el terrorismo" [1]

Líneas de acción más relevantes:

- Fomentar e impulsar la creación de medios y tecnologías para mantener canales de información y formación para contrarrestar la constante innovación de los organismos criminales en métodos y herramientas.
- Potenciar y fomentar toda tecnología que incrementa las capacidades en inteligencia estratégica, intercambio de información, instrumentos de anticipación y aquellas que puedan limitar la capacidad operativa del crimen organizado.

Después del estudio de las líneas de acción propuestas por el DSN, del estudio de las competencias, queda claro que el enfrentamiento de esta amenaza es competencia directa de las Fuerzas y Cuerpos de Seguridad, ya sean dependientes del estado o no. Por ello, toda tecnología y actividad, que fomente, mejore o desarrolle la creación de nuevos dispositivos, técnicas, tácticas o materiales que enfrenten al crimen organizado, en todas sus variables, pertenecerá al Sector Industrial de la Seguridad.

7.5. SEGURIDAD ECONÓMICA

Objetivo:

"Promover un crecimiento económico equilibrado basado en la competitividad, como base de un modelo socioeconómico inclusivo, sostenible y resiliente, capaz de crear empleo de calidad, que favorezca la innovación y la productividad en la actividad económica y empresarial y refuerce la defensa de los intereses y compromisos nacionales de seguridad" [1]

Líneas de acción más relevantes:

- Potenciar la creación y desarrollo de nuevos recursos y tecnologías que fomenten el intercambio de información entre las distintas Administraciones en el ámbito de la seguridad económico-financiera, además de en el sector privado, con el fin de dar respuesta eficaz a las amenazas de la economía española, y por ende, de la Seguridad Nacional.

Este apartado es de difícil interpretación. Si bien es cierto que la seguridad económica entra dentro del ámbito de la Seguridad Nacional, esto se debe a que la inestabilidad de la misma podría crear un ambiente de crispación y violencia en la sociedad.

Es por ello, que después de un estudio exhaustivo de las competencias, se determina que solo las tecnologías y actividades que fomenten mejoren y desarrollen nuevos dispositivos, técnicas o tácticas para la persecución, investigación y disuasión de delitos como fraude, apropiación indebida, etc. que estén relacionados con actos ilícitos que dañen la economía del ciudadano español entrarán dentro del Sector Industrial de la Seguridad. Si bien es cierto que queda definido que en ciertos ámbitos la Seguridad Económica forma parte de la frontera del sector, esta puede solaparse con otras amenazas, y es por ello que merece especial atención.

7.6. SEGURIDAD ENERGÉTICA

Objetivo:

"Diversificar las fuentes de energía, garantizar la seguridad del transporte y abastecimiento e impulsar la sostenibilidad energética" [1]

Líneas de acción más relevantes:

- Contribuir en la resiliencia de la Seguridad Energética.
- Asegurar la clara diversificación del conjunto de tecnologías que componen el mix energético español.
- Garantizar y fortalecer el abastecimiento y suministro de energía a toda la sociedad española.
- Potencia la transición hacia un modelo sostenible, renovable y eficiente.
- Fomentar la seguridad de toda aquella infraestructura, sobre todo aquellas consideradas críticas, que proporcione suministro energético frente a catástrofes, ya sean de origen natural, técnico, error humano o amenaza cibernética.

Una vez estudiadas las líneas de acción y competencias de las Fuerzas y Cuerpos de Seguridad, se ha considerado descarta la seguridad energética como parte de la frontera del Sector Industrial de la Seguridad. Esto se debe a que las mayores amenazas que provienen de este sector ya están contenidas a través de la Ciberseguridad y de la Protección de Infraestructuras Criticas. Es más, esto se podría considerar como un subapartado de ambas, por lo que sería redundante su consideración.

7.7. NO PROLIFERACIÓN DE ARMÁS DE DESTRUCCIÓN MÁSIVA, CONVENCIONALES Y EXPLOSIVOS

Objetivo:

"Combatir la proliferación de armas de destrucción masiva, sus vectores de lanzamiento, materiales conexos y tecnología asociada, así como impedir su acceso a actores no estatales, y en particular a organizaciones terroristas" [1]

Líneas de acción más relevantes:

- Garantizar y promover la seguridad de todo material o instalación radioactivo y nuclear.
- Potenciar la lucha contra el tráfico ilegal de tecnologías y materiales relacionados con armas de destrucción masiva y todo vector de lanzamiento.
- Potencia toda colaboración internacional en el fortalecimiento de la cadena logística y el controla en las fronteras para poder detectar cualquier tipo de tráfico ilegal de materiales susceptibles, incrementando las capacidades de identificación e información sobre dichas transacciones.
- Desarrollo y mejora de todo tipo de control aduanero.

Después del análisis de las distintas líneas de acción y las competencias, se ha llegado a una conclusión. La no proliferación de armas de destrucción masiva, convencionales y explosivos será competencia directa de las Fuerzas y Cuerpos de Seguridad, salvo ciertas excepciones. En el caso que las misiones para evitar esta proliferación sean fuera del territorio nacional y sus fronteras, y supongan un grave perjuicio para la Seguridad Nacional, las acciones que se lleven a cabo serán responsabilidad de las Fuerzas Armadas. Por otro lado, toda tecnología y actividad que fomente desarrolle o mejore cualquier dispositivo, técnica, táctica, material o equipo enfocado a la no proliferación de las ya mencionadas armas y materiales, será parte del Sector Industrial de la Seguridad. Si bien es cierto que en el ámbito de la protección física de las instalaciones nucleares y radioactivas forma parte de la Protección de Infraestructuras críticas, es un aspecto mejor dentro de las amenazas y se sobreentiende el solape.

7.8. ORDENACIÓN DE FLUJOS MIGRATORIOS

Objetivo:

"Prevenir, controlar y ordenar los flujos migratorios irregulares en las fronteras, así como garantizar una adecuada acogida e integración de los inmigrantes y solicitantes o beneficiarios de protección internacional" [1]

Líneas de acción más relevantes:

- Controlar y vigilar cualquier tipo de acceso a las fronteras nacionales exteriores, siempre dentro del Sistema Integrado de Gestión de las Fronteras Exteriores.
- Conservar la seguridad ciudadana a través de la promoción de la integración y luchar contra todo tipo de discriminación, con especial atención en los colectivos más vulnerables.
- Fomentar la cooperación con todo país, tanto de origen como de tránsito, para promocionar toda vía de inmigración legal, con especial énfasis en la lucha contra las redes de tráfico e inmigración ilegal de personas.

Una vez estudiadas las competencias y las líneas de acción de este tipo de amenaza, queda por concluir si definirá la frontera del sector. Cabe destacar un matiz, y este es que aunque las Fuerzas Armadas estén a cargo de la vigilancia de las fronteras marítimas del estado español, no son responsables de los flujos migratorios irregulares, incluso cuando puedan servir de apoyo o ayuda a los distintos cuerpos encargados de ello.

Por lo tanto, y una vez estudiado toda pesquisa, se concluye que la ordenación de flujos migratorios definirá la frontera del sector industrial de la seguridad. Por ello, toda actividad y tecnología que fomente, mejore o desarrolle cualquier tipo de técnica, táctica, dispositivo o material que enfrente la amenaza de flujo migratorios irregulares en las fronteras nacionales, con especial énfasis en el tráfico ilegal de personas, será considerado como parte del sector.

7.9. CONTRAINTELIGENCIA

Objetivo:

"Adoptar medidas en la defensa de los intereses estratégicos, políticos y económicos de España para prevenir, detectar y neutralizar las agresiones encubiertas, incluidas las efectuadas desde el ciberespacio, procedentes de otros Estados, de sus servicios de inteligencia o de grupos o personas, y que estén dirigidas a la obtención ilegal de información" [1]

Líneas de acción más relevantes:

- Potencias y fomentar la mejora de la protección de toda información clasificada.
- Incrementar la presencia de la contrainteligencia en el ciberespacio.
- Potenciar toda capacidad de cualquier órgano e institución nacional en materia de inteligencia, con el fin de proporcionar todo tipo de medios técnicos y humanos necesarios para enfrentar amenazas de este tipo.

En lo que a contrainteligencia concierne la conclusión es rápida y clara. Toda actividad y tecnologías que desarrolle, mejore o cree nuevos dispositivos, materiales, técnicas o tácticas enfocadas al servicio de la contrainteligencia y sus objetivos pertenecerán al sector industrial de la seguridad.

7.10. PROTECCIÓN ANTE EMERGENCIAS Y CATÁSTROFES

Objetivo:

"Consolidar el Sistema Nacional de Protección Civil como instrumento integrador de todas las capacidades de España para gestionar la respuesta ante emergencias y catástrofes y asegurar su integración bajo el Sistema de Seguridad Nacional" [1]

Líneas de acción más relevantes:

- Fomentar y promover toda colaboración entre organismos e instituciones público-privadas, con especial énfasis en materia de prevención.
- Incrementar, fortalecer y potenciar toda capacidad del Sistema Nacional de Protección Civil a través de la constitución de la Red de Alerta Nacional, aumentando sus capacidades, diseñando planes de acción y asistencia a las víctimas, y estableciendo protocolos de comunicación y gestión.

Una vez estudiados todos los objetivos y líneas de acción, y comparándolos con las competencias de las Fuerzas y Cuerpos de Seguridad se ha llegado a una conclusión. La Protección ante Emergencias y Catástrofes no formará parte de la frontera que define el sector Industrial de la Seguridad. Esto se debe a que tanto las Fuerzas Armadas como

las FCS tienen como competencia dar apoyo a toda institución y organismo que precise apoyo en caso de calamidad o desastre, pero solo apoyo en caso necesario, y con los materiales y las capacidades de que disponen para el cumplimiento de sus misiones. Es por ello, que al no ser una competencia directa, queda fuera de la clasificación.

7.11. SEGURIDAD MARÍTIMA

Objetivo:

"*Impulsar una política de seguridad en el espacio marítimo, tanto a nivel nacional como en el marco internacional y, especialmente, en la UE, con el fin de proteger la vida humana en el mar; mantener la libertad de navegación y proteger el tráfico marítimo y las infraestructuras marítimas críticas; prevenir y actuar ante actividades criminales y actos terroristas que se desarrollen en este medio; proteger y conservar el litoral, los recursos del medio marino, el medio ambiente marino y el patrimonio cultural subacuático; y prevenir y responder en casos de catástrofes o accidentes en este medio*" [1]

Líneas de acción más relevantes:

- Potenciar las capacidades de actuación del Estado español en materia marítima, tanto alta mar como su litoral, aprovechando de forma óptima sus recursos.
- Fomentar la colaboración con el sector privado.
- Potenciar las capacidades en materia de ciberseguridad en el ámbito marítimo.

Una vez declaradas todas las líneas de acción y objetivos se proceden a realizar un análisis. Este apartado o amenaza es uno de los más complejos a los que se enfrenta este proyecto debido a las competencias similares en materia por parte de las Fuerzas Armadas y de los FCS.

Todo acto terrorista fuera de las aguas territoriales españolas será responsabilidad de las Fuerzas Armadas, además de tener de forma compartida el mantenimiento de la libertad de navegación, y formar parte del apoyo en el caso de proteger el tráfico marino y proteger la vida humana en altamar.

Por lo tanto, las competencias directas de las FCS serán proteger las infraestructuras criticas (competencia que se solapa con la propia línea de acción definida por este nombre, pero al ser de gran importancia, se puede incluir), todo acto ilícito y terrorista cometido en aguas nacionales y su litoral, proteger el medioambiente, su patrimonio cultural subacuático, y sus recursos.

En el caso de la prevención de catástrofes o accidentes en el medio, tanto las Fuerzas Armadas como las FCS tendrán la obligación y competencia de dar apoyo. Pero al ser tareas de ayuda, no tendrán equipo especializado para tal fin.

Es por esto, que una vez diferenciadas las tareas y competencias tanto para Defensa como para Seguridad en esta línea de acción, todas las tecnologías y actividades que desarrollen, fomenten o creen nuevos materiales, dispositivos, técnicas o tácticas para el cumplimiento de las competencias de las FCS, será considerado parte del Sector Industrial de la Seguridad.

7.12. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Objetivo:

"Asegurar la correcta provisión de los servicios esenciales para la sociedad, haciendo más robusto y resiliente el sistema de infraestructuras críticas sobre el que se sustenta" [1]

Líneas de acción más relevantes:

- Incrementar todo tipo de infraestructuras criticas mejorando toda acción de prevención, planificación, mitigación del daño, reacción y restauración de la actividad.
- Fomentar, coordinar y promover la colaboración en todo tema relacionado con la protección de infraestructuras críticas, ciberseguridad y contraterrorismo, incrementando las capacidades para evitar y paliar los efectos de las mismas.
- Fomentar la cooperación entre organismos públicos y privados, para así incentivar el intercambio de información y capacidades.
- Potencia todo tipo de innovación en el campo de la seguridad, haciendo de las infraestructuras criticas sistemas con mejores equipos y componentes de seguridad, siempre apostando de forma prioritaria por el I+D+i nacional.
- Fomentar todo tipo de colaboración internacional, especialmente con Estados Unidos y los países miembros de la UE, para el intercambio de información y desarrollo de sistemas y estructuras seguras.

Una vez desarrollados los objetivos y las líneas de acción, queda concluir sobre esta área identificada por el DSN. Una vez revisadas todas las competencias de las FCS, se concluye que todos los objetivos son responsabilidad clara de estos organismos. Por ello, toda tecnología y actividad que fomente la creación, el desarrollo y la mejora de dispositivos, materiales, técnicas y tácticas enfocados a la protección de las infraestructuras criticas será considerado parte del Sector Industrial de la Seguridad.

7.13. SEGURIDAD DEL ESPACIO AEREO ULTRATERRESTRE

Objetivo:

"*Garantizar la seguridad del espacio aéreo y ultraterrestre en un marco compartido y orientado a prevenir las amenazas y desafíos que en ellos se desarrollan, así como a neutralizar sus consecuencias, conforme a los principios de eficiencia y máxima coordinación, tanto en el empleo de las capacidades de análisis y evaluación como en las de reacción ante los desafíos"* [1]

Líneas de acción más relevantes:

- Potenciar toda capacidad que tengan las instituciones y organismos, ya sean privados o públicos, para enfrentar toda amenaza propia del espacio ultraterrestre y aéreo.
- Fomentar, incrementar y desarrollar todo posible análisis de riesgo sobre los posibles actos ilícitos, ataques terroristas y ciberataques a las distintas instalaciones de transporte aéreo, aeroportuarias, ya sea fuera o dentro del espacio nacional.

Al igual que el anterior apartado de Seguridad Marítima, en el apartado de Seguridad del Espacio Aéreo y Ultraterrestre debe realizarse una clara diferenciación de las competencias de los distintos organismos.

Garantizar la seguridad del espacio aéreo y ultraterrestre es competencia absoluta de las Fuerzas Armadas. También lo es la persecución y paliación de cualquier acto terrorista llevado a cabo en este medio.

Por otro lado, la protección de las infraestructuras críticas y persecución de otros actos ilícitos cometidos en el espacio aéreo nacional serán responsabilidad y competencia de las FCS. Por ello, toda actividad y tecnología enfocada al desarrollo, creación y mejorar de nuevos dispositivos, materiales, técnicas y tácticas enfocadas a la consecución de estos objetivos formaran parte del Sector Industrial de la Seguridad.

7.14. SEGURIDAD FRENTE A PANDEMIAS Y EPIDEMIAS

Objetivo:

"Adoptar planes de preparación y respuesta ante riesgos sanitarios, tanto genéricos como específicos, bajo el principio de coordinación entre la Administración General del Estado y las Administraciones Autonómicas y con organismos internacionales, como la Organización Mundial de la Salud o, en el seno de la UE, el Centro Europeo para la Prevención y el Control de las Enfermedades" [1]

Líneas de acción más relevantes:

- En lo referente al incremento de los mecanismos y capacidades de actuación, se establecerá sistemas de coordinación entre las FA y las FCS para poder dar una respuesta eficaz frente a un ataque con agentes infecciosos intencionado.
- Fomentar y potenciar los sistemas de control y vigilancia para interceptar cualquier intento de introducción de un vector exótico y sus puntos de entrada.
- Incrementar y potenciar las capacidades de los equipos de respuesta en caso de intervención sanitaria, tanto interna como externamente.

Vistas las líneas de acción, cabe destacar que la mayoría de los objetivos forman parte del Ministerios de Sanidad y de los organismos dependientes de este, por ello, quedan fuera de la responsabilidad de todo organismo encargado de la Seguridad. Eso sí, hay algunas excepciones, y estas tienen que ver con los ataques intencionados utilizando patógenos. Todos estos ataques, su persecución, investigación y posterior proceso judicial serán competencias de las FCS. Las Fuerzas Armadas entraran como apoyo, con las mismas funciones que las FCS en caso de declararse zona de catástrofe.

Por ello, toda actividad y tecnología que fomente, cree o desarrolle nuevos dispositivos, materiales, técnicas y tácticas enfocadas a paliar, perseguir e investigar los posibles ataques intencionados con agentes infecciosos serán parte del Sector Industrial de la Seguridad.

7.15. PRESERVACIÓN DEL MEDIOAMBIENTE

Objetivo:

"Garantizar la conservación de un medio ambiente de calidad y la protección del patrimonio natural y de la biodiversidad, como medio para mejorar la calidad de vida y contribuir a un desarrollo sostenido y sostenible, con especial incidencia en la lucha contra el cambio climático" [1]

Líneas de acción más relevantes:

- Incrementar toda colaboración público-privada para la creación de las sinergias precisas en lo referente a la responsabilidad en la mejora y conservación del medioambiente.
- Incrementar y potenciar toda capacidad, ya sea especializada o genérica, en la lucha contra toda agresión al medioambiente que se considere una amenaza tanto para la calidad de vida de las personas como para el entorno natural.
- Incrementar la capacidad de los organismos pertinentes en la respuesta y prevención de todo tipo de contaminación marítima.
- Promover el uso de tecnologías y energías alternativas limpias.

Este apartado tiene clara y fácil clasificación. Existen FCS específicamente creados para la protección del medio ambiente, por ello la conclusión es clara.

Toda tecnología y actividad, enfocada al desarrollo, creación y mejorar de cualquier dispositivo, material, técnica o táctica dedicada a la protección del medioambiente formará parte del Sector Industrial de la Seguridad.

8. SITUACIÓN DENTRO DE LA AMENAZA

En este apartado se explicarán las distintas divisiones comunes que tienen las amenazas identificadas por el Departamento de Seguridad Nacional, y que ya han sido descritas y delimitadas para el sector en el apartado anterior. Dichas divisiones representan cada uno de los aspectos, etapas o fases a los que hay que hacer frente o que son parte del proceso de neutralización de esta. Además, debido a las características únicas de cada una de ellas, tendrán como protagonistas distintos grupos tecnológicos que no tendrán por qué ser partícipes en otras. Cabe destacar que no todas las amenazas deben tener todas y cada una de las divisiones, algunas son específicas, y otras simplemente no tienen razón de existencia debido a sus propias características.

Tras el estudio realizado, se han considerado como divisiones comunes las siguientes:

- Comunicaciones

En este aspecto se debe enfocar a cualquier actividad, protocolo o proceso relacionado con las comunicaciones. Con el fin de transmitir información, ya sea audiovisual o escrita, mensajes, archivos, o cualquier tipo de dato que aporte en el cumplimiento de la misión. En este aspecto se englobarán todas las tecnologías y actividades que permitan que los agentes encargados de enfrentar la amenaza puedan comunicarse con su destinatario de forma rápida y segura, sin que haya interrupciones ni filtraciones, siendo líneas seguras de posibles invasiones.

- Detección

Se englobarán toda tecnología y actividad que permita detectar cualquier tipo de amenaza, recopilar información y realizar un seguimiento de esta. Con detectar se hace referencia a localizar el peligro, la fuente de la que proviene, la naturaleza de la misma, y recabar los datos necesarios para una posterior toma de decisiones.

- Gestión de la Información

Englobará toda tecnología, actividad, técnica o proceso que facilite la gestión de la información de la que se dispone. Esta gestión es de vital importancia para el enfrentamiento de las amenazas. Supone escoger los datos relevantes y descubrir la forma eficaz y efectiva para cumplir con la misión, disminuyendo los riesgos y recursos a emplear.

- Posicionamiento

Tendrá en cuenta todas las actividades, tecnologías, técnicas o procesos que faciliten a las Fuerzas y Cuerpos de Seguridad un correcto posicionamiento ventajoso frente a la amenaza. Con posicionamiento no se refiere solo a un posicionamiento físico, sino táctico y estratégico, utilizar las ventajas que proporcionan sus dispositivos para enfrentar la amenaza desde una posición favorable.

- Evaluación de riesgos

Englobará toda tecnología, actividad, proceso, técnica y entrenamiento que favorezca la evaluación de la situación, teniendo en cuenta toda información, además de realizar un estudio en posibles casos parecidos de historial, para poder conocer con exactitud los riesgos que entrañará enfrentar la amenaza en cuestión y las medidas tomadas para paliar sus efectos.

- Conocimiento o consciencia de la situación

En este aspecto se englobará toda tecnología y actividad que proporcione a los agentes encargados de enfrentar a la amenaza, problema o catástrofe una imagen o consciencia real de la situación en la que se encuentran. Con esto se pretende dar toda la información necesaria para que los Cuerpos encargados de la misión tengan los datos necesarios para cumplir con éxito su cometido, tomando las mejores decisiones y arriesgando el menor número de recursos. No debe confundirse con la gestión de la información. En una se proporcionan datos, se ordenan y se filtran, en este apartado se agrupan las tecnologías que proporcionan una imagen real del problema a abordar. Esto no quiere decir que no haya tecnologías comunes, es más, habrá muchas en común, pero habrá otras completamente exclusivas de cada uno de los apartados.

- Entrenamiento

En este aspecto se englobará toda tecnología y actividad que favorezca el desarrollo de nuevas técnicas de entrenamiento o mejora de las ya existentes. Estas técnicas de entrenamiento son fundamentales para que los agentes encargados de enfrentar las amenazas estén preparados frente a cualquier reto que se les oponga, además de tener las habilidades y capacidades necesarias para cumplir con éxito y eficiencia su cometido.

- Doctrina y operaciones

Se englobarán todas las tecnologías, actividades, técnicas y procesos que favorezcan la creación de doctrinas o modos de operación para llevar a cabo la lucha contra las amenazas. Además, se incluirán todos los grupos tecnológicos que sirvan como apoyo al desempeño de la operación, siempre y cuando no se encuentren dentro de las demás clasificaciones.

- Respuesta al incidente

En este aspecto se englobarán toda tecnología, actividad, técnica, proceso y entrenamiento que favorezca que las Fuerzas y Cuerpos de Seguridad den una respuesta ante el incidente. Esta respuesta puede tener cualquier carácter, desde enfrentarse a la amenaza, como contenerla o paliarla.

9. GRUPOS TECNOLÓGICOS

En este apartado se procederá a mencionar, agrupar y describir todas las tecnologías que se han considerado participes dentro de las operaciones que llevan a cabo las Fuerzas y Cuerpos de Seguridad. Estos son:

9.1. AI AND DECISION SUPPORT

- Data and information management

Toda tecnología y actividad que facilite la gestión de datos e información obtenida durante las operaciones

- Data classification

Toda tecnología y actividad que facilite la clasificación de datos obtenido durante las operaciones

- Data collection

Toda tecnología y que facilite la recopilación de datos que provengan de los equipos o fuentes de información que los agentes utilicen

- Data fusion

Toda tecnología y actividad que facilite la fusión de datos para obtener nuevos o conclusiones que faciliten la posterior toma de decisiones

- Data mining

Toda tecnología y actividad que facilite la extracción de datos para el apoyo u obtención de información que facilite la tarea de los apartados anteriores

- Data/Information fusion technology

Toda tecnología que facilite la fusión de datos. Muy enlazado con el apartado “Data fusión”, pero en este caso solo concreta el aspecto de la tecnología. Se realiza una separación especifica debido a la importancia actual que tiene.

- Evacuation and consequence management techniques

Toda tecnología y actividad que mejore las técnicas de evacuación y gestión de las consecuencias de una situación de riesgo. Esto abarca desde los sistemas de comunicación y alarma (ya sea visual y sonora), hasta los sistemas de gestión y control de masas

- IKBS(Intelligence Knowledge-Based Systems)/AI/Expert techniques

Toda tecnología y actividad que favorezca o desarrolle los sistemas de inteligencias basadas en el conocimiento, bases de datos y su tratamiento, y la inteligencia artificial

- Impact Analysis concepts and impact reduction

Toda tecnología y actividad que favorezca o desarrolle las capacidades de análisis de impacto y capacite a los actores con mejores o nuevas técnicas de reducción del mismo

- Individual and team training

Toda tecnología y actividad que mejore o cree nuevas técnicas de entrenamiento, tanto en equipo como individual, para preparar a los agentes frente a las nuevas amenazas que se ciernen sobre la sociedad

- Information fusion

Toda tecnología y actividad que mejore las capacidades de fusión de la información. Esta se diferencia de las anteriores como “Data fusión” debido a que en este apartado la información no tiene por qué ser cuantificable. Puede ser cualquier tipo de información, desde previsiones hasta comunicados.

- Knowledge management

Toda tecnología y actividad que mejore la capacidad de gestión del conocimiento. En lo que respecta a conocimiento se centra en todo dato, información de la situación de tanto las amenazas como los agentes que la enfrentan.

- Mission simulation

Toda tecnología y actividad que disponga de las capacidades necesarias para recrear o simular situaciones reales de misión. Con ello, los agentes podrán practicar y entrenar frente a casos reales, o muy similares, a los que se encontrarán una vez enfrenten a las amenazas en su campo.

- Models to support preparedness exercises and actual crisis response

Toda tecnología y actividad que favorezca el desarrollo, creación o mejora de ejercicios de preparación ante situaciones y la creación de planes de respuesta ante crisis. Esto formaría parte del entrenamiento de los actores que enfrentan las amenazas, que debido a la importancia que tienen es merecedor de un apartado.

- Natural language processing technology

Toda tecnología y actividad que favorezca el desarrollo de tecnologías de procesamiento del lenguaje natural, para su posterior análisis. Con las conclusiones obtenidas se podrá gestionar y tomar decisiones en base a la información obtenida.

- Operational Analysis tools and techniques

Toda tecnología y actividad que favorezca el desarrollo y la creación de nuevas herramientas y técnicas de análisis operacional. El fin último seria mejorar la eficiencia y eficacia de los actores que enfrentan las amenazas cuando se encuentran en medio de una operación.

- Optimisation, Planning & Decision Support

Toda tecnología y actividad que optimice y mejore la planificación y el apoyo en la toma de decisiones. Abarca desde la toma de decisiones en directo, en medio de una operación, como en el proceso de análisis y gestión de la información y datos.

- Optimization, Planning and Decision Support Systems

Toda tecnología y actividad que optimice y mejore los sistemas de planificación y apoyo en la toma de decisiones. La diferencia con el apartado anterior es que centra el foco solo en sistemas y formas más complejas para el apoyo.

- Pattern recognition

Toda tecnología y actividad que permita el desarrollo de técnicas y sistemas capaces de reconocer patrones. Con dicho reconocimiento se realizará un posterior procesamiento de la información para poder gestionarlo y tomar decisiones al respecto.

- Simulation for decision making

Toda tecnología y actividad que permita simular situación de riesgo o crisis para practicar, mejorar y hacer más eficiente el proceso de toma de decisiones. En medio de una operación el tiempo es un factor crucial que juega en contra de los actores o agentes que la llevan a cabo, por ello la simulación con el fin de practicar y agilizar toda actuación puede tener gran repercusión en el éxito de las misiones.

- Synthetic environment

Toda tecnología y actividad que permita desarrollar y crear ambientes artificiales o sintéticos según necesidades de los actores o de la propia misión que lleven a cabo.

- Tactical/Crew training systems

Toda tecnología y actividad que favorezca el desarrollo o la creación de nuevos sistemas de entrenamiento táctico y en equipo. Con ello, se pretende entrenar a los actores que enfrenten las amenazas en las nuevas técnicas utilizadas para cometer actos ilícitos con el fin de evitar que alcancen el éxito.

- Task analysis modelling and scenario analysis

Toda tecnología y actividad que mejore las capacidades de modelado del análisis de tareas y escenarios, para optimizar la posterior toma de decisiones en campo.

- Text mining

Toda tecnología y actividad que mejore las capacidades de extracción de datos e información contenida en textos. Esta información posteriormente será analizada, procesada y gestionada para la toma de decisiones.

- Training techniques

Toda tecnología y actividad que fomente, desarrolle o cree nuevas técnicas de entrenamiento que ayuden a los actores y agentes, que enfrentan las amenazas, a mejorar en la toma de decisiones.

- Web and languages technologies

Toda tecnología y actividad que desarrolle sistemas y procesos de traducción de lenguajes y navegación Web. Esto se debe a que para los actores dispongan de toda la información de forma accesible, esta deberá traducirse o buscarse a través de la red. Con este tipo de tecnologías se pretende agilizar ese proceso y agilizar el cumplimiento de las misiones.

9.2. BIOMETRICS

- Digital fingerprints recognition

Toda tecnología y actividad que desarrolle métodos de reconocimiento a través del procesamiento e identificación de huellas dactilares. Apartado de gran importancia debido a que toda huella dactilar es única, siendo una característica de cada individuo, identificándolo de por vida a no ser que se realicen modificaciones de forma artificial.

9.3. BIOTECHNOLOGY

- Food testing and control techniques

Toda tecnología y actividad enfocada al desarrollo de técnicas para el control y testeo de alimentos y similares, con el fin de controlar posibles enfermedades o patógenos que supongan un peligro para la población.

- Rapid analysis of biological agents

Toda tecnología y actividad enfocada al desarrollo, creación o mejora de cualquier forma de análisis rápido de agentes biológicos. Enfocado prioritariamente a pruebas o test rápidos de campo.

- Water testing and purification techniques

Toda tecnología y actividad enfocada al desarrollo de técnicas para la purificación y testeo del agua, con el fin de controlar posibles enfermedades o patógenos que supongan un peligro para la población.

9.4. CBRNE

- Biological technologies for biological and medical countermeasures

Toda tecnología y actividad que este enfocada al desarrollo de nuevas contramedidas en los campos de la medicina y accidentes biológicos, con el fin de proteger a la población frente a los posibles efectos adversos de los mismos.

- CBRN sensors

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de sensores que sean capaces de detectar señales de actividad nuclear, radiológica, biológica y química. Además, deberán proporcionar información sobre el origen o posible localización del foco de la señal.

- Chemical and biological detection

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos procesos o dispositivos que sean capaces de detectar actividad química y biológica. Además, deberán proporcionar información sobre el origen o posible localización del foco de la señal.

- Chemical and biological detection tecniques

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevas técnicas para la detección de actividad química y biológica.

- Chemical and Biological Detection/identification

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos procesos, técnicas o dispositivos que sean capaces de detectar e identificar las fuentes de actividad química y biológica.

- Decontamination techniques

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevas técnicas o procesos de descontaminación de todas y cada una de las actividades descritas anteriormente en este apartado (CBRN).

- EM difficult scenarios

Toda tecnología y actividad enfocada al desarrollo y creación de nuevo escenario experimentales para el campo de la medicina, con el fin de poder recrear situaciones o experimentos que supongan nuevas posibilidades de avance en este campo.

- EMC evacuation and hardening

Toda tecnología y actividad que desarrolle mejore o cree nuevos planes de evacuación EMC

- Explosive detection sensors

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de sensores capaces de detectar cualquier tipo de explosivos. Además, deberán proporcionar información sobre su posible clasificación o composición.

9.5. COMMS

- Broadband access to mobile users in dynamic situations

Toda tecnología y actividad que favorezca o permita el acceso de banda ancha a cualquier usuario que se encuentre en una situación dinámica. Con esto se pretende mejorar el sistema de comunicación de los agentes o actores que se encuentren en medio de una misión para aumentar las posibilidades de éxito al enfrentar una amenaza.

- Communications and Information Systems security equipment

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de equipos o sistemas específicos para la comunicación y la transmisión de información.

- Communications network management and control equipment, network supervision

Toda tecnología y actividad dedicada al desarrollo, mejora o creación de nuevas técnicas o procesos de gestión de las redes de comunicación, control de equipo, y supervisión de redes.

- Information security

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos procesos, técnicas o medidas que incrementen la seguridad de la información.

- Mobile secured communications

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos procesos, técnicas o medidas que incrementen la seguridad de las comunicaciones móviles.

- Network management and control

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos procesos, técnicas o medidas de control y gestión de redes.

- Protocol technology

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevas tecnologías de protocolo.

- Reconfigurable communications

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos procesos, técnicas o dispositivos del campo de las comunicaciones que tengan la capacidad de ser reconfigurables.

- Secured wireless broadband data links for secured communications

Toda tecnología y actividad que enfocada al desarrollo, mejora o creación de enlaces de datos de banda ancha para contribuir a la creación de comunicaciones seguras.

9.6. ELECTRONIC AUTHENTICATION

- Electroning tagging systems

Toda tecnología y actividad que enfocada al desarrollo, mejora o creación de sistemas de etiquetado electrónico.

- Smart cards

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de los nuevos sistemas Smart Cards. La definición de Smart Card es pequeño chip que contiene cierta cantidad de información alojado normalmente en una tarjeta de plástico. Esta información puede ser borrada o actualizada, y normalmente facilita datos identificativos.

9.7. ENERGY GENERATION, STORAGE AND DISTRIBUTION

- Alternative power sources and devices

Toda tecnología y actividad que enfocada a la creación, mejora y desarrollo de equipos, dispositivos o fuentes de alimentación alternativa.

- Electric batteries

Toda tecnología y actividad enfocada al desarrollo, creación o mejora de eficiencia de las baterías eléctricas.

- Energy distribution

Toda tecnología y actividad enfocada a la creación de nuevas técnicas o la mejora de la eficiencia de la distribución energética.

- Power generators

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de generadores de energía. Cabe destacar, que en este apartado no se hace referencia a cualquier tipo de generador, descartando las plantas convencionales o generadores para uso civil. Este apartado centra el foco en todo aquel dispositivo que provea de energía a los actores o agentes que se encuentran en el cumplimiento de una misión, siempre que no dispongan de suministro corriente por vías convencionales.

9.8. FORENSIC

- Biometrics

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos biométricos.

- Facial/Fingerprint/Iris/Retina/Voice signature recognition

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos procesos, técnicas o dispositivos dedicados a la identificación de firma digital a través del reconocimiento facial/huella digital/iris/retina/voz.

9.9. GIS

- Advance image and geo-spatial analysis techniques

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de técnicas para la obtención avanzada de imágenes y el posterior análisis geoespacial.

- Earth observation

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de técnicas para la observación terrestre.

9.10. HUMAN SCIENCE

- Advanced Human behaviour modelling and simulation

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de sistemas de modelado y simulación avanzada del comportamiento humano.

- Human Behaviour Analysis and Modelling

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas técnicas de análisis y modelado del comportamiento humano

- Human Factor in decision process

Toda tecnología y actividad dedicada a contener la premisa factor humano en la toma de decisiones.

- Human survivability, protection and stress effects

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de equipos, dispositivos y técnicas que incrementen la protección y las posibilidades de supervivencia. Además, disminuir los efectos del estrés consecuencia de la participación en misiones por parte de los agentes y actores que enfrenten amenazas.

- Population behavior

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos y técnicas capaces de predecir, analizar y controlar el comportamiento de la población.

- Prediction of máss behavior

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos y técnicas capaces de predecir, analizar y controlar el comportamiento de masas. La diferencia con el apartado anterior es que masa se puede definir como aglomeración de personas, no hace referencia a la población total de la sociedad.

- Skills training

Toda tecnología y actividad que desarrolle mejore o cree nuevas técnicas de entrenamiento para preparar a los agentes o actores en el campo de las ciencias sociales.

9.11. INTEGRATED PLATFORMS

- Aircraft

Aeronave, queda definido como cualquier vehículo o dispositivo que sea capaz de volar, siendo dirigido y tripulado por una persona que se encuentra a bordo.

- Helicopters

Entran dentro de la categoría de aeronaves, pero debido a su importancia deben tener una mención especial. Vehículo o dispositivo que se sustenta y desplaza gracias a uno o más rotores horizontales.

- Vessels

Embarcación, queda definido como cualquier vehículo o dispositivo que sea capaz de navegar, siendo dirigido y tripulado por una persona que se encuentra a bordo.

- Land vehicles

Vehículo terrestre, queda definido como cualquier dispositivo que sea capaz de desplazarse por tierra, siendo dirigido y tripulado por una persona que se encuentra a bordo.

- On board Electric batteries

Toda tecnología y actividad enfocada a la creación, mejora y desarrollo de baterías eléctricas de a bordo.

- Surveillance and navigation satellites

Todo dispositivo dedicado a la vigilancia o a los sistemas de navegación que se encuentra en orbite alrededor de la Tierra

- Unmanned land/sea/air vehicles

Todo tipo de vehículo sea cual sea su medio por el que se desplaza, que en vez de estar tripulado por una persona que se encuentre a bordo, sea controlado por control remoto, sistema o programa.

9.12. IT

- Device integration/reliability

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de dispositivos dedicados a la integración y mejora de fiabilidad de sistemas IT.

- High integrity and safety critical computing

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de dispositivos de alta integridad y seguridad crítica.

- High performance computing

Toda tecnología y actividad que fomente el desarrollo, mejora o creación de nuevas generaciones de ordenadores de alto rendimiento.

- Image processors / autonomous vehicles

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevas capacidades para poder disponer de vehículos autónomos que se guíen a través del procesamiento de imágenes.

- Infrastructure to support information management and dissemination

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevas infraestructuras que apoyen las técnicas de gestión de la información y su diseminación.

- Protocol technologies

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevas tecnologías de protocolo en el ámbito de las tecnologías de la información.

- S/W architectures

Toda tecnología y actividad que fomente la creación de nuevas arquitecturas software para el desarrollo de nuevos programas y sistemas enfocados a las tecnologías de la información.

- Secure computing techniques

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevas técnicas para el uso seguro de los ordenadores y sistemas de información.

- S/W engineering

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevos procesos, técnicas dispositivo que apoyen la ingeniería de software.

9.13. IT SECURITY

- Access Control

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevas técnicas y protocolos de control de acceso enfocados a la seguridad en las tecnológicas de la información.

- Authentication

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevos procesos, técnicas y dispositivos enforcados a la identificación en las tecnológicas de la información.

- Crypto

Toda tecnología y actividad que fomente el desarrollo, mejora y creación de nuevos procesos, técnica y dispositivos criptográficos.

- Cybersecurity policy management tools

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas herramientas enfocadas a la gestión de las políticas de ciberseguridad y su posterior aplicación.

- Encryption and key management

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas herramientas y técnicas de gestión y cifrado de claves.

- Filtering technologies

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas herramientas, técnicas y dispositivo cuya función es el filtrado de información.

9.14. MATERIALS

- Anti blast glasses/concrete

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de hormigón y cristal capaz de soportar explosiones.

- Light materials for human protection

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de materiales ligeros dedicados exclusivamente a la protección física de las personas que los lleven.

- Materials for site protection

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de materiales dedicados exclusivamente a la protección de lugares de interés.

- Self-protective and explosive resistant material

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de materiales cuyo cometido es la protección personal, siendo resistentes a explosivos y sus efectos adversos.

- Smart textiles

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos tejidos inteligentes, que sean capaces de proporcionar información de su portador y el entorno que le rodea.

- Structural and smart materials

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos materiales inteligentes.

9.15. NAVIGATION & GUIDANCE

- Direction finding and map guidance

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos procesos, técnicas y dispositivos de orientación.

- Navigation technologies

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas técnicas de navegación.

- Radio navigation

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos procesos, técnicas y dispositivos para la navegación por radio.

- RFID based tracking

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos procesos, técnicas y dispositivos de rastreo a través de la identificación por radiofrecuencia.

9.16. SENSORS

- Acoustic sensors

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos sensores acústicos.

- Autonomous small sensors/smart dust technologies

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevos sensores SmartDust. Están compuesto por pequeñas redes de pequeños sensores electromecánicos capaces de detectar muchos tipos de señales. El nombre proviene de que cada dispositivo que compone la red parece una diminuta mota de polvo.

- Cameras

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de cámaras o sensores visuales.

- Early detection techniques

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de nuevas técnicas de detección temprana.

- Hyper-spectral / Multi-spectral

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de sensores hiper o multi espectrales. Con esto hace referencia a sensores que recopilan, procesan y analizan señales que provienen de todo el espectro electromagnético.

- Hyper-spectral/multi-spectral processing

Toda tecnología y actividad enfocada al desarrollo, mejora y creación de procesadores de información multi/hiper espectral.

- IR sensors

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de sensores infrarrojos.

- Micro and mm-wave sensors

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de sensores cuyo espectro de captación son las mm/micro ondas.

- Motion sensor systems

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de sistemas de sensores motrices.

- Motion sensors

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de sensores motrices.

- Nanotechnologies for sensors

Toda tecnología y actividad enfocada a la creación, mejora o desarrollo de nuevos sensores basados en la nanotecnología.

- Non cooperative target recognition

Toda tecnología y actividad enfocada a la creación, mejora y desarrollo de nuevas técnicas y dispositivos de reconocimiento del objetivo sin cooperación del mismo.

- Radar sensors

Toda tecnología y actividad enfocada a la creación, mejora y desarrollo de sensores basados en el radar.

- SAR/ISAR equipment

Toda tecnología y actividad enfocada a la creación, mejora y desarrollo de nuevos sensores y equipos que se utilizarían para labores de rescate.

- Sensors

  Toda tecnología y actividad enfocada a la creación, mejora y desarrollo de nuevos sensores. En esta clasificación entrarían todos los sensores que detectan o utilizan métodos distintos a los mencionados anteriormente.

- Smart clothes and equipment

Toda tecnología y actividad dedicada al diseño y creación de tejidos y equipos inteligentes, enfocado sobre todo a sensores capaces de dar información sobre el actor o agente que los utiliza y el entorno que le rodea.

- Smart video surveillance

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de sistemas de videovigilancia inteligentes.

- Teraherts sensors

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de sensores Terahercios. Estos están basados en una nueva generación de sistemas de detección a través de semiconductores para imágenes en terahercios. Son sensores visuales avanzados.

- Visible and IR cameras

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de cámaras que detectan imágenes desde el rango de los infrarrojos hasta la luz visible.

9.17. SIGNAL PROCESSING

- Digital processing

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos, procesos y técnicas de procesamiento digital.

- Filtering technologies

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos, técnicas o procesos de filtrado digital.

- Image/pattern processing

Toda tecnología y actividad enfocada al desarrollo, mejora o creación de nuevos dispositivos, procesos y técnicas de procesamiento de patrones e imágenes.

10. CONCLUSIONES Y TAXONOMÍA

Después de clasificar las líneas de acción y amenazas, fases dentro de las mismas, y los grupos tecnológicos existentes, ya estaría definida la Taxonomía del Sector Industrial de la Seguridad. Con estas explicaciones se habría definido toda "zona gris" donde no estaba claro la diferencia entre Defensa y Seguridad, además de esclarecerse los objetivos prioritarios donde la industria de la seguridad debe enfocarse. Este foco no tiene otro objetivo que ayudar a las Fuerzas y Cuerpos de Seguridad a cumplir con su cometido de forma eficaz y efectiva, con el mínimo de los recursos, tanto económicos como humanos, minimizando así los riesgos para estos últimos.

Para aclarar de forma final el resultado de la taxonomía se procederá a realizar un breve resumen de las líneas de acción escogidas, las fases, y por último, los grupos tecnológicos.

En primer lugar, las amenazas o líneas de acción que definen la frontera del Sector de la Seguridad son:

- Lucha contra el terrorismo
- Ciberseguridad
- Lucha contra el crimen organizado
- Seguridad Económica
- No proliferación de armas de destrucción masiva, convencionales y explosivos
- Ordenación de flujos migratorios
- Contrainteligencia
- Seguridad marítima
- Protección de infraestructuras críticas
- Protección del espacio aéreo ultraterrestre
- Seguridad frente a pandemias y epidemias
- Preservación del medioambiente

Todas ellas definen la frontera Sector Industrial de la Seguridad, si bien con matices ya explicados en sus correspondientes apartados, donde los productos y servicios ofrecidos por la industria deben ser enfocados.

Las fases, también definidas, que dividirán cada una de las líneas de acción son las siguientes:

- Comunicaciones
- Detección de la amenaza
- Gestión de la información
- Posicionamiento
- Evaluación de riesgos
- Conocimiento o consciencia de la situación

- Entrenamiento
- Doctrina y operaciones
- Respuesta al incidente

Todas estas fases que pueden dividir las distintas líneas de acción ya han sido descritas con anterioridad. Suponen el segundo nivel de la taxonomía, donde cada grupo tecnológico debe situarse y ofrecer sus productos.

A continuación, se presentará un breve resumen de los distintos grupos tecnológicos que se han identificado y definido para la taxonomía. Se ha considerado que estos son aquellos que abarcan todos los productos que ofrece el sector en la actualidad, y donde en un futuro se podrán incluir aquellos que irrumpan en el mundo de la seguridad. El listado de los grupos tecnológicos es:

- Inteligencia Artificial y apoyo en la toma de decisiones
- Biometría
- Biotecnología
- CBRNe
- Comunicaciones
- Autentificación electrónica
- Distribución, generación y almacenamiento de la energía
- Tecnologías forenses
- GIS
- Toda tecnología relacionada con las Ciencias Humanas
- Plataformas Integradas
- Tecnologías de la información
- Seguridad dentro de las Tecnologías de la Información
- Materiales
- Guía y navegación
- Sensores
- Procesamiento de la señal

Centrando la explicación en el objeto del proyecto, la taxonomía, quedaría dibujada como tres anillos. El anillo superior y frontera exterior, estaría compuesto por todas las líneas de acción y amenazas definidas por el Departamento de Seguridad Nacional, y diferenciadas en este proyecto. El segundo anillo, subordinado al primero, sería el anillo de las fases dentro de las amenazas. Por último, el tercer anillo, el de los grupos tecnológicos. Este sería el último paso para definir en que lugar del Sector de la Industria de la Seguridad se encuentra un producto de una empresa y organismo. A continuación, se presentaría una descripción gráfica de la taxonomía

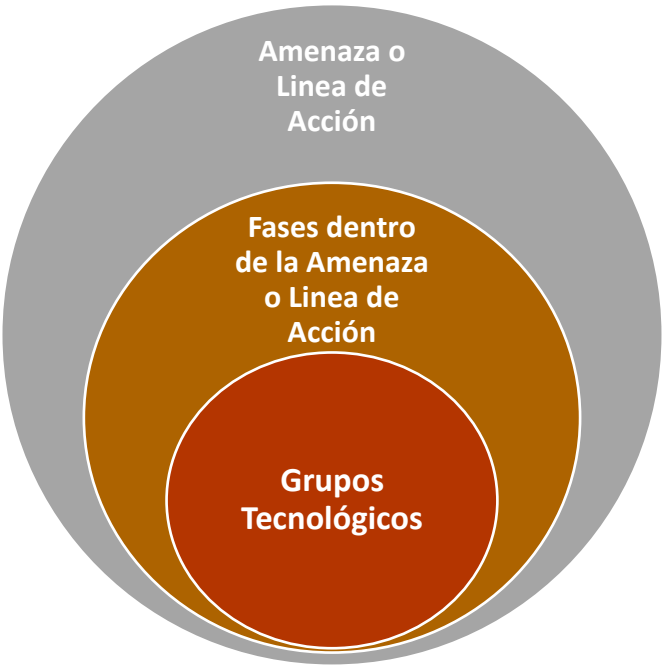


Ilustración 16: Esquema de la taxonomía

Para el aprovechamiento práctico de esta taxonomía, se ofrecerá un ejemplo en forma de matriz de como debería utilizarse este tipo de taxonomía en el ANEXO 1. EJEMPLO MATRIZ TAXONOMÍA. Esta se presenta como una propuesta, por lo que es susceptible de cambios, y debería ser un equipo, formado por personas de las distintas áreas que componen el sector industrial aquellos que deberían definir qué productos están implicados en las distintas categorías. Además, se presentará a continuación un organigrama ejemplo de como estarían organizado los productos a través de esta metodología. Se centra en una breve presentación de algunos productos, se escoge como línea de acción la Lucha contra el Terrorismo, y dentro de esta, la Fase Detección de la Amenaza. Además, se han escogido cinco tecnologías para una representación ilustrativa. Se puede observar claramente como las tecnologías seleccionadas a la que pertenecerían los productos o servicios estarían subordinadas dentro de los propios anillos. Hay que mencionar que el organigrama final sería mucho más elaborado, siendo su representación similar a la siguiente:

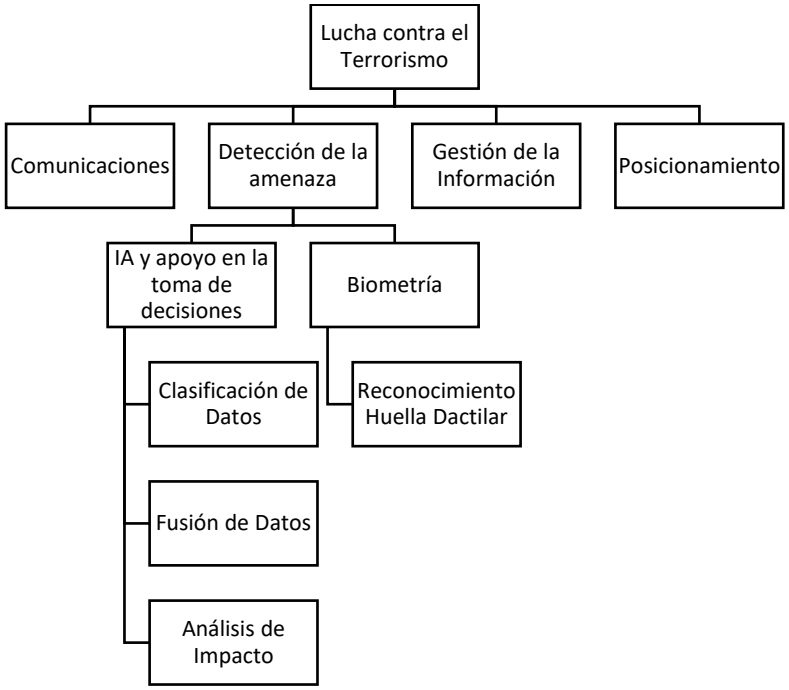


Ilustración 17: Ejemplo Organigrama de la Taxonomía

Cabe destacar que esta taxonomía final, definida a través de las capacidades y de las distintas leyes estudiadas es de naturaleza dinámica. Con dinámica se hace referencia a que la Seguridad, como se ha explicado anteriormente, es un sector que abarca un gran número de empresas pioneras en los avances tecnológicos de sus segmentos de mercado. Esto quiere decir que, en un breve espacio de tiempo, la matriz puede sufrir cambios con la aparición de nuevas tecnologías disruptivas. Además, por otro lado, las leyes en las que se han basado las competencias, y las líneas de acción pueden verse actualizadas algunas, descartadas otras, y producirse la aparición de otras nuevas. Con esto se quiere hacer hincapié en que el valor añadido que ofrece este proyecto es en la nueva metodología escogida para definir el Sector Industrial de la Seguridad. Esto es, en breves palabras, enfocar las amenazas o líneas a combatir, estudiar las competencias de las distintas Fuerzas y Cuerpos de Seguridad a los que irán enfocados los productos y servicios, dividir en sectores estas amenazas, e identificar los grupos tecnológicos útiles para enfrentar a los mismos.

Para concluir, se debe dar una opinión sobre el Sector Industrial de la Seguridad y lo que supone este proyecto. La seguridad es un pilar fundamental dentro de la sociedad, sustenta su modo de vida y protege el estado de bienestar nacional, referente a nivel mundial. Día a día adquiere mayor importancia debido al proceso de digitalización que está sufriendo todo aspecto de la vida cotidiana del ciudadano, y esto es debido al consecuente desarrollo de la Ciberseguridad, sector al alza que cada vez tiene más importancia y recibe mayor inversión en España. Además, es un sector principalmente enfocado a las nuevas tecnologías, su desarrollo e innovación. Es por ello que se considera estratégico, debido a que todo avance o producto es un activo de gran valor

añadido, robusteciendo la economía nacional y haciendo de este país un referente a nivel internacional. Es por ello, y por el carácter difuso ya explicado anteriormente de este sector, que este proyecto aporta valor al futuro de la seguridad nacional. Sentar las bases de la organización del mismo mejoraría el planteamiento estratégico de las distintas empresas, enfocando sus productos y servicios a los intereses reales de los agentes e instituciones beneficiarios. Además, atraería nuevos fondos y financiación, tanto nacional como internacional, ofreciendo apoyo económico a los proyectos que se están llevando a cabo, y como se ha explicado anteriormente, apoyando y robusteciendo la economía nacional.

11. BIBLIOGRAFÍA

[1] D. d. S. Nacional, 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf.

[2] R. F. R. R. K. W. (. R. &. C. F. F. R. K. R. v. L. (. P. d. H. A. T. R. v. B. (. U. B. Thordis Sveinsdottir, 2014. [Online]. Available: http://crisppproject.eu/wp-content/uploads/2016/05/CRISP-D1.2-Taxonomy-of-Security-Products-Systems-Services_REVISED.pdf.

[3] "Boletín Oficial del Estado, Viernes 1 de agosto de 2014," [Online]. Available: https://www.boe.es/boe/dias/2014/08/01/pdfs/BOE-A-2014-8276.pdf.

[4] "Real Decreto 512/2017, 22 de mayo," 2017. [Online]. Available: http://www.hacienda.gob.es/BoletinesHacienda/Boletines//2017/54730.pdf.

[5] "Real Decreto 1224/2006, 27 de octubre," 2006. [Online]. Available: https://www.boe.es/buscar/pdf/2006/BOE-A-2006-19916-consolidado.pdf.

[6] "Real Decreto 179/2005, 18 de febrero, sobre prevencion de riesgos laborales en la Guardia Civil," [Online]. Available: https://www.boe.es/buscar/pdf/2005/BOE-A-2005-3241-consolidado.pdf.

[7] "Real Decreto 1250/2001, de 19 de noviembre, por el que se aprueba el Reglamento de provisión de destinos del personal del Cuerpo de la Guardia Civil.," 2001. [Online]. Available: https://www.boe.es/buscar/pdf/2001/BOE-A-2001-22623-consolidado.pdf.

[8] "Real Decreto 1429, de 15 de septiembre, por el que se aprueba el Reglamento General de adquisición y pérdida de la condicion de militar de carrera del Cuerpo de la Guardia Civil," 1997. [Online]. Available: https://www.boe.es/buscar/pdf/1997/BOE-A-1997-20262-consolidado.pdf.

[9] "Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad," 1986. [Online]. Available: https://www.boe.es/buscar/pdf/1986/BOE-A-1986-6859-consolidado.pdf.

[10] "Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior," 2018. [Online]. Available: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-10755-consolidado.pdf.

[11] "Boletín Oficial del Estado, Viernes 21 de mayo de 2010," 2010. [Online]. Available: https://www.boe.es/boe/dias/2010/05/21/pdfs/BOE-A-2010-8115.pdf.

[12] "D1.3 Report on Technology Taxonomy and Mapping," 2012. [Online]. Available: http://pact.vitamib.com/deliverables/wp1-root-branch-review/d1.3/D1.3.pdf/view.

[13] “EDA Technology Taxonomy,” 2006. [Online]. Available: https://www.eda.europa.eu/docs/default-source/procurement/eda-technology-taxonomy.pdf.

[14] “Staccato Final Report Executive Summary,” 2008. [Online]. Available: http://www.iai.it/sites/default/files/staccato_final-report-executive-summary.pdf.

[15] “Estrategia de Seguridad Nacional, Departamento de Seguridad Nacional,” 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf.

[16] “Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional,” 2017. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN%202017.pdf.

[17] “Informe Anual de Seguridad Nacional, Departamento de Seguridad Nacional,” 2018. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/IASN2018.pdf.

[18] “Estrategia Anual de Ciberseguridad,” 2019. [Online]. Available: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20Nacional%20de%20Ciberseguridad%202019.pdf.

[19] “Constitución Española,” 1978. [Online]. Available: https://boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf.

[20] C. Europea, “Horizon 2020,” 2014. [Online]. Available: https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/H2020_ES_KI0213413ESN.pdf.

[21] “Fondos Estructurales y de Inversión Europeos,” [Online]. Available: https://ec.europa.eu/info/funding-tenders/funding-opportunities/funding-programmes/overview-funding-programmes/european-structural-and-investment-funds_es.

[22] “Fondo Europeo para Inversiones Estratégicas (FEIE),” [Online]. Available: https://ec.europa.eu/commission/priorities/jobs-growth-and-investment/investment-plan-europe-juncker-plan/european-fund-strategic-investments-efsi_es.

[23] “TEDAE,” 2018. [Online]. Available: https://www.tedae.org/es/publicaciones/etiqueta/memorias-de-actividad.

[24] “European Investment Bank,” 2019. [Online]. Available: https://www.eib.org/en/index.htm.

12. ANEXOS

ANEXO 1. EJEMPLO MATRIZ TAXONOMÍA. Fuente: Comisión de Seguridad, TEDAE[23]

TAXONOMÍA SECTOR INDUSTRIAL DE LA SEGURIDAD

MATRIZ LINEAS DE ACCIÓN O AMENAZAS / FASES / GRUPOS TECNOLÓGICOS

ENGLISH

Version 25.02.19

	Lucha contra el terrorismo						Protección contra I. Críticas						Seguridad frente a pandemias y epidemias						Lucha		
Cluster tecnológico	Communications	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Communications	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Communications	Detection	Doctrine & operations	Incident response	Information Management	Situation Awareness	Communication	Detection	Information Management
AI and decision support																					
Data and information management																		X		X	
Data classification					X													X		X	
Data collection					X													X		X	
Data fusion					X	X						X									
Data mining			X			X	X													X	X
Data/Information fusion technology			X																		X
Evacuation and consequence management techniques															X						
IKBS(Intelligence Knowledge-Based Systems)/AI/Expert techniques						X															
Impact Analysis concepts and impact reduction					X																
Individual and team training															X						
Information fusion																		X			X
Knowledge management			X																	X	X
Mission simulation															X					X	
Models to support preparedness exercices and actual crisis response																		X			
Natural language processing technology			X																		X
Operational Analysis tools and techniques															X					X	
Optimisation, Planning & Decision Support													X								
Optimization, Planning and Decision Support Systems					X	X												X			
Pattern recognition							X	X													X
Simulation for decision making											X										
Synthetic environment																					
Synthetic force generation																					
Tactical/Crew training systems															X						
Task analysis modelling and scenario analysis															X						
Text mining			X			X	X														X
Training techniques																					X
Web and languages technologies													X								
Biometrics																					
Digital fingerprints recognition																				X	
Biotechnology																					
Foord testing and control techniques											X					X					
Rapid analysis of biological agents																X				X	
Water testing and purification techniques																X					
CBRNe																					
Biological technologies for biological and medical countermeasures																X					
CBRN sensors				X				X						X							
Chemical and biological detection																					
Chemical and biological detection tecniques														X							

Chemical and Biological Detection/identification		X																			
Decontamination techniques																X					
EM difficult scenarios																					
EMC evacuation and hardening											X									X	
Explosive detection sensors		X						X						X						X	
Protection against hash environment							X													X	
Comms																					
Broadband access to mobile users in dynamic situations																					
Communications and Information Systems security equipment	X						X						X								
Communications network management and control equipment, network supervis													X								
Information security							X														
Mobile secured communications	X						X												X		
Network management and control							X														
Protocol technology											X										
Reconfigurable communications	X						X									X			X		
Secured wireless broadband data linkls for secured communications																			X		
Electronic authentication																					
Electroning tagging systems				X						X										X	
Smard cards				X																X	
Energy generation, storage and distribution																					
Alternative power sources and devices											X										
Electric batteries																X					
Energy distribution																X					
Power generators																X					
Forensic																					
Biometrics							X	X												X	
Facial/Fingerprint/Iris/Retina/Voice signature recognition		X																		X	
GIS																					
Advance image and geo-spatial analysis techniques																		X		X	
Earth observation																					
Human Science																					
Advanced Human behaviour modelling and simulation			X												X					X	X
Human Behaviour Analysis and Modelling					X															X	
Human Factor in decision process													X								
Human survavility, protection and stress effects																X					
Population behaviour																		X		X	X
Prediction of mass behaviour																		X			X
Skills training															X						
Integrated platforms																					
Aircraft																				X	
Helicopters																				X	
Lighter than air platforms																				X	
On board Electric batteries																					
Surveillance and navigation satellites																				X	
Unmanned land/sea/air vehicles								X				X				X		X		X	
IT																					
Device integration/reliability										X											
High integrity and safety critical computing			X						X								X				X
High performance computing			X						X								X				X
Image processors / autonomous vehicles																					
Infraestructure to support information management and dissemination			X																		X
Infrastructure to support Information Management & Dissemination													X		X						X
Protocol technologies			X						X								X				X
S/W architectures			X						X								X				X

Secure computing techniques			X						X													X
SW engineering			X						X								X					X
IT security																						
Access Control			X						X								X					X
Authentication																						
Crypto	X		X				X		X				X				X					X
Cybersecuritypolicy management tools		X																				
Encryption and key management	X		X				X		X				X				X					X
Filtering technologies			X						X								X					X
Materials																						
Anti blast glasses/concrete					X																	
Light materials for human protection																X						
Materials for site protection											X											
Self protective and explosive resistant material					X																	
Smart textiles																X						
Structural and smart materials											X											
Navigation & Guidance																						
Direction finding and map guidance										X												
Navigation technologies														X								
Radio navigation										X												
RFID based tracking				X																		
Sensors																						
Acoustic sensors																					X	
Autonomous small sensors/smart dust technologies						X															X	
Cameras				X																	X	
Early detection techniques											X										X	
Hyper-spectral / Multi-spectral								X													X	
Hyper-spectral/multi-spectral processing																					X	
Hyper-spectral/multi-spectral sensors																					X	
IR sensors																					X	
Micro and mm-wave sensors		X																			X	
Motion sensor systems																					X	
Motion sensors								X													X	
Nanotechnologies for sensors				X																	X	
Non cooperative target recognition																					X	
Radar sensors				X				X													X	
SAR/ISAR equipment																					X	
Sensors												X		X							X	
Smart clothes and equipment																X					X	
Smart video surveillance								X				X									X	
Teraherts sensors				X																	X	
Visible and IR cameras								X													X	
Signal processing																						
Digital processing																						
Filtering technologies			X				X															X
Image/pattern processing		X				X												X				X

contra el crimen organizado						Contrainteligencia									Ciberseguridad									Seguridad Marítima										
Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection
		X					X								X														X					X
	X	X					X			X					X													X						X
	X	X					X			X					X													X						X
	X	X								X					X											X		X						X
		X					X	X							X		X		X				X			X							X	X
								X								X	X			X			X											
				X									X																		X			
		X									X																							
															X				X	X														
			X	X								X	X				X				X										X			
								X							X											X								X
							X	X									X			X	X	X												
			X	X			X					X	X															X		X	X			
																				X			X					X						X
								X				X			X		X																	
				X			X					X	X									X			X						X			X
												X										X	X		X									
	X	X								X	X	X										X	X		X			X						
		X						X			X	X			X		X																X	X
																						X												
			X									X																		X				
			X									X																		X				
			X	X								X	X																		X			
		X		X							X		X			X	X	X													X			
		X						X			X							X								X							X	
			X					X				X									X									X				
															X																			
							X								X		X								X									
							X					X																						
												X																						
					X									X									X									X		
																																		X
								X																	X									
							X	X																										

							X																											
																								X										
							X																		X									X
							X																										X	
															X		X	X						X										
															X		X		X	X				X									X	
															X		X		X	X				X										
															X		X				X												X	
							X									X					X	X												X	
																			X		X		X										X	
	X									X							X		X		X		X					X						
	X				X	X				X				X	X		X		X	X								X				X	X	
						X									X		X	X		X				X										
X							X		X																									
X							X		X							X		X		X														
					X									X																		X		
					X									X																		X		
					X									X																		X		
							X								X	X	X								X								X	X
							X								X	X	X																	
		X					X				X																							
																									X									
				X			X	X					X			X	X		X												X			
							X									X			X															
																X	X	X	X				X											
					X									X					X				X									X		
		X					X	X			X							X	X	X														
		X						X			X					X			X	X														
			X	X								X	X				X			X	X										X			
			X				X					X																	X					
			X				X					X													X				X					
							X																						X					
																													X					
							X																						X					
		X	X		X		X				X	X		X											X				X			X		X
															X		X	X		X			X											
								X							X		X	X					X			X								
								X							X		X	X		X			X			X								
															X			X		X						X								
								X							X		X	X																
				X				X					X		X		X	X													X			
								X							X		X	X		X			X			X								
								X							X		X	X								X								

								X							X		X	X					X				X								
								X							X		X	X									X								
			X					X				X			X			X				X				X								
															X		X	X				X		X											
								X							X	X	X	X	X	X		X	X	X		X							X	
			X									X			X	X	X	X	X	X		X	X											
								X							X		X	X	X	X		X	X	X		X							X	
			X					X				X			X	X	X	X	X	X		X	X			X								
	X									X																	X							
	X				X					X				X													X				X			
	X									X																	X							
	X				X					X				X													X				X			
	X									X																	X							
X									X							X		X		X														
																X																			
X			X						X			X																						
X									X							X																		
		X					X				X																	X							
		X					X				X																	X							
X		X					X		X		X																	X							
	X	X					X			X	X																	X							
		X					X				X																								
		X					X				X																	X							
		X	X									X	X			X		X														X			
									X							X																		X		
		X	X						X			X	X			X	X																		

Seguridad Económica							Ordenacioón de flujos migratorios								No proliferación de armas de destrucción masiva									Preservacion del medioambiente								
Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response	Communication	Detection	Information Management	Positioning	Risk Assessment	Situation Awareness	Training	Doctrine & Operations	Incident Response
								X				X									X									X			
								X													X											
								X													X											
			X						X					X													X			X			
									X																		X						
														X																			X	
		X																					X									X	
	X																															
	X																						X									X	
									X												X						X						
													X		X								X									X	X	
															X						X											X	X	
												X																					
									X			X				X																	
									X												X												
									X					X																			
		X																															
													X		X																		
													X		X																		
														X									X									X	
														X									X									X	
									X																								
													X		X																	X	
																X																	
		X																						X									
																								X									
																								X									
																								X		X							X
																	X									X							
								X									X									X							
																	X									X							

																										X							
																								X		X							
							X																			X	X							
		X																								X							
								X										X									X							
																										X							
							X																		X									
							X									X								X									
							X									X								X									
		X																											X				
																								X					X				X
							X																		X									
	X																																
		X																															
																								X									X
																								X									X
																								X									X
								X																		X							
																					X												
								X																		X							
																							X										X	
																	X																	
																								X									X
																					X												
																					X												
																							X										X	
												X																		X			
								X																		X			X			
												X																		X			
												X																		X			
												X																		X			
			X					X			X									X			X		X			X			X
	X																																
X										X									X									X						
X										X									X									X						
										X																			X						
																	X							X										X	
X										X									X									X						
X										X									X									X						

X									X																		X						
X									X									X									X						
X									X									X									X						
							X																		X								
X							X		X							X		X							X		X						
X							X		X							X		X							X		X						
X									X									X									X						
																													X				
																								X					X				X
		X																															
																													X				
																								X					X				X
		X																											X				
	X																																
																	X																
	X																																
												X																		X			
								X																		X							
								X																		X							
		X																											X				
								X																		X							
								X																		X							
								X																		X							
								X																		X							
								X																		X							
								X																		X							
								X																		X							
			X														X																
																								X									X
			X																														
												X																		X			
												X									X									X			

ANEXO 2. CIFRAS POLO SEGURIDAD. Fuente: Comisión de Seguridad, TEDAE[23]

TEDAE | 10 años
Defensa, Seguridad, Aeronáutica y Espacio

GRANDES CIFRAS SEGURIDAD

INNOVACIÓN
11%
SOBRE FACTURACIÓN

FACTURACIÓN
155
MILLONES de EUROS
de volumen de actividad

PRODUCTIVIDAD
VECES LA MEDIA NACIONAL
2,6

EXPORTACIÓN
22%
SOBRE FACTURACIÓN

EMPLEADOS
974

¿QUÉ PASÓ EN INTERNET EN CADA MINUTO DE 2018?

FUENTE: TEDAE, ASD-EUROSPACE, MINCOTUR, INE (JUNIO 2019) - ANÁLISIS TEDAE

FUENTE: @LORILEWIS / @OFFICIALLYCHADD