Universitat Autònoma de Barcelona

TESIS DOCTORAL

Terrorismo y Protección de Infraestructuras Críticas: el índice de Seguridad Hospitalaria como Instrumento de Evaluación y Diagnóstico de la Seguridad la Protección Integral y la Resiliencia de los Hospitales Europeos.

Martín González y Santiago

Universitat Autònoma de Barcelona

Facultad de Derecho Público y Ciencias Histórico Jurídicas

Programa de Doctorado en Seguridad Humana y Derecho Público Global

TESIS DOCTORAL

Terrorismo y Protección de Infraestructuras Críticas:
El Índice de Seguridad Hospitalaria como Instrumento de Evaluación y Diagnóstico de la Seguridad, la Protección Integral y la Resiliencia de los Hospitales Europeos

Investigación presentada para la obtención del Grado de Doctor por la Universidad Autónoma de Barcelona en Seguridad Humana y Derecho Público Global.

Tesis Doctoral realizada por el doctorando
Martín González y Santiago

Dirigida por
Dra. Roser Martínez Quirante
Dr. José Julián Istúritz Pérez

Las Palmas de Gran Canaria a 15 de febrero de 2024.

Son muchas las lágrimas que nunca has visto por tus duras y gélidas ausencias
y muchas las sonrisas por cada una de tus presencias.
A mi hijo Martín, mi «Pequeño *Samurai*»,
con él, la palabra querer cobra todo su significado
hasta cotas inimaginables…

A mi Madre, por darlo siempre todo, por ser y estar.

A *Cathy*, *Bushi* y a *Ares in memoriam.*

AGRADECIMIENTOS

A mis directores de Tesis, a la Profesora Dra. Roser Martínez por su humanidad y ánimos para la culminación de la presente Tesis Doctoral, así como al Profesor Dr. José Julián Istúritz por su amistad, empuje y mecenazgo siempre. A ambos por ser parte activa de la presente investigación, así como por su permanente apoyo.

A Marta Delgado Galera, por su calidad humana, su apoyo callado y su inestimable ayuda en la logística administrativa universitaria que ha ido mucho más allá de sus propias responsabilidades profesionales. Sin ella «llegar a puerto» hubiese sido muchísimo más difícil.

Al Observatorio de Seguridad Integral de Centros Hospitalarios por su apoyo en el desarrollo de la presente investigación, por su inestimable colaboración en la cumplimentación de los Formularios del índice de Seguridad Hospitalaria de los distintos hospitales, a todos mis compañeros, verdaderos expertos en Seguridad Hospitalaria por dedicarme su tiempo, las llamadas, las explicaciones y atender mis demandas y requerimientos investigadores.

Al Prof. Dr. José Manuel Izquierdo Ramírez, al amigo que siempre está, por su permanente amistad a lo largo del tiempo, así como por acompañarme en el camino de la ciencia y de la investigación durante la realización y la defensa de mi primera Tesis Doctoral, sencillamente gracias.

A mi gran a mi leal amigo Daniel Miranda, por su permanente apoyo en cualquier empresa que emprenda, por su amistad incuestionable.

A mis alumnos, porque sin ellos éste Maestro de Artes Marciales, Instructor Policial y Académico no podría ser docente en ninguna de las distintas ramas que me apasionan, porque sin duda, para poder transmitir y enseñar ellos consiguen que nunca deje de ser el eterno aprendiz que todo lo cuestiona, ayudándome en mi superación permanente.

A *Yuki*, por su callada e intensa presencia y acompañamiento en la soledad del investigador durante la realización de la presente Tesis.

A mis amigos por su apoyo constante y, a los «no tan amigos» por forjar mi paciencia y mi carácter, por contribuir a hacerme cada día más fuerte y a enseñarme a superar las adversidades.

A todos un fuerte y leal abrazo en los férreos lazos de la Seguridad, de la amistad y de la vida, porque no hay nada como soñar para crecer, rememorando y en palabras de Facundo Cabral, "(…) ayer soñé que podía y hoy puedo» y porque nunca debemos de olvidar que, todo aquel que vive sin un sueño morirá sin ilusiones.

RESUMEN

Garantizar la seguridad de las Infraestructuras Críticas contra todo tipo de riesgos, incluido el terrorismo, es de vital importancia porque son esenciales para el funcionamiento y bienestar de la sociedad. La seguridad de estas instalaciones asegura la protección de vidas humanas en caso de ataques terroristas o cualquier otro tipo de amenaza. El daño o la interrupción de Infraestructuras Críticas pueden tener impactos económicos devastadores a nivel local, nacional e incluso global. La interrupción de servicios esenciales puede provocar pérdidas económicas significativas, interrumpir cadenas de suministro y afectar la capacidad de producción de bienes y servicios, además de que son vitales para garantizar la Seguridad Nacional. Todo ello, porque la interrupción de servicios esenciales puede causar caos y desorden social. Garantizar la seguridad de las Infraestructuras Críticas ayuda a mantener el orden y la cohesión social al garantizar la continuidad de servicios esenciales que son fundamentales para la vida diaria de las personas.

La implementación del Índice de Seguridad Hospitalaria de la Organización Mundial de la Salud (OMS) podría ser una valiosa herramienta que puede desempeñar un papel importante en la protección de las Infraestructuras Críticas frente a la amenaza terrorista debido a que proporciona un marco estructurado para evaluar la seguridad de los hospitales en diferentes áreas, como la infraestructura física, la capacidad de respuesta a emergencias, la gestión de riesgos y la protección del personal. Esta evaluación puede identificar vulnerabilidades específicas que podrían ser explotadas por actores terroristas para atacar las Infraestructuras Críticas de salud. De la misma manera porque se podrían implementar medidas de seguridad basándose en los resultados de la evaluación, los hospitales pueden implementar medidas específicas para mejorar su seguridad contra amenazas terroristas. Estas acciones fomentan la resiliencia de los hospitales frente a ataques terroristas al identificar áreas donde se pueden mejorar las capacidades de respuesta y recuperación. Esto podría incluir la planificación de contingencias para mantener la continuidad de los servicios de salud en caso de interrupciones causadas por actos terroristas.

Este estudio podría facilitar la coordinación entre los sectores de salud y seguridad en la protección de Infraestructuras Críticas. Al proporcionar un marco común de evaluación y planificación, puede promover la colaboración entre las autoridades de salud, agencias de seguridad y otros actores relevantes en la prevención y respuesta a amenazas terroristas.

ABSTRACT

Ensuring the security of critical infrastructure against all types of risks, including terrorism, is vital because they are essential for the functioning and well-being of society. The security of these facilities ensures the protection of human lives in the event of terrorist attacks or any other type of threat. Damage or disruption to critical infrastructure can have devastating economic impacts locally, nationally, and even globally. The interruption of essential services can lead to significant economic losses, disrupt supply chains, and affect the production capacity of goods and services, as well as being vital for ensuring National Security. All of this, because the interruption of essential services can cause chaos and social disorder. Ensuring the security of critical infrastructure helps maintain order and social cohesion by ensuring the continuity of essential services that are fundamental to people's daily lives.

The implementation of the World Health Organization's (WHO) Hospital Safety Index could be a valuable tool that can play a significant role in protecting critical infrastructure against the terrorist threat because it provides a structured framework for assessing the safety of hospitals in different areas, such as physical infrastructure, emergency response capability, risk management, and staff protection. This assessment can identify specific vulnerabilities that could be exploited by terrorist actors to attack critical health infrastructure. Similarly, because security measures could be implemented based on the assessment results, hospitals can implement specific measures to improve their security against terrorist threats. These actions promote the resilience of hospitals against terrorist attacks by identifying areas where response and recovery capabilities can be enhanced. This could include contingency planning to maintain the continuity of health services in the event of disruptions caused by terrorist acts.

This study could facilitate coordination between the health and security sectors in protecting critical infrastructure. By providing a common framework for assessment and planning, it can promote collaboration among health authorities, security agencies, and other relevant actors in the prevention and response to terrorist threats.

INTRODUCCIÓN

Son muchísimos los riesgos a los que cualquier tipo de organización está expuesta. La naturaleza del riesgo hace que exista una gran taxonomía clasificatoria al respecto. Riesgos a los que hay que sumar los riesgos actuales conocidos como «Riesgos Emergentes[1]».

El Terrorismo en general y el Terrorismo de Corte *Yihadista*, en particular, suponen la actualidad una grave amenaza para cualquier institución, y especialmente para las distintas Infraestructuras Críticas independientemente del sector en el que éstas quedan encuadradas.

Los hospitales son Infraestructuras Críticas, en puridad, tanto de *iure* como de *facto*, que nadie puede cuestionar, máxime, cuando hace escaso tiempo hemos padecido una pandemia producida por el Virus *Sars-Cov-2* que, expuso a la ciudadanía de muchísimos países, así como clarificó la importancia de centros hospitalarios como Infraestructuras Críticas y Centros Complejos por la especial importancia de sus normales funcionamientos y la criticidad que supondría su quebrantamiento para la salud y las vidas de cuántas personas puedan estar afectadas por cualquier tipo de patología, romper el estado de bienestar de la sociedad y no dar respuesta a cualquier tipo de contingencia en situación normal o sobrevenida por cualquier tipo de catástrofe o calamidad pública.

El fenómeno Terrorista conoce perfectamente que son objetivos estratégicos que pueden provocar la desestabilización total de una sociedad, así como servir de elemento vehicular para el favorecimiento de la publicidad que con tales actos de propaganda se busca para defender su causa. El terrorismo no entiende de acuerdos internacionales ni de aquellos que se alcanzaron en la Convención de Ginebra.

Poder garantizar una adecuada seguridad y protección integral a los centros hospitalarios es una tarea ardua como compleja por múltiples factores.

Los Hospitales son, *per se*, centros de muy alta complejidad, en los que, tradicional e históricamente existe una política de gestión denominada de «puertas abiertas»; lo que supone, una política laxa en relación con el acceso de cuántas personas y acompañantes

[1] Los riesgos emergentes pueden variar dependiendo del contexto y las circunstancias en las que se consideren. Sin embargo, algunos riesgos emergentes que se han identificado a nivel global en los últimos años incluyen, *grosso modo*, Pandemias y enfermedades infecciosas emergentes, Cambio climático, Ciberseguridad, Inestabilidad política y conflictos, Inteligencia artificial y automatización, inmigración ilegal, así como la Desigualdad Socioeconómica.

quieran acceder, un servicio el que se presta durante todos los días durante todo el año, lo que aumenta la criticidad en relación a la materialización de cualquier tipo de riesgo o amenaza.

Es importante destacar que el Sector Salud y por ende los hospitales integra uno de los 12 sectores de actividad que recoge la legislación específica en materia de Protección de Infraestructuras Críticas por ser un servicio a la vez sensible y estratégico que se presta a las distintas sociedades.

Además, que no exista una línea directriz común en atención a su gestión y administración supone un quebranto para dar una respuesta integral a su seguridad y protección integral, esta vulnerabilidad viene dada por las competencias que las distintas Comunidades y Ciudades Autónomas tienen delegadas y hay modelos de gestión que aumentan su seguridad y otros que la disminuyen.

Se hace necesario, en cualquier caso, de una adecuada Gerencia de Riesgos, para implementar cuántas medidas hagan falta para garantizar la Seguridad, la Protección Integral y la Resiliencia sea siempre impulsada y llevada a cabo por Directores de Seguridad debidamente habilitados por el Ministerio del Interior, con la formación académica adecuada, en una sociedad del cambio en el que la transformación digital es ya una realidad, y que supone en palabras de Istúriz, J.J. et al., (2022):

> (…) un concepto que engloba mucho más que la incorporación de nuevos equipos informáticos (tanto ordenadores, como aplicaciones informáticas), con una nueva concepción inteligente de la seguridad en términos de mejora eficiente de recursos, de procesos, de trabajo colaborativo en red y de capacitación profesional, en definitiva, una forma diferente de trabajar. (p. 109).

Además, de la tan necesaria experiencia previa necesaria para estar al frente de los distintos Departamentos de Seguridad de los Distintos Hospitales, para garantizar de esa manera la adecuada solvencia para la gestión y dirección de estos centros tan especiales por sus características y a la par Infraestructuras Críticas en las que convergen en un área o un perímetro bastante pequeño, una gran cantidad de riesgos de tipología, además muy heterogénea. En cualquier caso, es incuestionable ahondar en el binomio Director de Seguridad y Departamento de Seguridad, como principal medida de carácter organizativa para armonizar cuántos planes, procedimientos, instrucciones técnicas operativas, órdenes de puesto, sistema de gestión integrada y resto de subsistemas sean de aplicación para elevar el nivel de seguridad de los distintos centros hospitalarios.

Adoptar todo tipo de medidas se hace crucial y necesario para garantizar una adecuada protección en atención a las características propias de cada uno de ellos y su propia idiosincrasia.

En el entorno de la Unión Europea si existió el llamado proyecto *Protection of Health Infrastructure Resilience Management and Adaptation (PHIRMA)*[2], cuya traducción sería Protección de la Gestión y Adaptación de la Resiliencia de la Infraestructuras de Salud.

PHIRMA, proyecto en el cual pudimos investigar aspectos clave en la seguridad hospitalaria, su protección integral y la resiliencia de los servicios que tales Infraestructuras Críticas, de manera esencial, presta a la sociedad.

Por otro lado, la Organización Mundial de la Salud (OMS), a través de la Organización Panamericana de la Salud (OPS), conscientes de la necesidad de que existan, se diseñen y se construyan Hospitales Seguros, precisamente por el servicio tan esencial que presta a las distintas sociedades en las que se encuadren, ha elaborado desde hace ya unos años un cuestionario o formulario denominado Índice de Seguridad Hospitalaria, qué únicamente se ha llevado a cabo en algunos hospitales de algunos países de Sudamérica, nunca en hospitales dentro del contexto de algún país que integre la Unión Europea, con el objeto de saber si es extrapolable a nuestro entorno geográfico, dentro del marco legal y normativo de la UE.

Comprobar la posible extrapolación del formulario validado y contrastado por la OMS en relación al estudio del Índice de Seguridad Hospitalaria para promover Hospitales Seguros en el entorno de algún país de la Unión Europea se hacía necesario por si tuviese encaje en el marco de nuestro contexto geográfico, legal y normativo, o si por cambio habría que modificarlo y realizar propuestas de adaptación.

El Índice de Seguridad Hospitalaria, desarrollado por la Organización Mundial de la Salud (OMS), es una herramienta crucial para evaluar y mejorar la seguridad en los hospitales durante emergencias y desastres, cuyo objetivo es el de evaluar daños previsibles y reducir a un mínimo aceptable los posibles riesgos, así como mejorar su funcionamiento de los hospitales en cualquier situación sobrevenida de Emergencia, con un enfoque integral.

[2] En un apartado específico se describirá adecuadamente las actuaciones los estudios, investigaciones, así como actuaciones que se llevaron a cabo como «*PHIRMA Advisory Board Member*», es decir, miembro del Consejo Asesor. Proporcionando asesoramiento, conocimientos y experiencia en el área de Protección de Infraestructuras Críticas específicas hospitalarias con el objeto de ayudar a la toma de decisiones estratégicas.

La presente investigación correspondiente a la presente Tesis Doctoral en Curso considera el factor del Terrorismo, en especial el *Yihadismo*, como uno de los principales riesgos a los que las Infraestructuras Críticas Hospitalarias se enfrentan, independientemente de los riesgos que les son intrínsecos *per se*, y que podrían ser evaluados a través del Formulario reseñado con anterioridad en relación al Índice de Seguridad Hospitalaria, además de considerar cuántas disposiciones se establecen en materia de Protección de Infraestructuras Críticas, Protección Civil, a través del Esquema Nacional de Seguridad (ENS), Seguridad Nacional, etc.

En definitiva, todo un maremágnum legislativo, que les son de aplicación, en la que toda la normativa ha de converger y vertebrarse de manera adecuada, o por el contrario habría que adaptarlo para aumentar y mejorar el índice de protección que los Hospitales como servicios esenciales y estratégicos a la sociedad deben de tener.

No es objeto de la presente investigación hacer un análisis exhaustivo del Terrorismo, así como tampoco de las Infraestructuras Críticas, que podrían, sin ningún género de dudas, ser objeto *per se* de investigaciones específicas, como así se ha demostrado en la literatura científica, pero si, apuntar cuántas cuestiones son relevantes en las distintas materias, con el ánimo de contextualizar, de manera transversal la presente Tesis Doctoral con su finalidad específica para otorgarle una visión de conjunto en relación al objetivo general que nos planteamos que, aunque se exponen en el Marco Empírico en su apartado específico y que ahora anticipamos, no es otro, sino el de estudiar, a través de la presente investigación la pertinencia del Formulario Índice de Seguridad Hospitalaria en el contexto de los hospitales en España, y por extensión en el marco de la Unión Europea, todo ello en atención a la idiosincrasia de los riesgos específicos de nuestro entorno, así como a la legislación.

CAPÍTULO I

TERRORISMO

«Cuando ellos piensen que estás lejos has de estar cerca
Cuando ellos piensen que estás cerca, estate lejos»
Sun Tzú.

1. CAPÍTULO I. TERRORISMO.

El terrorismo es un acto de violencia perpetrado por grupos o individuos con el objetivo de alcanzar objetivos políticos, ideológicos o sociales mediante el uso del miedo, la intimidación y la violencia indiscriminada contra la población. Los actos terroristas pueden incluir ataques a personas, propiedades o instituciones del estado en cualquiera de sus administraciones.

Las motivaciones detrás del terrorismo pueden variar ampliamente, desde la búsqueda de independencia o autonomía política hasta la promoción de ideologías extremistas, religiosas o seculares. Los grupos terroristas a menudo justifican sus actos como una forma de resistencia contra la opresión, la injusticia o como una manera de llamar la atención sobre sus causas.

El terrorismo representa una amenaza significativa para la seguridad global, provocando no solo pérdidas humanas y materiales, sino también generando inestabilidad política, económica y social. Combatir el terrorismo requiere un enfoque multifacético que incluye medidas de seguridad, cooperación internacional, abordaje de las raíces socioeconómicas y políticas del extremismo, y esfuerzos para promover la paz y la reconciliación entre comunidades en conflicto.

1.1 INTRODUCCIÓN AL CAPÍTULO.

El presente capítulo se hace necesario debido a que es uno de los términos de importancia de la presente investigación. Es el primer concepto que recoge el propio título de la Tesis Doctoral que se desarrolla. Su importancia estriba en que la propia Ley de Protección de Infraestructuras Críticas (LPIC) y su normativa dimanante, se realiza precisamente para proteger tales infraestructuras del fenómeno terrorista y poder aumentar su nivel de protección en aras de la criticidad y esencialidad que, las Infraestructuras Críticas (IC) suponen para la sociedad. El fenómeno del terrorismo es una preocupación global que ha afectado a numerosos países en todo el mundo, incluida España.

Es importante realizar una aproximación terminológica en general al concepto de Seguridad y al de Seguridad Humana en particular. Todo ello porque el Terrorismo o cualquier tipo de riesgo Antrópico de Carácter Antisocial, supone una merma del concepto a las personas.

El terrorismo se caracteriza por la realización de acciones violentas, así como el uso del miedo y la intimidación como instrumento para alcanzar objetivos políticos, religiosos o

ideológicos. Sus consecuencias son muy graves y devastadoras, todo ello debido a que amenaza la seguridad, la estabilidad y los valores fundamentales de los distintos países.

Se hace complejo poder buscar una única y válida acepción al concepto de terrorismo en relación a sus distintas acciones, en cualquier caso cabe apuntar que, «una acción terrorista es una de las amenazas más graves para la paz y la seguridad internacionales, con independencia de quien lo cometa y de dónde y con qué propósitos». (ONU, 2006).

En el mismo sentido y debido a la falta de precisión conceptual, así como la gran cantidad de definiciones que existen en la actualidad, sería altamente deseable siempre en palabras de Laqueur, (1988) afirmaba que:

> (…) todas las discusiones sobre el terrorismo, sus motivos e inspiración, su carácter específico, sus modos de funcionamiento o sus consecuencias a largo plazo estuvieran basadas en una definición clara, precisa y comprensiva. (p. 88).

En el contexto internacional los Atentados del 11 de Septiembre (11-S), de 2001, en la ciudad de Nueva York, en el que fallecieron aproximadamente unas 2.977 personas, así como resultaron heridas casi unas 3.000. Entre las distintas víctimas se incluyen a ciudadanos de casi un centenar de países, con más exactitud, noventa países distintos, lo que supuso un antes y un después en relación a la nueva realineación y concepción de la seguridad global frente al terrorismo en relación a la nueva política mundial llevada a cabo al efecto. En el sentido expuesto, el atentado referenciado en relación a su percepción por la comunidad internacional fue descrito por Barber, E., (2014) con gran acierto como:

> Los ataques del 11 de septiembre contra Nueva York y Washington constituyeron un desafío de primer orden para la lógica del sistema en su conjunto (Estados Unidos y sus aliados), ordenado en base a esa sobrecapacidad tecnológico-militar, ya que dichos atentados se asientan en la asimetría del poder y fueron muy eficaces al demostrar la vulnerabilidad de la potencia hegemónica… Se ha pasado de hablar de la «guerra a distancia», que sólo los Estados Unidos podían ganar (por sus capacidades) a la «guerra asimétrica», en la que la supremacía militar convencional de Estados Unidos se ha visto subvertida por «radicales armados con nuevas tecnologías de muerte (…). (p. 331).

A partir del referenciado atentado es cuando se produce a nivel mundial, auspiciado por los Estados Unidos de América una realineación de las seguridades, realineación que no escapa al

entorno de la Unión Europea, al establecer la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de Infraestructuras Críticas europeas y la evaluación de la necesidad de mejorar su protección. Directiva que ha sido recientemente derogada por la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, que junto con la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas para un alto nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) N.º 910/2014 y la Directiva (UE) 2018/1972, y se deroga la Directiva (UE) 2016/1148 (Directiva NEI), refuerzan la importancia de la protección de tales infraestructuras, así como la pertinencia de la presente investigación.

Lo expuesto señala que el Terrorismo, y en especial el Terrorismo de Corte *Yihadista*, como fenómeno es de carácter transnacional y por ende global, traspasando todas las fronteras afectando a todos los estados. Por tanto, no ha de obviarse, según Remiro, A. (2009) que:

> Hasta los crímenes del 11-S, los terroristas se presentaban como el ariete más violento de grupos separatistas o «antisistema» dentro del Estado, eran la expresión desesperada y radical de movimientos de liberación de la ocupación extranjera, o respondían a políticas de Estado para afrontar la solución de sus problemas o realizar sus objetivos, domésticos o internacionales. Los crímenes del 11-S han añadido la evidencia de una red de organizaciones y células terroristas transnacionales que se sirven -pero son independientes- de los Estados y tratan de poner en jaque el orden internacional establecido mediante actos espectaculares de una violencia extrema y repercusión mediática global. (p. 18).

Nuestro país, España ha experimentado su propia lucha contra el terrorismo a lo largo de su historia reciente. Durante décadas, nuestro país se enfrentó a la actividad de grupos terroristas como *Euskadi Ta Askatasuna* (ETA), cuyo significado viene a ser País Vasco y Libertad, grupo o movimiento que reivindicaba la libertad de la Comunidad Autónoma Vasca y Navarra, que durante más de cinco décadas de su constitución y existencia ha llevado a cabo casi 1000 asesinatos, así como incontables heridos como víctimas directas de sus acciones terroristas.

Sin embargo, desde el cese definitivo de la actividad armada de ETA en 2011, la amenaza terrorista en España ha evolucionado hacia un enfoque más vinculado al *yihadismo*[3].

España, al igual que otros países europeos, ha sido objetivo de ataques *yihadistas* en los últimos años.

El atentado más grave sucedió el 11 de marzo (11-M), de 2004 en Madrid, cuando una serie de 10 explosiones sacudieron a cuatro trenes en plena hora punta de la mañana. Los trenes afectados se dirigían hacia la estación de Atocha y otras estaciones céntricas de Madrid. El atentado causó la muerte de 191 personas e hirió a más de 2.000 del que ha sido el más, execrable, grave y mortal por el número de víctimas de la historia de nuestro país.

La acción fue llevada a cabo por un grupo de extremistas de la *Yihad* con conexiones con la red terrorista de *Al Qaeda*, que, sin duda alguna, fue una respuesta a la participación de España en la Guerra de Irak en la que participó con la coalición liderada por Estados Unidos.

Además, el 17 de agosto de 2017 (17-B), se produjo un ataque terrorista en Barcelona, España, en el que un vehículo embistió a una multitud de personas en Las Ramblas, una popular zona turística de la ciudad, causando la muerte de 16 personas y dejando a muchas más heridas. Horas después, se produjo un segundo ataque en la localidad de Cambrils, donde un grupo de terroristas intentó perpetrar un ataque similar, pero fueron neutralizados por las Fuerzas y Cuerpos de Seguridad (FFCCS)[4].

Estos atentados fueron llevados a cabo por una célula *yihadista* que operaba en España y que tenía vínculos con el Estado Islámico (ISIS). Estos trágicos y luctuosos sucesos resaltaron una vez más la importancia de la lucha contra el *yihadismo* y la necesidad de fortalecer la seguridad y la prevención en el país.

Los atentados de Barcelona y Cambrils generaron un impacto significativo en la sociedad española y reforzaron la determinación del gobierno y las distintas Fuerzas y Cuerpos de Seguridad (FFCCS) para combatir el terrorismo. Se implementaron nuevas medidas de seguridad, se intensificaron los esfuerzos de inteligencia y se fortaleció la cooperación internacional en la lucha contra el extremismo de la *yihad*.

[3] El *yihadismo* se refiere a la ideología y las acciones de aquellos grupos extremistas que buscan imponer una interpretación radical del islam mediante el uso de la violencia.

[4] Las Fuerzas y Cuerpos de Seguridad, en España la integran la Policía Nacional, antes Cuerpo Nacional de Policía (CNP), Guardia Civil, Cuerpos de Policía Autonómicos, Policía Foral y las distintas Policías Locales, tiende a confundirse con Fuerzas y Cuerpos de Seguridad del Estado, éstas últimas integradas tan sólo y exclusivamente por Policía Nacional y Guardia Civil.

1.2 LA SEGURIDAD HUMANA.

La Seguridad es una necesidad básica y ancestral del ser humano, en el instinto primario figura como un componente fundamental tal como es el instinto de conservación[5] de las personas. Abraham Maslow[6]apuntaba su importancia al incluirla en la base de la pirámide por encima de las necesidades fisiológicas. Abraham Maslow fue un psicólogo humanista conocido por su teoría de la jerarquía de necesidades, que describió en su artículo de 1943 «Una teoría sobre la motivación humana». En esta teoría, Maslow propuso que las necesidades humanas se organizan jerárquicamente en cinco niveles, desde las necesidades más básicas hasta las más elevadas. Estos niveles son:

1. Necesidades fisiológicas: son las necesidades más básicas para la supervivencia, como el aire, el agua, la comida, el refugio y el sueño. Maslow sugiere que estas necesidades deben ser satisfechas antes de que una persona pueda avanzar hacia niveles más altos de la jerarquía.

2. Necesidades de seguridad: una vez satisfechas las necesidades fisiológicas, las personas buscan seguridad y estabilidad en sus vidas. Esto incluye la seguridad física, la salud, el empleo, los recursos financieros y la protección contra el peligro y la amenaza.

3. Necesidades de pertenencia y amor: una vez que se satisfacen las necesidades de seguridad, las personas buscan relaciones sociales, afecto y pertenencia a grupos

[5] El cerebro primario, también conocido como el cerebro «reptiliano», o complejo «reptiliano», es una parte del cerebro que se refiere a las estructuras más primitivas y básicas desde una perspectiva evolutiva, controla las funciones básicas necesarias para la supervivencia, como la respiración, la frecuencia cardíaca, la temperatura corporal y los reflejos básicos, tales como el Instinto de Supervivencia, como la búsqueda de alimento, el apareamiento, la defensa territorial y el comportamiento agresivo en situaciones de amenaza. Regula emociones básicas como el miedo, la ira, la ansiedad y el placer, que están relacionadas principalmente con la supervivencia y la reproducción. Es el responsable de la memoria implícita, que es la capacidad de recordar eventos y experiencias sin esfuerzo consciente, como los recuerdos asociados con el miedo o el placer. Controla la respuesta de «lucha o huida» frente a situaciones de peligro, activando la liberación de hormonas del estrés y preparando al cuerpo para reaccionar rápidamente ante una amenaza. Controla funciones motoras básicas, como la marcha y la coordinación motora, a través de estructuras como el tronco del encéfalo y la médula espinal.

[6]La pirámide de Maslow o Jerarquía de las Necesidades es una teoría psicológica propuesta por Abraham Maslow, formula una jerarquía de necesidades humanas y defiende que conforme se satisfacen las necesidades básicas se pueden ir alcanzando otras más elevadas que van ascendiendo hasta llegar a su cúspide.

sociales. Esto incluye el amor romántico, la amistad, la afiliación y el sentido de comunidad.

4. Necesidades de estima: posteriormente de satisfacer las necesidades de pertenencia, las personas buscan reconocimiento, respeto y aprecio por parte de los demás, así como una autoestima positiva y la confianza en sí mismos. Esto incluye el logro, el reconocimiento social, la reputación y el respeto por parte de los demás.

5. Necesidades de autorrealización: en el vértice superior de la pirámide de la jerarquía de Maslow, se encuentran las necesidades de autorrealización, que están representadas por el deseo de alcanzar el máximo potencial personal y cumplir con uno mismo. Esto implica el crecimiento personal, la creatividad, el logro de metas significativas y la búsqueda del propósito y la realización o la autorrealización en la vida.

Maslow sugiere, por tanto que, a medida que las personas satisfacen las necesidades en un nivel dado, buscan satisfacer las necesidades en el siguiente escalón, subiendo en la pirámide nivel más alto. La teoría de Maslow ha dejado su influencia en distintos campos, tales como la psicología, la educación, la administración y el desarrollo personal, al poner el acento en la importancia de comprender y abordar las necesidades humanas básicas para fomentar el crecimiento y el bienestar individual.

Figura 1

Pirámide de Maslow. Fuente: Elaboración propia.

La seguridad puede extenderse a las personas de los que uno se siente responsable, así como de los bienes, por lo que podríamos diferenciar de una seguridad referida a las personas y otra a los bienes o al patrimonio.

En lo que respecta a la seguridad referida a los bienes, patrimonio, procesos o cosas, puede entenderse como aquella que realmente esté libre de daños, fuera de riesgo o peligro de ser sustraídos del dominio de su legítimo dueño.

La seguridad referida a las personas tiene una doble vertiente, la de estar seguro y la de sentirse seguro, este último concepto puede referirse tanto a la percepción bien sea personal o social. Ambas concepciones pueden ser en ocasiones diametralmente opuestas apareciendo el concepto de seguridad real y la de seguridad aparente, al ser esta última la percepción, a veces errónea de la persona que la sienta de esa manera.

La Seguridad Real[7], es aquella que solo se produce en ausencia de riesgos y vulnerabilidades, sólo así puede hablarse de Seguridad. En cambio, la Seguridad Aparente es la percepción de seguridad o su ausencia por un individuo y que puede diferir de la Seguridad Real. En el sentido expuesto, según el artículo del Club Viro[8], se aborda la diferencia entre «la Seguridad Real (basada en estadísticas de los delitos registrados, y la Seguridad Percibida o aparente (la sensación personal de ser víctima de un delito)». Club Viro. (2016).

La Cultura de la Seguridad de las personas y bienes va adquiriendo cada vez más importancia en nuestro entorno social y económico.

Cada año aumenta la sensibilidad y preocupación por la prevención y por la seguridad, a pesar de ello, aún queda mucho camino por recorrer para lograr unos resultados razonables y situarla en el verdadero lugar que le corresponde. La gestión de la Seguridad como brazo articulado de la cultura preventiva, se hace necesaria, dado que, para salvaguarda de la vida humana, de la integridad física de las personas y de los bienes, se necesitan acciones que impidan la ocurrencia de cualquier tipo de siniestro.

[7] La seguridad real se basa en una evaluación objetiva de amenazas y riesgos reales, sin embargo, la seguridad aparente se refiere a una sensación de seguridad que puede no estar respaldada por una evaluación objetiva de las amenazas reales. Estos conceptos tienen implicaciones importantes para la formulación de políticas de seguridad y la toma de decisiones en diversos contextos, ya sea a nivel individual, comunitario o internacional.

[8] Extraída la información necesaria del siguiente enlace: https://www.clubseguridadviro.es/seguridad-real-frente-a-seguridad-percibida/

Una implicación correcta del nuevo concepto de Seguridad Global evidencia la necesidad de un cambio de concepción a la hora de tratar el término.

Mientras se siga considerando por cualquier gestor ese concepto como un gasto, seguirán produciéndose inexorablemente accidentes, robos, hurtos, sabotajes, e incluso, situaciones de emergencia, catástrofe o calamidad pública en la que el Terrorismo pudiera ser una de ellas, riesgos que podían haberse evitado o reducido a un coste bajo en comparación con el daño sufrido y, evitar significativamente el alto precio de los riesgos para las personas.

La Seguridad no puede ser un requisito legal y burocrático más, así como parte de la documentación necesaria que cualquier administración puede requerirnos.

No podemos dejar de pensar que, a pesar de todo lo expuesto, la Seguridad es un elemento sustancial que está relacionada con la calidad en todos sus aspectos y además es transversal a cualquier proceso en cualquier organización, institución y entidad, e incluso en la propia vida. La Seguridad debemos de entenderla como un concepto global e integrador por la transversalidad del concepto y sin sesgos.

El vocablo Seguridad va unido indefectiblemente al término riesgo y éste a su vez al de amenaza.

El riesgo puede definirse como la vulnerabilidad de los bienes jurídicos protegidos ante un posible daño para las personas y cosas y supone la probabilidad de que puedan sufrir algún daño, por ello, es cuantificable.

La amenaza, en cambio, supone la presencia de un riesgo y de que éste pueda materializarse. Hace referencia a las situaciones que pueden afectar y hacer variar la cualidad benéfica del bien o de las personas, por tanto, estamos en este caso ante un término cualitativo o descriptivo de lo que puede ocurrir. Podemos concluir que, la amenaza es por tanto una descripción cualitativa de lo que puede ocurrir y el riesgo cuantifica la probabilidad de lo que se pueda producir.

En relación con el concepto de vulnerabilidad, cabe apuntar que es el estado normal en el que se encuentran los bienes expuestos a una o varias amenazas. Es decir, el grado de facilidad con que podrán producirse daños tanto en las personas como en los bienes o en el patrimonio como consecuencia de las amenazas. Por tanto, en relación al concepto de «la seguridad total es imposible e indeseable». (Ramphele, M., 2004).

El concepto de seguridad humana, en cambio, se refiere a la protección y el bienestar de las personas en un sentido amplio. Las perspectivas más relevantes sobre la seguridad humana para la Organización de las Naciones Unidas (ONU), implica proteger a las personas contra amenazas crónicas como el hambre, la enfermedad y la represión. Garantizar la protección contra alteraciones súbitas y dolorosas en la vida cotidiana, ya sea en la comunidad, el hogar o el empleo.

Este enfoque multidimensional y universal fue puesto de manifiesto en el contexto organizacional oficial internacional, por la ONU. Se introdujo por primera vez en el Programa de la Organización de Naciones Unidas para el Desarrollo (PONUD), el «concepto de Seguridad Humana». (ONU, 1994).Concepto que genera un nuevo enfoque con una dimensión global que, integra a su vez siete componentes que son:

1. La Seguridad económica[9]. Sobre el concepto de seguridad económica y según PNUD, (1994):

   > Muchos ciudadanos de los países ricos se sienten hoy inseguros porque resulta cada vez más difícil obtener y conservar un empleo. Incluso quienes tienen empleo pueden sentirse inseguros si este e solo temporal. Las condiciones más inseguras de trabajo suelen hallarse en el sector no estructurado. La inseguridad en cuanto al ingreso ha afectado también a los países industrializados. (p. 28).

2. La Seguridad alimentaria.
   La Seguridad alimentaria ha de entenderse en relación a que todas las personas y atendiendo a Fernández, J.P. (2005):

   > (…) tienen acceso tanto físico como económico a los alimentos básicos. Esto requiere no solo que haya suficiente alimento para todos, sino que la gente tenga acceso inmediato a los alimentos, que tengan derecho al alimento. (p.45).

3. La Seguridad en la salud.
   Este enfoque debe de entenderse al derecho que los individuos tienen al acceso a la asistencia sanitaria hospitalaria, así como a posibles enfermedades que afectan a la

[9] Requiere una renta básica como contraprestación a un trabajo remunerado.

salud de las personas, en especial a aquellos países en vías de desarrollo, directamente relacionada la morbimortalidad con el entorno o el ambiente en el que se desarrollan sus vidas. En este sentido hemos de destacar que, según el PNUD (1994):

> (…) en los países en desarrollo las principales causas de defunción son las enfermedades contagiosas y parasitarias, que matan 17 millones de personas por año, incluidos 6,5 millones debido a infecciones respiratorias agudas, 4,5 millones de enfermedades diarreicas y 3.5 millones a la tuberculosis La mayoría de esas muertes se deben a la mala nutrición y a un medioambiente inseguro, particularmente el abastecimiento de agua contaminada que contribuye a casi 1000 millones de casos de diarrea por año. (p. 29).

4. La Seguridad ambiental.

   El crecimiento en progresión geométrica que ya apuntaba Malthus[10], así como el grandísimo desarrollo industrial, someten al medio ambiente a un deterioro sin precedentes.

5. La Seguridad personal.

   Hace referencia quizás al aspecto más importante para las personas, principalmente en aquellas cuestiones que puedan afectar a la integridad física y a la propia vida. «Para muchas personas, la mayor fuente de ansiedad es la delincuencia, particularmente la delincuencia violenta». (Fernández, J.P., 2005, p.47).

6. La Seguridad de la Comunidad.

   Son muchos los riesgos y amenazas emergentes que ponen en peligro la seguridad de la comunidad. Los riesgos y amenazas emergentes pueden variar dependiendo de la región, el contexto socioeconómico, político y medioambiental. Sin embargo, hay algunos riesgos y amenazas que han sido destacados como preocupaciones globales en los últimos años tales como:

[10]Thomas Robert Malthus era un economista y demógrafo británico del siglo XIX conocido por su teoría sobre la población y los recursos. Malthus argumentaba que la población tiende a aumentar en un ritmo geométrico, mientras que los recursos disponibles para mantener esa población aumentan solo en un ritmo aritmético. Este antagonismo o disyuntiva entre el crecimiento de la población y el crecimiento de los recursos daría lugar a crisis de subsistencia, ya que eventualmente la población superaría la capacidad de la tierra para producir alimentos suficientes.

a. Cambio climático: el cambio climático es una de las mayores amenazas para el planeta en la actualidad. Se manifiesta a través de fenómenos climáticos extremos, aumento del nivel del mar, acidificación de los océanos y pérdida de biodiversidad. Sus impactos pueden ser devastadores para la vida humana, la economía y los ecosistemas.

b. Pandemias y enfermedades emergentes: la aparición de nuevas enfermedades y pandemias, como la pandemia de COVID-19, representa una amenaza importante para la salud pública y la estabilidad económica y social a nivel mundial. La rápida propagación de enfermedades infecciosas puede tener consecuencias devastadoras si no se toman medidas efectivas de prevención y control.

c. Ciberseguridad: con el crecimiento de la tecnología digital, la ciberseguridad se ha convertido en una preocupación cada vez mayor. Los ciberataques pueden afectar a gobiernos, empresas e individuos, causando daños financieros, pérdida de datos y disrupciones en servicios críticos.

d. Desigualdad socioeconómica: la creciente brecha entre ricos y pobres en muchas partes del mundo representa una amenaza para la estabilidad social y política. La desigualdad socioeconómica puede conducir a tensiones sociales, conflictos y disturbios civiles.

e. Terrorismo y extremismo: el terrorismo y el extremismo violento continúan siendo una amenaza en muchos lugares del mundo. Los grupos terroristas pueden perpetrar ataques indiscriminados que causan pérdidas de vidas humanas y generan miedo y desestabilización.

f. Conflictos armados y guerras: los conflictos armados y las guerras civiles representan una amenaza para la seguridad y el bienestar de las poblaciones afectadas. Estos conflictos pueden causar desplazamiento masivo, violaciones de derechos humanos y destrucción de infraestructuras.

g. Pérdida de biodiversidad: la pérdida de biodiversidad es una amenaza importante para los ecosistemas del planeta y para la capacidad de la Tierra para sostener la

vida. La degradación del hábitat, la deforestación, la contaminación y la sobreexplotación de recursos contribuyen a esta pérdida de biodiversidad.

En cualquier caso, en relación a la Seguridad de la Comunidad es necesario considerar que, según el PNUD (1994):

> La mayoría de la población deriva seguridad de su participación en un grupo, una familia, una comunidad, una organización, un grupo racial o étnico que pueda brindar una identidad cultural y un conjunto de valores que le den seguridad a la persona. (p. 29).

7. La Seguridad política:

   La seguridad política se refiere al conjunto de medidas, políticas y acciones dirigidas a proteger y preservar la estabilidad, la integridad y la soberanía de un Estado o una comunidad política. Incluye la protección contra amenazas internas y externas que puedan poner en peligro la seguridad nacional, el orden público y la cohesión social. La seguridad política en relación a sus aspectos clave han de incluir una adecuada gestión de:

   a. La Defensa nacional: la protección del territorio, la soberanía y la integridad territorial contra amenazas militares, como la agresión de otros Estados o grupos armados.
   b. La Lucha contra el terrorismo: La prevención y la respuesta a actividades terroristas que puedan amenazar la seguridad y el bienestar de la población, así como la estabilidad política y económica.
   c. La Seguridad interna: la protección contra amenazas internas, como el crimen organizado, la insurgencia, la subversión política y la delincuencia.
   d. La Estabilidad política: la promoción de instituciones políticas sólidas, el respeto al Estado de derecho, la protección de los derechos humanos y la prevención de conflictos internos que puedan desestabilizar el país.
   e. La Gobernanza eficaz: la capacidad del Estado para proporcionar servicios básicos, mantener el orden público, garantizar la justicia y promover el desarrollo socioeconómico de manera efectiva y equitativa.

f. La Seguridad en las fronteras: la protección de las fronteras nacionales contra amenazas como el tráfico ilegal de armas, drogas, personas y mercancías.

La seguridad política se centra en garantizar la estabilidad y el buen funcionamiento de las instituciones políticas, así como en proteger a la población y los intereses nacionales contra diversas amenazas, tanto internas como externas.

En relación al concepto de Naciones Unidas y Seguridad Humana, hemos de decir que el primer académico que lo elevó a categoría dentro del derecho público, proponiendo incluso un Grado Universitario y la creación de una Escuela de Seguridad y Prevención Integral, fue el maestro Manuel Balbé.

Gracias a él, se defendieron tesis como la de Juan Pablo Fernández Pereira, titulada, precisamente, Seguridad Humana, y que fue defendida en el año 2005 en la Universidad Autónoma de Barcelona, en el Departamento de Derecho Público y Ciencias Histórico-Jurídicas, dentro del programa de doctorado en Seguridad y Prevención, de la que el Dr. Balbé era profesor.

En relación a la anterior definición, el concepto de seguridad humana según Balbé, M. (2006):

> (…) este término estaba dando un sentido integral y más completo a todos estos nuevos derechos y valores que se implantan y dan un nuevo sentido al papel del Estado y de los movimientos comunitarios. (p. 15).

En definitiva, en relación al concepto de Seguridad Humana puede entenderse según la ONU (1994):

> Actualmente, para la mayoría de las personas, el sentimiento de inseguridad se debe más a las preocupaciones acerca de la vida cotidiana que al temor de un cataclismo en el mundo. La Seguridad e en el empleo, la seguridad del ingreso, la seguridad en la salud la seguridad en el medio ambiente, la seguridad respecto al delito: son estas las preocupaciones que están surgiendo en el mundo acera de la seguridad humana.

El concepto de Seguridad Humana, desde una perspectiva más general, se refiere a la seguridad de los seres humanos independientemente de las fuerzas externas, como la naturaleza o la política. También abarca la protección entre los propios seres humanos a través de estructuras sociales estables, como el gobierno, en definitiva busca garantizar la protección

integral de las personas y su desarrollo humano en un mundo cada vez más complejo y cambiante.

Si tenemos que destacar que en el contexto organizacional oficial internacional, Sin embargo, en relación al concepto de Seguridad Humana y que ya vincula el término de terrorismo por primera vez a la acepción, podría definirse según Mahbub, (1998) como:

> (…) un concepto que surge no de las doctas escrituras de los eruditos sino de las diarias preocupaciones del pueblo. Se refleja todos los días en el ceño fruncido de los rostros de los niños inocentes, en la angustiada existencia de los sin techo, en el constante temor de los que no tienen trabajo, en los silentes gritos delos perseguidos, en la calma desesperación de las víctimas de las drogas, el SIDA, el terrorismo y la propagada contaminación.

En cualquier caso, en el Informe del Milenio de la Organización de las Naciones Unidas, y en palabras de su Secretario General, en relación al concepto de Seguridad y ya integrándolo con el concepto de seguridad humana y que, a su vez incardina el término de Terrorismo en una segunda ocasión, en palabras de Anan, K. (2000):

> La seguridad no puede ser definida sólo como la ausencia de conflicto armado, sea dentro de un estado o entre estados. Los abusos de los derechos humanos, los desplazamientos de la Población Civil, el terrorismo internacional, de la pandemia del SIDA, el tráfico de armas, de drogas y personas, los desastres ambientales, presentan una amenaza directa a la seguridad humana, forzándonos a adoptar una estrategia coordinada.

Una definición más precisa del término es que « (…) la Seguridad es el derecho humano más esencial, a la vida, a la integridad moral, en definitiva, un derecho a la seguridad preventiva». (Balbé, M., 2006).

En cualquier caso, «la seguridad como valor absoluto no existe y, por tanto, no podemos nunca alcanzarla totalmente. Podemos decir que la búsqueda de la seguridad es un camino que no tiene final». (Anitua, P., 2006).

Europa, en relación al terrorismo, indistintamente de sus causas motivadoras ha establecido un marco legal y normativo al respecto, según Bilbao, J.V., (2021):

> La presencia del terrorismo, de uno u otro signo, ha sido una constante en la vida política y social europea de los siglos XX y XXI que, con fluctuaciones en cuanto a su intensidad, ha amenazado, en mayor o menor medida, de forma directa la paz y la seguridad de las personas. El terrorismo internacional, en su vertiente del Islamismo radical, ha incluido a Occidente como objetivo de sus acciones, lo que ha motivado que se haya ido constituyendo un marco normativo, tanto nacional como internacional, para combatir este fenómeno. (p. 156).

De la misma manera es destacable el compromiso de Europa al establecer unas líneas de actuación que se vertebra en cuatro ejes bien estructurados, en palabras de Bilbao, J.V., (20021):

> (…) el primer eje busca PREVENIR la radicalización, impedir que las personas se conviertan en terroristas, y evitar atentados.
>
> Con el segundo eje se procura PROTEGER a la ciudadanía y a las infraestructuras y servicios, reduciendo vulnerabilidades, la inseguridad y el impacto de un atentado terrorista anticipando posibles efectos.
>
> El eje tercero se orienta a PERSEGUIR a los terroristas, detectándolos, investigándolos, deteniéndolos y poniéndolos a disposición judicial.
>
> Estar preparados para RESPONDER, adecuadamente ante un atentado y restablecer la normalidad a la mayor brevedad, como el último de los ejes, supone como imprescindible el prever y anticipar acontecimientos, ante la inexistencia del riesgo 0, y la seguridad de las personas no es ajena a esta circunstancia. (p. 157).

El compromiso de la Unión Europea frente al terrorismo internacional y, en palabras de Bilbao, J.V. (2021), supone:

> Luchar contra el terrorismo de forma global al tiempo que se respetan los derechos humanos y se crea una Europa más segura que permita a sus ciudadanos y ciudadanas vivir en un espacio de libertad, seguridad y justicia. (p.157).

1.3. HETEROGENEIDAD DE LOS RIESGOS ASOCIADOS AL *YIHADISMO*.

Son muchos y muy variados los riesgos asociados al Terrorismo de Corte *Yihadista*, de entre los principales, hemos de destacar los siguientes que, incluyen:

1. La radicalización[11]: Existe el riesgo de que individuos sean radicalizados y se involucren en las distintas actividades terroristas. La propagación de ideologías extremistas a través de la Red de Redes (*internet*) y las numerosas y distintas redes sociales ha facilitado el proceso de reclutamiento y radicalización. En el sentido que se expone y en relación con el Terrorismo de Corte *Yihadista* y, según Bilbao, J.V., (2021),

> La islamización de la radicalidad se ha demostrado como la más compleja de abordar, ya que las causas específicas de ello pueden ser múltiples, desde un problemas psicológico hasta el desarraigo, la frustración, la falta de afecto, etc. Lograr saber cuál o cuáles son las causas concretas permitirá un enfoque adecuado del problema y que la hoja de ruta se consensue más fácilmente. (p. 165).

2. El retorno de combatientes extranjeros: al igual que otros países, España se enfrenta al desafío de lidiar con ciudadanos que han viajado a zonas de conflicto, como Siria e Irak, para unirse a grupos terroristas. El retorno de estos combatientes plantea preocupaciones de seguridad y la necesidad de implementar medidas efectivas de rehabilitación y reintegración.

3. La radicalización del *yihadismo* en las prisiones: las cárceles son uno de los ámbitos en el que se produce una mayor radicalización de los internos, en el sentido expuesto destaca las conclusiones a las que Díez, E., (2021) establece y que refiere que:

> En estos últimos años, fruto de la colaboración entre funcionarios de prisiones, policía y guardia civil, se ha experimentado una notable evolución en la lucha contra el terrorismo *yihadista*, investigando e identificando células *yihadistas* emergentes en el ámbito penitenciario, que han evitado diversas acciones terroristas que se estaban fraguando intramuros. (p. 203).

En el sentido expuesto, Díez, E., (2021) afirma que:

> Prisiones viene desarrollando herramientas para el control y detección de la radicalización de internos islamistas desde hace más de 10 años. (p. 205).

[11] La radicalización de los individuos hacia el terrorismo de corte *yihadista* es un fenómeno complejo y multifacético que puede tener lugar en diferentes entornos que se han asociado con este proceso son: Internet y redes sociales, las mezquitas y centros religiosos, las prisiones, conflictos y zonas de guerra, así como los distintos entornos familiares y sociales.

4. La amenaza individual y células terroristas: Además de los ataques perpetrados por células terroristas organizadas, existe el riesgo de actos de terrorismo cometidos por individuos radicalizados que actúan por su cuenta. Estos actores pueden llevar a cabo ataques de baja escala pero con un alto impacto mediático que redunde en publicidad para su causa.

   La protección de Infraestructuras Críticas, turísticas y eventos: España cuenta con importantes Infraestructuras Críticas, así como turística, también muy significativa al ser un país que vive principalmente del turismo, de la misma manera ha sido sede de importantes eventos deportivos y culturales con un calendario nacional e internacional de grandes eventos. Por lo tanto, es necesario implementar medidas de seguridad y protección integral adecuadas al nivel de riesgo para proteger estos lugares y eventos de posibles ataques terroristas.

Para hacer frente a estos desafíos, España ha fortalecido su marco legal y su capacidad para prevenir cualquier tipo de acción terrorista, todo ello a través de la adecuada utilización de la inteligencia y sus servicios, así como de la seguridad.

Se han establecido mecanismos de cooperación internacional en los que España forma parte para compartir información y coordinar esfuerzos en la lucha contra el terrorismo, bien a través de la Comunidad de Inteligencia, así como de las distintas Fuerzas y Cuerpos de Seguridad, nuestro estado integra de manera efectiva organismos como EUROPOL[12] e INTERPOL[13]. Además, se han impulsado distintas iniciativas para fomentar la prevención, la detección temprana de radicalización, la promoción de la cohesión social y la integración cultural.

Es importante destacar que el fenómeno del terrorismo es complejo y en constante evolución. La colaboración internacional y el enfoque multidimensional son fundamentales para hacer frente a esta amenaza y garantizar la seguridad y el bienestar de las sociedades.

[12] EUROPOL, es una organización policial de los países integrantes de la Unión Europea, su sede está en la HAYA, su finalidad es la de prestar asistencia a los estados miembros de la UE para prevenir el delito en sus formas agravadas, así como combatir a la delincuencia organizada, entre los que se encuentra la lucha antiterrorista.

[13] La INTERPOL es la Organización International de Policía Criminal, de carácter intergubernamental integrada por 196 estados, entre sus fine está el intercambio, así como el acceso a información sobre tipologías delictuales y sus delincuentes, todo ello además de servir para la prestación de apoyo de carácter operativo y técnico de cualquier tipo.

En cuanto al contexto socioeconómico, es capital reconocer que muchas personas se ven empujadas hacia el extremismo y el terrorismo, en ocasiones debido a condiciones de pobreza, desigualdad y falta de oportunidades.

La inteligencia en general, y la Inteligencia de fuentes humanas en particular, nos permite obtener información valiosa sobre los factores socioeconómicos que pueden contribuir a la radicalización y reclutamiento de individuos, con lo que atendiendo a estas circunstancias y entendiéndolas se pueden implementar estrategias de tipo preventivas que sean más efectivas, al igual como la implementación de programas que puedan ayudar al desarrollo económico y social para abordar las distintas tipologías causales que subyacen en el terrorismo. Por tanto la Inteligencia en cualquiera de sus modalidades es necesaria como medida preventiva contra el Terrorismo en general y el Terrorismo de corte *Yihadista* en particular.

Además, en el contexto geoestratégico mundial, las amenazas terroristas trascienden las fronteras nacionales. En particular, la amenaza *yihadista* representa un desafío significativo en la época actual, en este sentido cabe destacar que: «la seguridad no es cara, la seguridad es inestimable y su ausencia genera la más absoluta incertidumbre y 'entropía'.» (González, M., 2022).

En un mundo en constante evolución, donde las amenazas terroristas representan un riesgo significativo, comprender y valorar la importancia de las fuentes de inteligencia se vuelve imperativo para prevenir y anticiparse a posibles acciones terroristas. Al obtener información oportuna y precisa, podemos tomar medidas preventivas proactivas, identificar y neutralizar las amenazas antes de que se materialicen, salvaguardando así la seguridad de las sociedades en todo el mundo. En el sentido referenciado cabe destacar que «la inteligencia y la seguridad son un binomio indisociable e indiscutible». (González, M., 2022).

Las distintas acciones terroristas y sus graves consecuencias por el número de víctimas ha sacudido prácticamente a todo el mundo, los medios de comunicación hacen que de manera global el impacto mediático sea además importantísimo, por lo que, es trascendental combatirla y prevenirla. En palabras de Montero, A. (2006):

> La emergencia del terrorismo como amenaza global de seguridad, ha puesto de manifiesto la necesidad de mejorar los procedimientos humanos de obtención de información (*HUMINT*) en las organizaciones de seguridad.

Para entender el terrorismo y cuántas medidas preventivas y reactivas son necesarias para garantizar una adecuada respuesta, es necesario entender una serie de conceptos que van íntimamente relacionados que serán desarrollados a lo largo de la presente investigación, conceptos tales como inteligencia, contrainteligencia, fuentes, ciberterrorismo, etc.

La importancia de una adecuada estrategia de prevención y protección de las Infraestructuras Críticas, Servicios Esenciales, así como estratégicos para la sociedad a través de la Ley de Protección de Infraestructuras Críticas, así como su Reglamento de desarrollo es capital para garantizar su adecuada protección integral, de manera especial aquellas Infraestructuras Críticas Hospitalarias.

1.4. TIPOS DE TERRORISMO.

Como se ha apuntado con anterioridad en la introducción al presente capítulo, aunque de manera más genérica, el terrorismo es un fenómeno complejo y diverso que puede manifestarse de diversas formas en función de sus objetivos, ideologías y métodos. A continuación, se apuntamos algunos de los tipos de terrorismo más comunes en relación a sus distintas causas, aunque es importante destacar que estos tipos pueden superponerse y variar en función de la región y el contexto:

A. Terrorismo Político: este tipo de terrorismo se centra en objetivos políticos, como el cambio de gobierno, la independencia de una región o la implementación de políticas específicas. Según González, M. (2010):

> Se fundamentan en un acto volitivo de ostentación del poder político frente a otro grupo, ya sea por representar ese poder o por discrepancias ideológicas. Con el asesinato de ese líder del grupo que lo pretende, generándose un cambio político. (p. 53).

Los grupos terroristas políticos a menudo buscan desestabilizar el sistema político actual y pueden utilizar la violencia para lograr sus objetivos.

En el sentido apuntado, Remiro, A. (2009):

> Como actos criminales con fines políticos realizados con la intención de provocar un estado de terror en la población en general, en un grupo de personas o en determinadas personas. (…). (p. 19).

B. Terrorismo Religioso: « (…) cuando la etiología nace del enfrentamiento entre dos o más grupos religiosos contrarios». (González, M., 2010, p. 54).

> Los grupos terroristas religiosos actúan en nombre de una religión o ideología religiosa específica. Su objetivo suele ser la promoción de una visión fundamentalista de la religión y la imposición de sus creencias a través de la violencia. Incluyen el terrorismo *yihadista*, así como el extremismo religioso en otras religiones. «Un ejemplo lo tenemos en la región de los Balcanes, así como en Israel entre otros muchos países». (González, M., 2010, p. 54).

El terrorismo cuya causa es la religión como excusa, en palabras y según Valverde, A., (2021):

> El fenómeno del terrorismo de pretexto religioso y sus consecuencias en occidente han propiciado una profunda alarma social entre la población en general. Dicha alarma contiene un riesgo implícito de consecuencias indeseadas, un riesgo cierto a la hora de fijar el propio imaginario colectivo un relato distorsionado incluso de la propia amenaza. Generando un principio de sospecha hacia colectivos, individuos, o profesiones de fe, que poco o nada tienen que ver con la referida amenaza latente.
>
> El alcance de dicho riesgo llega a inocular un pensamiento distorsionado incluso en las bases de los cuerpos policiales, que o son ajenos a la referida alarma, creando estereotipos e ideas erróneas con respecto a riesgos y signos de la amenaza. (p. 145).

C. Terrorismo Nacionalista, Étnico o racial, o supremacista: los grupos nacionalistas o étnicos buscan la autonomía o independencia de una región o grupo étnico específico. «El origen de esta causa nace de la xenofobia, de los enfrentamientos étnicos o interraciales». (González, M., 2010, p. 54). Utilizan la violencia para lograr sus objetivos políticos y a menudo están arraigados en diferencias culturales, étnicas o lingüísticas.

D. Terrorismo Ideológico: este tipo de terrorismo se basa en una ideología particular, que no necesariamente está vinculada a la religión o la política. Los grupos terroristas ideológicos pueden promover ideas extremistas como el anarquismo, el ecoterrorismo y, también en este caso, el supremacismo racial. En ocasiones puede integrarse con el

terrorismo de carácter religioso. «Estas causas suelen darse en países con un régimen autocrático y generalmente poco desarrollados». (González, M., 2010, p. 53).

E. Terrorismo por causas Psicológicas: González, M. (2010) contextualizaba que:

> Las personas o la persona que pretende atentar contra alguien, padece algún trastorno o desequilibrio mental. El objetivo es encauzar a través de su acción su deseo patológico de matar independiente y colateralmente a la fama o «prestigio» por la publicidad que su acto pueda entrañar. (p. 53).

F. Terrorismo por causas económicas: en relación con las referenciadas causas, González, M. (2010) referenciaba que:

> Se produce cuando el origen del atentado es de tipo monetario, por recibir precio o recompensa. Se busca el beneficio e interés económico. Cualquier persona que se pueda oponer a estos fines puede ser eliminado por una determinada persona o grupo. (p. 53-54).

G. Terrorismo por causas sociológicas: González, M. (2010) contextualizaba que:

> Son aquellas motivadas por el desencuentro de un grupo social insatisfecho que se autoexcluye de la sociedad, su desesperación puede llevarles a la comisión de cualquier acto delictivo que ponga en peligro la vida de aquella o aquellas personas que consideren culpables de la situación en la que se encuentran con el fin de cambiarla. Son propias de sociedades avanzadas. (p. 54-55).

H. Terrorismo de Estado: en algunos casos, los gobiernos utilizan la violencia y el terror como herramienta para reprimir a la oposición política o controlar a la población. Esto se conoce como terrorismo de estado y puede incluir detenciones arbitrarias, torturas y ejecuciones extrajudiciales.

   El terrorismo de Estado es una forma de ejercicio del poder estatal que implica la aplicación clandestina, impredecible y difusa de actos de terror con el objetivo de crear temor generalizado en la población. Aunque no existe una única definición comúnmente aceptada por la sociedad científica, se caracteriza por ser perpetrado por el propio estado o sus agentes, los métodos que se utilizan escapan

consecuentemente al Imperio de la Ley y sus límites legales. El propio Laqueur[14], W., (1977), en su obra «Terrorismo: una reseña histórica», aborda el fenómeno del terrorismo en general en la que aborda también el terrorismo de Estado. Un ejemplo clarificador de terrorismo de Estado es el régimen militar argentino durante la última dictadura (1976-1983). El gobierno argentino[15] llevó a cabo numerosas desapariciones forzadas de ciudadanos, torturas y ejecuciones «extrajudiciales» contra los opositores al régimen, lo que generó un clima de terror generalizado y con latencia permanente en la sociedad Argentina. Es importante recordar que el terrorismo de Estado es una violación grave de los derechos humanos y debe ser condenado en todas sus formas.

En España, salvando las diferencias, el Grupo Antiterrorista de Liberación (GAL) fue una organización clandestina que, operó en nuestro estado durante la década de 1980. Aunque no se le considera un ejemplo clásico de terrorismo de Estado, sus acciones han sido objeto de controversia y debate. El GAL fue creado por miembros de los servicios de inteligencia franceses y españoles con el objetivo de combatir a la organización separatista vasca ETA.

Sus acciones incluyeron secuestros, asesinatos y atentados con explosivos. En relación con el Estado: aunque no era una entidad oficial de nuestro estado, se ha argumentado que el GAL operó con la connivencia o incluso la colaboración de algunos funcionarios gubernamentales.

Algunos investigadores creen que hubo una tolerancia implícita o incluso, una dirección encubierta desde ciertos sectores del estado, cuestión que no ha podido contrastarse. Algunos argumentan que el GAL no cumple completamente con la definición de terrorismo de Estado, ya que no era una entidad gubernamental formal. Otros sostienen que su operación y la posible complicidad de algunos funcionarios lo sitúan dentro de esa categoría.

[14] La obra «Una historia del terrorismo» fue escrita por Walter Laqueur en el año 1977. Este influyente historiador y comentarista político estadounidense se especializó en temas relacionados con el terrorismo y la violencia política. Su trabajo aborda la historia de Europa en los siglos XIX y XX, centrándose en países como Rusia, Alemania y el Oriente Próximo. Además, Laqueur, también ha escrito sobre el sionismo, el Holocausto, el comunismo y la Guerra Fría.

[15] El presidente de *facto,* fue el general Jorge Rafael Videla, autoproclamado Presidente de la República Argentina. El golpe de Estado que derrocó al gobierno de María Estela Martínez de Perón el 24 de marzo de 1976 estableció este régimen dictatorial. La dictadura se autodenominó «Proceso de Reorganización Nacional» y dejó profundas secuelas en la sociedad, la economía y la cultura del país. Surgieron destacadas figuras de defensa de los derechos humanos, como las Madres y Abuelas de Plaza de Mayo, que obtuvieron reconocimiento internacional. La dictadura llegó a su fin el 10 de diciembre de 1983, cuando Ricardo Alfonsín asumió la presidencia de un gobierno democrático elegido en las elecciones de octubre de ese año.

En cualquier caso, mientras que el GAL no es un ejemplo clásico de terrorismo de Estado, su existencia y acciones han generado controversia y cuestionamientos sobre la relación entre el Estado y las operaciones clandestinas en la lucha contra el terrorismo.

I. Terrorismo Cibernético: a medida que la tecnología ha avanzado, han surgido grupos y actores individuales que emplean ataques cibernéticos, conocidos también como ciberterrorismo, para lograr objetivos de cualquier índole, ya sea políticos, económicos o ideológicos. Estos ataques pueden afectar a gobiernos, empresas o Infraestructuras Críticas.

   En este sentido y en relación con el uso de las nuevas tecnologías, según Zaragoza, J.I., (2021):

   > La nueva realidad virtual ha supuesto que las organizaciones terroristas de corte *yihadista* hayan visto en estas nuevas tecnológicas un campo fértil para la consecución de sus objetivos y la expansión de la doctrina radicalista.
   >
   > Frente a esa nueva amenaza los Estados Occidentales han reaccionado arbitrando mecanismos técnicos y legales que permitan luchar contra el *yihadismo* en la red. (p. 143).

J. Terrorismo Ecológico: algunos grupos extremistas buscan promover objetivos medioambientales a través de actos de sabotaje y violencia, como la destrucción de propiedades o instalaciones que consideran dañinas para el medio ambiente.

1.5. APROXIMACIÓN AL TÉRMINO LINGÜÍSTICO DE TERRORISMO.

Con el objeto de entender la adecuada contextualización, se hace necesaria realizar una la siguiente aproximación terminológica:

Terrorismo: es un fenómeno del que ninguna nación, ningún estado está al margen. Su manifestación puede darse y presentar diversos prismas debido a la gran cantidad de ramificaciones en los que el fenómeno terrorista puede representarse.

Etimológicamente, según la Real Academia de la Lengua Española, el vocablo proviene de la unión de las voces latinas *térror* e *ismus,* «elemento compositivo que entra en la formación de algunas voces españolas con el significado de doctrina, sistema, modo o partido». (RAE, 2001, P. 1305).

Otra acepción sería la «dominación por el terror, o la sucesión de actos de violencia ejecutados para infundir terror». (RAE, 2001, p. 2165).Tal aspecto es cuestionado debido a que, según Rees, (2006):

> El diccionario más completo no es capaz de distinguir una violenta batalla por la libertad de la actividad terrorista Si se acepta la definición del diccionario, palabras como insurgente, o guerrillero que no poseen las mismas connotaciones e maldad son superfluas porque todos los insurgentes o todos los guerrilleros serían terroristas. (p. 28).

Tal y como se apuntó en la introducción al presente capítulo el concepto, incluso a día de hoy es aceptado por unos y denostados por otros, por la imprecisión y la no aceptación de las distintas definiciones por muchos autores y expertos en la materia. En palabras de Torres (2010):

> La propia Organización No Gubernamental (ONG), Amnistía Internacional no usa el término debido a que postula que no es necesaria la utilización del vocablo en la condena de los ataques que puedan sufrir la población civil por la comisión de tales actos, precisamente por la falta de acuerdo en su semántica. (p. 78).

En el mismo sentido, cabe destacar que la propia Organización de las Naciones Unidas, en referencia al término explica que «no ha sido la intención del Grupo, concebir una definición de terrorismo, determinar sus distintas raíces o abordar casos concretos de la actividad terrorista». (ONU, 2002, p.5).

Para otros investigadores el término es subjetivo, consideran de consideración que tal cuestión no debe de obviarse, todo ello porque «pueden ser eventualmente imputados de terroristas, si el fin último es causar terror y no otro fin. Es decir, la subjetividad». (Wardlaw, G., 1886, p. 45).

Otra cuestión de interés es la confusión existente entre los términos terrorismo y terror, aparentemente sinónimos, pero que en puridad no lo son. Se hace necesario un acuerdo para acometer una distinción real en su uso. «El terror es miedo muy intenso», o la acción que produce una «persona o una cosa que produce terror». (RAE, 2001 p. 2165). El terror puede definirse como «un sistema de dominio por el miedo, aplicado por los poderosos» (Hacker, F., 1975, p. 19), en contraposición con el concepto de terrorismo que sería la «intimidación, esporádica u organizada, que esgrimen los débiles, los ambiciosos o los descontentos contra los poderosos.» (Hacker, F. Op. Cit. P.19).

Además de lo expuesto, cabe además precisar que, no todo el que cause terror es un terrorista, todo ello porque «existen conductas humanas que pueden causar terror y no son consideradas como terrorismo y quien la efectúa tampoco es calificado de terrorista» (Rees, P., 2006, p.26).

En relación a los actos de terrorismo, así como con el término de terrorismo, según Laborde, J.P. (2021):

> Hay que subrayar desde ya que los actos de terrorismo son considerados, tanto por la Asamblea General como parte del Consejo de Seguridad, como crímenes, mientras que el terrorismo no cuenta con una definición general a nivel de la Organización de las Naciones Unidas. Se distingue, pues entre los actos y el fenómeno (…). (p. 25).

Ante el nuevo fenómeno del terrorismo internacional los distintos países han empezado a tomar conciencia de que nos encontramos en una amenaza global de carácter mundial y que sus devastadores efectos tras las distintas acciones terroristas y sus efectos colaterales no hacen distinción entre las víctimas. En palabras de González (2006):

> El terrorismo se había convertido en una amenaza que afectaba al marco y al desarrollo de las relaciones internacionales y a los espacios propios de la seguridad y de la defensa.

En el marco de la Unión Europea, a través del propio Consejo Europeo tampoco se ha definido de una forma concisa el término de terrorismo, «en ninguna instancia internacional existe, una aceptación pacífica de la consideración de terrorismo». (Torres, 2010, p. 86).

Incluso en el momento actual y en el contexto sociopolítico de nuestro país, no hay acuerdo sobre la precisión del concepto, aspecto que ha quedado en la actualidad de manifiesto con la imputación de dirigentes políticos catalanes por la causa conocida como el *Process*, en la que, de una parte, según el Mundo, (2023):

> El juez[16] que investiga *'Tsunami Democràtic'* imputa a Puigdemont y Marta Rovira por "terrorismo" y, de otra parte, la Fiscalía recurrirá porque sólo ve "desórdenes".
>
> La imputación también se extiende a "ex altos cargos de la *Generalitat* un delito de terrorismo por su implicación en la plataforma puesta en marcha en 2019 para organizar protestas masivas contra la sentencia condenatoria del *procés.* Junto a ellos

[16] El magistrado de la Audiencia Nacional García Castellón sitúa al ex presidente catalán y la dirigente de ERC en el epicentro de las movilizaciones contra la sentencia del *procés.*

> hay otros 10 imputados entre los que se encuentran algunos considerados como 'estado mayor" del proceso independentista.

Tal imputación, *grosso modo*, se hace porque la Autoridad Judicial entiende que hubo implicación de los dirigentes políticos imputados en las directrices que los grupos Comités de Defensa de la República (CDR)[17] seguían. «Los CDR de la 'Operación Judas' acusados de terrorismo ya se escudan en la amnistía para intentar retrasar el procedimiento». (El Mundo.es, 2023). Incluso, entre la Fiscalía no se produce acuerdo al respecto y existen voces discrepantes en la calificación jurídica de lo acontecido, cuestión que incide en la inconcreción del término Terrorismo.

No obstante, el terrorismo se puede definir como el uso sistemático y premeditado de la violencia, el miedo y la intimidación por parte de grupos o individuos, con el objetivo de promover una agenda política, social o ideológica, y generar un impacto psicológico en la sociedad, para ello emplean el uso premeditado y sistemático de la violencia, promueven un ideario político, social o ideológico, así como pretenden generar un impacto psicológico a través del terror. «El terrorismo desafía nuestras nociones de guerra y paz, ley y soberanía, vida y muerte». (Bobbitt, P., 2008).

En relación al fenómeno terrorista, amenaza actual y latente, que ha impactado en el corazón de la Civilización Occidental, Lesaca, (2017) apuntaba que:

> El terrorismo moderno es un fenómeno de comunicación. Una táctica extrema, criminal y violenta, empleada para marcar la agenda de los medios y captar la atención de la opinión publica hacia una determinada reivindicación política.

Una definición más reciente del concepto de terrorismo viene a considerarlo como «un arma política que trata de usar el miedo y la intimidación para manipular a una audiencia con el fin de maximizar una posición política que no puede ser conseguida por otros medios democráticos o no». (Hoffman, 1999; citado en Díaz Matey, 2016, p.208).

El uso de las nuevas tecnologías en la actual era digital, así como de la Inteligencia Artificial (IA) va a suponer, según Cerviño (2020) que:

[17] Los Comités de Defensa de la República, eran conocidos con anterioridad, como Comités de Defensa del Referéndum, se constituyeron en el año 2017 con el objeto de facilitar y garantizar la celebración del Referéndum de Independencia del 1 de octubre del mismo año.

(…) el siguiente paso, sin duda, lo dará la inteligencia artificial, la robótica, las cuatro dimensiones, la computación cuántica que permitirán perfeccionar con gran cantidad de datos y herramientas nuevas formas de estrategia que modificarán de forma peligrosa los contextos y equilibrios de poder futuros, donde la disuasión será la principal herramienta de estrategia; es necesario analizar el futuro para poder influir en su configuración.

1.5.1 Breve aproximación conceptual a otros conceptos transversales al concepto de Terrorismo.

A. Inteligencia: etimológicamente el concepto de inteligencia deriva del Latín *intelligentia,* se define como: « (…) Trato y correspondencia secreta de dos o más personas o naciones entre sí». (RAE., 2001, p. 1288). En cualquier caso y de manera específica hay que hacer referencia a su acepción 20, cuyo tenor literal dice «Servicio de inteligencia» y cuya definición es la de « (…) Organización del Estado que proporciona al poder ejecutivo análisis e información para mejorar la toma de decisiones estratégicas orientadas a prevenir o neutralizar amenazas y a defender los intereses nacionales». (RAE., 2001, p. 2055).

   En cualquier caso, esa concreción conceptual viene a definirse por los expertos en terrorismo, así como en Ciencias de la Seguridad e Inteligencia que, en palabras de Lowental, (2003), lo define como:

   > (…) el conocimiento que las autoridades civiles y militares deben poseer para salvaguardar el bienestar del país. (Kent, 2019), en definitiva, la inteligencia es «una parte más de la maquinaria de ayuda al proceso de toma de decisiones desde la información.

B. Contrainteligencia: anglicismo que originario del término *counterintelligence*. En español, la RAE define el término como contraespionaje y define el concepto como el «Servicio de defensa de un país contra el espionaje de potencias extranjeras». (RAE., 2014).

   De consideración por su importancia funcional en relación a su aplicación, la siguiente definición de contrainteligencia que, determina que son aquellas: « (…) medidas de protección de las instancias en contra de actos lesivos, así como las acciones orientadas a disuadir o contrarrestar su comisión». (Ley 36/2015, de Seguridad Nacional, 2015).

C. Ciberinteligencia: al carecer de definición específica por la propia Real Academia de la Lengua Española (RAE), ha de destacarse la definición del concepto que viene determinado por la aparición de las nuevas tecnologías de la información e internet, irrumpe un nuevo prisma que ha de considerarse, el ciberespacio. El ciberespacio, según Gomes (2017), lo define como:

> El quinto dominio donde la globalización es la protagonista, en el que se han eliminado cualquier tipo de fronteras y en el que, las oportunidades, y también los retos han formado una nueva dimensión estratégica.

De la misma manera es de suma importancia atenerse al tenor literal de la definición legal que establece nuevamente el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, del término de Ciberespacio. El propio ESN (2022), lo define como:

> (…) dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual. (p. 77).

Figura 2

Cíberinteligencia. Fuente: Atlantico.net

D. Ciberseguridad: la ciberseguridad afecta a todas las organizaciones de cualquier índole debido al extendido uso de las tecnologías y de las comunicaciones por la sociedad y

por la gran transformación digital en la que nos encontramos. González, M. (2023) lo define como:

> El conjunto de prácticas, tecnologías y procedimientos diseñados para proteger los sistemas, redes y datos de ataques cibernéticos, así como para prevenir el acceso no autorizado, el robo de información y la interrupción de servicios. (p. 114).

En cualquier caso, ha de estarse a la definición que legalmente establece el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Es decir, el propio ENS (2022) define la Ciberseguridad como:

> La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. (p. 77).

En el sentido expuesto y en palabras de Miranda, D., (2023, p. 33) destaca que, «muchas organizaciones cuentan con una buena gestión de riesgos, pero carecen de una estrategia de ciberseguridad que lo cubra todo».

E. Ciberterrorismo: ha de entenderse, en una primera instancia, con la definición del prefijo «ciber» que sirve de elemento compositivo al unírsele el término de terrorismo[18] ya definido con anterioridad, en definitiva y según el Grupo de Expertos de Alto Nivel de la ONU (2004) que lo de fine como:

> Cualquier acto destinado a causar la muerte o lesiones corporales graves a un civil o a un no combatiente cuando el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un Gobierno o a una organización internacional a realizar una acción o abstenerse de hacerla (p. 54).

En atención a lo dispuesto por el Diccionario de la Real Academia de la Lengua Española, su etimología proviene del uso en castellano del anglicismo *cyber*. El término fue acuñado en 1980 por Barry Collin, al ser consciente y percibir adecuadamente la

[18] El Grupo de Expertos de las Naciones Unidas en Nombres Geográficos (UNGEGN), -en atención a sus siglas en inglés-, es un órgano consultivo y colegiado. Fue creado por el Secretario General de la ONU con el objeto de dar respuesta y cumplimiento a la resolución número 715 A (XXVII) de fechad 23 de abril del año 1959 del Consejo Económico y Social.

convergencia entre el mundo virtual y el físico. En cualquier caso, Mark M. Pollit (1998) acotó mejor el concepto y lo pudo definir como:

> Un ataque predeterminado, políticamente motivado contra información, sistemas, y programas informáticos y datos a través de la red como acto violento contra objetivos no combatientes por organizaciones o agentes clandestinos» (p. 9).

También no puede obviarse el uso que, las nuevas tecnologías proporcionan a los grupos terroristas, con distintos *íter* adicionales con el que implementar la transmisión y divulgación de la causa motivadora de sus actos, prácticamente de manera impune, sin consecuencias penológicas de ningún tipo, no en vano, en palabras de Merlos (2006):

> (…) no es de extrañar que se hayan inclinado hacia ella, y el ciberespacio, se haya transformado por las ventajas que ofrece en el marco ideal de sus operaciones» (Merlos, 2006).

La transformación digital en el que la sociedad actual está inmersa, también es utilizada por los distintos estados para combatir el fenómeno terrorista, así como «el uso de las nuevas tecnologías para prevenir y contrarrestar las actividades terroristas pueden ser una herramienta muy eficaz.» (Kamboj, 2022).

El referenciado concepto de ciberterrorismo, así como su actual vigencia puede albergar dos prismas diferentes, todo ello porque, en palabras de Subijana (2008):

> (…) se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de medios provenientes de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa. (p. 172).

La protección de las distintas Infraestructuras Críticas a través del Ciberterrorismo es una necesidad crucial para la resiliencia de nuestra sociedad, todo ello porque según refiere Maras, (2017):

> (…) el ciberterrorismo se refiere al uso de Internet para atacar Infraestructuras Críticas con la intención de provocar miedo y causar daños físicos a las personas (heridas graves o la muerte), para que tenga un efecto en el cambio de gobierno o en la misma población en base a metas políticas, o ideológicas. (p. 386).

En la misma línea que Maras, el concepto de Ciberterrorismo, también podría definirse según la OTAN (2008) como:

> Un ciberataque usando o explotando redes informáticas o de comunicación para causar una destrucción o disrupción suficiente para generar miedo o intimidar a una sociedad dirigiéndola hacia una meta ideológica.

F. *Yihadismo*: extranjerismo proveniente del árabe, *ğihād.* Según la propia Real Academia de la Lengua Española (RAE) en su vigésimo tercera edición, es una «tendencia ideológica radical que preconiza la *Yihad* (II guerra islámica)». (RAE, 2014). La *Yihad* tampoco escapa al uso de las nuevas tecnologías para enarbolar la bandera del Ciberterrorismo, todo ello y según Cano (2011), es debido a que:

> > El terrorismo de inspiración *yihadista* ha sido un entusiasta de la tecnología que le ha permitido dotar de una nueva efectividad sus actividades delictivas, y que, al mismo tiempo, le ha abierto nuevas posibilidades para interactuar y mantener viva una amplia red de partidarios dispersos por todo el planeta. (p. 115).

G. Amenazas Híbridas y zona gris: En el contexto de seguridad y geopolítica[19], la zona gris y la zona híbrida son conceptos distintos, aunque a veces pueden confundirse debido a su similitud.

   Zona Gris: la zona gris se refiere a situaciones o conflictos en las que no está claramente definido quién es el agresor o quién está llevando a cabo acciones hostiles. En esta zona, los actores pueden utilizar tácticas no convencionales, como la desinformación, la ciberseguridad o la influencia política, sin una declaración formal de conflicto bélico o de guerra.

   Ejemplos de zona gris incluyen la guerra híbrida[20], la competencia estratégica entre potencias y las operaciones encubiertas.

[19] La «geopolitica» surge a finales siglo XIX y se consideraba la ciencia del mapa y el poder directamente relacionada con la estrategia. Rudolf Kjellen fue su principal impulsor como rama del estado, mediante su publicación en 1916 «*El Estado como forma de vida».* (Correia, 2012).

[20] Concepto que se refiere a un tipo de conflicto que combina una variedad de métodos y tácticas, tanto convencionales como no convencionales, en un intento por conseguir los distintos objetivos estratégicos planteados. El concepto término se utiliza para describir conflictos actuales que integran una parte de guerra convencional, otra de guerra asimétrica, ciberataques, guerra de información, así como operaciones tanto de carácter militar como no militar. En la guerra híbrida, los actores pueden ser no estatales o estatales.

> Zona Híbrida: la zona híbrida se refiere a un entorno en el que se combinan diferentes formas de conflicto, como la guerra convencional, la guerra asimétrica, la ciberseguridad y la desinformación. En la zona híbrida, los actores estatales y no estatales utilizan una variedad de herramientas y tácticas para lograr sus objetivos, a menudo sin una clara distinción entre la guerra y la paz. Ejemplos de zona híbrida incluyen la anexión de Crimea por parte de Rusia y las operaciones de influencia en las elecciones.

En el análisis diferencial, por tanto, hemos de destacar que, la zona gris se refiere a la ambigüedad en la identificación de agresores, mientras que la zona híbrida, abarca una amplia gama de tácticas y conflictos combinados. Ambos conceptos son relevantes en el análisis de la seguridad internacional.

1.6 CONCEPTO LEGAL DE TERRORISMO.

El concepto legal de terrorismo puede variar de un país a otro, ya que cada país tiene su propia legislación y definición legal de este tipo de acciones. Sin embargo, *grosso modo*, el terrorismo, como ha podido entenderse en epígrafes precedente, se refiere a actos violentos o amenazas de violencia que tienen como objetivo causar miedo, pánico o intimidación en una población o en un grupo específico de personas, y que se realizan con un propósito político, ideológico, religioso o social.

Según lo expuesto y en palabras de Zaragoza, J.I., (2021):

> En los años 2010 y 2015 fue modificado ampliamente el Código Penal incluyendo figuras penales como, por ejemplo, la tipificación del adoctrinamiento, captación, y adiestramiento activo de personas para incorporarse a una organización terrorista (art. 577. 2CP), o el autoadoctrinamiento o autoadiestramiento pasivo respecto a quien, sirviéndose e internet o de las nuevas tecnologías, se forma en capacitación militar con estas finalidades (art. 575. CP). También fue abordada una modificación del tipo penal de enaltecimiento previendo una pena mayor cuando el mismo fuera cometido en la red.
>
> El delito de enaltecimiento (art. 578 CP) exige para su aplicación, además de los objetivos señalados en el tipo, la necesidad de que se genere riesgo de comisión de nuevos actos terroristas. (p. 143).

A continuación, realizamos una descripción general del concepto legal de terrorismo que suele ser común, con la inclusión de algunos de sus elementos que se recogen en muchas definiciones:

a. Uso de la violencia o amenazas: el terrorismo implica la utilización de la violencia, la amenaza de violencia o la coacción para lograr objetivos políticos, ideológicos, religiosos o sociales. Los actos terroristas pueden incluir atentados con explosivos, secuestros, asesinatos, sabotajes, toma de rehenes, entre otros.

b. Finalidad política, ideológica o religiosa: los actos terroristas están motivados por una finalidad política, ideológica, religiosa o social. Esto significa que quienes cometen estos actos buscan promover, imponer o cambiar una determinada ideología, religión o sistema político, o bien, intentan generar miedo o presionar a las autoridades para que tomen medidas específicas.

c. Intimidación o creación de temor: uno de los elementos clave del terrorismo es la intención de crear miedo, pánico o intimidación en la población en general o en un grupo específico de personas. Los actos terroristas a menudo se realizan de manera espectacular o impactante para lograr este efecto.

d. Carácter sistemático o planificado: los actos terroristas suelen ser planificados y ejecutados de manera sistemática por grupos u organizaciones que persiguen sus objetivos a través de la violencia.

e. Impacto en la seguridad pública: los actos terroristas amenazan la seguridad pública y pueden tener un impacto significativo en la sociedad, la economía y el funcionamiento de un país.

En España, el concepto legal de terrorismo está definido en el Código Penal español, en los artículos 573 y siguientes. A continuación, apuntamos el concepto legal de terrorismo según la legislación española:

El referenciado precepto, Código Penal (1995), en su tenor literal establece que:

> Se considera terrorismo cualquier acto que tenga como finalidad subvertir el orden constitucional o alterar gravemente la paz pública a través de la comisión de delitos graves, cuando se cometan con la intención de aterrorizar a la población o presionar a las autoridades.

El terrorismo, en relación al concepto estructural legal y según lo define Lamarka, C. (1985):

> Consiste en la estructura jerárquica que da unidad y coherencia interna a los actos de terrorismo como forma de ejecución de un programa político antitético al del orden constitucional del Estado. (p. 95).

En cualquier caso, ha de estarse a una serie de características claves que son trascendentales para entenderlo que son:

a. Finalidad: los actos de terrorismo en España deben tener una finalidad específica, que, puede incluir subvertir el orden constitucional o alterar gravemente la paz pública. Esta finalidad puede estar relacionada con objetivos políticos, ideológicos, religiosos o sociales.

b. Delitos graves: para que un acto se considere terrorismo, debe implicar la comisión de delitos graves, como homicidio, lesiones graves, secuestro, entre otros. Los delitos graves cometidos con la finalidad de generar terror a la población, pueden ser considerados actos terroristas, con lo que las penas pueden sumarse por concurso[21] cuando se han consumado varios delitos.

   En el sentido expuesto y en palabras de Zaragoza, J.I., (2021):

   > La relación con el delito de enaltecimiento terrorista y los tipos penales de odio (510 CP), adoctrinamiento (577 CP), colaboración con organización terrorista (art. 577 CP), o de la apología (18 CP) es la de concurso de normas (art. 8 CP). (p. 144).

c. Intención de aterrorizar: es necesario que los actos terroristas se realicen con la intención de causar pánico a la población o, coaccionar a sus autoridades. Esto implica la generación de miedo, pánico o intimidación como parte de los objetivos que los distintos grupos terroristas puedan plantearse.

[21] Los concursos pueden ser de varios tipos. Concurso real de delitos, concurso ideal y, por último, concurso medial. El concurso real se produce cuando distintas acciones materializan la comisión de varios delitos. Indistintamente si son los cometidos de un mismo tipo penal o tipos penales diferentes. El concurso real es también llamado concurso natural y es el que indefectiblemente ha de aplicarse si no existe o se aprecia otro tipo de concurso y manteniendo los factores de conexión y simultaneidad de los distintos tipos penales materializados.

d. Asociación ilícita: además de los actos terroristas en sí, el Código Penal[22] español prohíbe la participación en organizaciones, grupos o asociaciones que promuevan, fomenten o realicen actividades de terrorismo. Esto significa que la pertenencia a una organización terrorista también puede ser castigada como pertenencia a una organización criminal.

e. Penalidad: Las penas por delitos de terrorismo en España son de las más severas y pueden conllevar largas penas de prisión, incluida la prisión permanente revisable, así como multas y otras medidas de seguridad, dependiendo siempre de la gravedad del delito y la participación de los sujetos activos del delito, esto es, las personas involucradas en su comisión.

1.7 EL DELITO DE TERRORISMO Y NUESTRO VIGENTE CÓDIGO PENAL.

El delito de terrorismo en España está regulado en el Código Penal español, específicamente en el Título XXII, que comprende los artículos 572 a 580. Estos artículos definen los tipos penales relacionados con el terrorismo y establecen las penas correspondientes.

A continuación, realizamos una descripción general de los principales aspectos relacionados con el delito de terrorismo en el Código Penal español:

A. Definición del delito de terrorismo: el artículo 573 del Código Penal (1995) establece en su tenor literal que:

> Se considera terrorismo cualquier acto que tenga como finalidad subvertir el orden constitucional o alterar gravemente la paz pública a través de la comisión de delitos graves, como homicidio, lesiones graves, secuestro, entre otros, cuando se cometan con la intención de aterrorizar a la población o presionar a las autoridades.

B. Asociación ilícita: también es de aplicación a las organizaciones terroristas, el artículo 570 del Código Penal, que en su tenor literal castiga «la participación en organizaciones, grupos o asociaciones que promuevan, fomenten o realicen actividades de terrorismo».

[22]El texto legal viene dada por La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

C. Penalidades: las penas por delitos de terrorismo son severas y pueden incluir largas penas de prisión, multas y otras medidas de seguridad, dependiendo de la gravedad del delito y la participación de los involucrados.

D. Delitos de terrorismo específicos: El Código Penal español establece este tipo de delitos de manera específica, tales como el reclutamiento y adoctrinamiento de personas para fines terroristas, la financiación del terrorismo y la apología del terrorismo. Estos delitos se encuentran tipificados en los artículos 576 a 578 de nuestro vigente Código Penal.

E. Cooperación internacional**:** España coopera con otros países en la lucha contra el terrorismo, especialmente en la extradición de sospechosos de terrorismo y en la colaboración en investigaciones relacionadas con actividades terroristas transnacionales.

1.8 UNIÓN EUROPEA (UE) Y BRÚJULA ESTRATÉGICA.

La brújula estratégica es un documento estratégico de la Unión Europea (UE) que define las líneas de acción necesarias para que la UE pueda refundarse y reflotar del letargo en el que se encontraba, desde un punto de vista de seguridad y defensa. El adormilamiento y tranquilidad que daba el calor de la OTAN se puso en evidencia con la Guerra de Rusia y Ucrania.

1.8.1 Objetivos de la Brújula Estratégica:

Los principales objetivos que establece el documento publicado por el Consejo Europeo (2022) son:

- ✓ Establecer un marco estratégico global: La Brújula Estratégica establece un marco estratégico global para la Unión Europea (UE) que define los objetivos estratégicos y las áreas de acción prioritarias para el desarrollo de la seguridad y la defensa a largo plazo. El marco estratégico también establece una base para la coordinación de los esfuerzos de la UE en esta área.

- ✓ Fortalecer la autoridad y la responsabilidad de la UE: establece una responsabilidad clara para que la UE tome medidas para garantizar la seguridad, la defensa y la protección de sus ciudadanos. Esto incluye el fortalecimiento de su autoridad para desarrollar y poner en práctica una política común de seguridad y defensa que sea coherente y eficaz.

- ✓ Desarrollar las capacidades: promueve el desarrollo de capacidades en todos los niveles para mejorar la seguridad y la defensa de la UE. Esto incluye el apoyo a la investigación, el desarrollo, la innovación y la producción de equipos, tecnología y sistemas de defensa.

- ✓ Cooperar con terceros países y organizaciones: instruye la cooperación con terceros países y organizaciones para mejorar la seguridad y la defensa de la UE. Esto incluye la promoción del diálogo y la cooperación con los vecinos de la UE, así como la participación en los esfuerzos de la comunidad internacional para promover la paz y la seguridad mundiales.

- ✓ Promover la paz y la seguridad internacionales: continuar con el desarrollo de una política común de seguridad y defensa que sea coherente y eficaz, incluye el uso de la diplomacia, la resolución de conflictos, el desarme y la prevención de conflictos, la lucha contra la proliferación de armas y la promoción de los derechos humanos y la democracia. La Brújula también promueve el desarrollo de mecanismos de crisis y la preparación ante situaciones de emergencia.

  (pp. 27-29).

De manera particular, la Brújula Estratégica y según el Consejo Europeo (2022):

1. Ofrece una evaluación común de nuestro entorno estratégico, de las amenazas y los retos a los que nos enfrentamos y de sus repercusiones para la UE.

2. Aporta mayor coherencia y una unidad de propósito a las acciones ya emprendidas en el ámbito de la seguridad y la defensa.

3. Establece nuevas acciones y medios para:

   a. permitirnos actuar con mayor rapidez y decisión ante las crisis;
   b. defender nuestros intereses y proteger a nuestros ciudadanos mediante el refuerzo de la capacidad de la UE para anticiparse a las amenazas y mitigarlas;
   c. fomentar la inversión y la innovación a fin de desarrollar conjuntamente las capacidades y tecnologías necesarias;
   d. estrechar la cooperación con nuestros socios, en particular con las Naciones Unidas y la OTAN, para alcanzar los objetivos comunes.

4. Especifica objetivos y etapas claros para medir los avances.

(p. 6).

De especial relevancia la referencia al Terrorismo de Corte *Yihadista*, « (…) Los esfuerzos de la región para hacer frente al extremismo violento también serán de vital importancia en el contexto de la lucha mundial contra grupos terroristas como *Al Qaeda y Daesh*». (Consejo Europeo, 2022, p. 10).

Referencias que quedan totalmente expuestas en el epígrafe «Amenazas y desafíos emergentes y transnacionales», cuyo tenor (20022 literal, el Consejo Europeo) expone:

> Además de estos conflictos y tensiones regionales, también nos enfrentamos, a escala mundial, a amenazas transnacionales y complejas dinámicas de seguridad que repercuten directamente en la propia seguridad de la Unión.
>
> El terrorismo y el extremismo violento en todas sus formas e independientemente de su origen siguen en constante evolución y suponen una grave amenaza para la paz y la seguridad, tanto dentro como fuera de la UE. Se trata de una combinación de terroristas autóctonos y combatientes extranjeros retornados, de ataques dirigidos, impulsados o inspirados desde el extranjero, y de la propagación de ideologías y creencias que conducen a la radicalización y al extremismo violento. En concreto, la amenaza que plantean, *Daesh*, *Al Qaeda* y los grupos afiliados a estas organizaciones, sigue siendo importante y minando la estabilidad en diversas regiones, así como la seguridad de la UE. (p. 11).

1.9. *GLOBAL COMMONS* Y TERRORISMO.

El concepto de *Global Commons* deriva de la lengua inglesa y viene a definirse como aquellos espacios que son comunes, es decir que en ellos no recae la soberanía de algún país. Debemos de hacer especial referencia que, estos espacios comunes pueden ser en el mar, siempre referido a lo que legalmente se conoce como Aguas Internacionales, el espacio aéreo, reiteramos, fuera de la soberanía de cualquier estado por lo que no podría ejercerse, el espacio aéreo, el espacio exterior y ahora, muy acorde con la actual tecnología digital, el ciberespacio.

Los *Global Commons*, en español espacios comunes marítimos, espacios aéreos cualquier estado puede hacer uso movimientos militares en investigaciones etc., con el objeto de garantizar la sostenibilidad del planeta. Precisamente al ser comunes y no ejercerse por parte de los distintos estados la jurisdicción sobre ellos, se utilizan frecuentemente por terroristas, en el caso de las aguas internacionales actos de piratería o de «Terrorismo Marítimo», lo mismo ocurre con el ciberespacio en el que los ciberterroristas actúan, muchas veces con una gran impunidad que les da el «cíberanonimato».

Todas estas actividades, al igual que cualquier incidente, catástrofe o emergencia, dependen de una información en tiempo real y que a su vez sea clara y fiable para conseguir sus objetivos.

Cualquier contratiempo puede afectar al desarrollo sostenible internacionalmente, como podemos comprobar, por ejemplo, y de manera eufemística el conflicto armado de Rusia y Ucrania, donde la hibridación está provocando falsa propaganda y desinformación; o lo vivido estos últimos años con la pandemia provocada por el Virus *Sars-Cov-2* que provoca la enfermedad de la COVID-19, que la propia Organización Mundial de la Salud (OMS), la elevó a tal categoría el 11 de marzo del 2020 y que, el propio Gobierno de España declara el establecer el Estado de Alarma vehiculizado e instaurado a través del Real Decreto 463/2020, de 14 de marzo, para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, con el objetivo de establecer una serie de medidas con una cobertura legal, todo ello porque suprimían y limitaban derechos fundamentales, posteriormente, el que se hubiese establecido el Estado de Alarma al efecto fue declarado inconstitucional, por lo tanto, ilegal, por nuestro Tribunal Constitucional.

Todos estos espacios comunes, además pueden conllevar el traspaso o acceso a una gran cantidad de información y datos, en el que destaca de manera muy especial, el ciberespacio, (último espacio incluido como espacio común), así como los fondos marinos, donde se encuentran los cables submarinos de fibra óptica, entre otros. Por tal motivo la Organización de Naciones Unidas (ONU), incluya la información, así como la desinformación como piedra angular dentro de los nuevos *Global Commons*.

La utilización de la información puede ser definida de varias maneras refleja en la publicación «El desorden de la información: hacia un marco interdisciplinario para la investigación y la formulación de políticas» de Claire Wardle y Hossein Derakhshan, (2017), distinguiendo entre (Información errónea), *misinformation* (manifestación de odio, daño digital, daños mentales a

las personas, *malinformation*, (contenido manipulado), desinformación. (Margallón-Rosa, 2022).

Refiere Margallón-Rosas (2022) que:

> El arma de la información es la desinformación utilizada para cambiar perjuicios, modificar la opinión pública, dividir o camuflar la información y desacreditar al enemigo en los conflictos las informaciones políticas de los gobiernos.

Dentro del concepto de terrorismo marítimo se contemplan los actos de violencia contra un buque, su tripulación, o bienes y personas a bordo de ellos que, directa o indirectamente, pongan en peligro la seguridad de la navegación marítima o que afecte las instalaciones o servicios de la misma, es decir, en el año 2013 la Organización de Naciones Unidas publicó un estudio titulado «*Global governance and governance of the global commons in the global partnership for development beyond* 2015» [Gobernanza global y gobernanza de los espacios comunes globales como marco de cooperación global para el desarrollo a partir del 2015]. En este documento Naciones Unidas define los espacios comunes globales como «aquellas partes del planeta que se encuentran fuera de las jurisdicciones nacionales y a las cuales todas las naciones tienen libre acceso». (*United Nations*, 2013, p. 5).

> Es destacable, la breve referencia sobre la evolución del concepto y sobre algunos de los ámbitos – tangibles o intangibles – que pueden ser considerados Espacios Comunes Globales:
>
> «El derecho internacional contempla como *global commons*, Alta Mar, la Atmósfera, la Antártida y el Espacio Exterior. Estos espacios y sus recursos se consideran patrimonio común de la humanidad...», en cualquier caso, en la actualidad hay que añadir una nueva dimensión, el ciberespacio.
>
> Durante muchos siglos la mar ha sido la única *Global Commons*, si bien los avances tecnológicos que se han vivido durante el siglo XX han permito que actualmente podamos hablar de tres espacios más que los engloban:
>
> - ✓ El espacio aéreo.
> - ✓ El espacio exterior.
> - ✓ El ciberespacio.

No obstante, no debemos obviar que hay gran cantidad de publicaciones que hablan de un quinto *Global Commons*, nuestro entorno, el medio ambiente. El tránsito de transportes, vehículos, bienes o de datos, los beneficios o perjuicios de su conservación afectan de manera directa a todas las poblaciones del planeta.

Ahora bien, la característica común a todos los *Global Commons* es, además de que no se encuentran bajo la soberanía de ninguna nación, que se constituyen como espacios de tránsito de bienes, de servicios o de información, por lo que la interrupción del servicio por cualquiera de ellos supondría, aunque fuera por corto espacio de tiempo, importantes repercusiones en el ámbito económico, social y geopolítico que, sin ningún género de dudas, puede afectar a la seguridad de los distintos estados.

En lo referente al mar y de manera concreta a las Aguas Internacionales, hay que considerar la Convención de Naciones Unidas para la Ley del Mar (UNCLOS en relación al acrónimo en su terminología inglesa), tratándose de un acuerdo internacional cuyo objetivo es definir los espacios de soberanía y las zonas económicas exclusivas de los Estados. Igualmente es destacable que, más del 90% del comercio internacional en el mundo, y especialmente en lo referente a las materias primas y energéticas, usa el transporte marítimo como medio generalizado.

La legislación y normalización de lo «común» genera siempre problemas a los diferentes países, teniendo siempre la intención de regular en beneficio propio, sobre todo aquellos Estados que disponen de un estatus de potencia regional o mundial.

En cuanto a su aplicación concreta en el mar es interesante recordar la importante aportación de Alfred T. Mahan, gran estratega e historiador de Norte América que, consideraba que las aguas internacionales oceánicas eran como «grandes autopistas», lo que les otorgaba un importante y especial valor, al referir que, quién contralara el mar, dominaría por ello el mundo.

1.10. PRINCIPALES GRUPOS TERRORISTAS INTERNACIONALES.

Como principales grupos terroristas a nivel global podemos destacar fundamentalmente dos:

- ✓ *Al Qaeda*. (Quiere la unificación de todos los musulmanes del mundo y fijar un orden mundial nuevo).

- ✓ *Daesh*. (Pretende la unificación de todos los Estado Islámicos en una sola nación a través de un califato, así como recuperar los antiguos territorios del Islam).

En África destacan:

- ✓ El grupo terrorista *Boko Haram.* (Quiere instaurar la ley Sharia en Nigeria y extenderla por el Golfo de Biafra).
- ✓ El grupo terrorista *Al Gama´a al Islamiyya.* (Su misión es derrocar al gobierno en Egipto para reemplazarlo por un califato).

En Asia podemos mencionar:

- ✓ El grupo terrorista *Hezboláh.* (Su pretensión es derrocar al Estado de Israel a través de una lucha política, militar y religiosa en el Líbano).
- ✓ El grupo terrorista *Hamas.* (Lucha por la independencia de Palestina, convertirse en un Estado Islámico con la implantación de la ley de la *Sharia*[23]*).*

En América podemos nombrar:

- ✓ El Ejército de Liberación Nacional (ELN). (Cuya finalidad sería la de implantar un estado socialista en Colombia).
- ✓ Sendero Luminoso. (En el año 2018, solo queda una pequeña facción en la zona de los valles de los Ríos Apurimac y Ene. Su principal finalidad es la de hacerse con el control del narcotráfico en el país peruano).

1.11. INMIGRACIÓN ILEGAL Y TERRORISMO DE CORTE *YIHADISTA*.

El informe anual de Seguridad Nacional, (2021), publicado por la Presidencia del Gobierno, si establece que «es un fenómeno que ha aumentado durante el último año y ha afectado directamente a España. Esta realidad obliga a dotarse de instrumentos, tanto a nivel nacional como comunitario, para lograr contrarrestar este tipo de acciones con la máxima agilidad». (IASN21, pág.198).

[23]La *Sharia* es un término que se refiere al conjunto de leyes y principios que rigen la vida de los musulmanes de acuerdo con la religión islámica. La palabra *Sharia* se deriva del árabe y significa «camino» o «senda». La *Sharia* abarca una amplia gama de aspectos de la vida, incluyendo asuntos civiles, familiares, penales, comerciales y rituales. La ley de la *Sharia* se basa principalmente en dos fuentes principales: 1. El Corán: El libro sagrado del Islam, que se considera la palabra de Dios tal como fue revelada al profeta Mahoma.2. La *Sunnah*: Las enseñanzas y prácticas del Profeta Mahoma, registradas en los *hadices*, que son narraciones que describen las palabras, acciones y aprobaciones tácitas del Profeta.

En este sentido, en la cumbre de la OTAN celebrada en Madrid en junio de 2022, España manifestó su voluntad de incluir a la «migración ilegal» como una amenaza híbrida[24] a la que habría que enfrentarse con el apoyo de la Alianza militar. En el mismo sentido en un artículo de la Gaceta de la Iberoesfera, Buxadé, J. (2022) afirmaba que:

> Marruecos sigue utilizando la inmigración ilegal, las mafias, y las redes de trata de seres humanos en un modelo de guerra híbrida moderna contra España, Frontera Sur de Europa.

Como se desprende del párrafo anterior, el crimen organizado es otra de las amenazas relacionadas con los flujos migratorios irregulares que afectan a actividades como el tráfico de drogas, la piratería o ataques contra el tráfico marítimo lo que conlleva un potencial desestabilizador, en los territorios que actúan.

El aumento de la población global tiende a concentrarse en países en desarrollo y muy especialmente en los continentes asiático y africano. Factores como: los conflictos bélicos, los riesgos medioambientales, pobreza, desigualdad, etc., facilitan la previsión de flujos migratorios irregulares desde los países con la ausencia de garantías como la seguridad personal o la falta de derechos

Aunque los flujos migratorios son procesos que han tenido lugar en todos los momentos históricos, las dinámicas que han experimentado en las últimas décadas, así como su volumen los ha transformado en un fenómeno con implicaciones para la política de seguridad.

Actualmente, el escenario migratorio español se caracteriza por un grandísimo aumento en el número de llegadas, no exentas de la aparición de focos de conflictividad en el interior del país. La crisis económica y el empobrecimiento en determinadas zonas de la población conllevan a generar actos de rechazo contra le inmigración en general.

Esto nos hace reflexionar que la nueva situación exige una implicación por parte de las Administraciones Públicas para su protección, así como un cambio de mentalidad o enfoque de la migración en el ámbito económico, social y cultural con acciones de los distintos países globales y no unilaterales.

[24]Una amenaza híbrida es un enfoque integral y multifacético para la manipulación y el daño, que aprovecha una variedad de métodos y técnicas para lograr sus objetivos, ya sea políticos, económicos, militares o de cualquier otro tipo. Combina diferentes métodos y técnicas para alcanzarlos. Por lo general, estas amenazas integran elementos tanto convencionales como no convencionales.

Los flujos migratorios[25] son consecuentemente importantes ya que afecta a la vulnerabilidad económica, así como a la exclusión social y, en ciertos aspectos, a la radicalización extremista.

En España, este ítem es positivo en general, aunque puede generar el surgimiento de algunas minorías que realicen apología de una visión negativa de la inmigración.

Tras la última modificación de la Ley de Extranjería en nuestro país, a través del Real Decreto 629/2022, de 26 de julio, por el que se modifica el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por Ley Orgánica 2/2009, aprobado por el Real Decreto 557/2011, de 20 de abril, que, por tanto, refiere el (RD 629/2022), en su exposición de motivos:

> (…) una política migratoria eficaz constituye un activo de gran relevancia a la hora de maximizar el impacto positivo y los efectos de la movilidad humana internacional en economías interdependientes, apostando por potenciar la ejecución de planes de recuperación, transformación y resiliencia. (Secc. I, p. 1).

En el ámbito de la Unión Europea se han desarrollado normativas como la directiva UE 2002/90 respecto a la entrada, circulación y estancia de inmigrantes irregulares a través de políticas sociales y, también, sanciones. El objetivo europeo con relación de fronteras se centra en la gestión de los Estados como garantía de crear un entorno donde la libertad, seguridad y justicia garantice el orden político y la paz social. El reglamento UE 2019/196, de 13 de noviembre de 2019 sobre la Guardia Europea de Fronteras y Costas recoge y estable los cometidos de la denominada FRONTEX (Agencia Europea de la Guardia de Fronteras y Costas).

Podremos decir que un inmigrante irregular es aquella persona que no es de originaria de ninguno de los estados miembros de la Unión Europea y que no posee en vigor un visado o un permiso de residencia, pero que ha entrado en zona comunitaria de la UE.

Algunas de las principales amenazas de la inmigración irregular son:

- ✓ Amenazas a la seguridad nacional, donde puedan ingresar activos de potencias extranjeras o terroristas para el cometimiento de acciones ilícitas en suelo nacional.
- ✓ Amenaza la seguridad física de los inmigrantes, ya que son víctimas de la delincuencia y la violencia.

[25] Puede entenderse el concepto flujo migratorio como el número o la cantidad de inmigrantes que llegan o salen de los diferentes países en un plazo de tiempo inferior o igual a un año.

- ✓ Amenaza la seguridad económica de un país, puesto que no contribuyen a los sistemas de impuestos y a la economía en general.
- ✓ Amenaza la seguridad social de un país puesto que tienen acceso a los servicios sociales y pueden ser una carga para el sistema.
- ✓ Amenaza la seguridad ciudadana, puesto que, al vivir al margen de la ley, tenderán a vivir en condiciones insalubres y poco adecuadas, pudiendo ser objeto de mafias, tráfico de cualquier tipo, robos por pura necesidad para poder sobrevivir, etc.
- ✓ Amenazas en las relaciones internacionales con otros países por la presión que realicen los inmigrantes irregulares en base a su étnica, religión o esfera política.
- ✓ Amenazas en la sociedad legal del país al potenciar los fenómenos del racismo y la xenofobia en la ciudadanía, derivados de las consecuencias negativas que producen el resto de las amenazas.
- ✓ Amenazas a la salud pública por la inclusión de enfermedades ya olvidadas[26] o controladas que, debido a una falta de control médico, pudieran expandirse en la sociedad que les acoja, aunque, las causas subyacentes suelen incluir una combinación de factores como la globalización, la movilidad de la población (flujos migratorios), la falta de infraestructura sanitaria adecuada, la resistencia a los antibióticos o antimicrobianos y la evolución en relación a la mayor resistencia de los patógenos.

[26] Algunas emergencias sanitarias pasadas, además del COVID-19, referimos por su importancia: el Ébola Virus (2014-2016, 2018-2020), enfermedad viral muy grave y mortal con una alta tasa de mortalidad propiciada por la falta de infraestructura sanitaria adecuada en las regiones afectadas, así como la movilidad de las poblaciones, dificultaron los esfuerzos para contener el brote. La Gripe A (H1N1) (2009-2010), originada por una nueva cepa del virus de la gripe que surgió en 2009, la rápida propagación del virus, la falta de inmunidad de la población y la preocupación inicial sobre la gravedad de la enfermedad llevaron a una respuesta global coordinada. El Síndrome Respiratorio Agudo Severo (SARS), (2002-2003) es una enfermedad respiratoria viral causada por un coronavirus. La rápida propagación del virus debido a los viajes internacionales y la falta de protocolos de contención adecuados llevaron a una crisis sanitaria global. La Gripe Aviar (H5N1) (1997, 2003-2009), altamente patógena para las aves de corral y puede transmitirse a los seres humanos. La preocupación por la posibilidad de una pandemia mundial debido a la transmisión del virus de las aves a los humanos provocó una respuesta coordinada internacionalmente. Gripe porcina (H1N1) (1976, 2009-2010), se trata de una cepa de gripe que afecta a los cerdos y ocasionalmente puede infectar a los humanos, en el año 2009, una nueva cepa del virus de la gripe porcina causó preocupación por su capacidad para propagarse rápidamente entre los humanos. Virus del Nilo Occidental (1999-presente), se transmite principalmente a través de picaduras de mosquitos infectados. Existen brotes recurrentes en diversas partes del mundo, lo que ha generado preocupación por la salud pública y medidas de control de mosquitos. Síndrome Respiratorio de Oriente Medio (MERS) (2012-presente), causado por un coronavirus y se identificó por primera vez en Arabia Saudí en 2012, menos extendidos que el COVID-19, ha generado preocupación debido a su alta tasa de mortalidad.

El verdadero problema es no comprender la complejidad que representa la inmigración irregular desde una perspectiva superior. El conjunto de las amenazas debe comprenderse como con ámbito global, donde unas amenazas se relacionan con otras produciendo sus efectos en múltiples variables que, sin estudiarse de forma conjunta, quizás no pudiéramos identificarlos.

No podemos atacar cada una de las amenazas en solitario, porque estaremos perdiendo múltiples puntos de vista que debemos atender. Hemos identificado algunas amenazas aisladas que afectan a este fenómeno de la inmigración irregular, pero todas ellas pueden afectar a otras amenazas ya identificadas en la ESN 2021.

Una solución puede venir por garantizar una verdadera integración, todo ello partiendo de la propuesta de Bilbao, J. V., (2021) que expone que:

> La implicación de la comunidad musulmana resulta crucial en cualquier estrategia de lucha contra el terrorismo islamista radical, lo mismo que lograr estructuras resilientes entre la población a los mensajes radicalizadores de este tipo de terrorismo; siempre desde la perspectiva de igualdad en inclusión. No debemos olvidar que el objetivo último de los terroristas es provocar un estado de terror tal que derive en un enfrentamiento global entre civilizaciones. (p. 166).

Las campañas de desinformación o las injerencias de terceras partes podrían ser un ejemplo perfecto para atacar la posición de los diferentes países en el tratamiento de estas amenazas de la Inmigración ilegal. La ya compleja acción sobre esta lacra desmedida, podrás ser perfectamente utilizadas, por terceras partes para la desunión, movilización, tergiversación de cualquier acción que se quiera realizar para resolver este problema.

No es de extrañar que terceras partes quieran promover esta inmigración irregular para desestabilizar los países desde dentro. Pero no son sólo amenazas nuevas las que pueden darse internamente, las propias amenazas presentadas, pueden generar en nuevas amenazas o potenciar las anteriores. Por ejemplo, el tráfico de drogas también impactará en la salud pública, al afectar a mucha población, o a la seguridad social del estado, teniendo que invertir mucho más en poblaciones adictas, etc.

En relación a la inmigración ilegal en relación a las fronteras y a los distintos procesos de radicalización, en palabras de Bilbao, J.V, (2021), establece que:

> El terrorismo islamista radical, por internacional, es global, carece de fronteras físicas definidas, salvo las establecidas por sus propios intereses de acción, y de complejas implicaciones internacionales e históricas con un componente religioso utilizado en su ideario, por lo que las labores de inteligencia deben adquirir, buscando la anticipación, creación de escenarios buscados y la cooperación, un mayor protagonismo que otras más tradicionales o reactivas. (p. 166).

En relación a los datos estadísticos oficiales transversales con la inmigración irregular hemos de exponer que, según el último Informe quincenal de inmigración irregular, actualizado hasta el 31 de diciembre de 2022 y publicado por el Ministerio del Interior (2022):

> La inmigración irregular en España experimentó un descenso del 25,6% en comparación con el año anterior. En 2022, se registraron 31.219 llegadas de inmigrantes irregulares, en contraste con las 41.945 llegadas en 2021. Esta disminución se produce en un contexto de reformas en la política migratoria, que busca abordar los desafíos del mercado laboral y garantizar condiciones laborales adecuadas. El Real Decreto-ley 32/2021 establece un nuevo marco de contratación. A pesar de las particularidades geopolíticas, la migración sigue siendo un tema relevante en la Unión Europea. (Ministerio del Interior, 2022).

En cualquier caso, esta disminución no se corresponde con la situación actual del 2023, especialmente en el año en curso, todo ello debido a que ha sufrido un considerable aumento en relación a sus cifras. Además, la lectura que hacemos no se corresponde con las fuentes oficiales del gobierno que obvia que, aún se seguía a nivel mundial bajo la Pandemia por Emergencia Sanitaria Global por causa de la enfermedad de la COVID-19, motivo que restringió notablemente los movimientos migratorios. Precisamente la Organización Mundial de la Salud (OMS) declaró el fin de la Emergencia Sanitaria Global por la COVID-2019, el 5 de mayo de 2023, con la advertencia que la COVID-19 seguiría siendo una amenaza para la Salud Pública y que cuántas medidas higiénicas, de prevención, detección y tratamiento deberían de seguirse manteniendo.

1.12 Riesgos y Amenazas por la Inmigración Irregular.

La inmigración irregular en relación a su posible vinculación e Integración en el terrorismo internacional es, en ocasiones, un nicho de captación de los inmigrantes para convertirlos en terroristas, intensificado en los últimos años en las sociedades occidentales. Como ejemplos tenemos los atentados de EE. UU., y Madrid.

En el sentido que nos ocupa las distintas actuaciones han de dirigirse, según la ONU (2023) a:

> Aplicar y reforzar los programas de trabajo en materia de desarrollo e inclusión social en todos los niveles como fines en sí mismos, reconociendo el éxito en este ámbito, especialmente en lo relativo al desempleo de los jóvenes, podría reducir la marginación y el consiguiente sentimiento de victimización que impulsa el extremismo y el reclutamiento de terroristas. (ONU[27], 2023).

Tales aspectos han de considerar a su vez:

- ✓ Delincuencia y el crimen organizado. La desigualdad social y la falta de integración en nuestras sociedades, la cultura, son escenarios de la inclusión en estos grupos (tráfico ilegal, drogas, tráfico de armas) las organizaciones criminales transnacionales han comenzado también a nutrirse de estos mercados de inmigrantes.

- ✓ Problemas políticos con otros países. Los inmigrantes provocan presiones y problemas políticos al país en que se encuentran, con sus países de origen, mediante colonias, grupos de carácter étnico, religioso, social o cultural.

- ✓ Desajustes sociales. La estabilización de colonias en los territorios conlleva sus peculiaridades culturales, religiosas, sociales y étnicas con la problemática de falta de integración en los países de destino, incumpliendo los criterios y valores de convivencia de las sociedades nativas. Esta problemática va en aumento, puesto que van creciendo en cuanto a número y heterogeneidad.

- ✓ Problemas de racismo y xenofobia. En este caso se están dando problemas de la amenaza que en muchos países provoca la inmigración con el mercado laboral y las ayudas sociales, creándose grupos radicales de extrema derecha con fuertes episodios de violencia contra los inmigrantes.

- ✓ Amenazas sanitarias. Claro ejemplo lo hemos vivido con la enfermedad de la COVID-19, así como de expansión de otras enfermedades

- ✓ Desajustes económicos en los países receptores. Los flujos de inmigrantes producen importantes gastos en seguridad y acogida social.

[27] Extraído de la página https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy

- ✓ Desestabilización como estrategia hibrida. Los movimientos de refugiados en los conflictos como estamos viendo en la actual guerra de Ucrania, causando un problema para el resto de terceros países.

(Fernández, s.f.).

Según el CIS, (2022):

> La percepción que la sociedad española tiene actualmente sobre el fenómeno de la inmigración, ha experimentado en los dos últimos años un aumento considerable, más en contra que a favor. Una mayoría de la ciudadanía española, el (53,3%) piensa que hay un exceso de inmigrantes, más de 22 puntos sobre el año 2000 que era del (31,3%). Referente a las políticas a seguir, un 85% de los españoles consultados piensa que se debería pedir un contrato de trabajo, con respecto al año 2000 esta opinión ha aumentado un 15%.

La inmigración ilegal es un problema cuya solución pasa por una estrategia a nivel global, precisamente debido a su interrelación entre la mayoría de amenazas y que afecta a la economía, la educación, la vida social, la inseguridad. Son necesarias actuaciones policiales, judiciales, políticas de integración y educativas, en conjunto con toda la sociedad, para evitar efectos llamada y reducir la llegada de inmigración irregular. Todo ello para establecer líneas que mejoren la inmigración regular, la seguridad y con ello la estabilidad social y económica.

La inmigración irregular produce una grave amenaza que llega a desestabilizar a los distintos países receptores.

Tiene un claro objetivo de desestabilización, temor y de amenaza para los distintos países, en los que las distintas rutas y flujos de inmigración irregular contribuyen notablemente al incremento de ese temor por parte de los estados receptores.

La llegada masiva de inmigración irregular a un Estado produce una alarma social y muchos prejuicios a la sociedad que acoge a los inmigrantes. Pero, si existe un elemento que debemos tener muy especialmente en cuenta, es el de la utilización de la inmigración irregular por parte de grupos terroristas que operan sobre todo en el Sahel[28] para introducir en Europa terroristas camuflados, que llegan principalmente en pequeñas embarcaciones a las costas de España, o

[28] El Sahel, una región semiárida que atraviesa África desde el océano Atlántico hasta el mar Rojo, juega un papel crucial en la inmigración irregular hacia Europa, incluida España como su frontera sur de la Unión Europea.

bien intentan traspasar conocidas fronteras de Ceuta y Melilla saltando las vallas fronterizas delimitadoras.

La utilización de la inmigración irregular ha servido como nicho de captación de terroristas y que han sido utilizados para acometer sus acciones. Grupos tales como *DAESH*, a través de Grecia.

Gracias a los Servicios de Inteligencia franceses, se pudo alertar al resto de países de la Unión Europea. Sin embargo, no siempre es posible, como, por ejemplo, el caso del Brahim Aoussaoui, autor de los asesinatos con múltiples víctimas en la basílica de Niza, que se había adentrado por la conocida Isla de Lampedusa, en la que desembarcó con un número importante de personas de origen norteafricano con los que cometió tan execrable crimen.

En los últimos meses, se ha constatado por parte de las Fuerzas y Cuerpos de Seguridad del Estado, de nuestro país que de entre las personas que intentan acceder a nuestras fronteras, se encontraban individuos que provienen de la zona del Sahel de una gran corpulencia física, con gran agilidad, con cualidades de manejo de determinadas armas blancas o de diferentes instrumentos de ataque a la Policía Nacional o la Guardia Civil y donde se puede definir que tiene una preparación militar o paramilitar.

Según Loader, (2022):

> Respecto a la inmigración irregular, los problemas se definen claramente desde una perspectiva orientada a la seguridad. Por eso, las soluciones son un imperativo y no una opción.

Tras la última modificación de la Ley de Extranjería en España, a través de la promulgación y publicación del Real Decreto 629/2022, de 26 de julio, del 2022, en la exposición de motivos se recoge que:

> (…) una política migratoria eficaz constituye un activo de gran relevancia a la hora de maximizar el impacto positivo y los efectos de la movilidad humana internacional en economías interdependientes, apostando por potenciar la ejecución de planes de recuperación, transformación y resiliencia.

En el ámbito de la Unión Europea se han desarrollado legislación, tales como la directiva UE 2002/90 respecto a la entrada, circulación y estancia de inmigrantes irregulares a través de políticas sociales y, también, sanciones.

El objetivo europeo con relación de fronteras se centra en la gestión de los estados como garantía de crear un entorno en el que la libertad, seguridad y justicia garantice el orden político y la paz social del entorno de la Unión Europea.

En este sentido hemos de destacar el Reglamento UE 2019/196, de 13 de noviembre de 2019, sobre la Guardia Europea de Fronteras y Costas recoge y estable los cometidos de la denominada FRONTEX (Agencia Europea de la Guardia de Fronteras y Costas).

Para Mora, B. (2021):

> El terrorismo religioso islamista ha ido en aumento en los últimos años como contrapunto al poder de Estados Unidos en la Guerra Fría. El Sahel es uno de los escenarios predominantes de estas actividades, ya que es una zona con inestabilidad político-económica preexistente que los terroristas han aprovechado. El terrorismo está cambiando sus formas de actuar, mostrando su adaptabilidad en términos de geografía, métodos de actuación y adquisición de recursos. Francia ha demostrado ser el líder de la iniciativa occidental en la región y ha hecho progresos en la misma. Sin embargo, Occidente, especialmente los países europeos, deben empezar a prestar más atención a las causas de los problemas de esta región, recopilando datos y conociendo su realidad. Sólo entonces podrán abordar estos problemas con eficacia, ayudando a las instituciones autonómicas existentes, buscando soluciones a largo plazo que satisfagan a la población.

1.13. La Seguridad y la Protección en España como respuesta coordinada frente al Terrorismo.

España ha implementado varios mecanismos, estrategias y líneas de acción para prevenir y protegerse de acciones terroristas de cualquier índole, incluido el *yihadismo* o el conocido como Terrorismo de corte *Yihadista*. Para ello ha diseñado un marco legal robusto con la promulgación de leyes antiterroristas para combatirlo, además del establecimiento de mecanismos para la coordinación y cooperación internacional, lo que incluye el intercambio de información y la cooperación en investigaciones conjuntas, además de la estrecha colaboración entre los distintos cuerpos policiales. De la misma manera, nuestro país ha implementado programas de prevención y des radicalización destinados a detectar y abordar el proceso referenciado, así como fortalecido el proceso de inteligencia y vigilancia para la obtención de la información precisa frente a este tipo de amenazas.

1.13.1 El Departamento de Seguridad Nacional (DNS).

El Departamento de Seguridad Nacional en España es una institución encargada de coordinar y dirigir las políticas de Seguridad Nacional del país. Fue creado para hacer frente a las amenazas y riesgos que puedan afectar a la seguridad de España y de los españoles tanto en el ámbito nacional como internacional.

El Departamento de Seguridad Nacional se estableció en 2013, mediante la Ley 36/2015, de 28 de septiembre. La referenciada ley establece que el departamento tiene como objetivo la planificación, dirección y coordinación de las políticas de Seguridad Nacional, así como la evaluación y gestión de los riesgos y amenazas que puedan surgir.

Depende directamente del Presidente del Gobierno de España y tiene como principal fin la protección de los intereses de España, la integridad territorial del estado, la estabilidad, así como el bienestar de nuestra sociedad.

Algunos de los aspectos de especial consideración y relevancia del ámbito competencial más trascendentes del DNS son la elaboración de la Estrategia de Seguridad Nacional, la coordinación de cuántos aspectos sea necesarios en materia de Seguridad Nacional, la identificación, el análisis, evaluación de riesgos y amenazas, así como la cooperación internacional en materia de seguridad.

1.13.2 La Estrategia de Seguridad Nacional:

La Estrategia de Seguridad Nacional es un documento de gran importancia que establece los objetivos, así como las distintas líneas de acción en materia de seguridad nacional en España. Su finalidad es identificar, abordar los diferentes riesgos y amenazas que puedan afectar a la seguridad de nuestro estado y de la ciudadanía.

La Estrategia de Seguridad Nacional se elabora y coordina por el Departamento de Seguridad Nacional, órgano dependiente de la Presidencia del Gobierno de España.

Tiene como objetivo principal poder garantizar la protección de todos los intereses nacionales, en relación con la integridad territorial del estado, su estabilidad y el bienestar de la sociedad de nuestro país.

En la Estrategia se realiza un análisis y ulterior evaluación de los diferentes riesgos y amenazas en atención a su heterogénea tipología que afectan a España, tanto en aquellas materias que afectan interna como externamente.

Además, se establecen los principales ámbitos de actuación, como cuantas cuestiones afectan la ciberseguridad, la lucha contra el terrorismo en cualquiera de sus manifestaciones y tipologías, así como la protección de Infraestructuras Críticas independientemente del sector en la que se incardinen, así como la gestión eficaz de cuantas crisis que puedan producirse en nuestro estado.

La Estrategia de Seguridad Nacional también fomenta la cooperación y colaboración tanto a nivel nacional como internacional. Busca fortalecer las alianzas con otros países y organismos internacionales para hacer frente a los desafíos globales y comunes en materia de seguridad, tanto en sus aspectos preventivos, como reactivos y correctivos.

1.13.3 Estrategia Nacional contra el Terrorismo (ENT).

La Estrategia Nacional contra el Terrorismo (ENT) consiste en la elaboración e implementación de un plan integral que tiene como finalidad prevenir, combatir, neutralizar y mitigar la amenaza del terrorismo en España. Se basa en un enfoque con múltiples prismas que abarca aspectos relacionados con la seguridad, la prevención, la persecución judicial, la protección de las víctimas, así como el establecimiento de las adecuadas sinergias para la cooperación internacional.

La ENT se desarrolla bajo la dependencia y coordinación del Ministerio del Interior de nuestro país, busca poder garantizar la seguridad de la sociedad Española, preservar la convivencia democrática y proteger los valores fundamentales del Estado de Derecho frente a cualquier forma de terrorismo que pueda sucederse.

Entre los principales pilares de la Estrategia Nacional contra el Terrorismo se encuentran:

1. Prevención y disuasión del terrorismo: se busca evitar y prevenir la radicalización, captación o el «reclutamiento» de individuos por parte de grupos o células terroristas, así como promover la detección temprana de posibles amenazas y la colaboración ciudadana en la lucha contra el terrorismo.
2. Persecución judicial y desarticulación de organizaciones terroristas: se promueve la cooperación entre las distintas Fuerzas y Cuerpos de Seguridad, así como los servicios de inteligencia para investigar, desmantelar, neutralizar y poner a disposición de la justicia a los responsables de las distintas acciones y actividades de índole terrorista.
3. Protección de Infraestructuras Críticas: se establecen las adecuadas y pertinentes medidas de seguridad y protección, tanto de carácter general como específicas para

salvaguardar la integridad y adecuado funcionamiento de las Infraestructuras Críticas del país, como aeropuertos, centrales nucleares o sistemas de transporte, centros hospitalarios, etc., frente a posibles acciones terroristas.

4. Atención y apoyo a las víctimas del terrorismo: se presta asistencia y apoyo integral, con un enfoque multidisciplinar y global a las víctimas del terrorismo, ya sea desde el punto de vista emocional, así como en términos de reparación, justicia y memoria.
5. Cooperación internacional: se promueve la colaboración y el intercambio de información con terceros países y organismos internacionales para acometer de manera funcional, conjunta y coordinada la amenaza terrorista, así como participar en iniciativas, foros y acuerdos internacionales en esta materia antiterrorista.

La Estrategia Nacional contra el Terrorismo se revisa y actualiza periódicamente para adaptarse a las nuevas formas de terrorismo y a los cambios en el entorno de seguridad nacional.

1.13.4 Plan de Prevención, Protección y Respuesta Antiterrorista (PPPyRA[29]).

El Plan de Prevención, Protección y Respuesta Antiterrorista es un instrumento de marcado carácter estratégico que tiene como finalidad establecer las directrices y medidas necesarias de actuación para prevenir y hacer frente a la amenaza terrorista en nuestro país. Este plan se encuadra dentro de la Estrategia Nacional contra el Terrorismo y se actualiza de manera periódica para adaptarse a las nuevas formas de terrorismo, así como a los cambios que puedan existir en la situación actual de Seguridad Nacional.

El PPPyRA se basa en la cooperación y coordinación entre los diferentes actores involucrados, como las Fuerzas y Cuerpos de seguridad del Estado, la Comunidad de inteligencia y, en especial, los servicios de inteligencia, las autoridades autonómicas y locales, así como otros organismos relacionados con la seguridad.

Es importante destacar que el plan se adapta constantemente a las nuevas formas de terrorismo y a los cambios en la situación de seguridad, con el objetivo de garantizar una respuesta pragmática, efectiva y proporcionada ante cualquier tipo de amenaza terrorista.

El Plan de Prevención y Protección Antiterrorista establece las directrices generales que, parte de un esfuerzo permanente en el ámbito de la prevención, que permite asegurar la detección, seguimiento, análisis y evaluación, planificación continuada del riesgo de atentado

[29] Su última revisión y actualización fue en febrero del pasado año 2023.

terrorista, así como la puesta en marcha y coordinación de los dispositivos de carácter preventivo en caso necesario, que pueden entenderse como el conjunto de acciones llevadas a cabo con anterioridad a que se materialice una acción terrorista con el objetivo de evitar su materialización y consecuentemente los efectos y la severidad del daño.

En palabras de González, M. (2023):

> Ha de subrayarse por su importancia que, en el momento actual, nos encontramos en un nivel de Alerta Antiterrorista (NNA) 4 reforzado del Plan de Prevención, Protección y Respuesta Antiterrorista que el Gobierno Central, a través del Ministerio del Interior recientemente actualizado y que se ha implementado. (p. 83).

1.13.5 Nivel de Alerta Antiterrorista (NAA):

Consiste en una escala compuesta por varios niveles que se complementan, cada uno de los cuales se encuentra asociado a un grado de riesgo, en función de la valoración de la amenaza terrorista que se aprecie en cada momento. No es necesaria que se active de manera secuencial, cualquier acción puede activar un Nivel de Alerta Superior en atención a la criticidad del riesgo terrorista. La clasificación prevista en el Plan de Prevención, Protección y Respuesta Antiterrorista cuenta con cinco niveles de activación, es decir, es una escala «penta» asociada a un determinado nivel de riesgo: el Nivel 1 corresponde a riesgo bajo, el Nivel 2 a riesgo moderado, el Nivel 3 a riesgo medio, el Nivel 4 a riesgo alto y el Nivel 5 a riesgo muy alto.

Figura 3

Nivel Alerta Antiterrorista. Fuente: Ministerio del Interior.

Es importante destacar que en ocasiones no se activa un Nivel de Alerta Antiterrorista tan sólo por cuestiones políticas con el objeto de no generar alarma social y generar el ya

denominado concepto a la población de lo que se denomina Seguridad aparente, estas cuestiones o que realmente hacen es evitar que se adopten las medidas de seguridad y autoprotección necesarias, así como la adecuada información y formación a la sociedad sobre cómo tendría que procederse en una situación de emergencia provocada por cualquier acción terrorista.

En el sentido de lo expuesto y Según González, M. (2023) destaca que:

> El Gobierno para evitar y no generar la alarma social y no activar el nivel 5, con las implicaciones en cuanto a la protección de las distintas Infraestructuras Críticas por parte del ejército, activó el nivel 4 con la coletilla de «reforzado». (P. 83).

Figura 4

Nivel Actual de Alerta Antiterrorista. Fuente: Ministerio del Interior.

1.13.6 El Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC):

El Centro Nacional para la Protección de Infraestructuras Críticas es un organismo creado con el objetivo de garantizar la seguridad y protección de todas y cada una de las Infraestructuras Críticas de nuestro estado. Se estableció en el año 2005, y posteriormente fue amparado por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas.

El CNPIC se integra en la estructura del Ministerio del Interior, y directamente de la Secretaría de Estado de Seguridad, tiene como finalidad identificar, analizar, evaluar y planificar los distintos riesgos que afectan a las Infraestructuras Críticas del país, así como establecer medidas de protección y coordinar la respuesta en caso de incidentes o amenazas.

El CNPIC trabaja en estrecha colaboración y coordinación con otros organismos y entidades involucradas en la protección de Infraestructuras Críticas, así como las distintas Fuerzas y Cuerpos de Seguridad, los operadores críticos de las distintas infraestructuras, los organismos reguladores y otros organismos de carácter nacional e internacional.

1.13.7 Esquema Nacional de Seguridad (ENS):

El Esquema Nacional de Seguridad es un marco normativo y estratégico establecido en nuestro estado con el objeto de garantizar la seguridad de la información en el ámbito de la Administraciones Públicas.

Fue modificado y actualizado en el año 2022 a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Su modificación se realizado con el objeto de fortalecer de manera urgente las distintas capacidades de defensa ante las actuales ciberamenazas, tanto en el ámbito de las Administraciones públicas, como de aquellas entidades o empresas privadas que participen en la prestación de servicios de cualquier índole a las distintas Administraciones Públicas (AA.PP.).

El objetivo principal del ENS es establecer las políticas y medidas de seguridad que deben aplicarse en los sistemas y servicios de información utilizados por las administraciones públicas para proteger la confidencialidad, integridad y disponibilidad de la información que manejan.

El ENS se basa en los principios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y calidad en la gestión de la seguridad de la información. Establece una serie de requisitos técnicos y organizativos que deben ser cumplidos por los responsables de los sistemas de información en la Administración Pública.

El cumplimiento del Esquema Nacional de Seguridad es obligatorio para las administraciones públicas y se considera una herramienta fundamental para garantizar la protección de la información en el ámbito de la Administración Pública, así a cuantas empresas u organismos trabajen para las distintas Administraciones Públicas (AA.PP.).

Además de todas las cuestiones reseñadas, es importante referenciar que nuestro país ha diseñado, elaborado e implementado el Plan Estratégico Nacional de Lucha contra la

Radicalización Violenta (PEN-LCRV), que la Secretaría de Estado de Seguridad, a través del CITCO[30], (2015), define su objetivo como un:

> (…) instrumento eficaz de detección temprana y neutralización de los brotes y focos de radicalismo violento, actuando sobre aquellas comunidades, colectivos o individuos en situación de riesgo o vulnerabilidad. (Art. 2.1).

La relación de las distintas organizaciones de nuestro estado para luchar contra el terrorismo se hace necesaria, como también es necesaria la prevención del terrorismo de cualquier tipo y, especialmente el de corte *yihadista* a través de la inteligencia[31] y sus distintos tipos de fuentes, en las que la totalidad de la Comunidad de Inteligencia (CI), así como los Servicios de Inteligencia es trascendental para prevenir sus actos y, consecuentemente los efectos devastadores del daño que pueda desprenderse por la materialización del riesgo. Por lo tanto, enfrentar el fenómeno terrorista requiere un enfoque multidisciplinar que combine diferentes tipos de inteligencia para comprender las motivaciones, identificar amenazas, desarrollar estrategias efectivas y garantizar el respeto por los derechos humanos y las leyes internacionales, además y en palabras de Valverde, A. (2021):

> La respuesta eficiente, a la dimensión de la referida amenaza pasa por cimentar una coordinación real y basada en un criterio único que permita aglutinar todos los esfuerzos que hoy se encuentran diseminados en administraciones centrales, autonómicas y municipales.

[30] Acrónimo que hace referencia al Centro de Inteligencia contra el Terrorismo y Crimen Organizado.

[31] Inteligencia de Fuentes Humanas (*HUMINT*): esta proviene de las fuentes humanas, es decir, de las personas con información que actúan como informantes, agentes encubiertos, prisioneros capturados, desertores u otros individuos que proporcionan información sobre las actividades terroristas, sus planes, estructuras organizativas y recursos. Inteligencia de Señales (*SIGINT*): se refiere a la interceptación y análisis de señales electrónicas, como comunicaciones telefónicas, correos electrónicos, mensajes de texto, comunicaciones por radio, etc. estas fuentes pueden proporcionar información sobre la planificación y ejecución de actividades terroristas. Inteligencia de Imágenes (*IMINT*): involucra la recolección y análisis de imágenes satelitales, fotografías aéreas y otras imágenes para identificar ubicaciones, movimientos de personal, estructuras y actividades relacionadas con el terrorismo. Inteligencia de Fuentes Abiertas (*OSINT*): se basa en información disponible públicamente, como sitios web, redes sociales, informes *de* noticias, blogs y otros medios de comunicación. Esta fuente puede proporcionar información sobre reclutamiento, propaganda, financiamiento y otros aspectos del terrorismo. Inteligencia de Medios (*MEDINT*): implica el análisis de información obtenida de medios de comunicación convencionales y redes sociales para comprender la opinión pública, la narrativa y la percepción del terrorismo tanto a nivel nacional como internacional. Inteligencia de Finanzas (*FININT*): se centra en el seguimiento de flujos financieros y actividades económicas asociadas con el financiamiento del terrorismo, como el lavado de dinero, el contrabando y otras transacciones ilícitas. Inteligencia Cibernética (*CYBINT*): se refiere a la recopilación y análisis de datos digitales, incluidos ataques cibernéticos, actividad en línea de grupos terroristas, reclutamiento en línea y propaganda en *Internet*.

Simultáneamente a Planes Estratégicos, a multitud de esfuerzos por parte de diversas administraciones y servicios, se debe cimentar un instrumento aglutinador y eficiente; capaz de hacer frente a una amenaza real imprevisible, de orígenes tan estructurados, y de alcances inciertos. Un organismo estatal amparado por los siguientes cimientos:

-Una declaración parlamentaria de interés para la seguridad nacional. Apoyada por una legislación normativa que obligue a la colaboración forzosa con dicho organismo en cualquier ámbito de las administraciones públicas y regulando la obligada colaboración de las privadas.

- Con ámbito nacional y presencia efectiva en cada administración estatal, autonómica o local.

- Con una dirección cimentada en la inteligencia y con representación paritaria de todos los servicios y FFCCSS, así como organismos involucrados.

-Con la dotación presupuestaria suficiente y los recursos humanos y materiales acordes a las dimensiones del objetivo.

(p. 154).

Como puede observarse, la respuesta coordinada en la lucha contra el terrorismo en España se aborda de manera integral y coordinada entre diferentes niveles de gobierno. Aunque el Estado español tiene un papel central, no se trata de un monopolio exclusivo. Todo ello en atención a los siguientes puntos clave que exponemos a continuación:

1. Estrategia Nacional Contra el Terrorismo: la Estrategia Nacional Contra el Terrorismo establece los objetivos y principios para combatir el terrorismo. Aunque el Estado Central lo lidera, involucra indefectiblemente a las restantes Comunidades Autónomas, así como a las corporaciones locales.

2. Colaboración y Coordinación: las administraciones autonómicas y locales colaboran con el Estado en la prevención, protección y persecución del terrorismo. Cada nivel de gobierno tiene competencias específicas, y la cooperación es esencial para abordar eficazmente esta amenaza.

3. Adaptación Estratégica: la lucha contra el terrorismo debe adaptarse a una realidad cambiante. Como hemos podido comprobar, la Estrategia Nacional se ha de ajustar a los distintos cambios geoestratégicos, así como al resto de las amenazas emergentes.

4. Seguridad Nacional: por lo tanto, la seguridad nacional es un objetivo compartido, pero no sólo con el resto de las administraciones del estado referenciadas, sino que también integra al sector privado, así como a otros actores de la sociedad civil.

   Aunque el Estado español desempeña un papel central, la colaboración y la coordinación entre diferentes niveles de gobierno son esenciales para enfrentar eficazmente el terrorismo y garantizar la seguridad de la sociedad.

Consideramos que, una ley de mínimos o bien una ley de armonización en relación con la seguridad y la protección integral en el Estado español, que abarque todas las administraciones (estatales, autonómicas y locales), puede lograr varios objetivos importantes, en relación a la ley de mínimos serían:

1. Estándares básicos de seguridad: establece normas y protocolos mínimos que todas las administraciones deben seguir para garantizar un nivel básico de seguridad y protección para todos los ciudadanos, independientemente de su ubicación dentro del país.

2. Coordinación entre administraciones: promueve la coordinación y cooperación entre las diferentes administraciones (estatales, autonómicas y locales) para garantizar una implementación coherente de las medidas de seguridad en todo el territorio nacional. Esto incluye compartir información, recursos y mejores prácticas para mejorar la eficacia de las políticas de seguridad.

3. Claridad en las competencias: define claramente las responsabilidades y competencias de cada nivel de gobierno en materia de seguridad y protección integral, evitando superposiciones o vacíos legales que puedan dificultar la aplicación efectiva de las políticas de seguridad.

4. Equidad y acceso uniforme: garantiza que todos los ciudadanos, independientemente de su lugar de residencia, tengan acceso equitativo a medidas de seguridad y protección integral. Esto asegura que ninguna región quede desprotegida o desatendida en términos de seguridad pública.

5. Flexibilidad y adaptabilidad: aunque establece estándares mínimos, permite cierta flexibilidad para que las administraciones autonómicas y locales adapten las medidas de seguridad según las necesidades y realidades específicas de sus territorios, siempre y cuando cumplan con los requisitos mínimos establecidos por la ley.

Por lo tanto, una ley de mínimos en relación con la seguridad y la protección integral en el Estado español, que involucre a todas las administraciones, podría tener como objetivo principal establecer un marco legal coherente y coordinado que garantice un nivel básico de seguridad y protección para todos los ciudadanos, al tiempo que permite cierta adaptabilidad a las particularidades

En relación a una ley de armonización en cualquier materia referida a la seguridad en general, incluyendo la seguridad nacional y el terrorismo en particular, con todas las administraciones del Estado, puede lograr varios objetivos clave:

1. Coherencia normativa: establece un marco legal coherente y uniforme en toda España en lo que respecta a la seguridad nacional y la lucha contra el terrorismo. Esto garantiza que las leyes y políticas relacionadas con la seguridad sean aplicadas de manera consistente en todo el territorio nacional.

2. Coordinación interadministrativa: promueve la coordinación y cooperación entre todas las administraciones del Estado español (estatales, autonómicas y locales) en la formulación e implementación de estrategias de seguridad. Esto incluye compartir información, recursos y buenas prácticas para abordar de manera efectiva las amenazas a la seguridad.

3. Clarificación de competencias: define claramente las responsabilidades y competencias de cada nivel de gobierno en materia de seguridad nacional y lucha contra el terrorismo. Esto evita duplicaciones de esfuerzos y asegura una distribución eficiente de recursos para enfrentar estas amenazas.

4. Intercambio de información: facilita el intercambio de información entre las diferentes administraciones para mejorar la capacidad de detección, prevención y respuesta ante amenazas terroristas y otras formas de violencia.

5. Fortalecimiento de la seguridad nacional: contribuye al fortalecimiento de la seguridad nacional al garantizar una respuesta unificada y coordinada ante amenazas internas y externas, preservando la integridad territorial y la seguridad de los ciudadanos.

6. Adaptabilidad y flexibilidad: aunque busca establecer un marco legal uniforme, también puede permitir cierta flexibilidad para que las administraciones autonómicas y locales adapten las medidas de seguridad según las necesidades específicas de sus

territorios, siempre y cuando se respeten los principios y objetivos establecidos por la ley de armonización.

En el sentido expuesto, por tanto, una ley de armonización[32] en materia de seguridad nacional y lucha contra el terrorismo con todas las administraciones del Estado español buscaría garantizar una respuesta integral y coordinada ante las amenazas a la seguridad, promoviendo la coherencia normativa, la coordinación interadministrativa y el intercambio de información para proteger la integridad y la seguridad de todos los ciudadanos.

En el contexto legal español, una ley de mínimos y una ley de armonización son dos tipos de legislaciones que buscan abordar cuestiones similares, pero con enfoques distintos. Sus principales elementos diferenciadores a nuestro juicio serían:

1. Objetivo principal:

   - ✓ Ley de mínimos: su principal objetivo es establecer un conjunto básico de normas que deben ser cumplidas como mínimo por todas las entidades territoriales (como comunidades autónomas o municipios). Esta ley fija un umbral mínimo que todas las partes deben alcanzar, permitiendo a las entidades legislar y aplicar medidas que excedan esos mínimos.

   - ✓ Ley de armonización: se centra en garantizar la coherencia y uniformidad en la aplicación de normativas entre diferentes entidades territoriales. Su objetivo principal es coordinar las normativas y prácticas entre las distintas regiones para evitar discrepancias y conflictos en la interpretación y aplicación de la ley.

2. Flexibilidad:

   - ✓ Ley de mínimos: ofrece cierta flexibilidad a las entidades territoriales para adaptar las normas básicas a sus necesidades específicas, permitiéndoles legislar y aplicar medidas que superen los mínimos establecidos.

[32] Máxime cuando «La Seguridad Pública es competencia exclusiva del Estado». En el sentido expuesto hay que estarse a lo que define la propia Ley Orgánica de Fuerzas y Cuerpos de Seguridad, LFFCCSS, (1986), cuyo tenor literal recoge:

> Su mantenimiento corresponde al Gobierno de la Nación. Las Comunidades Autónomas participarán en el mantenimiento de la Seguridad Pública en los términos que establezcan los respectivos Estatutos y en el marco de esta Ley. Las Corporaciones Locales participarán en el mantenimiento de la seguridad pública en los términos establecidos en la Ley Reguladora de las Bases de Régimen Local y en el marco de esta Ley. El mantenimiento de la Seguridad Pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad. (Art. Primero, 1-4, p. 12).

- ✓ Ley de armonización: busca reducir la variabilidad normativa entre las diferentes regiones, promoviendo la uniformidad y coherencia en la aplicación de la ley. Puede limitar la autonomía legislativa de las entidades territoriales al imponer ciertos estándares comunes.

3. Alcance:

- ✓ Ley de mínimos: establece los mínimos necesarios para garantizar la protección de ciertos derechos o la prestación de servicios básicos, como la seguridad ciudadana o la protección ambiental.

- ✓ Ley de armonización: busca coordinar normativas específicas en áreas como la seguridad, el medio ambiente, la sanidad, entre otras, con el fin de evitar disparidades normativas y garantizar la coherencia en la aplicación de la ley en todo el territorio nacional.

Por lo tanto y a modo de conclusión, mientras que una ley de mínimos establecería estándares mínimos que deben ser cumplidos por todas las entidades territoriales, una ley de armonización busca coordinar normativas entre las diferentes regiones para garantizar la coherencia y uniformidad en la aplicación de la ley en todo el país. Bajo nuestro punto de vista, entendemos que una ley de armonización, en relación con la calidad lo que prima es «la autorregulación regulada».

Consideramos por tanto que, el establecer unos objetivos mínimos para la búsqueda de la excelencia con la realización de una ley de mínimos para que, de esa manera, cada comunidad vaya a más, en materia de seguridad, se ha demostrado que las Comunidades Autónomas han hecho más avances en determinados ámbitos en la búsqueda de la excelencia y que, esos modelos cuando se han comprobado como funcionales y eficientes, se han replicado en otras Comunidades Autónomas de nuestro estado.

En este sentido, se pueden establecer ciertos controles por parte de las distintas comunidades autónomas que podrían ser el empuje que necesitan para un mayor avance en la propia legislación estatal en la carrera por la excelencia en materia de seguridad, sin temores a la experimentación en materia que nos compete, todo ello porque el mejor laboratorio, si se nos permite el símil, son las administraciones locales o las propias comunidades autónomas para, posteriormente, en relación a ensayo experiencia, error, ensayo y éxito, replicar el modelo o en el resto del estado.

Hemos de destacar como argumento a lo anteriormente expuesto que, la Cátedra Manuel Balbé[33] de la Universidad Autónoma de Barcelona defiende, en palabras de Balbé, J., (2006) que, «la competencia entre el Estado y las Comunidades Autónomas puede conllevar una mejora en los distintos procesos por emulación de la calidad».

[33] La Cátedra Manuel Ballbé de Seguridad Humana y Derecho Global se crea con el propósito de dar continuidad al trabajo y pensamiento del Dr. Manuel Ballbé en el área del Derecho. Su legado supone una gran aportación a la regulación global orientada a garantizar la Seguridad Humana con una visión preventiva, transversal, integral e integradora. En palabras suyas: «La nueva Sociedad del Riesgo» trae esta nueva concepción de la seguridad: la protección integral en todos los campos donde se detecta un riesgo o un peligro para el ciudadano.

RESUMEN DEL CAPÍTULO.

La pertinencia del presente capítulo se hace necesaria por ser el terrorismo un elemento de estudio que se recoge en la presente investigación. La legislación en materia de Protección de Infraestructuras Críticas surge precisamente contra el riesgo terrorista.

Se ha constatado a lo largo del presente capítulo la dificultad de llegar a un consenso en la utilización y definición del término Terrorismo de manera unánime, a pesar de lo que se ha realizado una definición de autores que nos parecen de relevancia como estudiosos y expertos del fenómeno terrorista, al igual que distinguir de manera clara vocablos como terror y terrorismo.

Recoge el presente capítulo además otras breves definiciones de términos íntimamente relacionados con el terrorismo tales como inteligencia, contrainteligencia, ciberinteligencia, ciberterrorismo y *Yihadismo*.

Además de la concepción terminológica se incluye la definición legal en atención a nuestro vigente Código Penal.

Se incluye todas las organizaciones e instituciones que el Estado Español tiene para prevenir el fenómeno terrorista, con sus competencias básicas.

CAPÍTULO II

Infraestructuras Críticas

«**Nunca interrumpas a tu enemigo cuando está cometiendo un error**».
Napoleón Bonaparte

CAPÍTULO II

2. CAPÍTULO II. INFRAESTRUCTURAS CRÍTICAS.

De manera genérica, las Infraestructuras Críticas son sistemas, instalaciones y servicios fundamentales para el funcionamiento de una sociedad y la economía de un país. Estas infraestructuras son esenciales para garantizar la seguridad, el bienestar y el funcionamiento continuo de cualquier estado.

2.1. INTRODUCCIÓN AL CAPÍTULO.

Se hace necesario para la adecuada comprensión de las Infraestructuras Críticas realizar la adecuada retrospección histórica desde su origen hasta la actualidad, con el objeto de entender el origen de toda la legislación específica y conocer su especial importancia.

Es en el año 2001, concretamente a los atentados del 11-S[34,] perpetrados por una célula *yihadista* del Grupo Terrorista *Al-Qaeda*, que puso en jaque a la sociedad y al Gobierno de los Estados Unidos de América. La acción terrorista no fue de carácter indiscriminada, se sabía exactamente los objetivos que tenían que ser atacados, la planificación de tales acciones es patente. Los objetivos marcados, el Capitolio, el Pentágono, las Torres Gemelas, que, a su vez, representó un ataque a los iconos de la sociedad estadounidense.

Los ataques sufridos por los EE.UU., fue el precedente de la Guerra de Afganistán, y EE.UU. declaró la guerra contra el terrorismo conjuntamente con Inglaterra y España como aliados.

Además de las numerosas víctimas mortales y los miles de heridos ha de destacarse que, el ataque contra el del *World Trade Center*, supuso, además, una importante recesión económica en la sociedad norteamericana, todo ello a la par de la pérdida de confianza del pueblo norteamericano en sus administraciones. Hizo que el pueblo se sintiera inseguro y desprotegido ante el nuevo fenómeno terrorista de corte *Yihadista*.

Todas estas cuestiones que se apuntan, tales como la pérdida de confianza del gobierno, (George Bush perdió las elecciones), los fallecidos, heridos y damnificados, los residuos después de la acción terrorista con el desprendimiento de las Torres Gemelas y las secuelas respiratorias y pulmonares que han generado a multitud de personas, la recesión económica

[34] Referenciados con mayor detalle en el Capítulo 1 de la presente investigación.

posterior a los atentados, así como la desconfianza por parte de la población, es lo que se conoce en España, en relación a la legislación específica en materia de Protección de Infraestructuras Críticas, como Criterios Horizontales de Criticidad, es decir, son los distintos parámetros en función de los cuales se determina la gravedad y las consecuencias de la perturbación o destrucción de una Infraestructura Crítica y, que han de ser evaluados en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves o muy graves, así como las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas, así como el deterioro de productos o servicios.

3. El impacto medioambiental, degradación del lugar o de sus alrededores, es decir el área de influencia.

4. El impacto sociopolítico, por la incidencia en la desconfianza de la población en cuanto a la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de los servicios esenciales.

Tras los atentados sufridos en el corazón económico de los Estados Unidos, comienza el país a legislar y establece 16 sectores a proteger y, en especial con las Infraestructuras Críticas.

Precisamente y tras los atentados del 11 de septiembre y según Villena, J. (2021):

> Las medidas técnicas y procedimentales adoptadas en los aeropuertos se hacen más evidentes. Desde la OACI se exige la inspección al 100% del pasajero, personal y equipajes. También como consecuencia del intento de atentado de Richar Reid, en el que llevaba un explosivo en la suela falsa de sus deportivas, se exigió el descalzarse en los aeropuertos y se implementaron los arcos detectores de metal en el calzado. (p. 103).

Europa aún no era consciente de la magnitud y el calado de los ataques, hasta que, en el 11 de marzo del año 2004, con el atentado sufrido en Atocha, Madrid, con la gran cantidad de víctimas fallecidas y heridas, de manera similar a lo que pasó en EE.UU, salvando las lógicas diferencias, además de la pérdida de confianza de la población al Gobierno Central, en aquella

época presidido por José María Aznar, la población estigmatizó al colectivo musulmán, además de la percepción colectiva de la gran sensación de inseguridad en la sociedad española.

Posteriormente, El Consejo de Europa encargó a la Comisión la elaboración de un programa relacionado con la Protección de las Infraestructuras Críticas, ese programa es el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC). La comisión elaboró el Libro Verde, como hoja de ruta relacionada para la Protección de las Infraestructuras Críticas en la Unión Europea.

A continuación, se crea una Red de Alerta Temprana en relación a las I.C. llamada CIWIN. A raíz de todo esto, por la especial importancia para la Seguridad Nacional y de manera coetánea con las actuaciones llevadas a cabo por la Unión Europea, España elabora en el año 2005, El Plan de Prevención y Protección Antiterrorista (PPPA)[35]. A raíz de su elaboración se le encomienda por parte del Ministerio del Interior a la Policía Nacional y a la Guardia Civil como integrantes de las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSSE), la elaboración de unos listados de aquellas infraestructuras en el ámbito de sus distintas demarcaciones, puedan ser susceptibles de ser atacadas por terroristas. Esos listados posteriormente dieron lugar, posteriormente a lo que se conoce como Catálogo Nacional de las Infraestructuras Estratégicas.

En el año 2005, en Inglaterra, se sucede otra serie de atentados terroristas contra la línea de metro, así como de autobuses, tuvo su eco en el seno de la Unión Europea concienciándose de la nueva era, en la que la amenaza terrorista no puede obviarse.

Los referenciados atentados en Inglaterra, así como la ocultación de explosivos en la ropa de los terroristas en el interior de su ropa y adosado en sus cuerpos en las Infraestructuras Críticas aeroportuarias, también hacen que se adopten nuevas medidas de seguridad. En relación a las medidas adoptadas en seguridad aeroportuaria, según Villena, J. (2021):

[35] Tras la última actualización se cambia el nombre por el Plan de Prevención, Protección y Respuesta Antiterrorista (PPPyRA), con el objeto de proteger centros y organismos públicos u oficiales, así como cualesquiera otros activos, ya sean personas, bienes, servicios, tecnología de la información u otros intangibles, cuya destrucción, ataque o degradación suponga un daño importante conforme a la valoración ponderada de los siguientes criterios: daños a la vida humana, vulneración de derechos fundamentales, afectación al normal funcionamiento de las instituciones o de los sectores estratégicos, afectación al orden púbico o la convivencia, impacto público, social o simbólico y pérdidas económicas o patrimoniales. Instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

> Otras medidas técnicas han sido la implementación de detectores de explosivos en líquidos, los cuales fueron restringidos en el equipaje de mano, a causa de complot expuesto en el año 2006, los detectores de trazas y los escáneres corporales. Esta última medida como consecuencia del intento de atentado de Abdul Farouk en el 2009, dado que llevaba explosivo adosado a su ropa íntima. (p. 103).

En el año 2007, España ya elabora y publica el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), aprobado por la Secretaría de Estado de Seguridad. El Plan conlleva la materialización de aspectos de gran relevancia tales como, de una parte, la creación del Catálogo Nacional de las Infraestructuras Estratégicas, a partir de los listados que en el año 2005 realizaron tanto la Guardia Civil como la Policía Nacional y de otra, el Nivel de Seguridad, es decir, el Nivel de Alerta Antiterrorista que se establece en una escala «penta», es decir, en cinco niveles. Se recoge que la activación de cada nivel de Alerta Antiterrorista será por parte del Ministerio del Interior, pero la declaración de la Secretaría de Estado de Seguridad.

A las actuaciones desarrolladas le sigue en España la creación por parte del Consejo de Ministros del Centro Nacional de Protección de Infraestructuras Críticas, centro que se responsabiliza de la Protección de las Infraestructuras Críticas, además de auxiliar al Secretario de Estado de Seguridad en estas materias.

En el año 2008, la Unión Europea aprueba la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de Infraestructuras Críticas europeas y la evaluación de la necesidad de mejorar su protección. En ella se establecen las líneas básicas sobre la protección de las Infraestructuras Críticas de los países de la UE, en la que se da un plazo de 2 años para que los países legislen en la materia. Además, se establece que hay una responsabilidad pública privada, es decir, la responsabilidad va a ser una responsabilidad compartida por ambos sectores.

En el año 2010, una central nuclear es atacada, de manera insólita, en Natanz, en Irán[36] por un virus informático, se produce el primer ciberataque de la historia contra una infraestructura

[36] Irán es un país situado en el suroeste de Asia, con una posición geopolítica y geoestratégica significativa debido a su ubicación en el Medio Oriente y su extensa frontera con países como Irak, Turquía, Afganistán y Pakistán. Desde el punto de vista de la geopolítica se encuentra en una encrucijada entre Asia Central, el Cáucaso y el Golfo Pérsico, lo que le otorga una posición central en la región. Su ubicación le brinda acceso a importantes rutas de transporte, lo que le confiere un papel crucial en el comercio de energía mundial. Genera influencia religiosa de importancia en el mundo musulmán chiita. En relación al factor Geoestratégico, intenta reafirmar su influencia en el Medio Oriente, especialmente en países como Irak, Siria y Líbano, a través de alianzas con grupos políticos y militares afines. Mantienen relaciones de enemistad con países como Arabia Saudí e Israel, lo que ha

de estas características. El ataque se perpetró a los conocidos sistemas SCADA, por un virus[37] informático llamado *Stut Nek*, ordena a más de mil máquinas[38] su autodestrucción[39], acción neutralizada por los ingenieros informáticos, por lo que nunca se sabrá los efectos del ataque que, en remoto se realizó.

Quedó patente que se había descuidado la ciberseguridad, en la que los terroristas sumaban y empleaban otro *modus operandi*, u otra forma de atacar a través del ciberterrorismo. El ataque supuso un cambio de paradigma, en lo que el evento pudo representar a nivel global, la inseguridad en relación a la percepción de la ciberseguridad se quiebra, aspecto que hay que reforzar de manera permanente para su garantía, todo ello porque el evento ocurrido ha representado «el primer caso en el cual un equipo industrial es atacado con un arma cibernética». (Shakarian, 2012).

En cualquier caso, se concluye que el objetivo del ciberataque no fue destruir el equipamiento controlado por los sistemas SCADA, por el contrario, «ajustar las frecuencias de estas con el objetivo de disminuir la producción óptima de uranio». (Shakarian, 2012).

Su facilidad estriba en que los controladores lógicos programables (PLC) de este sistema suelen estar conectados a un ordenador, por lo que es relativamente simple poderlo infectar y, de esta manera, poder controlar los distintos componentes físicos que lo integran o son controlados por él. En el caso del virus referenciado era un *malware* que fue creado al efecto para atacar los distintos controladores lógicos.

También en el año 2010, en materia de seguridad aeroportuaria destacamos en palabras de Villena J., (2021), que:

> En tanto que las medidas de seguridad para los pasajeros y equipajes han ido incrementándose (…), los terroristas han focalizado su objetivo en la carga que transporta un avión. La revista Inspire, de propaganda *yihadista*, se hacía eco en noviembre de 2010 de una nueva trama terrorista. En esta ocasión la actuación de la inteligencia saudí evitó el desastre. Ibrahim al-Asiri, miembro de *Al-Qaeda* en la

contribuido a generar mayor tensión en Oriente Medio. Su programa nuclear ha generado preocupaciones y tensiones con la comunidad internacional.

[37] Su objetivo era infectar la Infraestructura Crítica referenciada para buscar una mayor hegemonía nuclear en la idiosincrasia geoestratégica y política entre Irán e Israel.

[38] El virus informático afectó a las máquinas centrifugadoras de una planta de enriquecimiento de uranio iraní y que puso de manifiesto la vulnerabilidad de los entornos industriales.

[39] Aunque no hay evidencias al efecto, el grupo de *hackers Anonymus* referenciaba que detrás del ciberataque se encontraba EE.UU.

> Península Arábiga (AQPA) había construido unos artefactos explosivos que iban dentro de cartuchos de tóner para impresoras. Los explosivos que fueron introducidos en aviones de transporte de mercancías en Yemen, debían explotar sobre alguna ciudad norteamericana, si bien los destinatarios finales eran sinagogas de chicago. (p. 103).

En el año 2011, España publica tras su promulgación la Ley 8/2011, de Protección de Infraestructuras Críticas, así como su reglamento de desarrollo. España establece 12 sectores a proteger frente a los 16 de EE.UU., con una serie de organismos y ministerios afectados que tendrán responsabilidades en su protección.

En el año 2013, el Sistema Nacional de Conducción de Situaciones de Crisis es sustituido por el Consejo de Seguridad Nacional, consejo que preside su Majestad el Rey de España y en su ausencia el Presidente del Gobierno. El Consejo establece las distintas estrategias de seguridad, entre ellas, la ciberseguridad, que dio lugar a la publicación de la Estrategia de la Ciberseguridad del año 2013 y modificada con posterioridad en el año 2019.

En el año 2014 se lleva a cabo la primera reunión constitutiva del Consejo nacional de Ciberseguridad, presida por el Secretario de Estado Director del Centro Nacional de Inteligencia (CNI). De la misma manera se crea la Oficina de Coordinación Cibernética, actualmente con el nombre de Oficina de Coordinación de Ciberseguridad.

En el año 2016 se crea el Centro Tecnológico para la Seguridad (CETSE). Centro de referencia con sede en el Pardo alberga a la subdirección General de Sistemas de Información y Comunicaciones y también al Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC).

En el mismo año se produjo un ataque a través de un *ransomware*[40] a nivel mundial, con un virus informático llamado «*Wanna Cry*». En España afectó a la Compañía de Telefónica, mientras que en el Reino Unido estuvieron afectados varios hospitales, cuestión que también refuerza el área de la ciberseguridad en las Infraestructuras Críticas y, en especial las Infraestructuras Críticas hospitalarias pertenecientes al sector salud.

De la misma manera en el año 2019, la nueva Estrategia de Ciberseguridad, destacan sobremanera tres órganos de importancia, el Consejo de Seguridad Nacional, El Consejo

[40] Término proveniente del inglés, *ransom*, 'rescate', y *ware*, acortamiento de *software* o «secuestro de datos». Es un programa de tipo dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado. Se suele pedir un rescate a cambio de levantar o quitar la restricción de acceso.

Nacional de Ciberseguridad y, el Comité de Situación. Todos ellos con responsabilidades en la materia y que, además serán auxiliados por la Comisión Permanente de Ciberseguridad, El Departamento de Seguridad Nacional y El Foro Nacional, lo que refuerza el interés por la protección de las Infraestructuras Críticas y lo que significan para la sociedad al ser y tener, la mayoría un carácter esencial.

En relación a los retos futuros en materia de ciberseguridad Miranda, D., (2023) destaca que:

> Los retos que tiene por delante la ciberseguridad en materia defensiva son cada año más complejos. Las ciberamenazas, además de ser cada vez más sofisticadas técnicamente han demostrado focalizar más sus recursos contra las organizaciones, cuestión que se evidencia en que el número de ataques y su impacto vaya en aumento. (p. 48).

2.2. El Derecho Administrativo y la Protección de las Infraestructuras Críticas:

Es importante destacar la importancia de la internacionalización del derecho, en definitiva, sus procesos de globalización, al respecto, es de suma trascendencia destacar trabajos de investigación en el ámbito jurídico del derecho de Balbé, J. & Martínez, R., (2010):

> *In order to understand the process of globalization of law, we must study the American regulatory model? and administrative State (belatedly created in the XX century) as well as the functioning and internal harmonization between the fifty States of the American Union and the Federal Government because both the European Union and the globalization process have been inspired by it.* [Para entender el proceso de globalización del derecho, debemos estudiar el modelo regulatorio estadounidense y el Estado administrativo (creado tardíamente en el siglo XX), así como el funcionamiento y la armonización interna entre los cincuenta estados de la Unión Americana y el Gobierno Federal, porque tanto la Unión Europea como el proceso de globalización se han inspirado en él]. (p. 137).

En lo que respecta a la característica por excelencia del Derecho Administrativo es su enfoque en regular las relaciones entre la administración pública y los ciudadanos, así como entre las propias entidades públicas. Este campo del derecho se centra en el estudio y la regulación de la actividad administrativa del Estado, incluyendo aspectos como la organización y funcionamiento de la administración pública, los procedimientos administrativos, la

responsabilidad del Estado, el control de la administración y la protección de los derechos de los ciudadanos o administrados, frente a la acción de la administración.

Otro de los ejemplos, en relación a los distintos modelos que integran el Derecho Administrativo y, en atención a lo expuesto por: Balbé, J. & Martínez, R., (2010):

> *Needless to say, the administrative model designed by Landis and Frankfurter as a precautionary measure for financial risks and auditing is now expanded to laborrisks and to other fields (i.e. environmental risks, precautionary or discrimination risks, etc.).* [No hace falta decir que el modelo administrativo diseñado por Landis y Frankfurter como medida de precaución para los riesgos financieros y la auditoría ahora se ha ampliado a los riesgos laborales y a otros campos (por ejemplo, riesgos ambientales, riesgos de precaución o discriminación, etc.). Este modelo de corresponsabilidad empresarial para el cumplimiento activo de la regulación ha inspirado las legislaciones de los países europeos y este es otro ejemplo de globalización, al igual que la americanización]. (p. 168).

El Derecho Administrativo es una rama del derecho que se ocupa, por tanto de las relaciones entre los ciudadanos y el Estado en su calidad de administrador público. Trata, por tanto y analiza temas tales como los procedimientos administrativos, los recursos administrativos, la responsabilidad del Estado, así como los actos administrativos.

En el sentido expuesto, consideramos que una de las definiciones más relevantes es la de García de Enterría, E., & Fernández, T. R., (2022) que, la definen como «aquella parte del derecho público que tiene por objeto la organización, los medios y las formas de la actividad de las administraciones públicas y las consiguientes relaciones jurídicas entre aquellas y otros sujetos», por lo tanto, el Derecho Administrativo es garantía de seguridad jurídica y proporciona un marco legal claro y previsible que regula las acciones y decisiones de la propia Administración Pública. Esto garantiza la seguridad jurídica tanto para los ciudadanos como para las autoridades administrativas, lo que contribuye a la estabilidad y al orden en la sociedad por las siguientes cuestiones que se plantean:

1. Control del poder estatal: el Derecho Administrativo establece límites y controles al ejercicio del poder estatal por parte de la Administración Pública. Define los procedimientos que deben seguirse para la adopción de decisiones administrativas, así como los recursos y mecanismos de control que tienen los ciudadanos para impugnar dichas decisiones.

2. Protección de los derechos fundamentales: el Derecho Administrativo garantiza el respeto y la protección de los derechos fundamentales de los ciudadanos en sus relaciones con la Administración Pública. Esto incluye derechos como el acceso a la información, la participación en los procedimientos administrativos, la igualdad ante la ley y la tutela judicial efectiva.

3. Promoción del interés general: el Derecho Administrativo busca promover el interés general y el bien común en la gestión de los asuntos públicos. Establece los principios y criterios que deben guiar la actuación de la Administración Pública, como la eficacia, la eficiencia, la transparencia, la imparcialidad y la rendición de cuentas.

4. Desarrollo del Estado de Derecho: el Derecho Administrativo es esencial para el desarrollo y consolidación del Estado de Derecho, que se basa en el respeto a la legalidad, la separación de poderes, la protección de los derechos individuales y el sometimiento de las autoridades al ordenamiento jurídico.

Desde el punto de vista legal, el derecho administrativo y las Infraestructuras Críticas hospitalarias pueden relacionarse de varias maneras, en cualquier caso, se entrelazan por:

1. Ley de Protección de Infraestructuras Críticas:

    - ✓ En España, existe la Ley 8/2011, que establece medidas para la protección de las Infraestructuras Críticas. Esta ley tiene como objetivo asegurar la funcionalidad, continuidad e integridad de estas infraestructuras para prevenir, paliar y neutralizar el daño causado por ataques deliberados contra ellas.

2. Hospitales como Infraestructuras Críticas:

    - ✓ Los hospitales son considerados Infraestructuras Críticas debido a su función vital en la sociedad. Su operación ininterrumpida es esencial para la salud y el bienestar de la población. Por tales cuestiones se aplican determinadas medidas en atención a su propia idiosincrasia con el objeto de garantizar su seguridad y protección integral, lo que incluye la seguridad de las tecnologías de la información y de las comunicaciones.

3. Regulación y Planeamiento:

   - ✓ El derecho administrativo regula aspectos como la gestión, el mantenimiento y la seguridad de las Infraestructuras Críticas hospitalarias. Esto incluye la designación de operadores críticos, la identificación de amenazas y la implementación de medidas de seguridad. A tal efecto se establecen determinados procedimientos a través de los distintos planes al efecto para su gestión, en especial en cualquier situación de crisis que pueda generarse en tales infraestructuras.

Por lo tanto, El derecho Administrativo proporciona el marco legal para proteger y regular las Infraestructuras Críticas en general y, las Infraestructuras Críticas hospitalarias en particular, con el objetivo de asegurar su funcionamiento continuo y su capacidad para enfrentar amenazas potenciales.

A continuación, intentaremos hacer una aproximación en la relación legal que se establece entre el Derecho Administrativo en el ámbito de la protección de las Infraestructuras Críticas hospitalarias que, vendría dado viene por:

1. Normativa específica: el Derecho Administrativo proporciona la base normativa específica para la protección de las Infraestructuras Críticas hospitalarias. Esto incluye leyes, reglamentos y disposiciones administrativas que regulan aspectos como la seguridad, la planificación, la construcción, la operación y el mantenimiento de los hospitales y otros servicios de salud.

2. Autorización y licencias: el Derecho Administrativo establece los procedimientos y requisitos para la autorización y obtención de licencias necesarias para la construcción y operación de Infraestructuras Críticas hospitalarias. Esto garantiza que estas instalaciones cumplan con los estándares de seguridad, calidad y eficiencia requeridos por la normativa.

3. Inspección y supervisión: el Derecho Administrativo otorga a las autoridades competentes la facultad de realizar inspecciones y supervisar el cumplimiento de las normas y regulaciones en las Infraestructuras Críticas hospitalarias. Esto ayuda a identificar posibles riesgos, deficiencias o incumplimientos y tomar medidas correctivas oportunas para garantizar la seguridad y el buen funcionamiento de los hospitales.

4. Planificación y gestión de emergencias: el Derecho Administrativo establece la obligación de elaborar planes de Protección Civil y de emergencias para las Infraestructuras Críticas hospitalarias. Estos planes incluyen medidas de prevención, preparación, respuesta y recuperación ante situaciones de emergencia, como desastres naturales, accidentes graves o ataques terroristas.

5. Contratación y gestión de recursos: el Derecho Administrativo regula los procesos de contratación pública y gestión de recursos para las Infraestructuras Críticas hospitalarias, incluyendo la adquisición de equipamiento médico, la contratación de personal especializado y la prestación de servicios de apoyo. Esto garantiza la eficiencia, transparencia y legalidad en el uso de los recursos públicos destinados a la salud.

Por todo ello, se destaca que, el Derecho Administrativo es esencial para garantizar la protección de las Infraestructuras Críticas hospitalarias al establecer el marco legal y los mecanismos necesarios para su seguridad, funcionamiento eficiente y protección de los derechos de los ciudadanos. Su cumplimiento adecuado contribuye a garantizar la calidad de los servicios de salud, la seguridad de los pacientes y el personal médico, y la resiliencia de los hospitales ante posibles emergencias y crisis.

Aunque ya hemos apuntado con anterioridad una aproximación jurídica, algunos puntos clave de esta aproximación incluyen:

1. Principios fundamentales: el Derecho Administrativo se fundamenta en una serie de principios básicos, como el principio de legalidad, que establece que la Administración Pública debe actuar dentro de los límites establecidos por la ley y de acuerdo con los procedimientos y formas prescritos. Otros principios importantes son la jerarquía normativa, la igualdad, la imparcialidad, la eficacia, la eficiencia, la buena fe y la protección de los derechos fundamentales.

2. Organización administrativa: el Derecho Administrativo regula la estructura y organización de la Administración Pública, incluyendo la distribución de competencias entre los diferentes órganos administrativos (central, autonómico y local) y la creación de entidades administrativas especializadas para el ejercicio de funciones específicas.

3. Actuación administrativa: este ámbito del Derecho Administrativo se refiere a las acciones y decisiones de la Administración Pública en el ejercicio de sus funciones.

Incluye aspectos como la actividad reglada y discrecional, la gestión de servicios públicos, la contratación administrativa, la responsabilidad patrimonial de la Administración y los recursos administrativos y jurisdiccionales.

4. Protección jurisdiccional: el Derecho Administrativo establece los mecanismos de protección jurisdiccional para garantizar el control de la legalidad de la actuación administrativa y la defensa de los derechos de los ciudadanos frente a la Administración. Esto incluye el recurso de alzada, el recurso de reposición, el recurso de revisión, el recurso contencioso-administrativo y, en última instancia, el recurso de amparo ante el Tribunal Constitucional.

5. Interacción con otras ramas del derecho: el Derecho Administrativo se relaciona estrechamente con otras ramas del derecho, como el Derecho Constitucional, el Derecho Civil, el Derecho Penal, el Derecho Financiero y el Derecho Internacional Público, entre otros. Estas interacciones se producen en ámbitos como la protección de los derechos fundamentales, la responsabilidad de la Administración, la fiscalidad, la contratación pública y las relaciones internacionales.

En lo que respecta a la relación del derecho administrativo y el terrorismo hemos de referenciar que son dos áreas jurídicas distintas, pero pueden tener interacciones y relaciones en ciertos contextos, tales como:

1. Competencia Jurisdiccional:

Los delitos considerados de terrorismo no son competencia de los juzgados de instrucción de cada partido judicial. En cambio, son competencia de la Audiencia Nacional, que se encuentra en Madrid. La referenciada jurisdicción especializada se crea, en origen para conocer de los delitos cometidos por personas que integran bandas armadas, crimen organizado, o en especial relacionados con los delitos de terrorismo.

2. Legislación Antiterrorista:

España cuenta con una legislación específica para combatir el terrorismo. La Ley 29/2011 establece medidas para reconocer y proteger a las víctimas de acciones terroristas. Las cuestiones que referenciamos, incluye la movilidad funcional y geográfica, la reorganización de los tiempos y pausas de trabajo, así como la consideración de cuantas necesidades de las víctimas, tanto físicas como psíquicas, sean necesarias para el

establecimiento de los planes y políticas de empleo activas para las víctimas del terrorismo.

3. Concepto de Terrorismo:

Existe, como ha quedado patente un debate sobre cómo definir el concepto de terrorismo desde una perspectiva legal. Algunos argumentan que debe ser acorde con la realidad del fenómeno terrorista, pero sin olvidar las garantías legales de un Estado Social, Democrático de Derecho. Se hace un esfuerzo por analizar el terrorismo como un comportamiento humano que busca delimitarlo frente a otros fenómenos delincuenciales que pueden generar la confusión conceptual que, hoy en la actualidad, se mantiene.

2.3. SISTEMAS DE CONTROL Y ADQUISICIÓN DE DATOS (*SCADA*).

El sistema de Supervisión y Control de Adquisición de datos (SCADA), por ser un término o un concepto muy estandarizado en inglés -*Supervisory Control And Data Acquisition*- es un sistema que se utiliza en diferentes industrias para supervisar y controlar procesos industriales, como plantas de energía, redes de distribución de agua, sistemas de transporte, y más.

Los sistemas SCADA consisten en componentes de *hardware* y *software* que permiten a los operadores monitorear y controlar remotamente los procesos industriales en tiempo real. Estos sistemas suelen incluir:

1. Unidad central de control: es el cerebro del sistema SCADA, donde se procesan y almacenan los datos. Puede estar compuesta por una computadora o un servidor dedicado.

2. Interfaz hombre-máquina (HMI): es la interfaz gráfica que permite a los operadores interactuar con el sistema, visualizar datos en tiempo real, recibir alarmas y enviar comandos de control.

5. Controladores remotos: dispositivos distribuidos en el campo que se encargan de recopilar datos de sensores y actuadores locales, así como de ejecutar comandos de control.

6. Comunicaciones: los sistemas SCADA se basan en una red de comunicaciones que conecta la unidad central de control con los controladores remotos. Estas redes

pueden ser cableadas o inalámbricas, y pueden utilizar diferentes protocolos de comunicación, como *Modbus, DNP3, OPC*, entre otros.

7. Sensores y actuadores: equipos instalados en el proceso industrial que recolectan datos (sensores) y ejecutan acciones (actuadores) en respuesta a las instrucciones del sistema SCADA.

Los sistemas SCADA son fundamentales para mejorar la eficiencia, la seguridad y la confiabilidad de los procesos industriales al proporcionar a los operadores información en tiempo real sobre el estado de los equipos y las condiciones del proceso, así como la capacidad de tomar acciones correctivas cuando sea necesario. Además, estos sistemas también pueden integrarse con otros sistemas de gestión empresarial para facilitar la toma de decisiones y la optimización de los procesos.

En España, los sistemas SCADA y otros sistemas de control y adquisición de datos suelen estar regulados por varias leyes y regulaciones, principalmente en el ámbito de la ciberseguridad, protección de datos y regulaciones específicas, entre las que destacamos genéricamente las siguientes por su estrecha relación:

1. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Esta ley establece las normas sobre la protección de datos personales y regula su tratamiento, incluido el tratamiento de datos que puedan ser recopilados por sistemas SCADA en relación con los operadores o personas que interactúan con los sistemas. No puede obviarse la legislación europea al respecto, de aplicación directa en nuestro estado como es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, (comúnmente denominado Reglamento General de Protección de Datos –RGPD 679/2016-).

2. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas: esta ley tiene como objetivo garantizar la seguridad de las Infraestructuras Críticas, incluyendo las redes de suministro de energía, agua, transporte, entre otros, que suelen ser supervisadas mediante sistemas SCADA.

3. Real Decreto 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información: esta normativa establece medidas para garantizar la seguridad de las redes y sistemas de información, incluyendo aquellos utilizados en sistemas SCADA, con el fin de proteger la Infraestructura Crítica y prevenir ciberataques.

4. Normativa sectorial: además de las leyes generales mencionadas anteriormente, existen regulaciones específicas en cada sector industrial que pueden afectar a la implementación y operación de sistemas SCADA.

En cualquier caso, hemos de exponer, según recoge la AEI (2022) que:

> (…) el sistema SCADA está compuesto de tres elementos lógicos fundamentales. En primer lugar, un bucle de control que, a través de los sensores que lo conforman, lleva a cabo una serie de actividades tales como mediciones, hardware de control o transmisiones de datos. El conocido como Interfaz hombre- máquina (*Human Machine Interface*) que lo conforman un conjunto de ingenieros y expertos en la materia cuya función será monitorizar, configurar indicadores, algoritmos y parámetros de control. Por último, las utilidades de diagnóstico y mantenimiento remoto que, en caso de que se produzca una incidencia van a ser capaces de no sólo de prevenir esta sino, también de identificar y recuperar la información.

2.4. CONCEPTO DE INFRAESTRUCTURAS EUROPEAS E INFRAESTRUCTURAS CRÍTICAS:

Las Infraestructuras Críticas pueden ser sistemas, recursos físicos, tecnológicos, humanos tecnológicos, así como cibernéticos que son no sólo necesario sino esenciales para el funcionamiento continuo de la sociedad, economía, etc., su interrupción o destrucción redundaría en un fuerte y negativo impacto, muy significativo en la Seguridad Nacional, la Salud Pública, las finanzas, así como la calidad de vida de la ciudadanía. Las Infraestructuras Críticas son capitales para el funcionamiento de cada país, así como esenciales para su bienestar y supervivencia.

Las Infraestructuras Críticas pueden abarcar una amplia gama de sectores y servicios, según la propia Ley de Protección de Infraestructuras Críticas integra doce sectores de actividad, tal y como se desprende del propio Anexo 1 de mencionado texto legal.

1. Energía: incluye la generación, distribución y transmisión de electricidad, así como la producción y distribución de petróleo y gas.

2. Agua potable y saneamiento: la infraestructura que garantiza el suministro de agua potable y la gestión de aguas residuales es esencial para la salud pública y el bienestar de la población.

3. Transporte: carreteras, puentes, aeropuertos, puertos marítimos y ferrocarriles son vitales para la movilidad de personas y mercancías.

4. Comunicaciones: redes de telecomunicaciones y servicios de Internet son fundamentales para la conectividad y la comunicación.

5. Salud: hospitales, clínicas y laboratorios médicos son esenciales para la atención médica y la respuesta a emergencias sanitarias.

6. Finanzas y banca: las instituciones financieras y las redes de pago son críticas para la estabilidad económica y el comercio.

7. Alimentación y agricultura: la producción, distribución y venta de alimentos son necesidades básicas para la población.

8. Gobierno y seguridad pública: infraestructuras como edificios gubernamentales, fuerzas de seguridad y sistemas de defensa nacional son esenciales para la gobernabilidad y la seguridad.

9. Ciberseguridad: los sistemas informáticos y de tecnología de la información son cada vez más críticos y deben protegerse contra amenazas cibernéticas.

La protección de las Infraestructuras Críticas es una preocupación importante para los gobiernos y las organizaciones en todo el mundo, ya que la interrupción de estas infraestructuras podría tener consecuencias graves. Por todo ello se hace necesario implementar las distintas medidas de seguridad, así como las adecuadas estrategias para la gestión y control de los distintos riesgos para su protección, indistintamente de la naturaleza del riesgo.

En relación a la seguridad y la protección integral de las Infraestructuras Críticas en relación a los distintos ciberataques que éstas pueden sufrir, y según Miranda, D., (2023):

> Las Infraestructuras Críticas son un suculento objetivo para los ciberataques. El nivel de amenaza sigue creciendo, y las consecuencias sólo se vuelven más graves. Resaltar lo fundamental que es tomar medidas de manera inmediata, pasando la prevención a

> estar en el centro de cada paso que estas compañías tomen para protegerse mejor. (p.34).

El contexto geoestratégico y político actual, propiciado por la Guerra de Rusia y Ucrania el número de ataques a las Infraestructuras Críticas se ha incrementado, por todo ello se hace más que «necesario conocer y reconocer unos ataques cibernéticos cada vez más sofisticados y que actúan con gran rapidez». (Page, 2023).

En palabras de Hull, (2006) define que:

> Las Infraestructuras Críticas son «uno de los activos fundamentales para cualquier Estado», por lo que «cualquier destrucción o degradación sobre estas tendrá un efecto de debilitamiento» no sólo sobre las funciones del gobierno sino, también, sobre cuestiones esenciales para el día a día de la población como la sanidad, la educación y, sin lugar a dudas, sobre la seguridad nacional.

De la misma manera hay que destacar que si se produjera cualquier tipo de fallo en la Protección de las Infraestructuras Críticas o en cualquier aspecto en relación a su seguridad, se generará «un fallo en cascada sobre el resto de sectores considerados como esenciales en el país». (Correa- Henao, 2013).

La aproximación conceptual de los distintos términos viene dada por la propia Ley 8/2011, de Protección de Infraestructuras, tales definiciones vienen dadas por el tenor literal de su artículo segundo, que ya otorga una definición legal. En cualquier caso, son definiciones algo farragosas, todo ello porque una definición de un concepto lleva a otro y podrían llevar a prestar confusión.

Para su entendimiento, por tanto, ha de seguirse el orden secuencial, escalonado y progresivo de distintas definiciones, con el objeto entender su significado legal. Para ello ha de definirse en primer lugar lo que es un servicio esencial. Tal concepto queda definido en el artículo 2 del referenciado texto legal, pero, en este caso en el apartado a), cuyo tenor literal reza que un Servicio Esencial es aquel:

> Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. (Art. 2.a).

Imprescindible entender el concepto de Sector estratégico por la especial importancia que conlleva en la protección de las Infraestructuras Críticas por la transversalidad de los distintos términos. El artículo 2 en su apartado b) lo define como:

> Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma. (Art. 2.b).

Importante debido a que cada sector puede subdividirse en otros lo que nos lleva a la definición del concepto de subsector estratégico, término que recoge el referenciado artículo 2, pero en su apartado c), que lo define como:

> Cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas. (Art. 2.c).

La definición de Infraestructuras estratégicas, por su especial carácter, quedan definidas en el apartado d), cuyo tenor literal reza que son:

> Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. (Art. 2.d).

En lo que respecta a las Infraestructuras Críticas, de manera genérica es aquella que su mal funcionamiento afecta de manera inasumible al bienestar de los ciudadanos, en cualquier caso, ha de estarse a lo dispuesto en el tenor literal del referenciado artículo, pero en su apartado e), cuya definición se corresponde con

> Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Art. 2.e).

En relación a las Infraestructuras Europeas, la Ley de Protección de Infraestructuras Críticas establece en el tenor literal de su artículo segundo en su apartado f), son:

Aquellas Infraestructuras Críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE). (Art. 2.f).

2.4.1 Concepto de Infraestructuras Europeas e Infraestructuras Críticas.

A. Concepto de infraestructuras europeas:

Las infraestructuras europeas se refieren a un conjunto de proyectos y redes de infraestructura que abarcan varios países dentro de Europa y que tienen como objetivo principal mejorar la conectividad, la cooperación y el desarrollo económico en toda la región europea. Estas infraestructuras están diseñadas para facilitar el transporte de personas y mercancías, fortalecer la integración económica y social, y promover la competitividad de los países europeos en el mercado global. Las infraestructuras europeas pueden incluir diversos sectores, como transporte, energía, comunicaciones, medio ambiente y más. Algunas infraestructuras europeas incluyen:

1. Redes de transporte: estas incluyen carreteras, ferrocarriles, puertos, aeropuertos y vías fluviales que conectan diferentes países europeos y promueven la movilidad y el comercio transfronterizo.

2. Energía: las interconexiones eléctricas y de gas natural que permiten el suministro y la distribución de energía a nivel regional y transfronterizo.

3. Comunicaciones: redes de telecomunicaciones, como fibra óptica y redes de telefonía móvil, que garantizan la conectividad y la comunicación eficiente en toda Europa.

4. Medio ambiente: infraestructuras relacionadas con la gestión de residuos, el tratamiento de aguas y la conservación de recursos naturales que contribuyen a la sostenibilidad ambiental en la región.

5. Investigación y educación: instalaciones científicas y educativas, como laboratorios de investigación, universidades y centros de innovación, que fomentan la colaboración en investigación y desarrollo en toda Europa.

6. Salud: infraestructuras médicas y hospitales de referencia que brindan atención médica avanzada y servicios de salud especializados a nivel europeo.

7. Seguridad y defensa: infraestructuras relacionadas con la seguridad nacional y la defensa, como bases militares y sistemas de vigilancia, que garantizan la protección y la seguridad en toda la región.

El desarrollo y la mejora de las infraestructuras europeas a menudo involucran la colaboración entre países miembros de la Unión Europea (UE) y otras naciones europeas.

La Comisión Europea y otros organismos europeos desempeñan un papel importante en la planificación, financiamiento y coordinación de proyectos de infraestructura que promueven la cohesión y el crecimiento económico en toda la región. Estos esfuerzos buscan fortalecer la integración europea y mejorar la calidad de vida de los ciudadanos europeos.

B. Relación entre las Infraestructuras Europeas y las Infraestructuras Críticas:

La relación entre las infraestructuras europeas y las Infraestructuras Críticas radica en que muchas de las infraestructuras europeas son consideradas Infraestructuras Críticas para la estabilidad y el funcionamiento de la Unión Europea y sus estados miembros. A continuación, se detallamos algunas de las conexiones clave entre estos dos conceptos:

1. Importancia estratégica: tanto las infraestructuras europeas como las Infraestructuras Críticas son esenciales para la seguridad, la economía y la calidad de vida de los ciudadanos europeos. La interrupción o el deterioro de cualquiera de estas infraestructuras puede tener graves consecuencias para la región y sus países miembros.

2. Interdependencia: las infraestructuras europeas a menudo están interconectadas y dependen unas de otras. Por ejemplo, una interrupción en la red de transporte puede afectar el suministro de energía o la distribución de alimentos. Esta interdependencia resalta la importancia de proteger y garantizar la resiliencia de estas Infraestructuras Críticas.

3. Vulnerabilidades compartidas: las infraestructuras europeas y las Infraestructuras Críticas enfrentan amenazas similares, como desastres naturales, ciberataques, terrorismo y otros riesgos. Por lo tanto, las estrategias de gestión de riesgos y

seguridad que se aplican a las Infraestructuras Críticas también son relevantes para las infraestructuras europeas.

4. Coordinación y regulación: La Unión Europea y sus estados miembros suelen trabajar en estrecha colaboración para establecer regulaciones y directrices que promuevan la seguridad y la resiliencia de las Infraestructuras Críticas y europeas. Esto incluye la inversión en proyectos de infraestructura estratégicos y la implementación de medidas de seguridad cibernética y física.

5. Financiamiento y apoyo: la financiación de proyectos de infraestructura europea a menudo proviene de fondos europeos, como el Fondo Europeo de Desarrollo Regional (FEDER) y el Mecanismo Conectar Europa (CEF). Estos fondos también pueden destinarse a mejorar la resiliencia y la seguridad de las Infraestructuras Críticas.

6. Respuesta a crisis: en situaciones de crisis, como desastres naturales o amenazas terroristas, la coordinación entre las autoridades responsables de las infraestructuras europeas y las Infraestructuras Críticas es esencial para una respuesta efectiva y una rápida recuperación.

Hemos de destacar por tanto que, las infraestructuras europeas son vitales para la integración y el desarrollo de la Unión Europea, y muchas de ellas también son consideradas Infraestructuras Críticas debido a su importancia estratégica. La protección, la resiliencia y la coordinación son elementos clave que vinculan estos dos conceptos, ya que ambas requieren medidas para garantizar su seguridad y funcionamiento continuo.

2.5. PROTECCIÓN CIVIL Y COMUNIDADES AUTÓNOMAS:

En España, las comunidades autónomas tienen competencias en materia de Protección Civil, aunque estas pueden variar ligeramente dependiendo de la distribución competencial establecida en sus respectivos estatutos de autonomía y la legislación específica promulgada por el Estado.

La Protección Civil en España tiene sus antecedentes en diversas normativas y acontecimientos a lo largo de la historia del país. Algunos de los hitos más relevantes son:

- ✓ Guerra Civil Española (1936-1939): durante este conflicto, se organizaron servicios de Protección Civil improvisados para atender a la población civil afectada por los bombardeos y otros riesgos asociados a la guerra.

- ✓ Ley de Bases de Protección Civil (1985): esta ley estableció las bases del sistema de Protección Civil en España, definiendo sus objetivos, principios y estructura organizativa. También creó el Consejo Nacional de Protección Civil como órgano consultivo del Gobierno.

- ✓ Crecimiento y desarrollo del sistema (1980-1990): durante estas décadas, se produjo un crecimiento significativo en la estructura y los recursos del sistema de Protección Civil en España, con la creación de unidades especializadas, la mejora de la coordinación entre administraciones y la formación de voluntarios.

- ✓ Ley de Protección Civil (2015): esta ley actualizó y amplió el marco normativo de la Protección Civil en España, adaptándolo a los nuevos desafíos y riesgos emergentes. Introdujo conceptos como la gestión integral de riesgos, la participación ciudadana y la cooperación internacional en situaciones de emergencia.

- ✓ Pandemia de COVID-19 (2020-2023): La pandemia de COVID-19 ha supuesto un importante desafío para el sistema de Protección Civil en España, que ha tenido que adaptarse y reforzarse para hacer frente a una crisis sanitaria sin precedentes, coordinando la respuesta a nivel nacional y autonómico.

Podemos observar que, la Protección Civil en España tiene una larga historia marcada por normativas, eventos y procesos de desarrollo que han contribuido a fortalecer el sistema de gestión de riesgos y emergencias en el país.

A pesar de lo expuesto, en cualquier caso, podríamos argumentar que la Cruz Roja fue un precursor de la Protección Civil en muchos aspectos.

Aunque son entidades diferentes con enfoques distintos, la Cruz Roja ha desempeñado un papel fundamental en la prestación de ayuda humanitaria, asistencia médica y atención a las víctimas en situaciones de emergencia y desastre. Aquí hay algunas razones por las cuales se puede considerar a la Cruz Roja como un precursor de la Protección Civil:

- ✓ Orígenes históricos: la Cruz Roja fue fundada en 1863 por Henry Dunant y un grupo de activistas humanitarios con el objetivo de prestar asistencia a los heridos y enfermos en tiempos de guerra. Este enfoque en la asistencia humanitaria en situaciones de crisis sentó las bases para el desarrollo posterior de la Protección Civil.

- ✓ Desarrollo de principios y normas: la Cruz Roja ha desarrollado una serie de principios y normas internacionales para guiar su acción humanitaria, incluidos el respeto a la dignidad humana, la neutralidad, la imparcialidad y la independencia. Estos principios han influido en el desarrollo de la Protección Civil y han sido incorporados en muchas legislaciones y políticas de gestión de emergencias.

- ✓ Experiencia en respuesta a emergencias: a lo largo de su historia, la Cruz Roja ha adquirido una vasta experiencia en la respuesta a emergencias y desastres naturales, conflictos armados y otras situaciones de crisis. Esta experiencia ha contribuido al desarrollo de prácticas y procedimientos utilizados posteriormente por los servicios de Protección Civil.

- ✓ Colaboración con autoridades y organismos internacionales: la Cruz Roja trabaja estrechamente con gobiernos, organismos internacionales y otras organizaciones humanitarias en la respuesta a emergencias y en la promoción de la preparación para desastres. Esta colaboración ha fomentado la integración de la Cruz Roja en los sistemas nacionales de Protección Civil en muchos países.

La Cruz Roja y la Protección Civil son entidades distintas, la Cruz Roja ha desempeñado un papel importante como precursora en la prestación de asistencia humanitaria y en el desarrollo de principios y prácticas que han influido en el campo de la Protección Civil. En el sentido expuesto y en palabras del Dr. Soto Ejarque, (2017), la Cruz Roja « (…) empezaría ya en la época de la Segunda República Española el despliegue de una red de Puestos de Primeros Auxilios por las carreteras de todo el Estado».

Ya muy posteriormente y, según Soto, J. M., (2017), apuntaba que se establecía en Cataluña el Sistema de Coordinación de Emergencias Médicas:

> […] despliegue progresivo en Catalunya de unidades de soporte vital avanzado medicalizado SVAM, (compuestos por personal médico, de enfermería y un conductor), en ambulancias terrestres y un helicóptero, además de su centro coordinador. Destacar también la puesta en marcha de los primeros cursos específicos en medicina prehospitalaria, con el soporte universitario en Barcelona y Tarragona. (p. 30).

Aspectos relacionales entre ambos organismos de interés:

La Cruz Roja y la Protección Civil son dos entidades que, aunque tienen objetivos y funciones diferentes, a menudo trabajan de manera coordinada y complementaria en situaciones de emergencia y desastres. A continuación, se detalla la relación entre ambas:

- ✓ Coordinación en emergencias: en situaciones de emergencia, tanto la Cruz Roja como los servicios de Protección Civil pueden intervenir para proporcionar ayuda humanitaria, asistencia médica, evacuación de personas, distribución de alimentos y suministros, entre otras acciones. La coordinación entre ambas entidades es fundamental para garantizar una respuesta eficaz y evitar duplicaciones de esfuerzos.

- ✓ Formación y capacitación: tanto la Cruz Roja como los servicios de Protección Civil ofrecen programas de formación y capacitación en primeros auxilios, atención psicológica en emergencias, gestión de desastres, entre otros temas relacionados. En muchos casos, colaboran en la organización y realización de cursos y ejercicios prácticos para mejorar la preparación de voluntarios y profesionales en situaciones de crisis.

- ✓ Intercambio de recursos: en ocasiones, la Cruz Roja y los servicios de Protección Civil pueden compartir recursos como vehículos, material de rescate, equipos de comunicación, entre otros, para reforzar sus capacidades operativas en situaciones de emergencia.

- ✓ Apoyo psicosocial: ambas entidades ofrecen apoyo psicosocial a las personas afectadas por emergencias y desastres, proporcionando atención emocional, asesoramiento y acompañamiento en momentos difíciles.

- ✓ Participación en plataformas de coordinación: en muchos países, la Cruz Roja y los servicios de Protección Civil forman parte de plataformas de coordinación de emergencias a nivel nacional o local, donde colaboran con otras organizaciones gubernamentales y no gubernamentales para planificar y responder a situaciones de crisis.

Por lo expuesto, podemos destacar la relación que puede existir entre la Cruz Roja y la Protección Civil que, se caracteriza por la colaboración, coordinación y complementariedad en la respuesta a emergencias y desastres, con el objetivo común de proteger y asistir a las personas afectadas.

A continuación, proporcionamos sinópticamente una visión general de las competencias de las comunidades autónomas en materia de Protección Civil, así como la legislación de referencia:

1. Legislación de referencia: la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, establece el marco jurídico general para la Protección Civil en España. Esta ley define los principios, objetivos y estructura organizativa del sistema nacional, así como las competencias y responsabilidades de las distintas administraciones públicas en materia de Protección Civil.

2. Competencias de las comunidades autónomas: las comunidades autónomas tienen competencias en materia de Protección Civil en el ámbito de sus respectivos territorios, de acuerdo con lo establecido en sus estatutos de autonomía y la legislación específica promulgada por el Estado. Entre las competencias de las comunidades autónomas en materia de Protección Civil se incluyen:

    - ✓ Elaboración y aprobación de planes de Protección Civil autonómicos, que complementan y desarrollan el marco establecido por la legislación nacional.

    - ✓ Coordinación y colaboración con las administraciones locales dentro de su territorio autonómico para la elaboración y ejecución de planes de Protección Civil locales y la gestión de situaciones de emergencia.

    - ✓ Gestión de recursos y medios para la Protección Civil dentro de su ámbito territorial, incluyendo la movilización y coordinación de servicios de emergencia, personal, equipamiento y otros recursos necesarios.

    - ✓ Desarrollo de acciones de formación, sensibilización y difusión de información en materia de Protección Civil dirigidas a la población y otros agentes implicados en la gestión de emergencias.

3. Coordinación con el Estado: aunque las comunidades autónomas tienen competencias en materia de Protección Civil dentro de su territorio, es importante destacar que la Protección Civil es una competencia compartida entre el Estado y las comunidades autónomas. Por lo tanto, existe un marco de coordinación entre el Gobierno central y las comunidades autónomas para garantizar una respuesta integral y coordinada ante situaciones de emergencia que puedan afectar a múltiples regiones o tener implicaciones a nivel nacional.

Como conclusión, las comunidades autónomas en España tienen competencias en materia de Protección Civil dentro de su ámbito territorial, que se establecen en sus respectivos estatutos de autonomía y la legislación específica promulgada por el Estado.

Estas competencias incluyen la elaboración de planes de Protección Civil, la coordinación con las administraciones locales, la gestión de recursos y la realización de acciones de formación y sensibilización en materia de Protección Civil. Todo ello se realiza en el marco de una coordinación con el Estado Central para garantizar una respuesta integral y coordinada ante cualquier tipo de situaciones de emergencia indistintamente de la naturaleza del riesgo.

2.6. PROTECCIÓN CIVIL Y PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS:

La Protección Civil en España se encuentra regulada por la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil. Esta ley establece el marco jurídico para la organización, planificación y coordinación de las actividades de Protección Civil en todo el territorio español.

A continuación, recogemos los aspectos más relevantes de la Protección Civil en España, en atención a su legislación específica:

1. Finalidad y objetivos: la Protección Civil tiene como finalidad proteger a las personas, los bienes y el medio ambiente ante situaciones de emergencia, catástrofe o calamidad pública.

   Sus objetivos principales son prevenir los riesgos, prepararse para hacer frente a las emergencias, responder de manera eficaz ante situaciones de crisis, así como contribuir a la recuperación y reconstrucción tras un desastre.

2. Organización y estructura: la Ley 17/2015 establece la creación del Sistema Nacional de Protección Civil, que se compone de las administraciones públicas estatal, autonómica y local, así como de otros organismos públicos y entidades privadas con competencias en materia de Protección Civil. Este sistema se organiza en torno al Consejo de Protección Civil y a las comisiones de Protección Civil a nivel estatal, autonómico y local.

3. Planificación y gestión de emergencias: la legislación establece la elaboración de planes de Protección Civil a nivel estatal, autonómico y local, que incluyen medidas de prevención, preparación, respuesta y recuperación ante situaciones de emergencia.

Estos planes se actualizan y revisan periódicamente para adaptarse a los cambios en los riesgos y amenazas.

4. Coordinación y colaboración: se establece la coordinación y colaboración entre las distintas administraciones públicas y otros organismos implicados en la Protección Civil, así como con organizaciones de voluntariado, entidades privadas y la sociedad civil en general.

   Esto se lleva a cabo a través de la participación en órganos de coordinación, la realización de ejercicios y simulacros, y la difusión de información y sensibilización pública.

5. Recursos y medios: la legislación prevé la asignación de recursos humanos, materiales y financieros para garantizar la adecuada preparación y respuesta ante emergencias. Se establecen los mecanismos de coordinación para la movilización y gestión de estos recursos en caso de necesidad, así como la colaboración con otros países y organismos internacionales en situaciones de emergencia transnacional y transfronteriza.

En el sentido expuesto habrá que considerar las conclusiones en relación sobre la Ley del Sistema Nacional de Protección Civil a las que llega Istúritz, J.J., (2015) que recoge que:

- Se ha tenido muy en cuenta la experiencia de la anterior Ley y los pronunciamientos del TC desde un punto de vista de distribución competencial.
- Estamos ante una ley oportuna tres décadas después de la aprobación de la anterior, que ya nación herida en su origen y fue motivo de varias sentencias del TC.
- La ley acomete varios aspectos que no incluyó la norma en vigor (1985), como es la formación, el papel de los medios de comunicación, la UME, el Centro Nacional de Coordinación, la evaluación e inspección del sistema, los reconocimientos, los precios unitarios y el régimen sancionador entre otros.
- La ley intenta desinflar una cierta dejación que ha existido por parte del Estado en materia de atención en emergencias, como, por ejemplo, la regulación del teléfono 112, al considerarlo como un instrumento de telecomunicaciones y no una política pública de atención de emergencias, e intenta recuperar un cierto liderazgo a golpe de ley que no trata igual al resto de administraciones que han venido a suprimir estas carencias durante treinta años.

- La ley desaprovecha la oportunidad de abordar aspectos necesarios tales como una mínima regulación de los bomberos, la coordinación de los 112 o las redes sociales aplicadas en emergencias.

(pp. 68-69).

En cuanto a la normativa dimanante, la Ley 17/2015 establece el marco general de Protección Civil en España, pero también prevé la elaboración de normativa específica y planes de Protección Civil por parte de las administraciones públicas competentes en función de sus áreas de responsabilidad y riesgos específicos. Esto incluye la regulación de aspectos como la gestión de riesgos naturales y tecnológicos, la protección de Infraestructuras Críticas, la seguridad en eventos públicos y la atención a situaciones de emergencia sanitaria, entre otros.

En conclusión, la Protección Civil en España se basa en una legislación específica que establece el marco jurídico para la organización, planificación y coordinación de las actividades de Protección Civil en todo el territorio nacional. Esta legislación establece los principios, objetivos, estructura organizativa, planificación, recursos y colaboración necesarios para garantizar la seguridad y protección de la población ante situaciones de emergencia y crisis.

2.7. PARTICIPACIÓN DE LAS COMUNIDADES AUTÓNOMAS EN EL SISTEMA DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS:

La Protección de las Infraestructuras Críticas es una competencia de carácter estatal, en cualquier caso, para garantizar su protección efectiva, el resto de las administraciones públicas han de participar y colaborar, así como estar representadas con el objeto de garantizar la adecuada seguridad de aquellas que les sean de su titularidad, por los siguientes motivos:

- ✓ Esa representación se debe en parte a que algunos de los Operadores Críticos son de Titularidad Pública, o bien pueden estará participados por alguna Comunidad Autónoma, o bien por alguna Corporación Local.
- ✓ El papel de aquellas Fuerzas y Cuerpos de Seguridad, al margen de las Fuerzas y Cuerpos de Seguridad del Estado desempeñan su labor de seguridad y protección operativa en las Infraestructuras Críticas de sus distintas demarcaciones.
- ✓ El propio espíritu de la Ley de Infraestructuras Críticas tiene un carácter integrador en todos los actores o agentes con responsabilidades al efecto. No debemos de olvidar que el ámbito de la Protección Civil es una materia delegada a las distintas Comunidades Autónomas, todo ello porque existen infraestructuras que están

afectadas por la propia legislación en materia de Infraestructuras Críticas y aunque a la vez están condicionadas por la normativa específica en materia de Protección Civil y Autoprotección ligada a las Comunidades Autónomas en función de sus atribuciones y competencias legales.

Además de todo lo expuesto, las Administraciones Públicas de las distintas Comunidades y Ciudades Autónomas, en función de sus competencias legales y reglamentarias, así como lo dispuesto por la legislación y normativa dimanante en materia de Infraestructuras Críticas, tres funciones de relevancia, a saber:

- ✓ Parte activa del Sistema de Protección de Infraestructuras Críticas al ser considerado un agente del sistema. Por todo ello participan en:
  - Órganos de decisión y dirección.
  - Intervienen en algunos estadios del proceso regulatorio, así como de las estructuras diseñadas al efecto integrados en la Comisión para la Protección de las Infraestructuras Críticas, así como en el Grupo de Trabajo Interdepartamental.
- ✓ Participan activa y administrativamente en la implantación de los siguientes planes que les son asignados cuando son designados Operadores Críticos:
  - Plan de Seguridad del Operador (PSO).
  - Plan de Protección Específico (PPE), uno para cada una de sus infraestructuras.
  - Planes de Apoyo Operativo (PAO).
- ✓ Seguridad, apoyo e intervención de carácter policial a través de sus cuerpos de policía autonómicos en aquellas Infraestructuras que están encuadradas dentro del ámbito de actuación legal o reglamentaria.

Las Comunidades Autónomas son actores, en puridad, agentes importantes en el Sistema de Protección de Infraestructuras Críticas, la Ley de Protección de Infraestructuras Críticas establece su participación de manera activa, todo ello a tenor del artículo 10 del referenciado texto legal, cuyo tenor dice que:

> Las Comunidades Autónomas participarán en el sistema de protección de Infraestructuras Críticas y en los órganos previstos en dicha Ley de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía. (Art.10.3).

Por ello las Comunidades Autónomas, *grosso modo*, respecto a sus Infraestructuras Críticas podrán y a tenor del RD 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas y que son:

> Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, las facultades previstas en los párrafos c), d, e) y f) del artículo anterior dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento. (Art. 10.1).
>
> En todo caso, la coordinación de las actuaciones que se lleven a cabo en materia de protección de las Infraestructuras Críticas entre las Fuerzas y Cuerpos de Seguridad del Estado y los Cuerpos policiales de las Comunidades Autónomas con competencias en materia de seguridad, se regirá por lo estipulado en los acuerdos de las Juntas de Seguridad correspondientes. (Art. 10.2).

Esta materia queda con mayor precisión redactada en el Reglamento para la Protección de las Infraestructuras Críticas, de cuyo tenor literal puede extraerse:

> En aquellos casos en que los operadores críticos del Sector Público estén vinculados o dependan de una Administración pública, el órgano de dicha Administración que ostente competencias por razón de la materia podrá constituirse en el interlocutor con el Ministerio del Interior a través del CNPIC en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto en este reglamento, debiendo comunicar dicha decisión al CNPIC. (Art. 15.2).

Otras competencias legales en relación a la propia Ley de Infraestructuras Críticas en relación con las distintas Comunidades y Ciudades Autónomas son:

> Las Comunidades Autónomas no incluidas en el apartado primero del presente artículo participarán en el Sistema y en los órganos colegiados del mismo de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía. (Art. 10.4).

De acuerdo con lo dispuesto en sus Estatutos de Autonomía, las Ciudades de Ceuta y Melilla, a través de sus Consejos de Gobierno y de acuerdo con la Delegación de Gobierno respectiva, podrán emitir los oportunos informes y propuestas en relación con la adopción de medidas específicas sobre las Infraestructuras Críticas y críticas europeas situadas en su territorio. (Art. 10.4).

Como conclusión y en base a lo expuesto podemos concluir en relación con las Comunidades Autónomas que:

- ✓ A pesar de las competencias que las Comunidades Autónomas tienen en materia de Protección Civil, no debe de inducir a error en las competencias en materia de protección de Infraestructuras Críticas, todo ello, porque de la normativa expuesta se desprende que no tienen capacidad para regular, al igual que no tienen capacidad sancionadora en la materia en cuanto a los Operadores Críticos se refiere.
- ✓ El nexo de interlocución con los operadores críticos de titularidad privada es la Secretaría de Estado de Seguridad a través siempre del Centro Nacional Para la Protección de Infraestructuras Críticas (CNPIC), de manera directa y no a través de las Comunidades Autónomas, salvo para aquellas que sean de su titularidad.
- ✓ Las Comunidades Autónomas con competencias en relación con sus propios Estatutos de Autonomías en lo que respecta la protección de personas y bienes, así como para el mantenimiento del orden público, si tienen competencias de carácter policial en base a lo que establezca la normativa y, únicamente en la inspección y revisión, tanto de los Planes de Protección Específicos (PPE) como de los Planes de Apoyo Operativo (PAO), pero con la supervisión final de la Secretaría de estado de Seguridad, quién en última instancia rubrica y aprueba los distintos planes en materia de Infraestructuras Críticas.
- ✓ Tampoco poseen la facultad de incluir determinadas infraestructuras en el Catálogo, la declaración de zona crítica y la adopción de medidas de seguridad sobre infraestructuras específicas en competencia exclusiva al Estado Central, canalizado siempre a través de la Secretaría de Estado de Seguridad, que podrá, en su caso, considerar cuantas propuestas sean efectuadas por otras Administraciones Públicas.

Al integrarse de manera activa en la Comisión Nacional para la Protección de las Infraestructuras Críticas, todo ello a tenor del Reglamento para la Protección de las Infraestructuras Críticas:

> (…) Asistirán a las reuniones de la Comisión un representante con voz y voto por cada una de las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público. También participará, igualmente con voz y voto, un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones. (Art. 11.3).

En relación con el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas:

> (…) Asistirá a las reuniones del Grupo de Trabajo un representante, con voz y voto por cada una de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y para el mantenimiento del orden público. Asimismo, participará con voz y voto un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones. (Art. 12.3).

En relación con la aprobación, registro y clasificación de los distintos Planes de Protección Específicos, las Comunidades Autónomas se atendrán a lo dispuesto por el artículo 26 del Reglamento para la Protección de Infraestructuras Críticas en lo que a ellos respecta:

> (…) se recabará informe preceptivo de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas o en las Ciudades con Estatuto de Autonomía en el que se considerará, en su caso, el criterio de los órganos competentes de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, así como del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente. (Art. 26.1).
>
> Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de

> personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean aprobados por el Secretario de Estado de Seguridad, todos los Planes de Protección Específicos de las Infraestructuras Críticas o Infraestructuras Críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Protección Específicos existentes. (Art. 26.3).

En relación con la aplicación y seguimiento de los distintos Planes de Protección Específicos, las Comunidades Autónomas se atendrán a lo dispuesto por el artículo 28.2 del Reglamento para la Protección de Infraestructuras Críticas en lo que a ellos respecta:

> En aquellas Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, las facultades de inspección serán ejercidas por sus órganos competentes, sin perjuicio de lo dispuesto en la legislación sectorial aplicable y de la necesaria coordinación con las Delegaciones del Gobierno en dichas Comunidades y los otros organismos reguladores competentes en virtud de su normativa sectorial. (Art. 28.2).

En lo que respecta a los Planes de Apoyo Operativo en cuanto a su finalidad, elaboración y contenido, las Comunidades Autónomas se atendrán a lo dispuesto por el artículo 28 del Reglamento para la Protección de Infraestructuras Críticas en lo que a ellos respecta:

> Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las Infraestructuras Críticas. (Art. 30.1).
>
> Por cada una de las Infraestructuras Críticas e Infraestructuras Críticas europeas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo

> Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura. (Art. 30.2).

Las Comunidades y Ciudades Autónomas en relación con el Delegado de Seguridad de la Infraestructura Crítica y en relación con el RD 704/2022, por el que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas han de:

> En el plazo de tres meses desde la identificación como crítica o crítica europea, de una de sus infraestructuras, los operadores críticos comunicarán a las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia e identidad de un Delegado de Seguridad para dicha infraestructura. (Art. 35.1).

2.8. MARCO LEGAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS:

El marco legal para la protección de las Infraestructuras Críticas tiene como objetivo principal garantizar la resiliencia, la seguridad y la continuidad operativa de las infraestructuras esenciales para el funcionamiento de la sociedad y la seguridad nacional. El derecho administrativo, viene a ser en el caso que nos ocupa el elemento jurídico necesario y «vehiculizador» para promover la coordinación y colaboración entre los actores involucrados en su gestión y protección.

2.8.1 Marco legal y normativo en la Unión Europea (UE).

La Unión Europea (UE) ha establecido un marco legal integral para la protección de las Infraestructuras Críticas a nivel europeo. Este marco legal se basa principalmente en la Directiva 2008/114/CE del Consejo, también conocida como la Directiva NIS[41] (*Network and Information Systems Directive*), que se ha modificado y fortalecido a lo largo de los años. En cualquier caso, los elementos clave de este marco legal son:

[41] El acrónimo «NIS» se refiere a la Directiva sobre la Seguridad de las Redes y los Sistemas de Información. Esta directiva es conocida por su nombre completo en inglés, NIS *Directive*, que viene del inglés, como se ha expuesto, *Network and Information Systems Directive.* La Directiva NIS es una legislación de la Unión Europea que tiene como objetivo mejorar la ciberseguridad en la Unión Europea. Fue adoptada en julio de 2016 y entró en vigor en agosto de 2016. La Directiva establece medidas para garantizar un nivel común de seguridad cibernética en toda la UE, con el fin de proteger las redes y sistemas de información críticos contra ciberataques y otros incidentes de seguridad.

1. Directiva NIS (Directiva 2008/114/CE y sus modificaciones): la Directiva NIS establece un marco común para la identificación y la gestión de los riesgos en el ámbito de la seguridad de las redes y sistemas de información en la UE. Si bien la directiva se centra en la ciberseguridad, también aborda la protección de Infraestructuras Críticas que dependen de sistemas de información. La directiva ha sido modificada y fortalecida con la Directiva (UE) 2016/1148, conocida como la Directiva NIS 2, para ampliar su alcance y reforzar las medidas de seguridad.

2. Reglamento sobre la ciberseguridad de la UE (*EU Cybersecurity Act*): este reglamento establece un marco para la certificación de productos, servicios y procesos relacionados con la ciberseguridad en la UE. Contribuye a la protección de las Infraestructuras Críticas al garantizar que los productos y servicios utilizados para su operación cumplan con los estándares de seguridad cibernética.

3. Planes nacionales de seguridad cibernética: los Estados miembros de la UE deben desarrollar planes nacionales de seguridad cibernética que incluyan medidas para proteger las Infraestructuras Críticas en su territorio. Estos planes deben cumplir con los requisitos y estándares establecidos en la Directiva NIS y coordinarse con otros países miembros.

4. Cooperación entre Estados miembros y la Comisión Europea: la Directiva NIS promueve la cooperación entre los Estados miembros y la Comisión Europea para compartir información sobre amenazas, incidentes de seguridad y buenas prácticas en el ámbito de la ciberseguridad e Infraestructuras Críticas.

5. Identificación de operadores de servicios esenciales (OSE) y proveedores de servicios digitales (DSP): la directiva clasifica a ciertos operadores de servicios esenciales y proveedores de servicios digitales como entidades que deben cumplir con requisitos específicos de seguridad cibernética y notificar incidentes significativos.

6. Mecanismos de supervisión y sanciones: los Estados miembros deben establecer mecanismos de supervisión y aplicar sanciones en caso de incumplimiento de las disposiciones de la Directiva NIS.

7. Cooperación con la Agencia Europea de Ciberseguridad (ENISA): la ENISA desempeña un papel importante en el apoyo a los Estados miembros y la Comisión Europea en la

implementación de medidas de seguridad cibernética y la protección de Infraestructuras Críticas.

El marco legal referenciado de la UE tiene como objetivo fortalecer la ciberseguridad y la resiliencia de las Infraestructuras Críticas en toda la Unión Europea, fomentando la cooperación entre los estados miembros para garantizar la protección de los servicios esenciales y la infraestructura estratégica.

2.8.2 Marco legal y normativo en España.

En España, la protección de las Infraestructuras Críticas se rige por un marco legal específico que se basa en la implementación de la Directiva 2008/114/CE del Consejo de la Unión Europea (Directiva NIS) y otras regulaciones nacionales. A continuación, se destacan las principales leyes y normativas que establecen el marco legal para la protección de las Infraestructuras Críticas en España:

1. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas: esta ley es la principal normativa nacional que regula la protección de las Infraestructuras Críticas en España. Establece las obligaciones y responsabilidades de los operadores de Infraestructuras Críticas, así como los procedimientos para su identificación y designación. También define las autoridades responsables de la protección de estas infraestructuras y establece sanciones por incumplimiento.

2. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas: este reglamento desarrolla la Ley 8/2011 y establece las medidas y procedimientos específicos para la identificación, designación y protección de las Infraestructuras Críticas en España. Además, define las categorías de Infraestructuras Críticas y establece los requisitos de seguridad y notificación de incidentes.

3. Plan Nacional de Protección de Infraestructuras Críticas: este plan, desarrollado en cumplimiento de la Ley 8/2011, establece las estrategias y medidas para la protección de las Infraestructuras Críticas en España. Define las responsabilidades de las diferentes autoridades y operadores, así como los procedimientos de gestión de riesgos y la coordinación en caso de incidentes.

4. Cooperación con el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC): el CNPIC es el organismo encargado de coordinar y supervisar las medidas de protección de las Infraestructuras Críticas en España. Colabora estrechamente con los operadores y las autoridades competentes para garantizar la seguridad de estas infraestructuras.

5. Cooperación con ENISA: la Agencia Europea de Ciberseguridad (ENISA) desempeña un papel importante en la cooperación europea en materia de seguridad cibernética y protección de Infraestructuras Críticas. España participa en esta cooperación a través de sus autoridades competentes.

Este marco legal proporciona las bases para la identificación, designación y protección de las Infraestructuras Críticas en España y establece las medidas de seguridad necesarias para garantizar su resiliencia frente a amenazas y riesgos. Además, promueve la cooperación entre los sectores público y privado en la protección de estas infraestructuras esenciales.

2.9. AGENTES PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS.

La protección de las Infraestructuras Críticas involucra a diversos agentes, tanto en el ámbito nacional como en el internacional, que trabajan de manera coordinada para poder garantizar la seguridad y la resiliencia de estas infraestructuras esenciales. De manera genérica:

Ministerio del Interior, Secretaría de Estado de Seguridad, Centro Nacional para la Protección de las Infraestructuras Críticas,

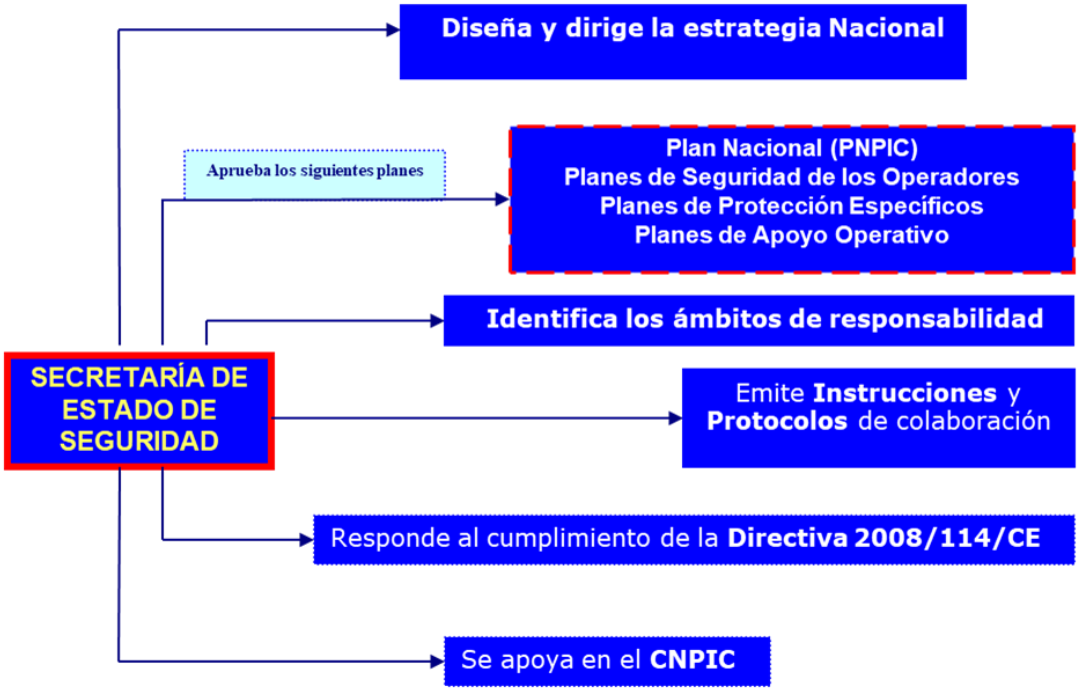
Mientras que la ley nacional establece las competencias y responsabilidades específicas de estas autoridades a nivel nacional, el reglamento de la UE busca coordinar y armonizar las acciones entre los diferentes Estados miembros.

Los principales agentes y sus cometidos en la protección de las Infraestructuras Críticas son: La Secretaría de Estado de Seguridad. El Centro Nacional para la Protección de las Infraestructuras Críticas. Los Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía. La Comisión Nacional para la Protección de las Infraestructuras Críticas. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas. Los Operadores Críticos.

En relación con la Secretaría de Estado de Seguridad (SES): presentamos en la siguiente figura los cometidos específicos de la SES en relación con las Infraestructuras Críticas.

Figura 5

Diagrama de Flujo de Datos. Competencias Secretaría de Estado de Seguridad. Fuente: elaboración propia



1. **Operadores de Infraestructuras Críticas (OIC)**:

   - ✓ Cometidos: los operadores de Infraestructuras Críticas son las entidades responsables de la operación y gestión de las Infraestructuras Críticas. Sus cometidos incluyen implementar medidas de seguridad, evaluar riesgos, notificar incidentes y colaborar con las autoridades competentes para garantizar la protección de sus infraestructuras, que a la vez tienen que ser previamente estratégicas.
   - ✓ Comunicación con el CNPIC: los operadores Críticos han de comunicarse con el Centro Nacional para la Protección de las Infraestructuras Críticas a través una plataforma que se llama Plataforma de Intercambio de Información de Infraestructuras Plataforma (PI3), el origen del nombre viene dado porque el número 3 hace referencia a las tres «ies» provenientes de las palabras Intercambio de Información de Infraestructuras.

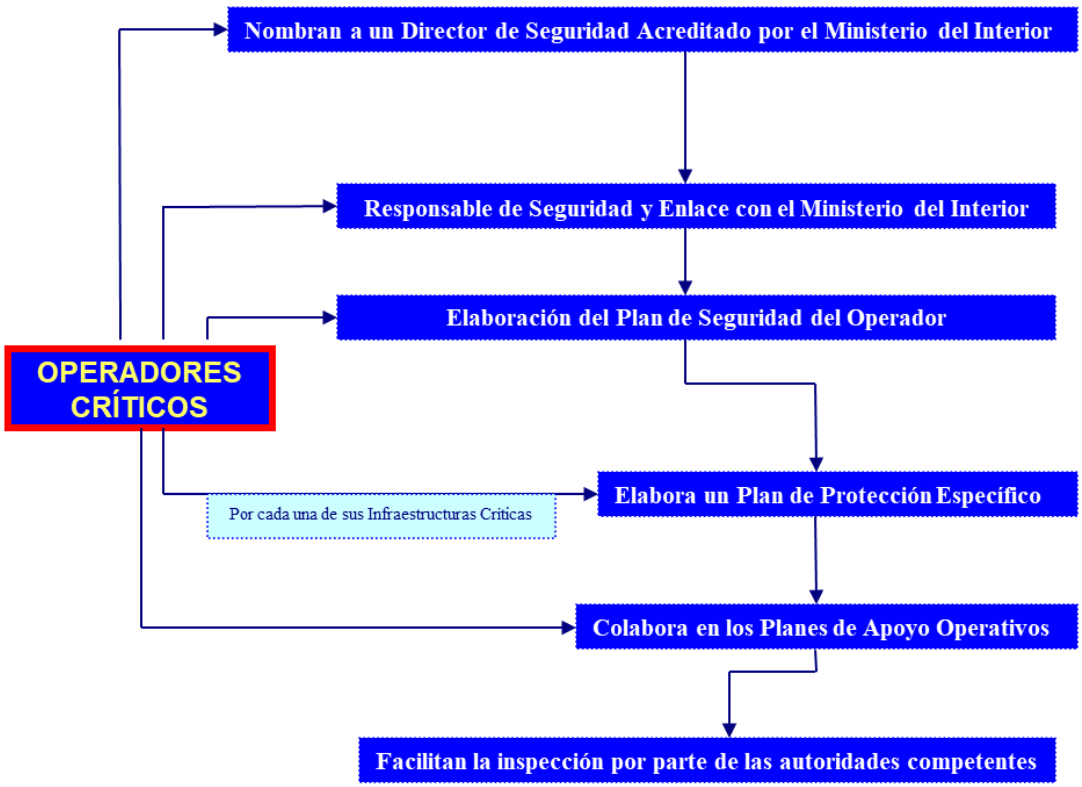
     Esta plataforma utiliza para la comunicación efectiva un programa encriptado que recibe el nombre de HERMES, impenetrable certificado por COMMON

CRITERIA, norma que certifica el Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia, a través de una malla que es facilitada por Presidencia del Gobierno y recibe el nombre de «Malla B».

Cuando el CNPIC recibe cualquier tipo de información, para evitar una posible brecha de seguridad, vuelve a volcar la información en la plataforma que gestiona el Catálogo Nacional de Infraestructuras estratégicas. Esta plataforma recibe el nombre de ARGOS, plataforma que no está interconectada directamente con la plataforma PI-3, para evitar que pueda haber una filtración, o un robo de datos relacionados con las Infraestructuras Críticas de nuestro país.

Figura 6

Diagrama de Flujo de Datos. Operadores Críticos. Fuente: elaboración propia.



2. **Autoridades Nacionales de Protección de Infraestructuras Críticas**:

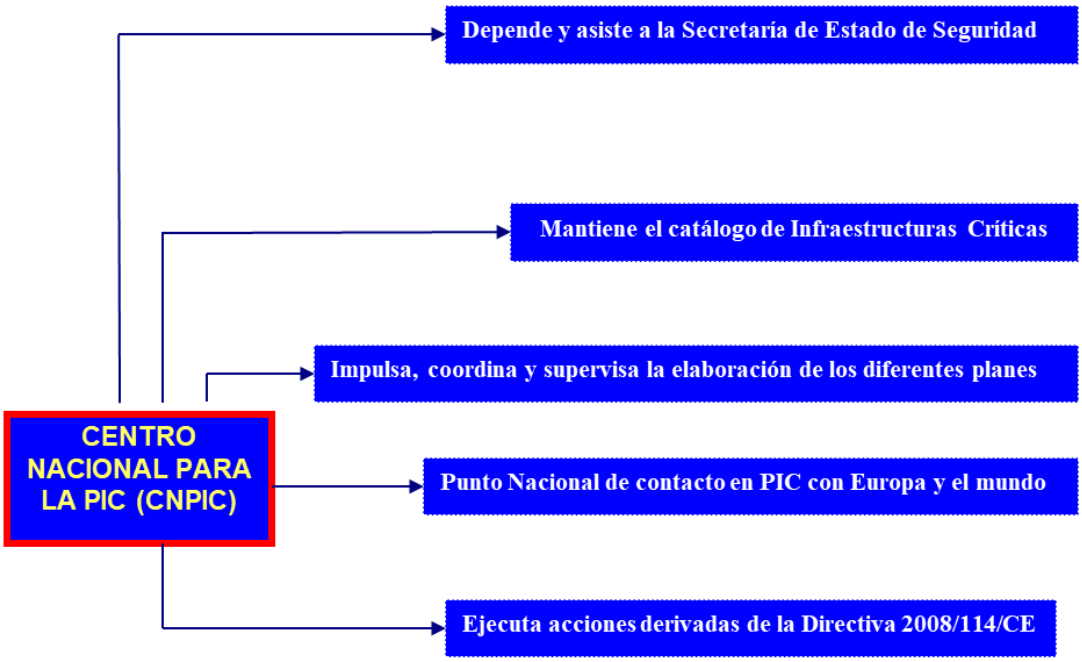
Cometidos: estas autoridades, designadas por los Estados, son responsables de identificar, designar y supervisar las Infraestructuras Críticas en el país. También coordinan la implementación de medidas de seguridad y la respuesta a incidentes.

3. **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)**:

Cometidos: el CNPIC es el organismo central encargado de la coordinación y supervisión de la protección de las Infraestructuras Críticas a nivel nacional. Facilita la colaboración entre operadores y autoridades competentes, promueve la concienciación sobre la seguridad, y coordina la respuesta a incidentes y crisis relacionados con Infraestructuras Críticas.

Figura 7

Diagrama de Flujo de Datos. Centro Nacional Para la Protección de las IC. Fuente: elaboración propia



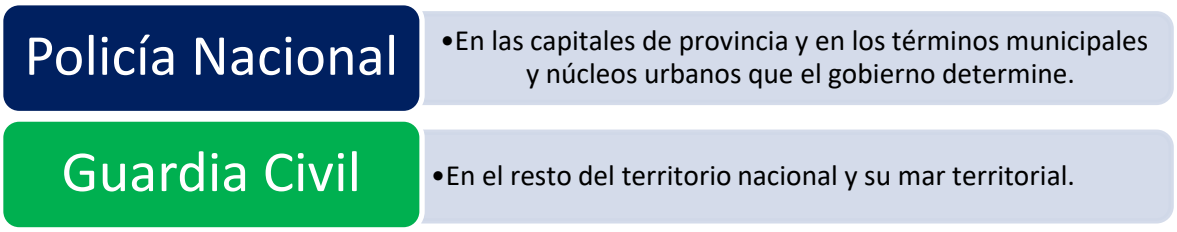
4. **Fuerzas y Cuerpos de Seguridad:**

Aunque no son agentes para la protección de las Infraestructuras Críticas de *iure*, si lo son de *facto* por su especial cometido en lo que respecta a su protección. Los cometidos en materia de Infraestructuras Críticas de las fuerzas de seguridad, son de especial importancia, debido a que tienen un papel crucial en la protección de Infraestructuras Críticas.

Su labor incluye la vigilancia, la prevención y la respuesta a incidentes que amenacen la seguridad de las Infraestructuras Críticas. También es importante el resto de Fuerzas y Cuerpos de Seguridad[42] en sus ámbitos de actuación territorial tal y como se recoge en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

Figura 8

Diagrama. Ámbito competencial de las Fuerzas y CC.SS., del Estado. Fuente: elaboración propia.



Las distintas Fuerzas y Cuerpos de Seguridad han de elaborar e implementar el Plan de Apoyo Operativo de las distintas Infraestructuras Críticas. A continuación, se adjunta la figura correspondiente con los aspectos de mayor relevancia. En cualquier caso, ha de implementarse posteriormente al Plan de protección Específico de cada una de las Infraestructuras que el Operador Crítico, declarado como tal, posea.

De la misma manera hay un actor importante en materia de Seguridad, el Personal[43] de Seguridad Privada, en el aspecto referenciado hay que destacar que, la Ley 5/2014, de 4 de

[42] Hay que distinguir conceptualmente la diferencia entre los integrantes de las Fuerzas y Cuerpos de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado. En Relación a las Fuerzas y Cuerpos de Seguridad integra generalmente a todas las policías, esto es decir, Policía Nacional (anteriormente Cuerpo Nacional de Policía, Guardia Civil, Policías Autonómicas, Policía Foral y Policías Locales. En cambio, las Fuerzas y Cuerpos de Seguridad del Estado, sólo están integradas por la Policía Nacional y la Guardia Civil.

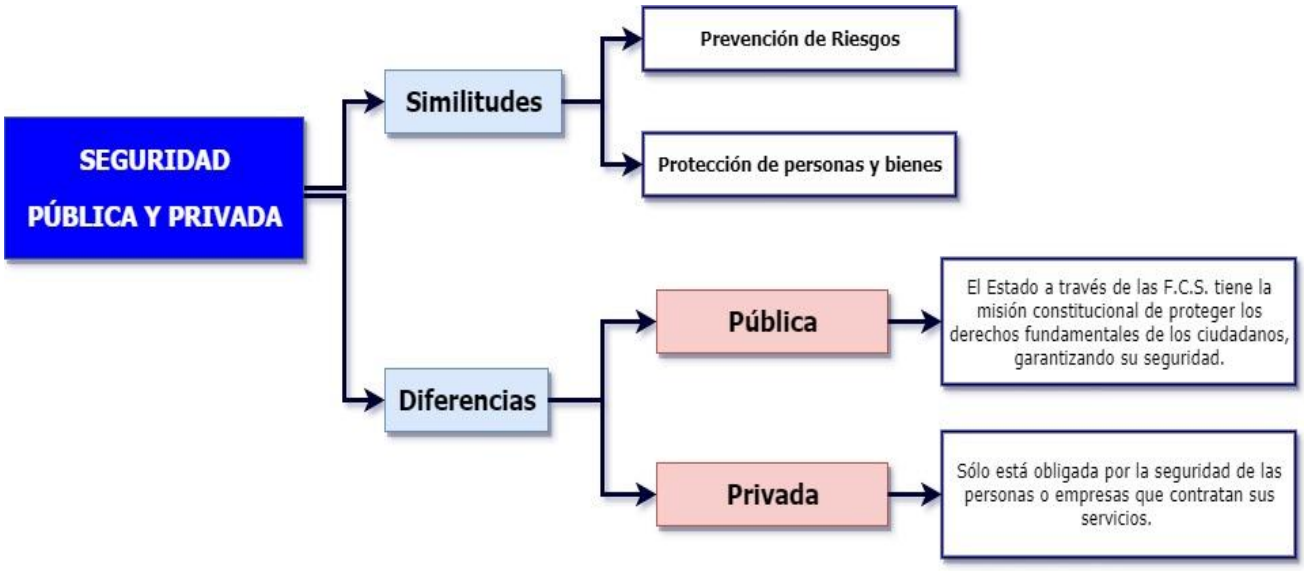
[43] Vigilantes de seguridad: Son aquellas personas que, debidamente habilitadas, tienen como función principal la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados. Vigilantes de explosivos: Son una especialidad de los vigilantes de seguridad que han recibido una formación especializada y están habilitados para llevar a cabo tareas de vigilancia y protección en instalaciones o actividades que impliquen el manejo, transporte o almacenamiento de explosivos y sustancias peligrosas. Guardas rurales: Son profesionales encargados de la vigilancia y protección de fincas, explotaciones agrícolas, ganaderas o forestales, así como de la prevención de incendios y protección del medio ambiente en áreas rurales. Los guardas pescas marítimos son otro grupo importante dentro del personal de seguridad privada, especialmente en el ámbito marítimo y costero. Tienen la responsabilidad de garantizar la seguridad de las instalaciones y actividades pesqueras, así como de prevenir actividades ilegales como la pesca furtiva o la piratería marítima. Jefes de seguridad: Son personas habilitadas y responsables de la dirección, coordinación y control de los servicios de seguridad privada en empresas, entidades o establecimientos prestatarias de servicios de seguridad. Directores de seguridad: Son profesionales con una formación específica en seguridad y una habilitación legal que los capacita para ejercer funciones de dirección y coordinación de la seguridad integral en

abril, de seguridad privada (LSP). Establece el carácter de complementariedad de la Seguridad Privada con la Seguridad Pública.

En materia de protección de Infraestructuras Críticas es de capital importancia el papel que juegan, no sólo los Vigilantes de Seguridad, sino que, de manera muy especial la figura de los Directores de Seguridad, especialistas en gerenciar riesgos de cualquier tipología, que han de velar por la seguridad y la protección integral de las Infraestructuras Críticas, indistintamente del sector de actividad al que pertenezca. Figura obligatoria y que, legalmente ha de implementarse en las Infraestructuras Críticas tal y como se expondrá con posterioridad y que, en cualquier caso, recoge la propia Ley 8/2001, de protección de Infraestructuras Críticas a tenor de su artículo 16.

Figura 9

Diagrama de Flujo de Datos. Seguridad Pública y Privada. Fuente: elaboración propia.



En relación a las más importantes similitudes y diferencias entre la Seguridad Pública y la Seguridad Privada, en atención a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, en el caso de la Seguridad Pública, así como a la Ley 5/2014, de 4 de abril, de seguridad privada concluimos las siguientes similitudes y diferencias:

---

empresas, organismos públicos u otras entidades. Los directores de seguridad son responsables de elaborar planes de seguridad, coordinar la protección de bienes y personas, y establecer medidas preventivas contra posibles riesgos.

Similitudes:

1. Regulación legal: ambas leyes establecen un marco legal para la seguridad, ya sea pública o privada, en España.

2. Control estatal: tanto la seguridad pública como la privada están sujetas a regulación y supervisión por parte del Estado, aunque en el caso de la seguridad privada, también se contempla la autorregulación y el control por parte de la Administración Pública.

3. Cooperación: ambas áreas pueden cooperar en determinadas circunstancias para garantizar la seguridad ciudadana.

Diferencias:

1. Responsabilidades y funciones: la seguridad pública está a cargo de las Fuerzas y Cuerpos de Seguridad, que tienen la responsabilidad de garantizar el orden público y la seguridad ciudadana, investigar delitos, y otras funciones relacionadas con el mantenimiento del orden público y la seguridad. Por otro lado, la seguridad privada se refiere a actividades de seguridad llevadas a cabo por entidades privadas, como empresas de seguridad, y sus funciones están orientadas principalmente a la protección de bienes, instalaciones y personas en el ámbito privado.

2. Formación y requisitos: las personas que trabajan en seguridad pública suelen pasar por formación específica y cumplir con requisitos establecidos por las autoridades competentes. En el caso de la seguridad privada y su personal, se requiere la obtención de la correspondiente habilitación profesional, así como cumplir con los requisitos y criterios establecidos en la ley.

3. Ámbito de actuación: la seguridad pública tiene un ámbito de actuación más amplio, ya que se encarga de garantizar el orden público y la seguridad en todo el territorio nacional. Por otro lado, la seguridad privada actúa principalmente en el ámbito de la protección de bienes, instalaciones y personas de carácter privado.

En relación a lo expuesto, la importancia de esas sinergias que legalmente se establecen se disponen en la LSP (2014) y cuyo tenor literal reza:

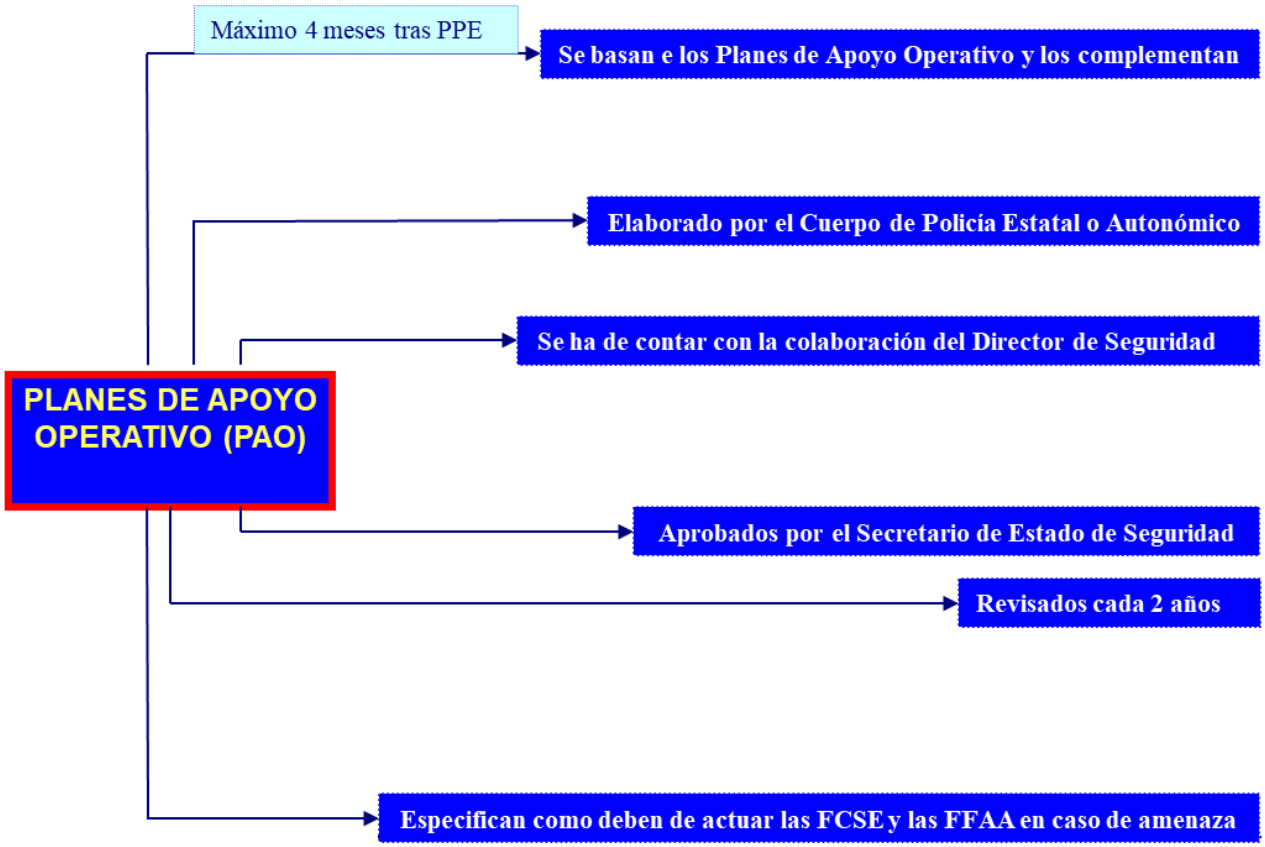
> La ley pasa de poner el acento en el principio de la subordinación a desarrollar más eficazmente el principio de complementariedad a través de otros que lo desarrollan, como los de cooperación o de corresponsabilidad, mediante una técnica legislativa

> más flexible que permite una adaptación permanente a los cambios que experimente la sociedad sin que sea precisa una reforma de rango legal para ello. (Preámbulo, III, p. 8).

En relación a los Planes de Apoyo Operativo que han de realizar los miembros de las distintas Fuerzas y Cuerpos de Seguridad con competencias en el territorio en el que se encuentre la Infraestructura Crítica a proteger, adjuntamos el Diagrama de Flujo de Datos en relación a sus características más importantes:

Figura 10

Diagrama de Flujo de Datos. Planes de Apoyo Operativo. Fuente: elaboración propia.



5. **Organizaciones de ciberseguridad**:

En relación a sus cometidos más representativos: en el ámbito de la ciberseguridad, agencias y organismos especializados, como la Agencia de Seguridad Cibernética de la UE (ENISA) o la Agencia Española de Ciberseguridad (INCIBE), colaboran en la protección de

Infraestructuras Críticas mediante la identificación de amenazas cibernéticas y la promoción de buenas prácticas de seguridad.

6. **Cooperación internacional y organismos internacionales**:

En relación a los cometidos más relevantes: los estados suelen colaborar a nivel internacional en la protección de Infraestructuras Críticas, compartiendo información sobre amenazas y riesgos. Además, organismos como la Organización de las Naciones Unidas (ONU) y la Unión Europea (UE) promueven la cooperación y la armonización de estándares de seguridad en este ámbito.

7. **Sector privado y operadores de servicios esenciales**:

Los cometidos con mayor representatividad: los operadores de servicios esenciales, en colaboración con el sector privado, tienen la responsabilidad de implementar medidas de seguridad para proteger sus infraestructuras y sistemas críticos.

8. **Organismos reguladores**:

En relación con el principal cometido de las entidades reguladoras: en algunos países, los organismos reguladores, como las autoridades de energía, transporte o comunicaciones, supervisan y regulan la seguridad de las Infraestructuras Críticas en su sector respectivo.

9. **Ciudadanos y sociedad civil**:

En relación a los cometidos de la buena ciudadanía: fomentar la concienciación sobre la importancia de la protección de las Infraestructuras Críticas y reportar actividades sospechosas o incidentes es fundamental para la seguridad de estas infraestructuras. En el caso que nos ocupa son las distintas administraciones quiénes tienen que dar la oportuna información al respecto a la sociedad civil.

La colaboración efectiva entre estos agentes es esencial para garantizar la seguridad y la resiliencia de las Infraestructuras Críticas, ya que cada uno desempeña un papel crucial en la identificación de riesgos, la implementación de medidas de seguridad y la respuesta a incidentes que puedan afectar a estas infraestructuras esenciales. Por ello, se hacen muy necesarias e indispensables las campañas informativas, anuncios con píldoras informativas,

jornadas y congresos en los que el ciudadano de a pie pueda recibir información de cómo actuar en algún tipo de ilícito penal y especialmente en relación con las distintas Infraestructuras Críticas y otros servicios esenciales.

2.10. SEGURIDAD NACIONAL E INFRAESTRUCTURAS CRÍTICAS:

En una aproximación conceptual en relación al concepto de Seguridad Nacional y, en atención al tenor literal del artículo 3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (LSN), hemos de entenderla como:

> La acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos. (Art. 3).

La Ley de Seguridad Nacional tiene como objetivo regular los principios básicos, órganos superiores, autoridades y componentes fundamentales relacionados con la Seguridad Nacional. En relación a la política que afecta a la Seguridad Nacional ha de atenderse a Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. La LSN (2015) recoge que:

1. La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional. (Art. 4.1).

2. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración. (Art. 4.2).

3. La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez

> aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley. (Art. 4.3).

En el ámbito de la seguridad nacional, se establece (Ley 36/2015) que:

> Las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional están obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas (Art. 11.1).

En este mismo sentido, en su apartado segundo, expone, en su tenor literal que:

> (…) habrán de asegurar la disponibilidad de los servicios esenciales y la garantía de suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico. (Art. 11.2).

En relación a las funciones que competencialmente les atribuye el mencionado texto legal son:

> Al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema. (Art. 19).

Es importante destacar la estructura del Sistema de Seguridad Nacional, para ello y en relación con la LSN (2015) cuenta con:

1. El Presidente del Gobierno dirige el Sistema asistido por el Consejo de Seguridad Nacional. (Art. 20.1).
2. El Departamento de Seguridad Nacional ejercerá las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo, así como las demás funciones previstas en la normativa que le sea de aplicación. (Art. 20.2).

3. Los órganos de apoyo del Consejo de Seguridad Nacional, con la denominación de Comités Especializados u otra que se determine, ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen. (Art. 20.3).

4. Será objeto de desarrollo reglamentario, en coordinación con las Administraciones Públicas afectadas, la regulación de los órganos de coordinación y apoyo del Departamento de Seguridad Nacional, así como de los mecanismos de enlace y coordinación permanentes con los organismos de todas las Administraciones del Estado que sean necesarios para que el Sistema de Seguridad Nacional pueda ejercer sus funciones y cumplir sus objetivos; todo ello sin perjuicio de las previsiones que en materia de gestión de crisis se contienen en el título III. (Art. 20.4).

Al igual que en la Ley de Infraestructuras Críticas, el sector privado ha de participar activamente en el mantenimiento de la Seguridad Nacional, tal y como dispone la propia LSN (2015), precepto que recoge que:

> El sector privado participará en la contribución de recursos a la Seguridad Nacional. (Art. 27.5).

Por todo ello y a modo de realizar una síntesis de su contenido hemos de destacar los siguientes aspectos de relevancia:

La Ley de Seguridad Nacional tiene como objetivo regular los principios básicos, órganos superiores, autoridades y componentes fundamentales relacionados con la Seguridad Nacional. A continuación, te presento los aspectos más relevantes de esta ley:

1. Definición de Seguridad Nacional: la ley establece el concepto de Seguridad Nacional como una Política de Estado. Además, promueve la Cultura de Seguridad Nacional y busca la cooperación con las Comunidades Autónomas, el sector privado y la sociedad en general.

2. Sistema de Seguridad Nacional: la ley aborda la dirección, organización y coordinación del Sistema de Seguridad Nacional. Este sistema integra diversos componentes y agentes para abordar los desafíos de seguridad de manera eficiente.

3. Gestión de Crisis: la Ley de Seguridad Nacional contempla la gestión de crisis, permitiendo una respuesta rápida y efectiva ante situaciones que afecten la seguridad del país.

4. Contribución de Recursos: establece cómo se deben contribuir los recursos necesarios para garantizar la Seguridad Nacional.

Es importante hacer referencia a la ley de Seguridad Nacional que, en España tiene como objetivo regular los principios básicos, órganos superiores y autoridades, así como los componentes fundamentales de la Seguridad Nacional. Las claves que presenta para su comprensión y su ulterior relación con las Infraestructuras Críticas son:

1. Estrategia de Seguridad Nacional 2021:

   - ✓ La Estrategia de Seguridad Nacional se configura como el marco político estratégico de referencia para la Política de Seguridad Nacional Española.
   - ✓ Contiene:
     - Un análisis del entorno estratégico.
     - La concreción de riesgos y amenazas que afectan a la seguridad de España.
     - La definición de líneas de acción estratégicas en cada ámbito de actuación.
     - Promoción de la optimización de recursos existentes.

2. Objetivos:

   - ✓ Proteger la vida de las personas y sus derechos y libertades, así como el orden constitucional.
   - ✓ Promover la prosperidad y el bienestar de los ciudadanos.
   - ✓ Participar en la preservación de la paz y la seguridad internacional, así como defender los intereses estratégicos de nuestro país.

Por lo que, en definitiva, la Ley de Seguridad Nacional busca garantizar la seguridad y el bienestar de la sociedad española, así como su participación activa en el contexto internacional.

La Ley de Seguridad Nacional en España y la Legislación en materia de Infraestructuras Críticas están estrechamente relacionadas y desempeñan un papel crucial en la protección y funcionamiento seguro del país. Tal relación viene dada porque en materia de Protección de

Infraestructuras Críticas y de manera específica en lo que respecta a su legislación, tiene como objetivo proteger las infraestructuras esenciales cuyo funcionamiento es indispensable y no admite soluciones alternativas. Estas infraestructuras son vitales para los servicios esenciales y su perturbación o destrucción tendría un grave impacto en nuestro País, afectando por tanto a todas las cuestiones que afectan y expone la Legislación en materia de Seguridad Nacional.

2.11. MEDIDAS ORGANIZATIVAS PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Las medidas organizativas para la protección de Infraestructuras Críticas son un componente esencial de la estrategia de seguridad de estas infraestructuras. Estas medidas se centran en la organización interna de los operadores de Infraestructuras Críticas y su colaboración con las autoridades responsables de la protección. A continuación, se presentan algunas de las medidas organizativas clave:

1. Nombrar un responsable de seguridad: los operadores de Infraestructuras Críticas deben designar a un responsable de seguridad, que deberá estar en posesión de la preceptiva habilitación de Director de Seguridad por el Ministerio del Interior. Aspecto de carácter obligatorio que se recoge en la Ley de Protección de Infraestructuras Críticas en su artículo 16.
2. Establecer un equipo de gestión de crisis: se debe formar un equipo de gestión de crisis compuesto por personal con roles y responsabilidades definidos. Este equipo debe estar preparado para responder eficazmente en situaciones de emergencia y coordinar la recuperación de la infraestructura.

3. Realizar evaluaciones de riesgos y vulnerabilidades: los operadores deben llevar a cabo evaluaciones periódicas de riesgos y vulnerabilidades para identificar las amenazas que pueden afectar a la Infraestructura Crítica y evaluar su nivel de riesgo. Estas evaluaciones ayudan a priorizar las medidas de protección.

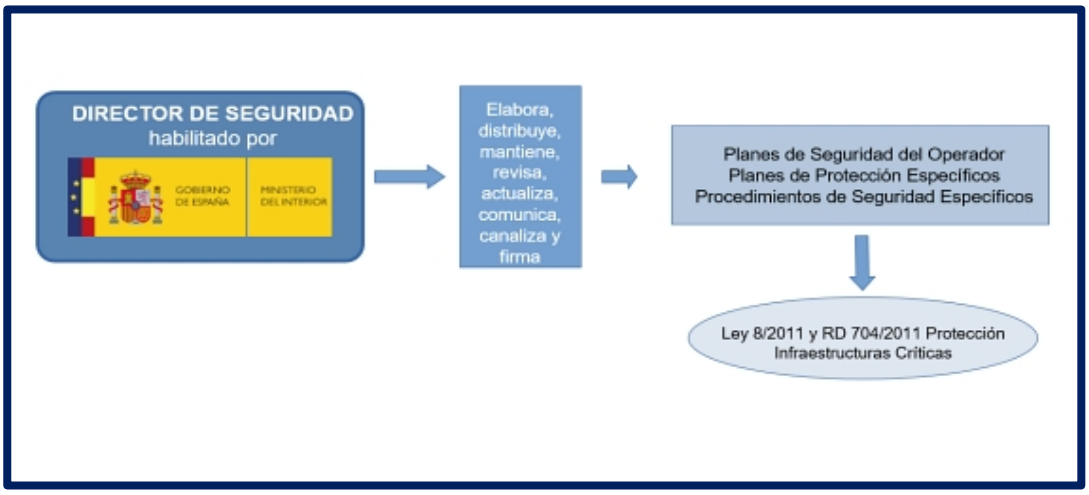
4. Desarrollar planes de seguridad y contingencia: se deben crear planes de seguridad y planes de contingencia que describan las medidas de seguridad implementadas, los procedimientos de respuesta a incidentes y las acciones a seguir en caso de una interrupción de la infraestructura. Pero de manera específica en materia de Protección de Infraestructuras Críticas, el Plan de Seguridad del Operador, los distintos Planes de Protección Específicos de cada una de las infraestructuras, así como participar activamente en la elaboración por parte de las Fuerzas y Cuerpos de Seguridad de los

Distintos Planes de Apoyo Operativo. Este aspecto es crucial debido a que es el propio Director de Seguridad el que conoce de manera pormenorizada todas las amenazas y los riesgos a los que está expuesta su organización, cuestión que genera valor por la información que se le presta en esa especial colaboración a las distintas Fuerzas y Cuerpos de Seguridad con competencias en la protección de esa infraestructura, así como por la funcionalidad que le otorga tales conocimientos al plan.

Una vez nombrado el Director de seguridad, por designación por parte de los distintos operadores Críticos de las distintas Infraestructuras Críticas, hemos de conocer cuáles son los planes que se le asignan para su ulterior elaboración, el siguiente Diagrama de Flujo de Datos da una información gráfica y rápida al respecto.

Figura 11

Diagrama de Flujo de Datos. Planes Competencias del Director de Seguridad. Fuente: elaboración propia.



2.11.1. Planes de Seguridad del Operador (PSO).

La Ley 8/2011, de Protección de Infraestructuras Críticas, así como el Real Decreto 704/2011, por el que se aprueba el Reglamento por el que se protegen las Infraestructuras Críticas, recoge una serie de medidas de carácter organizativo para aumentar la seguridad de estas infraestructuras.

Cada Operador designado como crítico por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior, deberá de nombrar a un Responsable de Seguridad y Enlace

con la habilitación profesional de Director de Seguridad quién será quién realice los distintos Planes de Seguridad aplicables a este tipo de organizaciones.

Los contenidos de estos planes vienen desarrollados en la Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.

El PSO ha de definir la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

El Plan de Seguridad del Operador, integrará, además de un índice referenciado sobre los contenidos del Plan que se enunciarán a continuación, información sobre:

- ✓ La Política General del Seguridad del Operador y Marco de Gobierno.
- ✓ La relación de Servicios Esenciales prestados por el Operador Crítico.
- ✓ La Metodología del análisis de Riesgos, tanto de amenazas físicas como de Ciberseguridad.
- ✓ Los criterios de aplicación de medidas de Seguridad Integral.

Contenidos del Plan de Seguridad del Operador:

Los aspectos que deben recogerse en el Plan de Seguridad del Operador, de acuerdo con la Resolución de la Secretaría de Estado de Interior de 2015, así como la forma en que deben ser abordados:

1. Identificación de Infraestructuras Críticas:
   - ✓ El operador debe enumerar todas las Infraestructuras Críticas bajo su responsabilidad, identificando su ubicación exacta, función y nivel de criticidad.
   - ✓ Se debe realizar una evaluación detallada de cada Infraestructura Crítica para determinar su importancia estratégica y las posibles consecuencias de un incidente de seguridad en su funcionamiento.
2. Análisis de riesgos:
   - ✓ El plan debe incluir un análisis exhaustivo de los riesgos que enfrentan las Infraestructuras Críticas, considerando amenazas potenciales, vulnerabilidades y posibles impactos.

- ✓ Este análisis debe basarse en metodologías reconocidas y establecer un proceso sistemático para la identificación, evaluación y tratamiento de los riesgos.

3. Medidas de protección:
   - ✓ Se deben definir medidas de protección específicas para cada Infraestructura Crítica, incluyendo medidas físicas, técnicas y organizativas.
   - ✓ Estas medidas deben diseñarse para mitigar los riesgos identificados y proteger las Infraestructuras Críticas contra amenazas y ataques, garantizando su continuidad operativa.
4. Coordinación y colaboración:
   - ✓ Se debe establecer un marco de coordinación y colaboración con otros operadores, autoridades competentes y partes interesadas relevantes en materia de seguridad de Infraestructuras Críticas.
   - ✓ Esto incluye la definición de roles y responsabilidades, así como la participación en ejercicios y simulacros de coordinación.
5. Gestión de incidentes y crisis:
   - ✓ Deben establecerse protocolos claros para la gestión de incidentes y crisis, que incluyan la notificación, respuesta, recuperación y comunicación de incidentes de seguridad.
   - ✓ Se deben designar equipos de respuesta y establecer procedimientos de comunicación interna y externa para garantizar una respuesta eficaz y coordinada.
6. Formación y concienciación:
   - ✓ El plan debe contemplar programas de formación y concienciación para el personal del operador, con el fin de mejorar la preparación y respuesta ante posibles amenazas.
   - ✓ Esto incluye la formación en procedimientos de seguridad, el reconocimiento de incidentes y la promoción de una cultura de seguridad dentro de la organización.
7. Evaluación y revisión:
   - ✓ Se debe establecer un proceso para la evaluación periódica y revisión del plan de seguridad, con el fin de garantizar su eficacia y adecuación a los cambios en el entorno de seguridad.

- ✓ Esto implica la realización regular de ejercicios de simulación, revisiones de riesgos y análisis de lecciones aprendidas para mejorar continuamente la capacidad de respuesta del operador.

El Plan de Seguridad del Operador debe ser un documento completo y bien estructurado que aborde todos los aspectos relevantes de la protección de las Infraestructuras Críticas, desde la identificación de riesgos hasta la gestión de incidentes y la formación del personal. Debe ser dinámico y estar sujeto a revisión periódica para garantizar su eficacia y adaptación a un entorno de seguridad en constante cambio.

2.11.2. Planes de Protección Específicos (PPE).

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y Ciberseguridad) de todas sus Infraestructuras Críticas.

Por ejemplo, Un Servicio de Salud de Carácter autonómico sería el Operador Crítico, y sus Infraestructuras Críticas, objeto del Plan de Protección Específico por cada una de esas infraestructuras, sería cada uno de sus hospitales.

Contenidos del Plan de Protección Específico:

Además de un índice referenciado a los contenidos del Plan que serán expuestos posteriormente, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

1. Descripción detallada de la infraestructura específica:
   - ✓ Identificación precisa de la infraestructura a proteger, incluyendo ubicación geográfica, dimensiones, funciones y operaciones específicas.
2. Análisis exhaustivo de riesgos específicos:
   - ✓ Evaluación detallada de los riesgos a los que está expuesta la infraestructura, considerando amenazas potenciales, vulnerabilidades específicas y consecuencias probables de incidentes de seguridad.
3. Medidas de protección adaptadas:
   - ✓ Definición de medidas de protección específicas y adecuadas a las características de la infraestructura, incluyendo seguridad física, tecnológica y de personal, así como sistemas de detección y prevención de intrusiones.

4. Procedimientos operativos y de respuesta:
    - ✓ Establecimiento de procedimientos operativos claros para la gestión de incidentes y crisis, incluyendo protocolos de notificación, activación de medidas de seguridad y coordinación con autoridades competentes.
5. Coordinación interinstitucional y colaboración:
    - ✓ Definición de roles y responsabilidades de los diferentes actores involucrados en la protección de la infraestructura, así como mecanismos de coordinación con otras entidades y autoridades relevantes.
6. Formación y concienciación del personal:
    - ✓ Implementación de programas de formación y concienciación para el personal que opera y trabaja en la infraestructura protegida, con el fin de mejorar su preparación y capacidad de respuesta ante situaciones de emergencia.
7. Plan de comunicación y divulgación:
    - ✓ Establecimiento de un plan de comunicación interna y externa para informar sobre medidas de seguridad, procedimientos de emergencia y acciones preventivas a seguir en caso de incidentes. De especial importancia la información y formación específica sobre las cuestiones reseñadas, todo ello con el objeto de favorecer las actuaciones específicas para garantizar que no se comprometa la seguridad en relación al desconocimiento de las personas, así como por falta de interiorización de las respuestas.
8. Evaluación continua y revisión periódica:
    - ✓ Implementación de un sistema de monitorización y evaluación continua del plan de protección, con revisiones periódicas para garantizar su eficacia y adaptación a cambios en el entorno de seguridad. Los simulacros y puesta en práctica de lo establecido en los distintos planes suponen la evaluación periódica al implementar cuántas medidas son efectivas en detrimento de aquellas que no lo son.
9. Actualización y mejora continua:
    - ✓ Compromiso con la mejora continua del plan de protección, mediante la identificación de lecciones aprendidas, tras el juicio crítico que ha de realizarse al final de cada ejercicio de adiestramiento, capacitación o simulacro que, conllevarán la actualización de medidas de seguridad y la incorporación de nuevas tecnologías y prácticas recomendadas.

10. Cumplimiento normativo y legal:
    - ✓ Aseguramiento de que el plan de protección cumple con la normativa y regulaciones vigentes en materia de seguridad y protección de Infraestructuras Críticas.

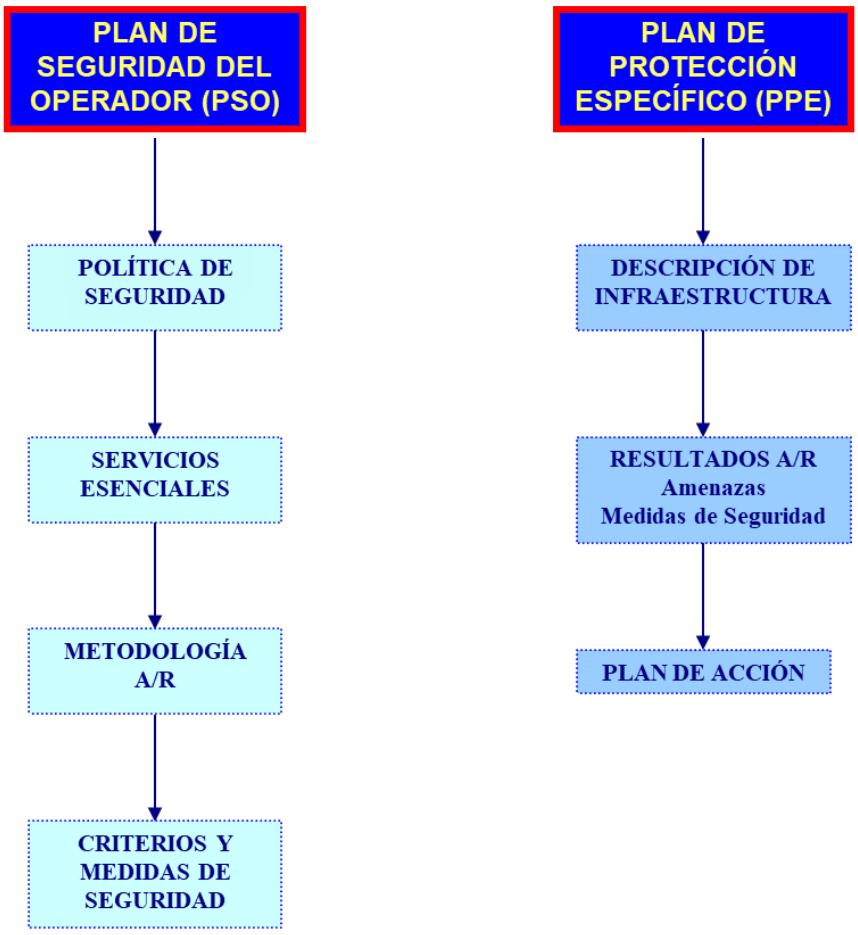
      Ha de considerarse siempre que, cualquier plan o procedimiento integra unos mínimos que pueden mejorarse en la búsqueda de la funcionalidad, la eficacia, la eficiencia en la búsqueda de la excelencia en materia de seguridad y protección integral.

      En el sentido expuesto se debe de estar a lo dispuesto por Ministerio del Interior. (2015). Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. Boletín Oficial del Estado, 9 de septiembre de 2015.

Los planes[44] de mayor interés que han de realizar El Director de Seguridad del Operador Crítico designado al efecto como tal por el Operador Crítico de la Infraestructura Crítica . Sus contenidos más importantes se reflejan en el siguiente Diagrama de Flujo de Datos:

Figura 12

Diagrama de Flujo de Datos. Contenidos del PSO y del PPE.



1. Implementar políticas de seguridad: definir y comunicar políticas de seguridad claras para el personal que trabajará en la Infraestructura Crítica. Estas políticas deben abordar el acceso a sistemas críticos, la gestión de contraseñas, la protección de datos y otros aspectos relacionados con la seguridad.

2. Establecer un sistema de gestión de la seguridad: implementar un sistema de gestión de la seguridad que siga estándares y mejores prácticas reconocidos, como ISO 27001

[44] En atención a la propia Ley de Infraestructuras Críticas y su normativa dimanante son los Planes de Seguridad del Operador (PSO), así como los Planes de Protección Específicos (PPE), por cada una de sus infraestructuras.

para la gestión de la seguridad de la información, que ayuden a garantizar un enfoque estructurado y efectivo de la seguridad.

3. Fomentar la concienciación y la formación: se ha de formar y capacitar al personal en temas de seguridad y concienciarlo sobre la importancia de seguir buenas prácticas de seguridad, incluyendo la detección y respuesta a incidentes.

4. Establecer relaciones con autoridades competentes: se ha de mantener una comunicación regular y colaborar con las autoridades responsables de la protección de Infraestructuras Críticas a nivel nacional y local con una periodicidad razonable. Esto facilita la coordinación en caso de incidentes y permite compartir información sobre amenazas.

5. Realizar ejercicios y pruebas de seguridad: llevar a cabo ejercicios y pruebas de seguridad con una periodicidad adecuada para evaluar la efectividad de los planes de seguridad y contingencia, y para identificar áreas de mejora. Tales ejercicios han de ser tanto a cuántas cuestiones pertenezcan a la seguridad física como a la seguridad lógica, en la búsqueda de un entrenamiento para las oportunas respuestas en materia de seguridad y protección integral.

6. Gestionar proveedores y terceros: evaluar y asegurar que los proveedores y terceros que interactúan con la Infraestructura Crítica cumplan con los estándares de seguridad necesarios y no representen un riesgo para la infraestructura. De importancia el estricto cumplimiento con el nuevo Esquema Nacional de Seguridad aprobado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en atención a su artículo 2, cuyo epígrafe reza ámbito de aplicación y que, el ENS (2022), en su tenor literal expone:

> El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma. (Art. 2.1).
>
> Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para

dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales. (Art. 2.2).

Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas[45] de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos. (Art. 2.3).

Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo. (Art. 2.4).

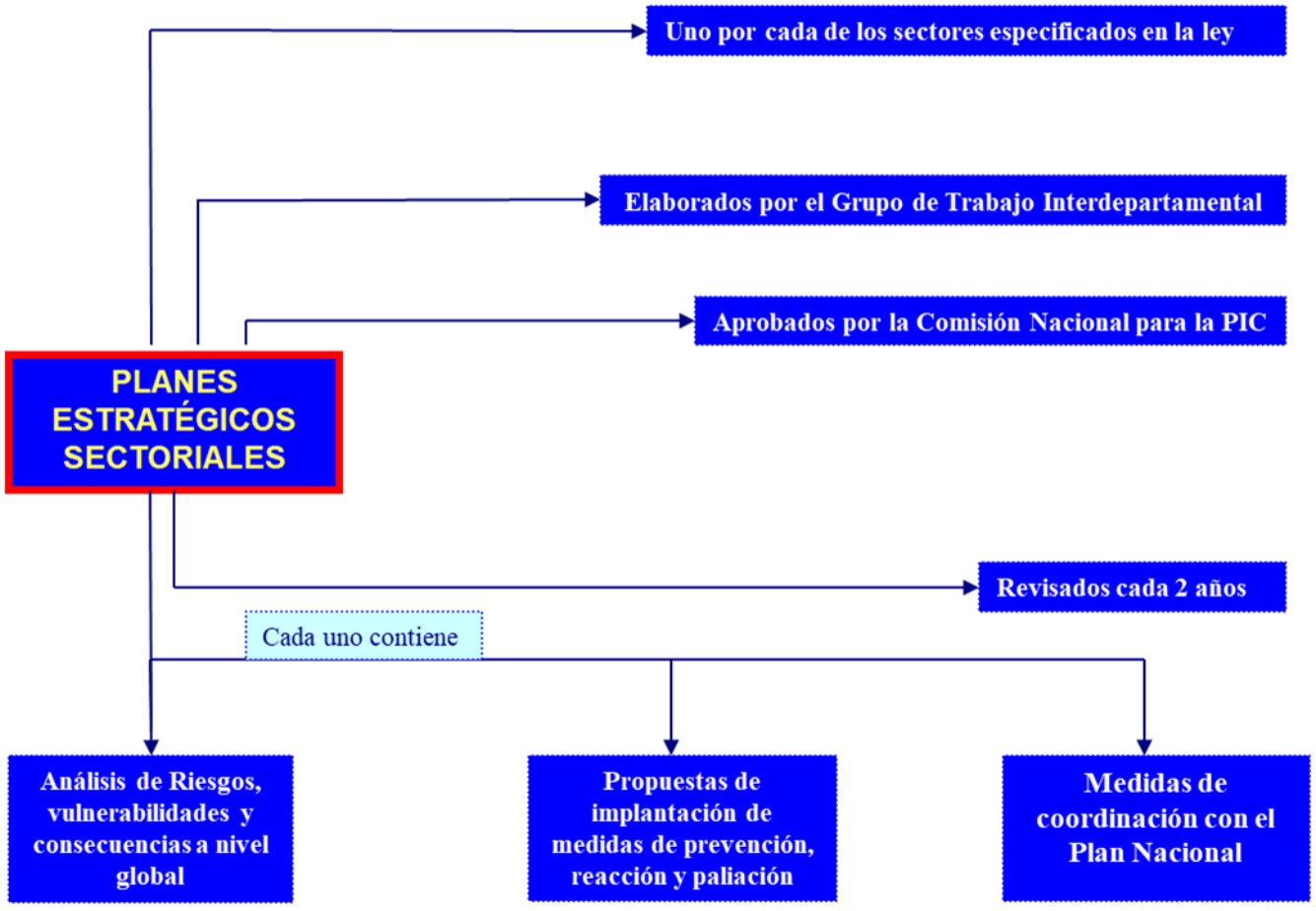
[45] La importancia del Derecho Administrativo como área vertebradora de cuántas cuestiones regulan a la seguridad y protección de las distintas Infraestructuras Críticas, así como la aplicación de legislación y normativa transversal es manifiesta.

Estas medidas organizativas son esenciales para fortalecer la seguridad y la resiliencia de las Infraestructuras Críticas, ya que permiten una gestión eficiente de los riesgos y la respuesta efectiva a aquellos incidentes que, puedan amenazar su funcionamiento. Además, contribuyen a garantizar la continuidad de las operaciones y la protección de los activos críticos.

Una vez se implanta el Plan Nacional para la Protección de las Infraestructuras Críticas, otra de las medidas organizativas correspondientes a la planificación viene dada por los distintos Planes Estratégicos Sectoriales por cada uno de los doce sectores de actividad que establece la Ley de Protección de Infraestructuras Críticas ya comentadas.

Figura 13

Diagrama de Flujo de Datos. Planes Estratégicos Sectoriales. Fuente: elaboración propia

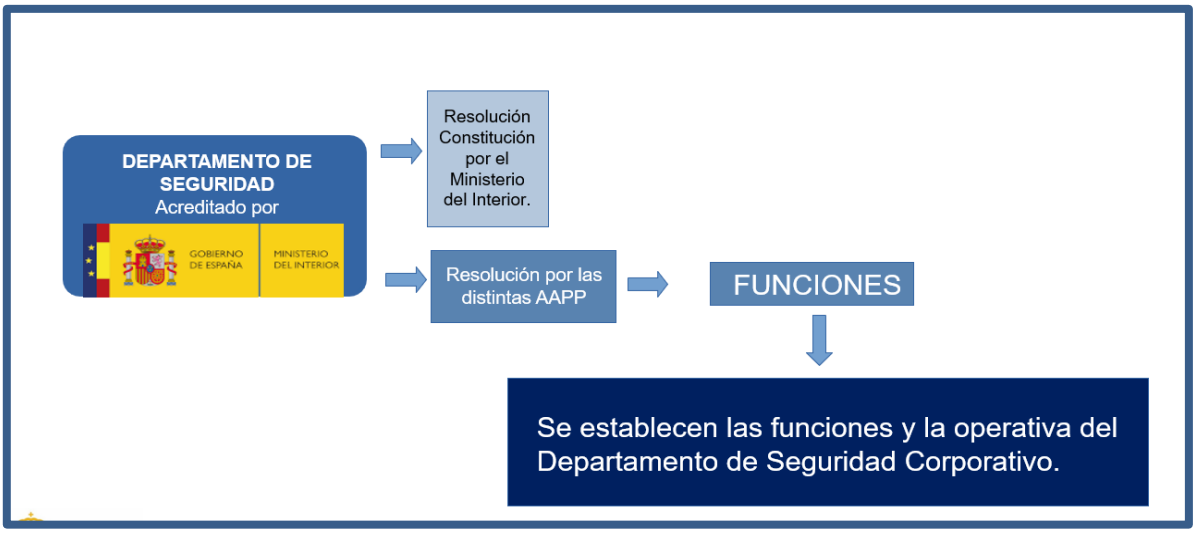


2.11.3 El Departamento de Seguridad

El departamento de seguridad desempeña un papel fundamental en la protección de Infraestructuras Críticas, ya que está encargado de planificar, implementar y supervisar las medidas de seguridad necesarias para garantizar la integridad y la continuidad de las operaciones de estas infraestructuras esenciales.

Figura 14

Diagrama de Flujo de Datos. Constitución de un Departamento de Seguridad. Fuente: elaboración propia



En relación a la necesidad de la implementación de los Departamentos de Seguridad en las distintas instituciones, organizaciones, Administraciones Públicas y empresas, en palabras de González, M., (2022):

> La inteligencia y la seguridad son un binomio indisociable e indiscutible. Desde estas humildes líneas, abogo por, además de ser indispensables, la creación y constitución de Departamentos de Inteligencia y Seguridad Patrimoniales Corporativos en las distintas administraciones, organizaciones, instituciones o empresas, debidamente dados de alta por el Ministerio del Interior. Recordemos siempre que: "La seguridad no es cara, la seguridad es inestimable y su ausencia genera la más absoluta incertidumbre y 'entropía". (p. 88).

Su importancia radica en su rol de liderar y coordinar los esfuerzos relacionados con la seguridad de la Infraestructura Crítica. A continuación, se detallan la importancia y el

funcionamiento de un departamento de seguridad en este contexto con actuaciones genéricas:

A. **Importancia del Departamento de Seguridad**:

1. Gestión de Riesgos: el departamento de seguridad es responsable de evaluar los riesgos y vulnerabilidades que pueden afectar a la Infraestructura Crítica. Esta evaluación ayuda a priorizar las medidas de seguridad necesarias para mitigar o reducir los riesgos.

2. Prevención de Amenazas: trabaja en la prevención de amenazas mediante la implementación de medidas de seguridad física, ciberseguridad y de otro tipo que protejan contra posibles incidentes o ataques.

3. Preparación y Respuesta a Incidentes: prepara al personal y establece protocolos para responder eficazmente a situaciones de crisis o incidentes que puedan afectar la Infraestructura Crítica. Esto incluye la coordinación de equipos de respuesta de emergencia.

4. Cumplimiento Normativo: asegura que la Infraestructura Crítica cumple con las regulaciones y estándares de seguridad, nacionales e internacionales aplicables.

5. Coordinación con Autoridades: colabora con las autoridades nacionales y locales responsables de la protección de Infraestructuras Críticas para garantizar una respuesta coordinada en caso de incidentes.

6. Gestión de Recursos: administra los recursos necesarios para la seguridad, incluyendo presupuesto, personal, tecnología y equipos de seguridad.

B. Funcionamiento del Departamento de Seguridad:

1. Evaluación de Riesgos: identifica y evalúa los riesgos que enfrenta la Infraestructura Crítica, incluyendo amenazas físicas, cibernéticas y otras.

2. Planificación de la Seguridad: desarrolla planes de seguridad que incluyen medidas preventivas y de contingencia.

3. Implementación de Medidas de Seguridad: pone en marcha medidas de seguridad física, tecnológica y organizativa para proteger la infraestructura.

4. Formación y Concienciación: capacita al personal en prácticas de seguridad y promueve la concienciación sobre la importancia de la seguridad.

5. Gestión de Incidentes: establece protocolos de respuesta a incidentes y coordina la gestión de crisis en caso de amenazas o incidentes.

6. Auditoría y Evaluación: Realiza auditorías y evaluaciones regulares de la efectividad de las medidas de seguridad y ajusta los planes y procedimientos en función de los resultados.

7. Coordinación Externa: colabora con organismos gubernamentales, fuerzas de seguridad, otros operadores de Infraestructuras Críticas y organizaciones de seguridad para compartir información y coordinar esfuerzos.

8. Mantenimiento de Tecnología de Seguridad: gestiona la adquisición y el mantenimiento de tecnologías de seguridad, como sistemas de vigilancia, control de acceso y sistemas de detección de intrusiones.

9. Notificación de Incidentes: cumple con la obligación de notificar incidentes significativos a las autoridades y a otros operadores de Infraestructuras Críticas, cuando sea necesario.

Por tanto, el departamento de seguridad desempeña un papel esencial y es la columna vertebrar en la que se sustentan todas las medidas de seguridad de carácter organizativo en la protección de Infraestructuras Críticas al identificar riesgos, implementar medidas de seguridad, preparar al personal y coordinar la respuesta a incidentes. Su funcionamiento adecuado contribuye a garantizar la continuidad de las operaciones y la protección de los activos críticos en caso de amenazas, materialización del riesgo, situación de emergencias o catástrofe.

En relación a los Departamentos de Seguridad y, especialmente a los Departamentos de Seguridad Corporativos en relación al uso de las tecnologías emergentes ha de estarse a lo referenciado por Rubio, G., (2023) que establece que:

> (…) por lo tanto, la tecnología es un catalizador de los datos recabables para la evaluación de los múltiples riesgos y a la vez, un multiplicador exponencial de las capacidades del Departamento de Seguridad Corporativo (DSC) para afrontar los riesgos evaluados y las amenazas detectadas. (p. 51).

En relación al adecuado uso de la tecnología por los distintos Departamentos de Seguridad Corporativos, como principal medida de carácter organizativa, garantiza una veracidad incontestable que puede, sin ningún género de dudas, constituirse en pruebas irrefutables ante cualquier requirente, así como, por parte de la Autoridad Judicial, en el sentido apuntado

Rubio, G. (2023), refiere que:

> (…) y quizás esta palabra, la objetividad, es la que defina el uso de los subsistemas, lo importante del uso de la tecnología en este sentido, es que bien aplicada, no permite el sesgo cognitivo humano, pues presenta una realidad basada en datos y no en relatos. (p. 58).

Gestionar la información precisa para la toma de decisiones, para prevenir, controlar, neutralizar o minimizar los riesgos, adoptar decisiones que en ningún momento sean extemporáneas y por lo tanto inútiles, poder establecer la planificación oportuna con las distintas medidas de seguridad pertinentes, conocer toda la legislación transversal y ser un *compliance officer* de la prevención, la seguridad y la protección integral, por todo ello, «los Departamentos de Seguridad son auténticas "unidades de inteligencia". Con la información disponible y sus diversas fuentes han de analizar y gestionar todo tipo de riesgos». González, M., (2022, p. 84).

2.11.4 El Director de Seguridad en el entorno de las Infraestructuras Críticas:

La experiencia profesional previa en la gestión y dirección de la seguridad, al frente de Departamentos de Seguridad, el nivel académico en áreas relacionadas directamente con la seguridad, así como la formación periódica y permanente son piezas de gran trascendencia y de consideración que han de acompañar a los Directores de Seguridad al frente de cualquier tipo de Infraestructura Crítica. En palabras de Istúritz, J.J., (2014), destaca que:

> La formación tiene la finalidad de impulsar un cambio cultural en las organizaciones sanitarias, que estimule el liderazgo activo de los equipos directivos e implique a todos los profesionales en la gestión de la calidad. Además, pretende ser parte de los Planes de Calidad de los centros, garantizando la existencia en cada uno de ellos de un sistema para la monitorización y mejora continua de la calidad, que permita conseguir los mejores resultados posibles en términos de efectividad, eficiencia y satisfacción de todos los clientes. (p. 46).

En el sentido expuesto, no sólo es necesaria la formación reglada, académica, de carácter oficial y la pertinente y preceptiva habilitación, sino también la experiencia previa, en el sentido que exponemos hay que destacar, en lo que respecta al perfil profesional de los

responsables corporativos en materia de seguridad, es decir, a los gerentes de riesgos o Directores de Seguridad, lo que al respecto, en relación a los requisitos, refiere Istúritz, J.J., (2023):

> - Titulación universitaria, al menos de nivel 2 de MECES.
> - Director de Seguridad habilitado por el Ministerio del Interior.
> - Experiencia superior a 3 años en gestión de la seguridad.
>
> Perfil profesional –a valorar-:
>
> - Formación específica en seguridad de organizaciones.
>
> Perfil profesional actitudinal-: Habilidades directivas; capacidad de liderazgo; Empatía.
>
> (p. 26).

De todo lo anteriormente expuesto, puede desprenderse que, un responsable ha de ser primero, un Delegado del Director de Seguridad, o estar de segundo en la gestión o dirección de áreas de responsabilidad para acreditar esos tres años de gestión de recursos específicos en materia de seguridad y emergencias, por lo que, las personas que ocupen las posiciones en áreas de responsabilidad o titularidad, se adecuarán al referenciado perfil profesional.

En el mismo sentido que el Dr. Istúritz y, en palabras de González, M., (2022):

> Hemos de empezar a tomarnos la seguridad muy en serio, pero siempre con directores de seguridad debidamente habilitados por el Ministerio del Interior, con la debida solvencia técnica, formación académica y experiencia, que permita liderar una auténtica cultura de la prevención y de la seguridad en las distintas organizaciones. No debemos de olvidar que los directores de seguridad han de formarse10 y convertirse en verdaderos analistas de inteligencia para realizar una adecuada "gerencia de riesgos" en atención a la información disponible, tomando siempre las decisiones adecuadas para evitar comprometer a la organización que han de proteger frente a todo tipo de riesgos, indistintamente de su naturaleza. (p. 88).

Sin duda alguna, la aprobación y publicación de la Ley 5/2014 supone un salto cuantitativo y a la vez cualitativo en el desarrollo profesional de la figura del Director de Seguridad. Es la figura más potenciada no sólo por este nuevo marco normativo que precisa aún más sus actuaciones competenciales, sino también por la ya publicada ley 8/2011 de Protección de

Infraestructuras Críticas y el Real Decreto 704/02001 que desarrolla el Reglamento para la Protección de tales infraestructuras.

Ese salto cualitativo se debe principalmente, según Istúritz, J.J. (2014) a que:

> La figura del director de Seguridad es inexistente en la ley de Seguridad Privada anterior, datada de 1992, ya que en su Capítulo II, dedicado al «personal de seguridad», no recoge esta figura y ha tenido que esperar a tener «rango de ley», a la recientemente aprobada ley de Seguridad Privada (LSP), que entró en vigor el 5 de junio de 2014. En origen, allá por los comienzos de la década de 2000, la figura del director de Seguridad estaba enmarcada en el ámbito de los jefes de Seguridad, de forma que constantemente se confundían las funciones de ambas figuras. En los últimos 10 años, la dirección de Seguridad ha venido regulándose y cogiendo fuerza como profesión propia en el ámbito de la Seguridad Privada y diferenciada con la del jefe de Seguridad, limitando esta última a las empresas de seguridad. (p. 86).

Los Directores y Jefes de Seguridad, en atención con las competencias que legalmente poseen, entre las que quedan integradas el establecimiento de cuántas medidas de seguridad sean necesarias para el control de los Riesgos en Seguridad, para aumentar el nivel de seguridad, neutralizar un riesgo o minimizarlo o, en su caso, hacer que ese riesgo sea al final un riesgo controlado.

Además de la habilitación para poder ejercer como Director de Seguridad hay que incidir nuevamente en los distintos aspectos formativos en diversas áreas para que pueda gestionar la seguridad desde distintos prismas en los que confluyan de manera transversal y trazable toda la legislación y normativa dimanante en materia de Seguridad y Protección Integral, la piedra angular por tanto y en palabras de Istúritz, J.J., (2014):

> (…) el punto de partida es la formación, como instrumento no sólo de aprendizaje, sino como herramienta básica que contribuya al cambio organizacional, formación no sólo como instrumento de competencia («saber hacer»), sino también como elemento que contribuya a un cambio de comportamientos y actitudes («saber ser») en un conjunto integrador. (pp. 46-47).

Las actuaciones que les son encomendadas al Director de Seguridad, primero en atención a la fecha de promulgación y aprobación de las distintas leyes y evidentemente en atención a su clasificación según el Principio de Jerarquía Normativa de nuestro ordenamiento jurídico, son, aunque no exhaustivas las siguientes:

Por un lado, la Ley 8/2011 de Protección de Infraestructuras Críticas en su artículo 16 establece la obligatoriedad por parte de los Operadores críticos de nombrar a un Responsable de Seguridad y Enlace que, ha de contar con la habilitación específica como Director de Seguridad por el Ministerio del Interior.

Este aspecto que puede resultar además de novedoso, un tanto ambiguo, no lo es debido a que como dice el precepto, el máximo responsable de la seguridad y de la protección en el sentido más amplio de la palabra, integrando tanto la Seguridad Física como la Seguridad Lógica por primera vez.

De manera gráfica se sintetizan las competencias legales atribuidas a los Directores de Seguridad en relación a la Ley de Infraestructuras Críticas y demás normativa dimanante.

Figura 15

Diagrama de Flujo de Datos. Competencias del Director de Seguridad en Infraestructuras Críticas. Fuente: elaboración propia.

De igual forma, el Real Decreto 704/2011 que desarrolla el Reglamento para la Protección de Infraestructuras Críticas, en su artículo 34, atribuye al Director de Seguridad el siguiente desarrollo competencial que citamos a continuación:

Tras la designación por los Operadores Críticos en los términos y requisitos previstos en el ya mencionado artículo 16 de la Ley 8/2011 y su ulterior comunicación a la Secretaría de Estado de Seguridad, a través del CNPIC, le corresponde al Director de Seguridad los siguientes cometidos:

- ✓ Representará al Operador Crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento.
- ✓ Canalizará las necesidades operativas e informativas que surjan.

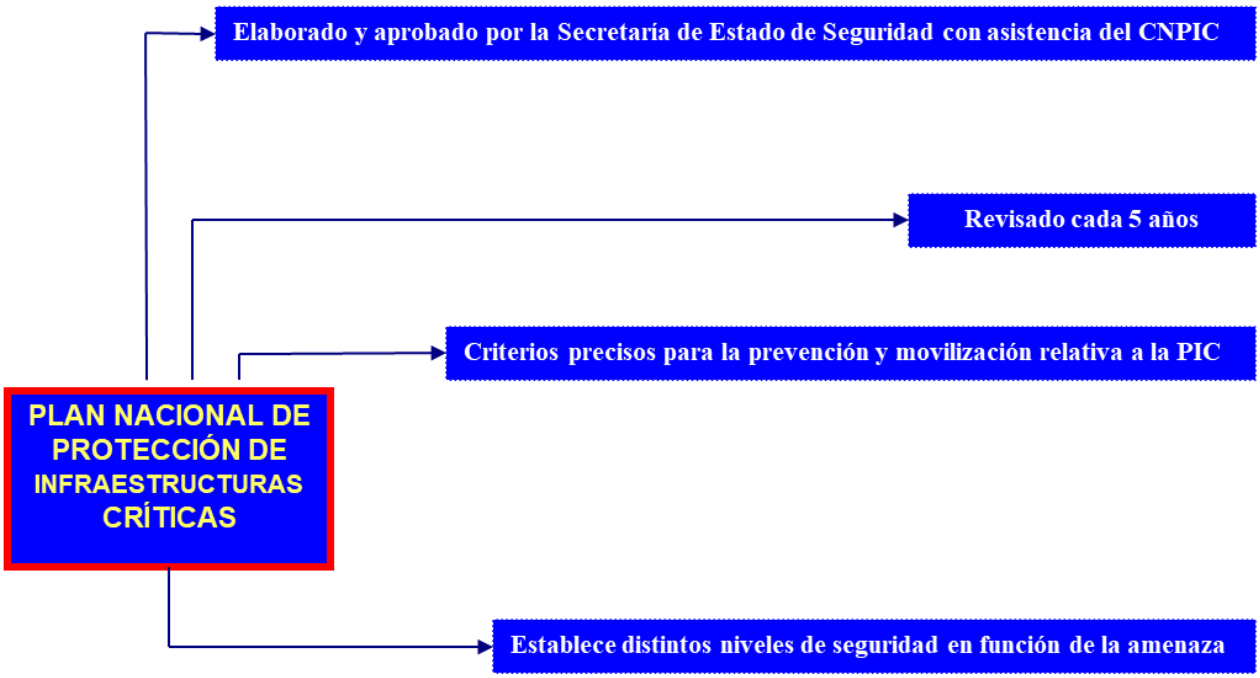
Implicaciones para el Director de Seguridad los dos puntos del precepto anterior:

Tal y como dice la norma, además de ser el Responsable de Seguridad y Enlace, habrá de Elaborar, distribuir, mantener, revisar, actualizar, comunicar y canalizar para su posterior aprobación por el Secretario de Estado de Seguridad los diferentes planes que el RD 704/2011 destaca y que enumeramos y que representaremos a continuación de forma esquematizada:

- ✓ Plan de Seguridad del Operador.
- ✓ Plan de Protección Específico.
- ✓ Planes de Apoyo Operativo (que complementarán los Planes de Protección Específicos y que, aunque han de hacerse por las FFCCSS, el Director de Seguridad de la Infraestructura colaborará en su realización).

Figura 16

Diagrama de Flujo de Datos. Plan Nacional Para la Protección de las IC. Fuente: elaboración propia



Estamos, por tanto, en la implantación de Medidas de Seguridad para el control de los riesgos de carácter organizativo. Todo lo que suponga la elaboración de memorias de seguridad, planes de seguridad de cualquier naturaleza (Planes Integrales de Seguridad, Planes Directores de Seguridad, Planes de Seguridad del Operador, Planes de Protección Específicos, Planes de Apoyo Operativo, o de cualquier otro tipo, así como procedimientos y protocolos en materia de seguridad, e incluso la creación de un Departamento de Seguridad encajaría perfectamente en las Medidas de Seguridad de Tipo Organizativo para el control de los riesgos.

Por otro lado, si nos hacemos eco de la Ley 5/2014 de Seguridad Privada y a tenor del artículo 36 y 38-5 tenemos que ese abanico de disposiciones competenciales profesionales del Director de Seguridad y sus atribuciones aumenta y, que reflejamos literalmente a continuación a modo de capitulación de lo ya expuesto en la presente investigación.

De manera sinóptica y gráfica adjuntamos las competencias legalmente establecidas que se recogen en los dos siguientes Diagrama de Flujo de Datos en el ámbito específico de la LSP.

Figura 17

Diagrama de Flujo de Datos. Competencias del Director de Seguridad LSP (I parte). Fuente: elaboración propia.

Figura 18

Diagrama de Flujo de Datos. Competencias del Director de Seguridad LSP (II parte). Fuente: elaboración propia

En relación con la empresa o entidad en la que presten sus servicios, corresponde a los Directores de Seguridad el ejercicio de las siguientes funciones en atención al artículo 36 de la Ley 5/2014, de 4 de abril, de seguridad privada:

> La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles. (Art. 36.1 a).

En relación con este punto hemos de reseñar que no sólo organizará, dirigirá, inspeccionará y administrará los Servicios de Seguridad Privada de forma conveniente en atención a su formación y experiencia previa, sino que también hará lo mismo con los recursos o medidas de seguridad privada, a tenor del artículo 52.1 de la ley de Seguridad Privada 5/2014, los tipos de medidas de seguridad, destinadas a la protección de personas y bienes aplicables también al entorno de las Infraestructuras Crítica, por tanto, según la LSP,(2014) son:

> De seguridad física, cuya funcionalidad consiste en impedir o dificultar el acceso a determinados lugares o bienes mediante la interposición de cualquier tipo de barreras físicas. (Art. 52.1 a). También son conocidas como Medidas de Seguridad Pasiva.

> De seguridad electrónica, orientadas a detectar o advertir cualquier tipo de amenaza, peligro, presencia o intento de asalto o intrusión que pudiera producirse, mediante la activación de cualquier tipo de dispositivos electrónicos. (Art. 52.1 b). También son conocidas como medidas de Seguridad Activas.
>
> De seguridad informática, cuyo objeto es la protección y salvaguarda de la integridad, confidencialidad y disponibilidad de los sistemas de información y comunicación, y de la información en ellos contenida. (Art. 52.1 c). Tales medidas de seguridad se denominan también de Seguridad Lógica.
>
> De seguridad organizativa, dirigidas a evitar o poner término a cualquier tipo de amenaza, peligro o ataque deliberado, mediante la disposición, programación o planificación de cometidos, funciones o tareas formalizadas o ejecutadas por personas; tales como la creación, existencia y funcionamiento de departamentos de seguridad o la elaboración y aplicación de todo tipo de planes de seguridad, así como cualesquiera otras de similar naturaleza que puedan adoptarse. (Art. 52.1 d).

Es decir, el resto de los medios de cualquier naturaleza que puedan garantizar una adecuada y mayor seguridad y protección de la instalación de la que el Director de Seguridad es responsable.

En ese sentido, es importante destacar otras de las competencias legales de los Directores de Seguridad que la LSP, (2014) expone en su tenor literal:

> La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio. (Art. 36.1.b).

La función principal de la seguridad es la protección, que consiste principalmente en dos actos bien diferenciados, pero estrechamente ligados entres sí que son:

- ✓ La prevención del riesgo.
- ✓ La respuesta y reacción en el supuesto de que aquél se materialice en un daño.

La identificación, análisis y evaluación de riesgos se realiza para diseñar y organizar sistemas de seguridad, adaptados específicamente para los bienes, personas, instalaciones y procesos productivos a proteger dependiendo de la tipología de la amenaza y el nivel de riesgo con el objeto de minimizarlos, neutralizarlos o controlarlos.

El objetivo es identificar el posible riesgo, analizar la probabilidad de que se produzcan y estudiar sus consecuencias. Podemos clasificar los riesgos en función de: el agente causal o de su origen, el bien que afecta, de su manifestación y el daño que causa.

Hay que destacar en este apartado la conveniencia de realizar por el Director de Seguridad una correcta evaluación de las distintas situaciones de riesgo que no sólo puedan afectar a las personas, sino también al patrimonio que se pretende proteger.

Para ello utilizará el método de análisis o de evaluación más adecuado a cada circunstancia y en especial al tipo de riesgo, tales métodos genéricamente pueden ser Métodos cualitativos, cuantitativos o semicuantitativos.

Algunos de los métodos más conocidos son: el Método de William Fine, el Método Mosler, Método del coeficiente K y factores alfa, Método de riesgo intrínseco, Método Gretener, Método Gustav Purt, Método Eric, Método Fram, Método Meseri, Método Maguerit, etc.).

Es trascendental realizar una identificación exhaustiva y una evaluación rigurosa de todos los riesgos y amenazas de la organización, las evaluaciones de riesgos, a través de una metodología específica y adaptada, son fundamentales para su gestión efectiva, lo que ayuda a minimizar la posibilidad de impactos negativos en los objetivos que se plantean y establecen previamente en la organización.

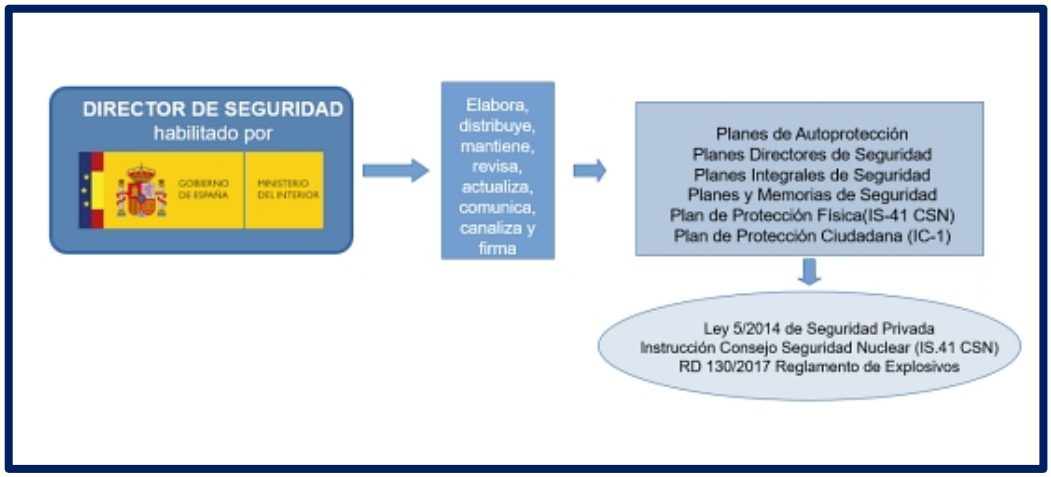
Otra de las especiales competencias de los Directores de Seguridad es la Planificación integral de toda tipología de riesgos, aspecto secuencial y ulterior a la identificación y evaluación de los riesgos. A tenor de la LSP, (2014):

> La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes[46] de seguridad aplicables. (Art. 36.1.c).

[46] Aspecto de especial relevancia para la elaboración como Técnico Competente también en Planes de Autoprotección por asimilación, ya que es entendible que un Plan de Autoprotección es un Plan de Seguridad, además de expresar el precepto riesgos de cualquier naturaleza y que se complementa con el apartado precedente de identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad física de las personas y al patrimonio.

Figura 19

Diagrama de Flujo de Datos. Competencias en planificación de los Directores de Seguridad. Fuente: elaboración propia



Atribución, en relación con todas las medidas de seguridad existente, modo de funcionamiento, pertinencia, proporcionalidad, así como la comprobación de los distintos sistemas de integración, subsistemas y medidas estén operativos para el control de los riesgos es otra de las funciones que la ley otorga a los Directores de Seguridad, así, según el tenor literal de la LSP, (2014), dispone también:

> El control del funcionamiento y mantenimiento de los sistemas de seguridad privada. (Art. 36.1.d, p. 30).

Los Directores de Seguridad, mientras se implementa cualquier tipo de medida de seguridad necesaria tras el análisis y evaluación previa para la protección de la organización, extensivo también a las Infraestructuras Críticas, pueden dar el Visto Bueno a cualquiera de los sistemas, subsistemas, mecanismos o medidas, hasta la ulterior comprobación por parte de la Administración Pública competente o cualquiera de sus entes instrumentales. En ese sentido, la LSP, (2014) en su tenor literal dice:

> La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada. (Art. 36.1.e, p. 30).).

La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes. (Art. 36.1.f).

La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones. (Art. 36.1.g).

La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo, sobre gestión de todo tipo de riesgos. (Art. 36.1.h).

Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial. (Art. 36.1.i).

El Director de Seguridad desempeña un papel esencial en la protección de Infraestructuras Críticas, ya que es el responsable de liderar y supervisar las actividades relacionadas con la seguridad de estas infraestructuras esenciales. Sus funciones y papel incluyen:

A. Funciones generales del Director de Seguridad a raíz de sus competencias legales:

1. Evaluación de Riesgos: el Director de Seguridad realiza evaluaciones de riesgos y vulnerabilidades para identificar las amenazas que pueden afectar a la Infraestructura Crítica. Esto implica analizar tanto los riesgos físicos como los riesgos cibernéticos y otros factores que puedan poner en peligro la seguridad de la infraestructura.
2. Planificación Estratégica: desarrolla planes estratégicos de seguridad que establecen las políticas, estrategias y medidas necesarias para proteger la Infraestructura Crítica .
3. Implementación de Medidas de Seguridad: supervisa la implementación de medidas de seguridad física, ciberseguridad y organizativa diseñadas para prevenir incidentes y mitigar riesgos.

4. Coordinación: colabora con otros departamentos y equipos dentro de la organización para garantizar que las medidas de seguridad se integren adecuadamente en las operaciones y los procesos de la Infraestructura Crítica.
5. Formación y Concienciación: capacita al personal en prácticas de seguridad y promueve la concienciación sobre la importancia de la seguridad entre los empleados y las partes interesadas.
6. Gestión de Incidentes: establece protocolos de respuesta a incidentes y coordina la gestión de crisis en caso de amenazas o incidentes que puedan afectar la seguridad de la infraestructura.
7. Cumplimiento Normativo: Asegura que la Infraestructura Crítica cumpla con las regulaciones y estándares de seguridad nacionales e internacionales aplicables.
8. Gestión de Recursos: administra los recursos necesarios para la seguridad, incluyendo presupuesto, personal, tecnología y equipos de seguridad.
9. Auditoría y Evaluación: realiza auditorías y evaluaciones regulares de la efectividad de las medidas de seguridad y ajusta los planes y procedimientos en función de los resultados.
10. Coordinación Externa: colabora con organismos gubernamentales, fuerzas de seguridad, otros operadores de Infraestructuras Críticas y organizaciones de seguridad para compartir información y coordinar esfuerzos.

B. Papel del Director de Seguridad:

El Director de Seguridad desempeña un papel de liderazgo en la protección de Infraestructuras Críticas y actúa como el principal defensor de la seguridad dentro de la organización. Su papel incluye:

1. Liderazgo Estratégico: define la estrategia de seguridad y la visión a largo plazo para garantizar la protección continua de la Infraestructura Crítica.
2. Toma de Decisiones: toma decisiones críticas relacionadas con la seguridad y la gestión de riesgos.
3. Gestión de Equipos: supervisa a los equipos encargados de la seguridad, incluyendo a los especialistas en ciberseguridad, seguridad física y otros profesionales de seguridad.
4. Comunicación: comunica de manera efectiva las políticas de seguridad, los protocolos y los procedimientos a todo el personal y las partes interesadas.

5. Gestión de Crisis: coordina la respuesta a situaciones de emergencia y crisis que puedan poner en peligro la Infraestructura Crítica .
6. Colaboración: colabora con otras partes interesadas, incluyendo autoridades gubernamentales, organismos reguladores y otros operadores de Infraestructuras Críticas para garantizar una respuesta coordinada y efectiva.

Grosso modo, el Director de Seguridad juega un papel crucial en la protección de Infraestructuras Críticas al liderar la planificación estratégica, la implementación de medidas de seguridad y la gestión de riesgos. Su función es garantizar la integridad y la resiliencia de la Infraestructura Crítica ante diversas amenazas y riesgos.

La base legal para la actuación del Director de Seguridad en la protección de las Infraestructuras Críticas variará según el país y su marco normativo específico. Sin embargo, en la mayoría de los países, incluyendo aquellos de la Unión Europea, existen regulaciones y leyes que establecen las responsabilidades y el marco de actuación de los Directores de Seguridad en el contexto de la protección de Infraestructuras Críticas. A continuación, mencionamos algunas de las bases legales y regulaciones comunes que suelen aplicarse:

1. Legislación Nacional: cada país tiene su propia legislación que regula la seguridad de Infraestructuras Críticas y define el papel y las responsabilidades de los Directores de Seguridad. Esta legislación incluye leyes específicas de protección de Infraestructuras Críticas, leyes de seguridad cibernética, regulaciones de seguridad física, entre otras.
2. Directivas y Regulaciones de la Unión Europea (UE): en el contexto de la Unión Europea, existen directivas y regulaciones que abordan la seguridad de Infraestructuras Críticas y establecen estándares mínimos de seguridad. Por ejemplo, la Directiva NIS (*Network and Information Systems Directive*) y la Directiva 2008/114/CE establecen obligaciones y responsabilidades para los operadores de Infraestructuras Críticas y sus Directores de Seguridad.
3. Normas y Estándares Internacionales: muchas organizaciones y países adoptan normas y estándares internacionales reconocidos para la seguridad de Infraestructuras Críticas. Por ejemplo, la norma ISO 27001 se utiliza comúnmente para la gestión de la seguridad de la información, y la norma ISO 22301 se aplica a la gestión de la continuidad del negocio.
4. Regulaciones de Ciberseguridad: en el ámbito de la ciberseguridad, se pueden aplicar regulaciones específicas que exigen la protección de Infraestructuras Críticas contra

amenazas cibernéticas. Esto puede incluir regulaciones de notificación de incidentes, estándares de seguridad cibernética y regulaciones de seguridad de la información.

5. Regulaciones Sectoriales: en algunos casos, las regulaciones específicas para sectores como el energético, el de transporte, el de comunicaciones o el financiero pueden incluir disposiciones relacionadas con la seguridad de las Infraestructuras Críticas en esos sectores, y esto puede afectar el papel del Director de Seguridad.

Es importante destacar que el Director de Seguridad en la protección de Infraestructuras Críticas debe cumplir con las leyes y regulaciones vigentes y trabajar en estrecha colaboración con las autoridades competentes y los operadores de las distintas infraestructuras para garantizar el cumplimiento de los requisitos de seguridad y la resiliencia de la infraestructura. La base legal es abundante y heterogénea, de ahí la importancia de la cualificación académica de los Directores de Seguridad. Por lo tanto, es fundamental conocer y cumplir con la normativa aplicable en cada caso y estar al día de cualquier cambio legal o normativo.

C. El Delegado de Seguridad de las Infraestructuras Críticas

Los Delegados de Seguridad desempeñan un papel importante en la protección de Infraestructuras Críticas y en la implementación de medidas de seguridad. Su función es trabajar en estrecha colaboración con el Director de Seguridad y el personal de la organización para garantizar que se cumplan los requisitos de seguridad y que se mantenga un entorno seguro.

Sus competencias son las mismas que la de los directores de seguridad, todo ello porque actúan en su representación y por delegación.

En el sentido que nos ocupa ha de estarse al artículo 99 del Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, por analogía al Jefe de Seguridad, se procede con el Delegado de los Directores de Seguridad, con el epígrafe lleva por rúbrica de «la Delegación de funciones», cuyo tenor literal reza:

> Los jefes de seguridad podrán delegar únicamente el ejercicio de las facultades para autorizar el traslado de armas o la obligación de efectuar personalmente el traslado, y las relativas a comunicación con las Fuerzas y Cuerpos de Seguridad y a subsanación de deficiencias o anomalías, así como las de dirección e inspección del personal y servicios de seguridad privada, lo que requerirá la aprobación de las empresas, y habrá de recaer, donde no hubiera jefe de seguridad delegado, en persona del Servicio o

> Departamento de Seguridad que reúna análogas condiciones de experiencia y capacidad que ellos; comunicando a las dependencias de las Fuerzas y Cuerpos de Seguridad el alcance de la delegación y la persona o personas de la empresa en quienes recae, con expresión del puesto que ocupa en la propia empresa. Asimismo, deberán comunicar a dichas dependencias cualquier variación que se produzca al respecto, y en su caso la revocación de la delegación. (Art. 99).

Es decir, por analogía a la delegación de funciones del Jefe de Seguridad se hace con los Delegados del Director de Seguridad, así como que también se ha de estar a lo que dispone la legislación específica en materia de Protección de Infraestructuras Críticas.

En lo que respecta por tanto a Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas, y en especial en lo que respecta a su artículo 17, que lleva por epígrafe «el Delegado de Seguridad y enlace», cuyo tenor literal expone:

> Los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno o, en su caso al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un Delegado de Seguridad para dicha infraestructura. (Art. 17.1).

Por tanto, el papel de los Delegados de Seguridad es fundamental para garantizar que se implementen y mantengan medidas de seguridad efectivas en la Infraestructura Crítica . Actúan como enlaces entre el personal y la dirección de la organización en cuestiones de seguridad, asegurando que se sigan las políticas y procedimientos de seguridad establecidos. Su papel incluye la supervisión continua y la detección temprana de amenazas y vulnerabilidades, lo que contribuye a mantener la resiliencia de la Infraestructura Crítica y a prevenir incidentes de seguridad. La colaboración efectiva entre los Delegados de Seguridad y el Director de Seguridad es esencial para garantizar la protección adecuada de las Infraestructuras Críticas, máxime cuando el Delegado depende orgánica y funcionalmente del Director de Seguridad, ejerciendo sus mismas funciones competenciales legales.

D. Otras medidas de carácter organizativas:

Además de las medidas organizativas básicas mencionadas anteriormente, existen otras medidas de carácter organizativo que pueden ser de gran importancia para la protección de Infraestructuras Críticas. Estas medidas se centran en la gestión, la coordinación y la planificación estratégica para garantizar la seguridad y la resiliencia de las infraestructuras esenciales. A continuación, se presentan algunas de estas medidas adicionales:

1. Planificación de la Continuidad del Negocio (BCP, por sus siglas en inglés): desarrollar y mantener planes de continuidad del negocio que permitan a la organización mantener operativas sus funciones esenciales en caso de interrupciones o desastres. Estos planes deben incluir procedimientos detallados para la recuperación y la continuidad de las operaciones críticas.
2. Gestión de Crisis: establecer equipos y procedimientos de gestión de crisis que sean responsables de coordinar la respuesta y la recuperación en situaciones de emergencia. Esto incluye la designación de líderes de crisis y la realización de ejercicios de simulación de crisis.
3. Gestión de Proveedores y Terceros: evaluar y gestionar los riesgos asociados con los proveedores y terceros que tienen acceso o interactúan con la Infraestructura Crítica. Esto incluye asegurarse de que estos proveedores cumplan con estándares de seguridad y tengan medidas de protección adecuadas.
4. Coordinación Intersectorial: colaborar con otros operadores de Infraestructuras Críticas y autoridades de otros sectores para compartir información sobre amenazas, vulnerabilidades y mejores prácticas. Esto puede ser especialmente importante en situaciones de amenazas transversales.
5. Evaluaciones de Impacto en la Seguridad (SIA, por sus siglas en inglés): realizar evaluaciones de impacto en la seguridad que analicen cómo las amenazas y los riesgos pueden afectar a la Infraestructura Crítica y su entorno operativo. Esto ayuda a priorizar las inversiones en seguridad.
6. Capacitación y Concienciación Continua: proporcionar formación y concienciación continuas al personal en temas de seguridad y en la detección de amenazas y riesgos emergentes.
7. Revisión y Actualización Periódica de Políticas y Procedimientos: revisar y actualizar regularmente las políticas y los procedimientos de seguridad para reflejar cambios en las amenazas, las tecnologías y las operaciones de la infraestructura.

8. Evaluaciones de Cumplimiento: realizar evaluaciones regulares para asegurarse de que se cumplan las políticas y los estándares de seguridad y para identificar cualquier incumplimiento o debilidad.
9. Investigación y Análisis de Incidentes: llevar a cabo investigaciones y análisis detallados de los incidentes de seguridad para identificar las causas raíz, aprender lecciones y mejorar las medidas de seguridad.
10. Conexión con la Comunidad de Seguridad: mantener conexiones con la comunidad de seguridad, incluyendo compartir información y mejores prácticas con otras organizaciones y participar en grupos de intercambio de información de seguridad.

Estas medidas organizativas adicionales contribuyen a fortalecer la seguridad y la resiliencia de las Infraestructuras Críticas al permitir una gestión más efectiva de los riesgos y una respuesta más eficiente a situaciones de emergencia. La gestión y la coordinación adecuadas son esenciales para proteger estas infraestructuras esenciales.

RESUMEN DEL CAPÍTULO.

El presente capítulo recoge la importancia del derecho administrativo que desempeña un papel crucial en la estructura y el funcionamiento del Estado moderno, al garantizar la legalidad, la justicia y la eficiencia en la acción de la Administración, así como la protección de los derechos y libertades de los ciudadanos, así como la especial relación con la seguridad en general, la seguridad hospitalaria en particular, así como con las Infraestructuras Críticas.

También recoge la especial trascendencia de dar una respuesta adecuada para la protección de las distintas Infraestructuras Críticas, su especial relación con la Protección Civil. Su protección es esencial para la seguridad nacional, el bienestar económico, la seguridad de la población y la continuidad del gobierno, así como para proteger contra amenazas cibernéticas en un mundo cada vez más interconectado.

Además de los distintos agentes que garantizan su protección así como las distintas medidas organizativas en relación a los distintos planes, ha podido objetivarse la necesidad de implantarse un Departamento de Seguridad bajo la dirección de un Director de Seguridad debidamente habilitado por el Ministerio del Interior para que pueda llevare a cabo el gran abanico competencial que esta figura y la de sus delegados poseen con el objeto de protegerla de todo tipo de ataques y garantizar su funcionamiento y continuidad como servicios estratégicos y esenciales que son para la sociedad.

CAPÍTULO III

Seguridad Hospitalaria

«**No hay nada más atroz y execrable que atentar contra los que prestan asistencia en un acto de empatía y humanidad**».
Martín González

CAPÍTULO III

3. CAPÍTULO III. LA SEGURIDAD Y LA PROTECCIÓN INTEGRAL EN HOSPITALES.

La seguridad y la protección integral en los hospitales son aspectos críticos para garantizar un entorno seguro y propicio para la atención médica, tanto para pacientes como para personal médico y visitantes. Estos centros complejos e Infraestructuras Críticas desempeñan su labor asistencial en ocasiones en un entorno caótico y a veces impredecible, especialmente en emergencias médicas o situaciones de alta tensión, tensión que puede verse incrementada por mantener la atención asistencial durante una catástrofe. La implementación de medidas de seguridad adecuadas ayuda a proteger tanto al personal médico como a los pacientes de cualquier forma de violencia, agresión o abusos. Ambos conceptos se suman y son trascendentales para garantizar un entorno seguro y propicio para la atención sanitaria y médica de calidad, así como para proteger la salud y el bienestar tanto del personal como de los pacientes.

De consideración en materia de seguridad hospitalaria y los distintos sistemas de salud y, en palabras de Istúritz, J.J. (2014)

> Para que un sistema de seguridad sea excelente en el ámbito de las organizaciones de salud debe contar con un sistema de formación, adaptable, ágil, que responda a las necesidades de cada momento, evaluable y acreditable. (p. 48).

3.1 INTRODUCCIÓN AL CAPÍTULO.

Los hospitales son instituciones de vital importancia en cualquier sociedad. Desempeñan un papel integral en la promoción de la salud, la prevención y el tratamiento de enfermedades, la investigación médica, la formación de profesionales de la salud, el apoyo emocional y social en la atención de patologías mentales, así como ayudan de manera sinérgica al impulso económico de una sociedad. Su importancia no puede ser subestimada en la provisión de atención médica y el bienestar general de la población. Pero en cualquier caso su importancia viene dada por los siguientes motivos:

1. Atención médica y emergencias: los hospitales proporcionan atención médica de emergencia y atención especializada a personas que sufren enfermedades graves,

lesiones traumáticas o cualquier otra condición médica que requiera atención inmediata y experta.

2. Prevención y tratamiento de enfermedades: los hospitales no solo tratan enfermedades, sino que también desempeñan un papel crucial en la prevención y el control de enfermedades. Ofrecen programas de vacunación, detección temprana de enfermedades, asesoramiento sobre salud y educación para promover estilos de vida saludables.

3. Investigación médica: muchos hospitales están asociados con instituciones de investigación médica donde se llevan a cabo estudios clínicos y experimentos para desarrollar nuevos tratamientos, medicamentos y procedimientos médicos. Esta investigación es fundamental para avanzar en la medicina y mejorar la calidad de la atención médica en general.

4. Formación y educación: los hospitales también son centros de enseñanza médica donde los estudiantes de medicina, enfermería y otros profesionales de la salud reciben formación práctica y clínica. Esto es esencial para garantizar que haya una fuerza laboral médica capacitada y calificada en el futuro. Este aspecto académico se incardina en los llamados Hospitales Universitarios[47] que, se caracterizan porque instituciones médicas que están afiliadas a una universidad o institución de educación superior. Poseen ciertas características distintivas que los diferencian de otros hospitales tales como:

    a. Enseñanza y formación: una característica fundamental de los hospitales universitarios es su función como centros de enseñanza y formación para estudiantes de medicina, enfermería y otros profesionales de la salud. Estos hospitales ofrecen oportunidades de aprendizaje práctico y clínico bajo la supervisión de profesores y profesionales médicos experimentados.

    b. Investigación médica: los hospitales universitarios suelen estar asociados con programas de investigación médica y académica. Aquí se llevan a cabo estudios clínicos, ensayos y proyectos de investigación para avanzar en el

[47]Son centros médicos multifacéticos que combinan la atención médica, la educación y la investigación para ofrecer servicios de salud de alta calidad, formar a futuros profesionales de la salud y contribuir al avance de la medicina y la ciencia.

conocimiento médico y desarrollar nuevas terapias, tratamientos y procedimientos.

c. Atención médica especializada: la mayoría de los hospitales universitarios son centros de atención médica especializada que ofrecen servicios avanzados en diversas áreas de la medicina, como oncología, cardiología, neurología, trasplantes de órganos, entre otros. Estos hospitales suelen ser referencias regionales o nacionales para el tratamiento de enfermedades complejas o poco comunes.

d. Integración con la comunidad académica: los hospitales universitarios están estrechamente integrados con la comunidad académica, trabajando en colaboración con facultades de medicina, escuelas de enfermería y otros departamentos relacionados con la salud. Esta integración fomenta la investigación interdisciplinaria y el intercambio de conocimientos entre profesionales de diferentes campos.

e. Atención centrada en el paciente: a pesar de su enfoque en la enseñanza y la investigación, los hospitales universitarios siguen priorizando la atención centrada en el paciente. Se esfuerzan por proporcionar atención médica de alta calidad y compasiva a los pacientes, al tiempo que integran la formación de estudiantes y la investigación médica en su práctica clínica.

f. Recursos avanzados y tecnología: los hospitales universitarios suelen tener acceso a recursos y tecnología médica de vanguardia. Esto incluye equipos de diagnóstico avanzado, instalaciones quirúrgicas de última generación, unidades de cuidados intensivos especializados y laboratorios de investigación bien equipados.

5. Apoyo emocional y social: los hospitales brindan apoyo emocional y social a los pacientes y sus familias durante momentos difíciles de enfermedad o lesión. Esto puede incluir servicios de asesoramiento, grupos de apoyo, servicios pastorales y otros recursos para ayudar a las personas a sobrellevar las dificultades emocionales y sociales relacionadas con la salud.

6. Contribución a la economía: los hospitales generan empleo y contribuyen a la economía local al proporcionar trabajo a médicos, enfermeras, personal de apoyo y

otros profesionales de la salud. También impulsan la economía al invertir en equipos médicos avanzados y tecnología, y al atraer a pacientes de otras áreas que requieren atención especializada.

En lo que respecta a la Seguridad Hospitalaria a nadie se le escapa la suma importancia que comporta en estos centros complejos por múltiples razones cruciales para proteger a pacientes y personal, prevenir infecciones nosocomiales, proteger la información confidencial, evitar riesgos laborales y garantizar la continuidad del servicio médico en todo momento. Es un componente esencial de la calidad de la atención médica y del bienestar general de la comunidad, por lo que se hace necesaria la:

1. Protección de pacientes y personal: los centros hospitalarios son lugares donde las personas acuden en busca de atención médica y tratamiento. La seguridad en los hospitales garantiza la protección de los pacientes y del personal médico y de apoyo contra cualquier amenaza o peligro que pueda surgir, ya sea interno (como accidentes o errores médicos) o externo (como robos, violencia o desastres naturales).

2. Prevención de infecciones nosocomiales: la seguridad en los hospitales incluye medidas para prevenir la propagación de infecciones nosocomiales, es decir, infecciones adquiridas durante la estancia en el hospital, lo que comporta aumentar la «Seguridad Biológica», especialmente en las llamadas áreas críticas hospitalarias. Estas medidas pueden incluir prácticas de higiene adecuadas tales como la limpieza y desinfección rigurosas, el uso de los distintos equipos de Protección Individual (EPI), el riguroso y estricto control de la administración de antibióticos para prevenir la resistencia bacteriana.

3. Protección de la información confidencial: los hospitales manejan una gran cantidad de información confidencial de los pacientes, que incluye datos médicos, financieros y personales. La seguridad en los hospitales garantiza, o al menos debe de garantizar la protección de esta información contra accesos no autorizados, robos de identidad y otras formas de intrusión digital, asegurando la privacidad y confidencialidad de los pacientes en relación a las distintas Historias Clínicas en las que se guardan todo tipo de datos de carácter personal concernientes a la salud.

4. Prevención de riesgos laborales: los hospitales pueden presentar una serie de riesgos laborales para el personal, incluidos los accidentes por exposición a sustancias químicas, lesiones por manejo de equipos médicos pesados, agresiones de pacientes o

familiares, entre otros. La seguridad en los hospitales implica la implementación de medidas de prevención de riesgos laborales y la capacitación del personal en prácticas seguras de trabajo.

5. Mantenimiento de la continuidad del servicio: la seguridad en los hospitales es esencial para garantizar la continuidad del servicio médico, incluso en situaciones de emergencia o crisis. Esto implica tener planes de contingencia y protocolos de respuesta ante desastres para mantener la atención médica ininterrumpida y asegurar la seguridad de los pacientes y el personal durante eventos como incendios, terremotos o pandemias.

No podemos obviar que los Centros Hospitalarios son Infraestructuras Críticas y como tales, debido a su importancia para el funcionamiento continuo de una sociedad y su papel vital en la salud pública, la resiliencia comunitaria y la seguridad en general. Su capacidad para mantener la operación continua y responder eficazmente a emergencias es fundamental para el bienestar y la seguridad de la sociedad. Todo ello, debido especialmente a las siguientes razones:

1. Vitalidad comunitaria: los hospitales son pilares de la salud pública y juegan un papel crucial en el mantenimiento del bienestar de la comunidad. Proporcionan atención médica esencial para tratar enfermedades, lesiones y emergencias, contribuyendo así a la salud y la seguridad de la población en general.

2. Resiliencia y respuesta ante emergencias: los hospitales deben estar preparados para responder a una variedad de emergencias y desastres, como pandemias, desastres naturales, incidentes químicos o biológicos, y eventos terroristas. Su capacidad para mantener la operación durante situaciones de crisis es fundamental para la resiliencia de la comunidad y la capacidad de recuperación.

3. Continuidad de la atención médica: la interrupción de los servicios médicos podría tener consecuencias catastróficas para una comunidad. Los hospitales deben asegurar la continuidad de la atención médica, incluso en situaciones de emergencia, para garantizar que los pacientes reciban el tratamiento y la atención necesarios.

4. Protección de información confidencial: los hospitales manejan una gran cantidad de información confidencial sobre pacientes, incluidos datos médicos y personales. La

protección de esta información es fundamental para garantizar la privacidad y la seguridad de los pacientes y mantener la confianza en el sistema de salud.

5. Impacto económico y social: los hospitales no solo proporcionan atención médica, sino que también son importantes motores económicos y empleadores en muchas comunidades. Su funcionamiento continuo es crucial para mantener la estabilidad económica y social de la región.

6. Colaboración y coordinación: los hospitales trabajan en estrecha colaboración con otras organizaciones de la administración y sus distintos equipos de respuesta a emergencias para garantizar una respuesta efectiva a situaciones de crisis. Su participación en planes de preparación y coordinación es esencial para la gestión eficaz de emergencias y desastres.

La Organización Mundial de la Salud elevó el 11 de marzo de 2020 la situación ocasionada por la Covid-19 de emergencia de salud pública a pandemia internacional, lo que ha dado lugar a una crisis sanitaria sin precedentes y de enorme magnitud, tanto, por el muy elevado número de ciudadanos afectados como por el extraordinario riesgo para sus derechos.

La rapidez en la evolución de esta pandemia, tanto a escala nacional, como a nivel internacional, ha provocado la adopción de diferentes medidas orientadas a proteger la salud y seguridad de las personas, contener la progresión de la enfermedad, reforzar el sistema de salud pública, garantizar el funcionamiento de servicios públicos esenciales y, hacer frente al impacto económico y social negativo derivado de este tipo de incidentes. Por todo ello, la pandemia originada por el Virus *Sars-Cov*-2, ha destacado la importancia crítica de las infraestructuras hospitalarias de varias maneras:

1. Capacidad de atención médica: durante la pandemia, se ha evidenciado la necesidad de contar con suficientes camas hospitalarias, equipos médicos y personal capacitado para hacer frente a una afluencia masiva de pacientes. Las infraestructuras hospitalarias bien equipadas y preparadas pueden proporcionar una atención adecuada a un gran número de pacientes afectados por COVID-19, así como a aquellos con otras condiciones médicas.

2. Equipamiento médico y suministros: las infraestructuras hospitalarias dependen de un suministro constante de equipos médicos, dispositivos de protección personal y suministros médicos esenciales para garantizar la seguridad y la atención adecuada de

los pacientes. La escasez de estos recursos durante la pandemia resaltó la importancia de tener sistemas de suministro robustos y reservas estratégicas para hacer frente a emergencias de salud pública.

3. Infraestructura digital y tecnológica: la pandemia aceleró la necesidad de infraestructuras digitales y tecnológicas en hospitales, como sistemas de telemedicina, registros médicos electrónicos y herramientas de comunicación remota. Estas infraestructuras permiten la coordinación eficiente del personal médico, la monitorización remota de pacientes y la prestación de atención médica a distancia, lo que es crucial para el manejo de emergencias sanitarias como la pandemia de COVID-19.

4. Resiliencia y capacidad de adaptación: la capacidad de las infraestructuras hospitalarias para adaptarse rápidamente a situaciones cambiantes y responder de manera efectiva a emergencias de salud pública es fundamental. La pandemia ha resaltado la importancia de la resiliencia y la flexibilidad en el diseño y la operación de las infraestructuras hospitalarias para hacer frente a crisis inesperadas y garantizar la continuidad de la atención médica.

La pandemia por el Virus del *Sars-Cov2*, ha subrayado la importancia crítica de las infraestructuras hospitalarias bien equipadas, resistentes y adaptativas para garantizar la capacidad de respuesta efectiva ante emergencias de salud pública y proporcionar atención médica de calidad a la población.

Además de lo expuesto, las carencias que los distintos centros hospitalarios se pusieron de manifiesto frente al colapso asistencial en el que miles de personas enfermaban gravemente y otras fallecían por la enfermedad de la COVID-19, cuestiones que quedaron desgraciadamente constatadas por:

1. Sobrecarga del sistema de salud: en muchos lugares, el aumento repentino y masivo de casos de COVID-19 llevó a un colapso del sistema de salud, no sólo en España y sus distintas Comunidades Autónomas, sino a nivel mundial. Los hospitales se vieron totalmente desbordados por el gran número de pacientes que requerían atención médica, lo que resultó en la falta de camas, equipos médicos tales como respiradores en áreas críticas o especiales como son las Unidades de Cuidados Intensivos, así como por la falta de personal capacitado para manejar la situación que, a la vez carecían de

los Equipos de Protección Individual (EPI), adecuados al riesgo biológico y su peligrosidad.

2. Escasez de suministros médicos: la alta demanda de suministros médicos, como ventiladores, EPI y medicamentos, superó la capacidad de producción y distribución, lo que llevó a escaseces y dificultades para proporcionar atención médica adecuada a los pacientes.

3. Falta de personal médico y agotamiento del personal existente: el aumento repentino de casos de COVID-19 agotó los recursos humanos en el sector de la salud. Muchos hospitales enfrentaron escasez de personal médico y de enfermería, lo que resultó en largas horas de trabajo y agotamiento del personal existente.

4. Falta de capacidad de respuesta rápida y coordinación: en algunos lugares, la falta de infraestructuras y sistemas de salud preparados para responder rápidamente a una pandemia resultó en una falta de coordinación entre los diferentes niveles de atención médica y dificultades para implementar medidas efectivas de contención y control de la enfermedad. En España se puso de manifiesto entre la administración estatal y el resto de las administraciones autonómicas, las respuestas iniciales fueron extemporáneas, con lo que no fueron adecuadas.

5. Necesidad de adaptación tecnológica: la pandemia destacó la necesidad de infraestructuras hospitalarias modernizadas y sistemas de salud digitalizados que pudieran facilitar la atención médica remota, la monitorización de pacientes y la gestión eficiente de los recursos.

Por todo ello, el colapso asistencial durante la pandemia de COVID-19 puso de relieve las carencias en las infraestructuras hospitalarias, incluyendo la falta de capacidad, suministros insuficientes, escasez de personal médico y la necesidad de adaptación tecnológica. Estos desafíos resaltaron la importancia de invertir en infraestructuras hospitalarias sólidas y sistemas de salud resilientes para hacer frente a crisis sanitarias futuras en los que la Seguridad Privada, de la mano de la Seguridad Pública y el resto de Servicios de Emergencia fueron pieza fundamental para evitar la propagación y «vectorización» de la enfermedad al controlar y hacer que las personas adoptasen siempre todas las medidas preventivas e higiénicas al efecto, tales como la utilización de las mascarillas adecuadas, distancia interpersonal de bioseguridad, utilización de virucidas alcohólicos, en un porcentaje adecuado para que sean germicidas, etc.

Pudo constatarse la necesidad de la creación de los Departamentos de Seguridad Hospitalarios con los que poder establecer sinergias otras áreas como son la Medicina Preventiva, la Seguridad y Salud gestionada por los Servicios de Prevención que habrían de velar por la implantación de los distintos protocolos que emanaban del Ministerio de Sanidad y de las distintas consejerías de sanidad de las distintas autonomías.

La creación de los distintos Departamentos de Seguridad en los hospitales liderados por Directores de Seguridad debidamente habilitados por el Ministerio del Interior, así como con la formación académica y experiencia previa es un pilar fundamental para garantizar la seguridad, la protección integral y la resiliencia de los centros hospitalarios.

En relación a los titulares de los Departamentos de Seguridad, es decir los Directores e Seguridad o los Directores de Seguridad Delegados integrados en su estructura y en palabras de González, M. (2018):

> Tales expertos son legal y profesionalmente los Directores de Seguridad. Son aquellos profesionales que ejercen una verdadera "Gerencia de Riesgos de carácter integral" en las distintas organizaciones en las que desarrollan su labor profesional. En cualquier caso, esa competencia profesional viene dada en distintas disposiciones legales y normativas, (Ley 8/2011 y RD 704/2011, ambos de Protección de Infraestructuras Críticas. Ley 5/2014 de Seguridad Privada. Real Decreto 130/2017, de 24 de febrero, que aprueba el Reglamento de Explosivos. Instrucción del Consejo de Seguridad Nuclear IS-41 de Protección Física de Fuentes Radioactivas). (p. 59).

3.2. APROXIMACIÓN CONCEPTUAL AL TÉRMINO DE SEGURIDAD HOSPITALARIA.

En capítulos previos hemos definido conceptos como el terrorismo, la seguridad y otros términos transversales.

La seguridad hospitalaria se refiere al conjunto de medidas, políticas y procedimientos implementados en un entorno hospitalario con el fin de proteger a los pacientes, visitantes, personal médico y las instalaciones en sí mismas.

El objetivo principal de la seguridad hospitalaria es prevenir accidentes, incidentes, violencia, y garantizar un entorno de atención médica seguro y eficiente. Aquí hay algunas áreas clave de enfoque dentro del concepto de seguridad hospitalaria:

1. Seguridad del Paciente: incluye medidas para evitar errores médicos, lesiones y complicaciones durante el tratamiento médico. Esto puede involucrar la identificación adecuada de pacientes, la administración segura de medicamentos, la prevención de infecciones nosocomiales y la mejora de la comunicación entre el personal de salud y los pacientes.

2. Seguridad del Personal: asegurar la seguridad del personal médico y no médico es fundamental para mantener un entorno de trabajo efectivo y protegido. Esto incluye la capacitación en seguridad, medidas para prevenir accidentes laborales, y la implementación de políticas para lidiar con la violencia en el lugar de trabajo.

3. Seguridad de las Instalaciones: la seguridad de las instalaciones implica la protección física de los edificios y equipos hospitalarios. Esto puede incluir sistemas de seguridad, acceso controlado a áreas sensibles, y medidas para prevenir incendios, inundaciones y otras emergencias.

4. Seguridad de la Información: la seguridad de la información en un hospital se refiere a la protección de datos médicos y personales de los pacientes. La gestión adecuada de registros médicos electrónicos, la privacidad de los pacientes y la ciberseguridad son componentes clave de esta área.

5. Seguridad en la Atención de Emergencia: Los hospitales deben estar preparados para enfrentar situaciones de emergencia, como desastres naturales, accidentes graves o actos de violencia. Los planes de respuesta a emergencias y la capacitación adecuada son esenciales para garantizar la seguridad en estos eventos.

6. Seguridad contra la Violencia[48]: la violencia en entornos hospitalarios es una preocupación creciente. La seguridad hospitalaria incluye medidas para prevenir la violencia contra el personal médico, como la implementación de sistemas de seguridad, capacitación en manejo de situaciones conflictivas y políticas de tolerancia cero hacia la violencia.

   Para ello los miembros del Observatorio de Seguridad Integral de Centros Hospitalarios elaboramos conjuntamente con la Secretaría de Estado de Seguridad la Instrucción 3/2017, medida implementada en España por el Ministerio del Interior para abordar

[48] Al efecto, y con el objeto de prevenir y reducir las agresiones al personal sanitario hospitalario, colaboramos a través del OSICH, de manera muy estrecha para la elaboración y redacción de la Instrucción 3/2017, de la Secretaría de Estado de Seguridad.

las agresiones al personal sanitario desde el ámbito de la seguridad y la policía. La instrucción establece directrices específicas para prevenir y combatir las agresiones físicas y verbales contra los profesionales de la salud.

> Entre las disposiciones principales de la referenciada norma se incluyen el promover campañas de sensibilización pública sobre las consecuencias de las agresiones al personal sanitario y las sanciones legales correspondientes. Establecer protocolos de coordinación entre las autoridades policiales, sanitarias y judiciales para garantizar una respuesta rápida y eficaz ante las agresiones. Capacitar al personal policial en técnicas de intervención y mediación para prevenir conflictos y gestionar situaciones de agresión de manera adecuada. Implementar sistemas de registro y seguimiento de las agresiones al personal sanitario para evaluar la magnitud del problema y orientar las estrategias de prevención. Brindar protección y apoyo integral a las víctimas de agresiones, incluyendo asistencia legal y psicológica. En definitiva, se busca fortalecer la seguridad y protección del personal sanitario, así como garantizar un entorno laboral seguro para que puedan desempeñar sus funciones con tranquilidad y sin temor a represalias por parte de los pacientes o sus familiares. (I. SES, 2017).

Al respecto, la Policía Nacional establece la Circular de la jefatura Central para el cumplimiento de la Instrucción 3/2017, sobre medidas policiales a adoptar frente a agresiones a profesionales de la salud.

7. Seguridad en la Atención a Niños y Ancianos: los pacientes más vulnerables, como niños y ancianos, requieren una atención y protección especial.

   Los hospitales deben implementar medidas adicionales para garantizar su seguridad y bienestar. Se crean de manera especializada hospitales geriátricos para la prestación asistencial de carácter sanitario a las personas seniles, así como hospitales materno infantil, para la atención de las mujeres, así como de los niños.

8. Seguridad en el Transporte: los hospitales también deben considerar la seguridad en el transporte de pacientes, especialmente en casos de ambulancias o traslados entre instalaciones médicas.

La seguridad hospitalaria es esencial, por tanto, para brindar atención médica de calidad y mantener la confianza de los pacientes y sus familias en el sistema de atención médica. Además, las regulaciones y estándares de seguridad en el ámbito de la salud son estrictos y están diseñados para garantizar que los hospitales cumplan con los más altos niveles de seguridad y atención médica.

Cabe destacar, por tanto, en palabras de Istúritz, J.J., (2018) que:

> Además, desde el punto de vista tanto de los usuarios, como de las personas que trabajan en los hospitales, la seguridad es la sensación de sentirse en un entorno seguro y controlado, un elemento objetivo capaz de ser medido. Y, en cualquier caso, la seguridad es algo que transmite, que los trabajadores manifiestan a los clientes en su actividad ordinaria y en su estilo de realizar las tareas que desempeñan, y que todas las personas que entran en cualquier centro sanitario perciben constantemente. Estamos por lo tanto ante una nueva cultura como es la seguridad organizacional. (p. 50).

En relación a la Seguridad Hospitalaria y los distintos conceptos expuestos con anterioridad, con un enfoque integral y aglutinador del término de Seguridad Hospitalaria y según González, M., (2017) refiere que es la:

> Condición y garantía de que los trabajadores, enfermos, visitas, acompañantes, proveedores de servicios, así como infraestructura, instalaciones, información y datos, tecnología, dotación y equipamiento estén libre de todo tipo de riesgos o, en su caso, sean riesgos controlados.
>
> La seguridad hospitalaria integra la suma de otras "subseguridades", que son: seguridad estructural, seguridad física, seguridad lógica[49], seguridad contraincendios, seguridad industrial (instalaciones), seguridad biológica o bioseguridad, seguridad alimentaria (aunque para ser más exactos, hemos de referirnos también a la tecnología de los alimentos), seguridad y salud laboral (prevención de riesgo laborales) para que revierta todo en un último punto que es la seguridad del paciente. (p. 51).

[49]Es la seguridad referida a los distintos sistemas de información y nuevas tecnologías.

En España tiene una gran relevancia en materia de Seguridad Hospitalaria el Observatorio de Seguridad Integral de Centros Hospitalarios (OSICH[50]), al ser referentes en cualquier aspecto que atente contra las distintas subseguridades de cualquier centro hospitalario.

La anticipación a la materialización del riesgo, su identificación y evaluación para la adopción de cuántas medidas preventivas sean necesarias implementar es un aspecto fundamental de la seguridad en general y de la seguridad hospitalaria en particular, en el sentido expuesto, atendiendo a Istúritz, J.J., (2018):

> Cabe señalar, que bajo el término de «seguridad», se engloban una serie de componentes clave que la hacen ambigua, pero que resulta una inversión y no un gasto. Hablamos de una parte del análisis de riesgos, de «prever» (ver antes de), imaginar qué tipo de situaciones pueden afectar al discurrir ordinario de la vida del hospital y, por otro lado, de gestionar los riesgos previstos, tomando medidas preventivas para evitar que ocurran e interviniendo eficazmente, en el supuesto de que aparezcan. (p. 50).

Otro de los conceptos terminológicos que se hacen necesario definir por la importancia dentro del ámbito de la seguridad hospitalaria es el concepto de Seguridad Biológica o Bioseguridad, concepto que, en ningún momento recoge la Real Academia de la Lengua Española, en cambio, según la OMS (2005), podría definirse como:

> (…) el conjunto de normas y medidas para proteger la salud del personal, frente a riesgos biológicos, químicos y físicos a los que está expuesto en el desempeño de sus funciones, también a los pacientes y al medioambiente. (OMS 2005).

[50] El Observatorio de Seguridad Integral de Centros Hospitalarios se crea en el año 2002, a iniciativa de los responsables de seguridad de varios hospitales con los siguientes objetivos: Promover la cultura de la seguridad en el ámbito sanitario. Crear un foro permanente de colaboración, discusión, divulgación y formación técnica para sus socios. Establecer una mesa de colaboración permanente con las instituciones y los centros sanitarios-hospitalarios. Potenciar la colaboración de las instituciones sanitarias y las distintas Fuerzas y Cuerpos de Seguridad. Colaborar con el legislador en la creación de la normativa más adecuada a la realidad de los centros sanitarios-hospitalarios, así como servir de nexo de unión entre los profesionales del sector.
El OSICH desarrolla su actividad a través de colaboraciones con otras entidades dedicadas a promover la seguridad sobre todo las que tienen carácter divulgador o investigador, el desarrollo de jornadas divulgativas propias a nivel estatal, regional, provincial o local. Participación en grupos de trabajo para el desarrollo legislativo con las asociaciones del ámbito de la seguridad a nivel nacional. La interlocución con las Fuerzas y Cuerpos de Seguridad, así como la colaboración con las distintas administraciones en el ámbito sanitario-hospitalario para fomentar la creación de Departamentos de Seguridad

En palabras de González, M., (2018), la define como:

> El conjunto de medidas que se aplican en las zonas críticas hospitalarias destinadas a garantizar los adecuados niveles de asepsia para evitar las infecciones nosocomiales, además de la morbimortalidad y, garantizar la seguridad biológica frente a los riesgos higiénicos mediante medidas preventivas, así como aquellas de carácter reactivas tras exposición.
>
> Evidentemente, las primeras están destinadas a la prevención de la aparición de los riesgos por infección frente a los distintos agentes biológicos, además de otras enfermedades por exposición al resto de riesgos higiénicos, es decir, a agentes químicos y físicos y, las segundas, para la eliminación, neutralización, reducción o control de los riesgos tras su exposición. (p. 51).

En la misma línea argumental hay que destacar la mayor parte de las debilidades en los hospitales que puedan significar brechas en la seguridad o sus vulnerabilidades son derivadas, según García, S., (2017) por:

Vulnerabilidades derivadas del tipo de usuario:

- ✓ Usuarios dependientes con escasa o nula movilidad, que, en muchos casos, no pueden colaborar en la propia evacuación.
- ✓ Pacientes y acompañantes desconocedores del edificio y de las vías de evacuación.
- ✓ Elevada ocupación de los edificios (…).

Vulnerabilidades derivadas del servicio prestado:

- ✓ Atención constante durante las 24 horas de los 365 días del año.
- ✓ Trabajo por turnos y una alta rotación del personal, lo que dificulta notablemente tanto la información sobre los riesgos como la formación para su prevención y control.
- ✓ Gran número de instalaciones tecnológicas y alta demanda de electricidad lo que multiplica el riesgo de fuego (…).
- ✓ Unidades especiales como urgencias, psiquiatría, farmacia hospitalaria y laboratorios de investigación o helipuertos con sus propios riesgos intrínsecos.

Vulnerabilidades derivadas del tipo de edificación:

- ✓ Edificios antiguos, en muchos casos, incluso adaptados de otros usos previos, muy difíciles de adecuar a las nuevas necesidades normativas en prevención y control de riesgos o de evacuación.

Vulnerabilidades estructurales derivadas de la organización:

- ✓ Organizaciones muy verticales y cerradas con imposibilidad de hacer frente a los cambios de forma ágil y con una estructura económica muy compleja, reticente a realizar inversiones que no tengan que ver con la prestación asistencial y su generador de valor.

(p.86).

3.3. APROXIMACIÓN A UNA TAXONOMÍA INTEGRAL DE RIESGOS EN HOSPITALES.

Es de vital importancia que los Directores de Seguridad, aquellos que legalmente tienen las atribuciones profesionales para ejercer las funciones de Dirección o Gestión, es decir, los Directores y Jefes de Seguridad, e incluso, los Técnicos Superiores en Prevención de Riesgos Laborales, conozcan una estructura lógica, reglada y ordenada en lo que a la clasificación de los riesgos se refiere.

Existen en muchos documentos profesionales carencias conceptuales, en los que puede comprobarse que no existe una adecuada clasificación de los riesgos, una taxonomía coherente en atención a los distintos factores que pueden exponer a cualquier persona, actividad u organización, a un riesgo, independientemente de que cualquiera de esos riesgos pudiera materializarse ulteriormente en un daño.

La clasificación coherente de los riesgos es toda una ciencia, por ello rehúsa utilizar la palabra clasificación de los riesgos para suplirla por la de la Taxonomía[51] de los Riesgos[52]. Si seguimos esa secuencia ordenada como una verdadera aproximación adecuada a los distintos

[51]La Taxonomía (del griego τάξιςτάxis 'ordenamiento' y νόμοςnómos 'norma' o 'regla') es, en su sentido más general, la ciencia de la clasificación.

[52] Taxonomía extraída del libro Tácticas Policiales en Protección de Personas y Técnicas de Escolta publicado por la Editorial AC ISBN: 978-84-937917-0-4 EAN: 9788493791704 en octubre de 2009. Autor, Martín González y Santiago.

tipos de riesgos en función de su naturaleza y características, la planificación que se realice en atención a ella, no presentará lagunas o sesgos importantes que pueda aumentar la vulnerabilidad y estará dimensionada de forma adecuada.

Suele confundirse la conceptualización de los distintos términos, se separa equivocadamente, por ejemplo, los riesgos tecnológicos, así como otros de los riesgos antrópicos, cuando en puridad, salvo los riesgos naturales todos los que sean por la acción del hombre son riesgos antrópicos, la tecnología el trabajo, son cuestiones propias e indivisibles a la evolución humana y por tanto, inherentes a ella, en este sentido es de necesaria consideración lo que explicaba González, M., (2018):

> Riesgos Antrópicos de Carácter Laboral como son aquellos riesgos asociados a la Especialidad de Higiene en el Trabajo por la presencia de Riesgos Químicos, Riesgos Físicos y Riesgos Biológicos, así como aquellos riesgos asociados a la Especialidad de Seguridad en el Trabajo e, incluso, a los Riesgos Antrópicos de Carácter Tecnológico, por el aparataje electromédico específico de estas áreas; al igual que los Riesgos Antrópicos de Carácter Imprudente cuando no se tiene la debida cautela en esta confluencia de riesgos y no se tienen en cuenta ni los procedimientos ni el adecuado uso de la tecnología médica. Los riesgos Antrópicos de Carácter Antisocial también son de consideración. En cualquier caso, el principal riesgo en estas áreas, además de los riesgos que podrían asociarse a unos deficitarios niveles de Bioseguridad, es el de incendio y explosión. (p. 59).

Como puede desprenderse, existen los riesgos de carácter natural y los riesgos antrópicos con el carácter que los defina en atención a sus características, es decir, riesgos antrópicos de carácter antisocial, aquellos que se definen por la comisión de cualquier ilícito penal, e incluso por cualquier tipo de reproche social en atención a las normas de convivencia normalmente aceptadas.

Riesgos antrópicos de carácter tecnológico, es decir, no puede disociarse de ninguna manera que la tecnología la crean las personas, con lo cual la exposición al riesgo que se considera siempre será antrópica, pero de carácter tecnológico, igual se materializa el riesgo por falta de mantenimiento en instalaciones críticas que puedan materializarse con un incendio o una explosión. En relación a aquellos riesgos que se materialicen por el propio desempeño profesional, serían por tanto Riesgos Antrópicos de Carácter Laboral, que, si se quiere ser mucho más explícito, podría asociarse a cualquiera de las distintas especialidades técnicas

establecidas legalmente al efecto, es decir, Riesgos Antrópicos de Carácter Laboral asociados a la Especialidad de Seguridad en el Trabajo, o bien asociados a la Especialidad de Higiene Industrial, ya sean biológicos, químicos o físicos, o bien asociados a la especialidad de Ergonomía, e incluso asociados a la especialidad de Psicosociología Aplicada.

3.1.1. Riesgos de Carácter Antrópico[53]:

Por todo lo expuesto, los Riesgos Antrópicos son todos los riesgos generados por la acción de las personas. Su etiología proviene del griego *ἀνθρωπικόςanthrōpikós* 'humano', der. *deἄνθρωποςánthrōpos* 'hombre, ser humano'. 1. adj. Producido o modificado por la actividad humana. Es decir, todo lo que sea consecuencia por la acción u omisión del «hombre» (masculino genérico), o sea, de las personas, conlleva ineludiblemente a nombrar tales riesgos como Riesgos Antrópicos, previo e, independientemente al carácter de esos riesgos, que ya nos definirán con más claridad, la especificidad del tipo de riesgo que estemos tratando.

Por lo tanto, los riesgos antrópicos pueden subdividirse atendiendo a la naturaleza o a las características comunes aglutinadoras del riesgo, tales como:

a) Riesgos Antrópicos de Carácter Antisocial:

Son aquellos riesgos que van en contra de las obligadas normas de conducta social, no obstante, no se relacionan en este epígrafe todo aquello que pueda ser reprochable desde el punto de vista ético o moral, muy al contrario, este tipo de riesgos son los que entrañan por su especial gravedad reproche penal por estar tipificado como delito en nuestra vigente Ley Orgánica del Código Penal. Se extraen los tipos penales de mayor relevancia en atención a la gravedad del delito, y relacionado con la seguridad, en atención a sus consecuencias. En cualquier caso, no todos los delitos entrañan riesgo para las empresas, instituciones u organizaciones, es por ello, por lo que se relacionan tan sólo aquellos tipos delictivos, que, de una forma u otra, en mayor o menor medida, pueden comprometer de alguna forma a la institución, corporación u evento a la que se intenta dar protección a través de un adecuado análisis de riesgos que ha de ser trazado con una adecuada planificación que mitigue, neutralice o minimice los riesgos previamente estudiados. De ahí la importancia de una adecuada taxonomía integral de los riesgos.

[53]Antrópico (del gr. ἀνθρωπικός *anthrōpikós* 'humano'), der. de ἄνθρωπος *ánthrōpos* 'hombre, ser humano'.1. adj. Producido o modificado por la actividad humana. La erosión antrópica del terreno. RAE, 2021).

Como Riesgos Antrópicos de Carácter Antisocial relevantes destacan:

Delitos contra la Seguridad Colectiva:

- ✓ Riesgos Catastróficos:
    - Relativos a la energía nuclear y a las radiaciones ionizantes.
    - Estragos.
    - De otros delitos de riesgo provocados por explosivos y otros agentes
    - De los incendios:
        - Forestales.
        - No forestales.
        - En bienes propios.

- ✓ Delitos contra la salud pública.
- ✓ Delitos contra la seguridad vial.

Delitos contra el Orden Público:

- ✓ Sedición.
- ✓ Atentados contra la autoridad o sus agentes.
- ✓ Resistencia.
- ✓ Desobediencia.
- ✓ Desórdenes Públicos.
- ✓ Tenencia, tráfico depósito de armas, municiones o explosivos.
- ✓ Organizaciones y Grupos Criminales.
- ✓ Organizaciones y grupos terroristas.
- ✓ Delitos de terrorismo.

Delitos contra la Constitución:

- ✓ Rebelión.
- ✓ Delitos contra la Corona.
- ✓ Delitos contra las Instituciones del Estado.

Delitos contra la Libertad:

- ✓ Detenciones Ilegales.

- ✓ Secuestros.
- ✓ Amenazas.
- ✓ Coacciones.
- ✓ Torturas.

Delitos contra la Vida e Integridad Física:

- ✓ Homicidio/Asesinato.
- ✓ Lesiones (Agresiones).

Delitos contra la Libertad Sexual:

- ✓ Agresiones Sexuales.
- ✓ Abuso Sexual.
- ✓ Acoso Sexual.

Descubrimiento y revelación de secretos.

Delitos contra el patrimonio:

- ✓ Hurtos.
- ✓ Robos.
- ✓ Extorsión.
- ✓ Robo y hurto de uso de vehículos.
- ✓ Usurpación.
- ✓ Defraudación.
- ✓ Estafa.
- ✓ Administración desleal.
- ✓ Apropiación indebida.
- ✓ Defraudación de fluido eléctrico y análogos.
- ✓ Delitos contra los derechos de los trabajadores.
  - o Sabotajes.
  - o Vandalismo.

b) Riesgos Antrópicos de carácter Tecnológico:

La tecnología es la ciencia aplicada a la resolución de problemas concretos. Constituye un conjunto de conocimientos científicamente ordenados, que permiten diseñar y crear bienes o servicios que facilitan la adaptación al medio ambiente y la satisfacción de las necesidades esenciales y los deseos de la humanidad. La etimología, es una palabra de origen griego, *τεχνολογία*, formada por *téchnē* (τέχνη, arte, técnica u oficio, que puede ser traducido como destreza) y logía (*λογία*, el estudio de algo).

Los riesgos tecnológicos son, por tanto, riesgos asociados a la actividad humana, (por tanto, también son riesgos antrópicos), y, en concreto, con el progreso de la sociedad fruto de ese desarrollo.

Son riesgos percibidos como fenómenos controlables por el hombre. En cualquier caso, los Riesgos Antrópicos de Carácter Tecnológico son muy diversos en relación directa con el tipo de actividad, sector o área en la que se encuadren.

Como Riesgos Antrópicos de Carácter Tecnológico destacan los siguientes:

- ✓ Accidentes en instalaciones: por uso inadecuado, inadecuado mantenimiento, fatiga (vida útil) o fallo e imprudencia.
- ✓ Riesgos Asociados al uso de la tecnología:
    a. Informática[54] y seguridad lógica.
        - Ciberataques (en cualquiera de sus modalidades, principalmente por *malware*[55]).

[54]Afecta a la seguridad informática, rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. Abarca una serie de medidas de seguridad, tales como programas de *software* de antivirus, *firewalls*, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de *software*, como *scripts* de Java, *ActiveX*, cuidar del uso adecuado del ordenador, los recursos de red o de Internet.

[55]El *malware* o *software* malicioso son una categoría de *software* diseñado para infiltrarse y dañar un sistema de información sin ser detectado. Entre los más utilizados, destacan los virus, códigos malignos en forma de archivo ejecutable (o archivo.exe), que infecta los ficheros delos dispositivos, valiéndose del desconocimiento de los usuarios para conseguir el acceso.Otros *malwares* son “los gusanos” (*software* algo más sofisticado que el virus, que crea copias de sí mismo con el objetivo de afectar otros equipos), los troyanos (programas diseñados para ingresar en los sistemas de seguridad y permitir el acceso a

- Ciberterrorismo.
- Brechas de seguridad en materia de Protección de Datos.

b. Instalaciones.

- ✓ Caída de basura espacial
- ✓ Incendio.
- ✓ Explosiones.
- ✓ Fugas tóxicas.
- ✓ Fugas radioactivas.
- ✓ Otras.
- ✓ Ciberataques o ciberamenazas.
- ✓ Otras.

c) Riesgos Antrópicos de Carácter Laboral:

Este apartado recoge todos los riesgos antrópicos derivados del trabajo. Han de considerarse todos los factores de riesgos que por la realización de un trabajo puede materializarse en un daño.

No sólo contempla los accidentes laborales que surjan con ocasión de éste. Hay que contemplar las enfermedades profesionales derivadas o trazables directamente al desempeño profesional o laboral, así como, aquellos accidentes que el trabajador sufra *in itinere*, es decir, del domicilio a su centro de trabajo y del centro de trabajo a su domicilio.

De la misma manera y según jurisprudencia de nuestro alto tribunal, el Tribunal Supremo, también han de considerarse accidentes de trabajo los accidentes *in misión,* cuando al trabajador se le encomiende cualquier labor o gestión, incluso fuera de su centro de trabajo y de su horario en su cumplimiento.

---

otros archivos maliciosos), los *spyware* (programas que espían un dispositivo para obtener información privada y que pueden instalar otros softwares maliciosos) y, los ya famosos *ransomwares*, que secuestran la información de valor de un dispositivo, con el fin de solicitar una transferencia en criptomoneda o monedas digitales como rescate.

A tenor del artículo 4 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, se entenderá por «prevención» el conjunto de actividades o medidas adoptadas o previstas en todas las fases de actividad de la empresa con el fin de evitar o disminuir los riesgos derivados del trabajo.

De la misma forma, se entenderá como «riesgo laboral» la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo. Para calificar un riesgo desde el punto de vista de su gravedad, se valorarán conjuntamente la probabilidad de que se produzca el daño y la severidad del mismo.

Clasificación de los Riesgos Laborales:

a. Asociados a la Seguridad en el Trabajo.

Todos los riesgos que se materializan en caídas al mismo nivel, a distinto nivel, riesgo de explosión, de incendios, contactos eléctricos, tanto directos como indirectos y aquellas cuestiones que comprometan la seguridad del trabajador, todo ello a tenor de la propia Ley 31/1995, de 8 de noviembre de prevención de riesgos laborales y demás normativa dimanante, en especial el Real Decreto 486/1997, de 14 de abril, por el que se establecen las disposiciones mínimas de seguridad y salud en los lugares de trabajo.

b. Asociados a la Higiene Industrial.

Esta especialidad integra tres tipos diferentes de riesgos bien diferenciados unos de otros. Riesgos que llegan a configurar verdaderos grupos dentro la referenciada especialidad que son: los Riesgos Biológicos, los Riesgos Químicos y los Riesgos Físicos. No obstante, se relaciona la documentación legal de referencia de los distintos tipos de riesgos que integran la Especialidad Preventiva de Higiene Industrial.

- ✓ Riesgo Biológico RD 664/1997 de 12 de mayo, sobre protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos en el trabajo y Orden 25 de marzo de 1998 por la que se adapta, en función del progreso técnico el RD 664/1997.

- ✓ Agentes Cancerígenos, de importancia el Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo.

- ✓ Agentes Químicos, de consideración el Real Decreto 374/2001, de 6 de abril, sobre la protección de la salud y seguridad de los trabajadores contra los riesgos relacionados con los agentes químicos durante el trabajo, así como el Riesgo Químico que regula el Real Decreto 374/2001 de 6 de abril sobre la protección de la salud y seguridad de los trabajadores contra los riesgos relacionados con los agentes químicos en el trabajo.

- ✓ En relación a los Agentes Físicos, de consideración el Real Decreto 286/2006, de 10 de marzo, sobre la protección de la salud y la seguridad de los trabajadores contra los riesgos relacionados con la exposición al ruido. También el Real Decreto 1029/2022, de 20 de diciembre, por el que se aprueba el Reglamento sobre protección de la salud contra los riesgos derivados de la exposición a las radiaciones ionizantes.

c. Asociados al Riesgo Ergonómico.

La Ergonomía es una disciplina de carácter científico-técnica y de diseño que estudia la relación entre el entorno de trabajo (lugar de trabajo), y quienes realizan el trabajo (los trabajadores). Etimológicamente, el término ergonomía Deriva del griego *έργον* (ergon, 'trabajo') y *νόμος* (nomos, 'ley'), el término denota la ciencia del trabajo.

Es una disciplina sistemáticamente orientada, que ahora se aplica a todos los aspectos de la actividad humana con las máquinas.

Dentro del mundo de la prevención es una técnica preventiva que intenta adaptar las condiciones y organización del trabajo al individuo. Su finalidad es el estudio de la persona en su trabajo y tiene como propósito último conseguir el mayor grado de adaptación o ajuste, entre ambos. Su objetivo es hacer el trabajo lo más eficaz y cómodo posible.

Por ello, la ergonomía estudia el espacio físico de trabajo, ambiente térmico, ruidos, vibraciones, posturas de trabajo, desgaste energético, carga mental, fatiga nerviosa, carga de trabajo, y todo aquello que pueda poner en peligro la salud del trabajador y su equilibrio psicológico y nervioso. En definitiva, se ocupa del confort del individuo en su trabajo.

El amplio campo de actuación de la ergonomía hace que tenga que apoyarse en otras técnicas o ciencias como son: la seguridad, la higiene industrial, la física, la fisiología, la psicología, la estadística, la sociología, la economía etc. Es un claro ejemplo de ciencia interdisciplinar que trata de la adaptación y mejora de las condiciones de trabajo al hombre.

La ergonomía es la disciplina que se encarga del diseño de lugares de trabajo, herramientas y tareas, de modo que coincidan con las características fisiológicas, anatómicas, psicológicas y las capacidades de los trabajadores que se verán involucrados.1 Busca la optimización de los tres elementos del sistema (humano-máquina-ambiente), para lo cual elabora métodos de la persona, de la técnica y de la organización.

Es una disciplina sistemáticamente orientada, que ahora se aplica a todos los aspectos de la actividad humana con las máquinas.

d. Asociados al Riesgo Psicosocial.

La Psicosociología es la disciplina que estudia, analiza e interviene en los procesos de interacción y comunicación humana a través de una mirada inter e intrasubjetiva. Se podría considerar la Psicosociología como el punto de encuentro entre la psicología y la sociología que, sumadas a los aportes de otras disciplinas o áreas del conocimiento, tales como, la filosofía, la comunicación, el derecho o la medicina, entre otros. Se constituye en una ciencia particular y autónoma. En el caso que nos compete siempre en todo lo que sea de aplicación en el entorno laboral constituyendo la Psicosociología Aplicada.

Los principales riesgos asociados a esta clasificación son:

- ✓ Estrés.
- ✓ Distrés.
- ✓ Acoso Laboral (*moobing*).
- ✓ Acoso Sexual.
- ✓ Síndrome del Quemado (*bournout*).

e. Riesgos Antrópicos de Carácter Organizativo:

Son aquellos riesgos derivados principalmente la redacción, desarrollo e implantación de cuantas medidas sean necesarias para la organización, gestión o dirección de la seguridad. Estos riesgos pueden ser, de una parte, por acción (Ej.: Se realizan planificaciones o se instauran procedimientos carentes de rigor, de una metodología adecuada, se yerra en el análisis específico de los riesgos y se reflejan riesgos genéricos no adaptados a la idiosincrasia de la organización, uso o actividad a la que haya que dar seguridad o protección, etc.) y, de otra parte, por omisión, es decir, no se instaura o implanta ninguna medida de carácter

organizativa. Son, en definitiva, riesgos asociados a una mala o nula planificación en lo que a la organización de la seguridad, planificación e implantación de procedimientos se refiere.

3.1.2. Riesgos Naturales:

Son aquellos riesgos que pueden desencadenarse por fenómenos naturales con carácter extraordinario en un territorio y hábitat determinado y que su materialización produzca daños de especial importancia en la propia área del suceso, así como en su área de influencia.

Tipos de Riesgos Naturales:

a. Geológicos:

- ✓ Sismos o terremotos.
- ✓ Vulcanismo (erupciones volcánicas).
- ✓ Terremotos, maremotos y Tsunamis.

b. Meteorológicos o Climatológicos Adversos:

- ✓ Sequías y desertización.
- ✓ Riesgo térmico por temperaturas extremas: (Olas de frío o calor).
- ✓ Tormenta con riesgo de inundación, Tormenta eléctrica con riesgo de caída de rayos, etc.

c. Alteraciones de carácter antrópicos de la atmósfera:

- ✓ Cambio climático.
- ✓ Agujero de la capa de ozono.

d. Geomorfológico:

- ✓ Movimiento del terreno:
- ✓ Subsidencia (movimiento de una superficie en la que la componente vertical del desplazamiento es claramente predominante sobre la horizontal asociado a la explotación minera).
- ✓ Aludes.

- ✓ Deslizamientos.
- ✓ Solifluxión (desplazamiento masivo y lento por gravedad de formaciones arcillosas.

e. Riesgos Actuales o Vigentes (generalmente se materializan o van acompañados de la materialización del riesgo en un daño):

- ✓ Volcán activo en erupción.
- ✓ Aludes por abundancia de nieve suelta no compactada con pequeños deslizamientos.
- ✓ Acuíferos y manantiales contaminados.

f. Riesgos Potenciales:

- ✓ Laderas rocosas bien ancladas sin desprendimiento.
- ✓ Volcanes inactivos.
- ✓ Probabilidad de tormenta y posible inundación.

g. Riesgos Biológico de carácter natural (sin intervención humana[56]):

- ✓ Plagas.
- ✓ Epidemias.
- ✓ Pandemias.

h. Cósmicos:

- ✓ Colisión de planetas.
- ✓ Desprendimiento de asteroides y meteoritos.
- ✓ Contaminación espacial:
- ✓ Desprendimiento de basura espacial (estaciones, satélites, etc.).

Se hace por tanto imprescindible y altamente necesaria la creación de una adecuada taxonomía de los riesgos, de carácter integral e integradora, en un lenguaje técnico universal en relación a su terminología conceptual, de cada uno de ellos, con el objeto de establecer las

[56] Con intervención humana de carácter antrópico asociado al Riesgo Biológico.

ulteriores rigurosas y completas planificaciones como elemento de control para su mitigación, neutralización, reducción o eliminación, según proceda.

3.4. CONCEPTO DE HOSPITAL, ORIGEN Y TIPOS.

Antes de profundizar en el concepto de la Seguridad Hospitalaria, se hace necesario por la especial idiosincrasia realizar una aproximación conceptual a lo que es un hospital, sus orígenes, así como sus tipos, este último aspecto es de relevancia para saber el nivel de criticidad del hospital en relación a su tipología.

3.4.1 Concepto de Hospital:

Un hospital es una organización sanitaria que, proporciona atención médica generalista y especializada a través de los distintos tratamientos diferenciados e individualizados a aquellas personas o pacientes que sufren alguna patología o enfermedad.

Los hospitales están integrados por personal muy heterogéneo para poder dar una asistencia integral, compuesto por celadores, auxiliares de enfermería, Técnicos en Radiología y Diagnóstico a través de la imagen, Graduados en fisioterapia, Graduados en Dietética y Nutrición Humana, graduados en enfermería, graduados o licenciados en medicina, médicos especialistas, farmacéuticos, farmacéuticos especialistas en Farmacia Hospitalaria, etc., además de todo el personal de apoyo del servicio de cocina hospitalaria y sus distintas categorías, personal del servicio de limpieza, personal del servicio técnico de mantenimiento, servicio de ingeniería y de electro medicina, servicios administrativos, entre otros, así como con instalaciones y equipos médicos avanzados para diagnosticar, tratar, asistir y cuidar a los pacientes.

En cualquier caso, la Ley 37/1962, de 21 de julio, sobre Hospitales, define el concepto de hospital en su artículo primero, cuyo tenor literal reza:

> Son hospitales, cualquiera que sea la denominación que ostenten, los establecimientos destinados a proporcionar una asistencia médico-clínica, sin perjuicio de que pueda realizarse en ellos, además, en la medida que se estime conveniente, medicina preventiva y de recuperación, y tratamiento ambulatorio.
>
> Los hospitales son también Centros de formación del personal técnico y sanitario y de investigación científica, siempre que reúnan las condiciones adecuadas a tales fines,

> que lo consientan el carácter y finalidad de cada Institución, y que se establezca la debida coordinación con los Centros docentes oficiales. (Art. 1).

La Real Academia de la Lengua Española recoge su etimología derivada del latín *hospitalis* 'relativo al huésped', `hospitalario'. La RAE, (2001), lo define en su primera acepción como:

> «Establecimiento destinado al diagnóstico y tratamiento de enfermos, donde a menudo se practican la investigación y la docencia», en cambio, en su segunda acepción lo define como «casa que servía para acoger a pobres y peregrinos por tiempo limitado». (p. 1232).

3.4.2 Origen de los Hospitales:

El origen de los hospitales tiene sus raíces en la historia de la atención y los cuidados asistenciales de cuántos padecían algún tipo de enfermedad o dolencia, así como de la caridad.

Los hospitales actuales tienen sus antecedentes en las organizaciones de asistencia médica y caritativas del Antiguo Egipto, la antigua Roma y Grecia, en lo que a occidente se refiere, pero también y, coetáneamente en la antigua India y China.

En Europa, durante la Edad Media, las distintas órdenes religiosas, así como las distintas instituciones benéficas jugaron un papel relevante en el establecimiento, creación y perpetuación en el tiempo de los hospitales de la época.

Uno de los hospitales más antiguos que se conocen es el Hospital de Santiago, fundado en el año 1200 en nuestro país, concretamente en Santiago de Compostela. En cualquier caso, en la Edad Media, también surgieron hospitales en el mundo islámico, como el Hospital de Al-Mansur, en El Cairo, Egipto, que se considera uno de los hospitales más antiguos y de importancia del mundo, Meca de muchísimos médicos del resto del mundo que asistían a aprender los avances en la medicina de la época.

A lo largo de la historia, la función y la organización de los hospitales han evolucionado significativamente, y en la época moderna, los avances en la medicina, la tecnología médica y la atención al paciente han llevado a la creación de hospitales modernos y especializados en todo el mundo.

3.4.3 Tipos de Hospitales:

1. Hospitales Generales: aportan una amplia gama de servicios médicos y quirúrgicos para pacientes de todas las edades y con diversas afecciones médicas. Suelen ser centros de atención médica de nivel secundario y terciario.

2. Hospitales Especializados: se centran en una especialidad médica o un tipo específico de tratamiento. Por ejemplo, pueden ser hospitales pediátricos, hospitales oncológicos, hospitales cardíacos u hospitales psiquiátricos para el tratamiento de cualquier tipo de patología mental.

3. Hospitales de Enseñanza: asociados a universidades y escuelas universitarias, se crearon para la formación de médicos y otros profesionales de la salud. Ofrecen una amplia gama de servicios médicos y son centros de investigación médica.

4. Hospitales de Rehabilitación: estos hospitales se especializan en la rehabilitación de pacientes a través de técnicas varias que recoge la medicina física y rehabilitadora, apoyada en la Fisioterapia sobre aquellos enfermos que han sufrido lesiones graves o enfermedades crónicas, como accidentes cerebrovasculares, lesiones de médula espinal, traumas o amputaciones, etc.

5. Hospitales de Cuidados a Largo Plazo: también conocidos como hogares de ancianos, geriátricos o residencias de atención, estos hospitales proporcionan atención a largo plazo a personas mayores o discapacitadas que requieren cuidados continuos.

6. Hospitales de Atención de Emergencia: estos hospitales se especializan en la atención de emergencia y trauma y suelen estar ubicados en áreas urbanas para responder a situaciones de emergencia

La variedad de hospitales refleja la diversidad de necesidades médicas y de atención en la sociedad moderna, y cada tipo de hospital tiene un enfoque específico para brindar atención de calidad a los pacientes en función de sus necesidades

3.5. DESCRIPCIÓN DE LA CADENA DE VALOR DEL SISTEMA HOSPITALARIO.

La cadena de valor del sistema hospitalario se refiere al conjunto de actividades interconectadas que una institución hospitalaria realiza para brindar atención médica a los pacientes y proporcionar servicios de salud de alta calidad. Estas actividades están diseñadas para agregar valor a través de cada paso del proceso y, en última instancia, mejorar la salud y

el bienestar de los pacientes. Los distintos procesos que integran la cadena de valor son los siguientes:

1. **Recepción y Registro del Paciente:**

   - ✓ La cadena de valor comienza cuando un paciente llega al hospital y se registra en el sistema.
   - ✓ Se recopila información demográfica, médica y de seguro para establecer un historial del paciente.

2. **Evaluación y Diagnóstico:**

   - ✓ Los profesionales de la salud, como médicos, enfermeros y especialistas, evalúan al paciente y realizan exámenes médicos para determinar el diagnóstico.
   - ✓ Se utilizan pruebas de laboratorio, imágenes médicas y otras herramientas para identificar enfermedades y afecciones.

3. **Tratamiento Médico:**

   - ✓ Basado en el diagnóstico, se desarrolla un plan de tratamiento que puede incluir medicamentos, cirugía, terapia u otros procedimientos médicos.
   - ✓ Se administra atención médica y terapéutica de acuerdo con las necesidades individuales del paciente.

4. **Seguimiento y Cuidado Continuo:**

   - ✓ Después del tratamiento, se proporciona seguimiento y atención continua para garantizar la recuperación del paciente.
   - ✓ Esto puede incluir consultas de seguimiento, terapia de rehabilitación o cuidados a largo plazo.

5. **Gestión de Registros Médicos:**

   - ✓ Se mantiene un registro médico electrónico o en papel que documenta todas las interacciones médicas y la información del paciente.
   - ✓ Esto facilita la coordinación de la atención y el acceso a la información médica relevante.

6. **Operaciones Administrativas y de Apoyo:**

   - ✓ La cadena de valor también incluye actividades administrativas, como facturación, gestión de seguros, programación de citas y gestión de recursos humanos.
   - ✓ Estas funciones respaldan la operación eficiente del hospital.

7. **Gestión de la Calidad y Seguridad del Paciente:**

   - ✓ Se implementan prácticas y protocolos de gestión de calidad y seguridad para garantizar que los pacientes reciban atención segura y efectiva.
   - ✓ Esto incluye la gestión de riesgos, la prevención de infecciones y la formación continua del personal.

8. **Educación y Comunicación:**

   - ✓ Se brinda educación al paciente y a sus familiares sobre su afección, el tratamiento y la prevención.
   - ✓ La comunicación efectiva entre el personal médico, el paciente y la familia es esencial para una atención de calidad.

9. **Investigación y Desarrollo:**

   - ✓ Algunos hospitales también participan en actividades de investigación médica y desarrollo de nuevos tratamientos y procedimientos.
   - ✓ Esto contribuye al avance de la medicina y a la mejora de la atención médica en general.

La cadena de valor del sistema hospitalario es un proceso complejo que requiere una coordinación eficiente de recursos humanos, tecnológicos y financieros para brindar atención médica de calidad.

Uno de los problemas que pueden ir contra de la propia cadena de valor de los hospitales y según García, S., (2016) es que los hospitales son:

> Organizaciones muy verticales y cerradas con imposibilidad de hacer frente a los cambios de forma ágil y con una estructura económica muy compleja, reticente a

> realizar inversiones que no tengan que ver con la prestación asistencial y su generador de valor. (p.86).

La atención centrada en el paciente y la mejora continua de los procesos son fundamentales para el éxito de esta cadena de valor, de manera especial, aunque se obvia el concepto de seguridad por su transversalidad con todos los procesos referenciados.

En el mismo sentido y en palabras de García, S., (2016)

> En ningún caso, un director de seguridad de un hospital no puede olvidar que el proceso generador de valor de la organización es la actividad sanitaria y que su misión es la protección de dichos procesos. Por lo tanto, el objetivo principal de cualquier sistema de gestión de la seguridad enfocada al control de emergencias es la vuelta, en el menor tiempo posible de la forma más eficiente a la normalidad de la organización y al normal desarrollo de dichos procesos. (p. 88).

En cualquier caso, la materialización de cualquier tipo de riesgo, ya sea de Carácter Natural o Antrópico, incluso Antrópico de Carácter Antisocial por cualquier tipo delictual, inclusive por el terrorismo, afectará significativamente, ya que, indefectiblemente tendrá efectos devastadores en la cadena de valor del sistema hospitalario, al afectar la capacidad del hospital para proporcionar atención sanitaria y médica adecuada, socavar la confianza pública y desestabilizar el entorno operativo normal del hospital.

3.6. CONCEPTO DE RESILIENCIA.

La resiliencia es un concepto que se refiere a la capacidad de una persona o comunidad para adaptarse, recuperarse y sobrellevar adversidades, traumas, desafíos o situaciones difíciles. Es la habilidad de mantener un estado de bienestar emocional y funcional a pesar de enfrentar circunstancias estresantes o crisis. La resiliencia no implica evitar el sufrimiento, sino aprender a afrontarlo de manera constructiva y, en última instancia, salir fortalecido de la experiencia.

Algunos aspectos clave del concepto de resiliencia incluyen:

1. Adaptación: la resiliencia implica la capacidad de adaptarse a circunstancias cambiantes y difíciles. Las personas resilientes son flexibles y pueden ajustar sus estrategias y comportamientos para hacer frente a situaciones desafiantes.

2. Superación: la resiliencia implica la capacidad de superar obstáculos y adversidades. Las personas resilientes no se rinden fácilmente y buscan soluciones a los problemas en lugar de rendirse ante ellos.

3. Aprendizaje: la resiliencia a menudo involucra la capacidad de aprender de las experiencias difíciles. Las personas resilientes pueden usar la adversidad como una oportunidad para el crecimiento personal y el desarrollo de habilidades.

4. Apoyo social: tener una red de apoyo social sólida es un factor importante en la resiliencia. El apoyo emocional y práctico de amigos, familiares y comunidades puede ayudar a las personas a enfrentar y superar dificultades.

5. Autoconfianza: la resiliencia se relaciona con la confianza en uno mismo y en la capacidad de tomar decisiones efectivas. La autoestima y la autoeficacia son componentes clave de la resiliencia.

6. *Coping*[57] eficaz: las personas resilientes suelen utilizar estrategias de afrontamiento efectivas para gestionar el estrés y las emociones negativas. Estas estrategias pueden incluir el establecimiento de metas, el manejo del estrés, la búsqueda de apoyo y la autoevaluación.

Es importante destacar que la resiliencia no es una característica innata, sino una habilidad que se puede desarrollar y fortalecer a lo largo de la vida. Las experiencias y la educación pueden influir en la capacidad de una persona para ser resiliente.

Además, la resiliencia no implica ausencia de sufrimiento o traumas; más bien, se trata de cómo una persona o comunidad se recupera y se adapta después de enfrentar dificultades. La resiliencia es un concepto ampliamente estudiado en psicología y se aplica en diversas áreas, incluida la psicología clínica, la educación, la gestión del estrés y la salud mental.

En el contexto de hospitales y atención médica, la resiliencia se refiere a la capacidad de las organizaciones hospitalarias y su personal para adaptarse, recuperarse y mantener la calidad de atención en situaciones de adversidad, crisis o desafíos significativos. La resiliencia

[57] Se refiere a las estrategias y habilidades que una persona o una organización o institución utiliza para hacer frente y adaptarse de manera efectiva a situaciones de estrés, adversidad o desafío. El *coping* es el proceso de manejar las demandas internas y externas que exceden los recursos de una persona u organización, según se trate. En el caso de las organizaciones implica la capacidad del personal para gestionar el estrés, adaptarse a situaciones cambiantes, trabajar en equipo, cuidar su bienestar emocional y contribuir a la resiliencia organizativa en momentos de emergencias, crisis, u otros desafíos.

hospitalaria implica la capacidad de continuar brindando atención segura y efectiva a los pacientes incluso cuando se enfrentan a obstáculos o amenazas que podrían afectar negativamente la prestación de servicios de salud.

Algunos aspectos clave del concepto de resiliencia para poder garantizarla en las Infraestructuras hospitalarias deben de incluir:

1. Preparación para Emergencias y Desastres: los hospitales deben estar preparados para enfrentar situaciones de emergencia, como desastres naturales, pandemias, incidentes de seguridad, entre otros. La resiliencia hospitalaria implica la capacidad de planificar y responder eficazmente a estas situaciones, garantizando la seguridad de los pacientes y el personal. En el sentido apuntado es de consideración que «De nada sirve tener un plan de autoprotección si quienes deben ponerlo en práctica no lo conocen». (Ponce, T., 2016, p. 80).

2. Gestión de Crisis: la resiliencia hospitalaria se refiere a la capacidad de mantener la calma y tomar decisiones efectivas durante crisis inesperadas. Esto incluye la gestión de recursos, la coordinación de equipos y la comunicación eficaz en situaciones de alta presión.

3. Continuidad de la Atención: la resiliencia hospitalaria implica la capacidad de mantener la continuidad de la atención médica incluso en situaciones de estrés extremo. Esto incluye la capacidad de seguir brindando atención a pacientes críticos, garantizar el suministro de medicamentos y suministros, y mantener la infraestructura esencial en funcionamiento.

4. Apoyo al Personal de Salud: la resiliencia también se relaciona con la atención y el apoyo al personal de salud que puede verse afectado emocionalmente por situaciones traumáticas. Los hospitales deben proporcionar recursos para el bienestar emocional y la gestión del estrés de su personal.

5. Aprendizaje y Mejora Continua: la resiliencia hospitalaria implica aprender de las crisis y situaciones adversas para mejorar la preparación y la capacidad de respuesta en el futuro. Esto incluye la revisión de protocolos y la implementación de cambios basados en lecciones aprendidas.

6. Colaboración y Comunicación: la colaboración efectiva y la comunicación tanto internamente dentro del hospital como con otras organizaciones y agencias externas

> son esenciales para la resiliencia hospitalaria. Esto garantiza una respuesta coordinada y eficiente en situaciones de crisis.

Todos y cada uno de los aspectos referenciados han de ser dirigidos, gerenciados o gestionados por el Director de Seguridad de la Infraestructura Hospitalaria, pero para ello, para que la cultura de seguridad llegue a todos los estamentos y categorías profesionales del hospital, «El departamento de seguridad debe de pertenecer a la máxima línea jerárquica del hospital». (González, M., 2017, p. 34).

Si no hay una dependencia directa de la máxima autoridad del centro del Director de Seguridad, todas las políticas, procedimiento, instrucciones técnicas operativas, planes, órdenes de puesto, etc., podrían ser totalmente estériles, todo ello porque según González, M. (2017):

> El director de seguridad habrá de estar a un nivel suficiente en su estructura organizacional, de tal forma que pueda garantizarse el cumplimiento y la aplicación de la política y de los requisitos establecidos para la protección de las Infraestructuras Críticas bajo su responsabilidad. (p. 34).

Si no se implementan cuántas medidas de seguridad son necesarias e imprescindibles para la protección integral del centro hospitalario nunca podría garantizarse ni la cadena de valor, ni la seguridad ni la protección de la vida e integridad física de las personas, así como de los bienes muebles e inmuebles que integran el patrimonio del hospital, para ello, según cita González, M., (2017):

> (…) Todos los hospitales deberían de tener un departamento de seguridad, planes integrales de seguridad, procedimientos de seguridad específicos, seguridad humana llevada a cabo por vigilantes de seguridad debidamente habilitados, sistemas de vídeovigilancia o Circuito cerrado de Televisión y Grabación Permanente de Imágenes (CCTV), puesto de control o puesto permanente de seguridad, sistema de alarma mínimo un grado 3 con conexión al puesto de control o puesto permanente de seguridad, o en su defecto a la Central Receptora de Alarmas. (p. 35).

La resiliencia hospitalaria es fundamental para garantizar la seguridad de los pacientes y la prestación de atención médica de calidad en todo momento, incluso en situaciones difíciles o

excepcionales. Los hospitales deben contar con planes y protocolos sólidos de gestión de crisis y preparación para emergencias para fortalecer su capacidad de respuesta y recuperación.

En relación con el término de Resiliencia, ha de considerarse que, «siempre que se consigue una disminución de la vulnerabilidad, lo que se genera automáticamente es un aumento de la capacidad de resiliencia de la organización.» (García, S., 2016, p.88).

En el contexto hospitalario gestión de la seguridad con el objeto de garantizar una resiliencia se hace una labor compleja, precisamente por la tipología de sus riesgos, según González, M., (2018):

> (…) para los expertos en la materia la tarea tan ardua que supone garantizar una adecuada Seguridad[58](1) y una protección integral en un centro hospitalario[59] por la gran heterogeneidad y concentración de sus riesgos, además de la escasa o nula cultura de la seguridad en el sentido más amplio de la palabra, se hace más complejo aun cuando hablamos de bioseguridad en áreas críticas o especiales que integran las Infraestructuras Críticas Hospitalarias.
>
> Estas áreas contienen gases medicinales (oxígeno, vacío, aire medicinal, protóxido, nitrógeno, etc.); una gran diversidad de equipamiento electromédico (respiradores con sus distintos gases anestésicos, láseres de clase 3 B y 4; arcos quirúrgicos y equipos portátiles de Rx, salas de hemodinamia para la realización de Cirugía Vascular Intervencionista; equipos como electrobisturíes. A todo lo anterior, hay que sumarle que en el área quirúrgica también hay otros Servicios Centrales Hospitalarios como es la Central de Esterilización que contienen autoclaves de vapor y, a la vez, podrían contener también, autoclaves de óxido etileno, autoclaves de formaldehído, etc. Deben ser también de especial consideración los climatizadores o las Unidades de Tratamiento de Aire (UTA) e, incluso, las líneas de distribución tanto de agua fría para el consumo humano (AFCH), así como el de agua[60]caliente sanitaria (ACS), depósitos o

[58]Hace referencia el autor a los Directores de Seguridad.

[59]Actualmente es la organización más compleja a la que garantizar una adecuada seguridad y protección integral muy por encima de cualquier otra.

[60]El autor hace referencia a su taxonomía de los riesgos y expone que los «Riesgos Antrópicos de Carácter Laboral como son aquellos riesgos asociados a la Especialidad de Higiene en el Trabajo por la presencia de Riesgos Químicos, Riesgos Físicos y Riesgos Biológicos, así como aquellos riesgos asociados a la Especialidad de Seguridad en el Trabajo e, incluso, a los Riesgos Antrópicos de Carácter Tecnológico por el aparataje electromédico específico de estas áreas; al igual que los Riesgos Antrópicos de Carácter Imprudente cuando no se tiene la debida cautela en esta confluencia de riesgos y no se tienen en cuenta ni los procedimientos ni el adecuado uso de la tecnología médica. Los riesgos Antrópicos de Carácter

> aljibes que la suministran, acumuladores, intercambiadores de calor, etc. Integran también estas áreas especiales los Sistemas de Alimentación Ininterrumpida (SAI's) con sus correspondientes baterías, al igual que el conexionado del área quirúrgica con el Grupo Electrógeno en atención a la criticidad del área, al ser un imperativo poder garantizar el suministro eléctrico. (p. 50).

Lo expuesto pueda darnos una idea de la alta complejidad de estos centros y a la par Infraestructuras Críticas. Cualquier tipo de riesgo, Antrópico de Carácter Tecnológico, Antrópico de Carácter Antisocial haría que la magnitud del daño sea muy alta, tal y como recoge González, M., (2018):

> Es difícil obviar que tanto los elementos del triángulo como los del tetraedro del fuego están presentes de forma permanente: - Como elementos combustibles tenemos agentes químicos con base alcohólica, químicos inflamables, gases medicinales, gases anestésicos, vello y tejido humano, medicación, productos desinfectantes, cánulas y tubos plásticos respiratorios, tejido textil de sábanas, paños quirúrgicos, pijamas, batas de papel para pacientes y un largo etcétera. - Como comburente las distintas líneas y botellas de oxígeno. No podemos ignorar que las distintas cirugías se realizan con una atmósfera enriquecida por el oxígeno superando su concentración normal hasta más de un 3%, situándose en niveles cercanos al 24%. - Posibles fuentes de ignición (energía de activación) a través de los distintos equipos (desfibriladores, equipos de luz láser, electrobisturíes con cauterización eléctrica, aparataje de traumatología y cirugía ortopédica como brocas, sierras, implante de distintos elementos de osteosíntesis (tornillería, clavos, placas, etc.). (p. 51).

Garantizar la seguridad, protección integral y la resiliencia en el sector sanitario es una labor no al alcance de cualquier Director de Seguridad, es debido según Rivas, A. (2017) porque:

> La sanidad, a día de hoy, es uno de los segmentos estratégicos de mayor envergadura en el mundo de la seguridad. Los hospitales son edificaciones de alta complejidad, con una configuración estructural muy específica (…). (p.44).

Antisocial también son de consideración. En cualquier caso, el principal riesgo en estas áreas, además de los riesgos que podrían asociarse a unos deficitarios niveles de Bioseguridad, es el de incendio y explosión».

3.7. PROTECCIÓN DE HOSPITALES Y CONVENCIÓN DE GINEBRA FRENTE A CONFLICTOS.

La Convención de Ginebra es en realidad una serie de convenciones internacionales que se han celebrado en Ginebra, Suiza, desde el siglo XIX. Estas convenciones tratan principalmente sobre el derecho internacional humanitario, que establece normas para proteger a las personas afectadas por conflictos armados. Algunos de los acuerdos más importantes adoptados en las Convenciones de Ginebra incluyen:

1. Protección de personas heridas en el campo de batalla.
2. Protección de personas enfermas y heridas en el mar durante conflictos armados.
3. Trato humano a prisioneros de guerra.
4. Protección de civiles en tiempos de guerra, incluyendo a los no combatientes, los heridos, los enfermos y los prisioneros civiles.
5. Protección de personas en poder del enemigo.

Estos acuerdos forman la base del derecho internacional humanitario y han sido ratificados por la mayoría de los países del mundo. Además de las Convenciones de Ginebra originales, hay protocolos adicionales que han ampliado y fortalecido estas protecciones en conflictos armados.

En el contexto de las Convenciones de Ginebra y el derecho internacional humanitario, se adoptaron varios acuerdos importantes en relación con los hospitales y el personal médico durante conflictos armados. Algunos de los principales acuerdos incluyen:

1. Protección de Hospitales y Personal Médico: la Convención de Ginebra establece la obligación de los Estados en conflicto de respetar y proteger los hospitales, unidades médicas y el personal médico que proporciona atención médica a los heridos y enfermos, siempre y cuando no se utilicen para fines militares.
2. Distinción entre Objetivos Militares y Médicos: las partes en conflicto deben distinguir claramente entre los objetivos militares legítimos y los hospitales u otras instalaciones médicas. Atacar deliberadamente hospitales y personal médico es considerado un crimen de guerra.

3. Emblema de la Cruz Roja o la Media Luna Roja: las Convenciones de Ginebra establecen que los hospitales y unidades médicas deben ser claramente identificados mediante el uso del emblema de la Cruz Roja, la Media Luna Roja o cualquier otro emblema médico reconocido internacionalmente. Este emblema sirve como señal de protección y neutralidad.

4. Acceso Humanitario a los Heridos y Enfermos: las partes en conflicto tienen la obligación de permitir y facilitar el acceso humanitario rápido y sin obstáculos a los heridos y enfermos, así como a las unidades médicas y hospitales, por parte de personal médico y organismos humanitarios.

Estos acuerdos buscan proteger la prestación de atención médica durante conflictos armados, garantizando que los heridos y enfermos reciban tratamiento adecuado y que el personal médico pueda realizar su trabajo de manera segura y efectiva.

En cualquier caso frente a los Riesgos Antrópicos de Carácter Antisocial y de manera específica a lo que respecta al terrorismo, hemos de decir que lo convenido en Ginebra no es respetado por los distintos grupos terroristas en relación al respeto por las instituciones hospitalarias, inclusive en los distintos conflictos bélicos que sufrimos en la actualidad, hemos podido comprobar como los hospitales son atacados constantemente por la merma de recursos asistenciales a la población y por la consideración de servicios esenciales y estratégicos.

3.8. HOSPITALES QUE HAN SIDO OBJETO DE DESASTRES.

Las Infraestructuras Críticas Hospitalarias sufren todo tipo de daños, desastres naturales, daños por Riesgos Antrópicos de Carácter Tecnológico, por Riegos Antrópicos de Carácter Antisocial (acciones terroristas, conflictos bélicos, etc.), la Convención de Ginebra *per se,* no minimiza ni protege del riesgo de que los hospitales puedan ser el blanco de los distintos ataques, con la gran repercusión e impacto que esto tiene en la sociedad como servicio esencial y a la par estratégico. Nos parece pertinente hacer una relación de aquellos hospitales que han sido objeto de desastres:

3.8.1. Hospitales objeto de desastres en América del Sur:

1. Hospital del Mar, Lima, Perú (2001): un incendio arrasó con gran parte del hospital, causando numerosas muertes y heridos. La causa exacta del incendio no se determinó, pero se especuló sobre un posible cortocircuito eléctrico.

2. Hospital Regional de Cusco, Perú (2007): un terremoto de magnitud 8,0 afectó la región sur de Perú, dañando el Hospital Regional de Cusco y requiriendo la evacuación de pacientes y la atención médica en áreas temporales.
3. Hospital de Santa Cruz, Bolivia (2008): inundaciones severas causadas por las lluvias torrenciales afectaron al Hospital de Santa Cruz, inundando áreas clave del hospital y dificultando la prestación de servicios médicos.
4. Hospital Borda, Buenos Aires, Argentina (2012): se produjo un incendio en el hospital psiquiátrico Borda que resultó en la muerte de al menos 7 pacientes y dejó a varios heridos. La causa del incendio se atribuyó a un cortocircuito eléctrico.
5. Hospital de Arica, Chile (2014): un terremoto de magnitud 8,2 golpeó la región norte de Chile, dañando gravemente el Hospital de Arica y obligando a trasladar a los pacientes a instalaciones médicas temporales.
6. Hospital de San Pedro de Jujuy, Argentina (2014): inundaciones repentinas causadas por fuertes lluvias afectaron al Hospital de San Pedro de Jujuy, interrumpiendo temporalmente los servicios médicos y causando daños en la infraestructura.
7. Hospital de Chosica, Perú (2015): las fuertes lluvias e inundaciones causaron graves daños al Hospital de Chosica, dejándolo fuera de servicio y requiriendo la atención médica de emergencia en otros centros de salud.
8. Hospital Universitario de Maracaibo, Venezuela (2018): un incendio afectó varias áreas del hospital, obligando a la evacuación de pacientes y personal médico. Las causas del incendio aún están bajo investigación, pero se cree que pudo haber sido causado por un cortocircuito eléctrico.
9. Hospital dos Servidores do Estado, Río de Janeiro, Brasil (2019): un incendio afectó varios pisos del hospital, obligando a la evacuación de pacientes y causando la muerte de al menos 11 personas. La causa del incendio se atribuyó a un cortocircuito en un generador eléctrico.
10. Hospital Santa Rosa, Lima, Perú (2020): un incendio se desató en el hospital, obligando a la evacuación de pacientes y causando daños significativos en algunas áreas. La causa del incendio aún está siendo investigada.

3.8.2. Hospitales objeto de desastres en Estados Unidos (EE.UU.).

1. Hospital de la Trinidad, Chicago, EE. UU. (1915): un incendio devastador arrasó el hospital, causando más de 600 muertes, principalmente debido a la propagación rápida del fuego y la falta de medidas de seguridad adecuadas.

2. Hospital General de Massachusetts, Boston, EE. UU. (2013): dos bombas explotaron cerca de la línea de meta del Maratón de Boston, causando numerosas lesiones y muertes. Muchos de los heridos fueron trasladados al Hospital General de Massachusetts para recibir tratamiento. El incidente lo destacamos porque produjo un colapso asistencial por la avalancha de heridos, lo que le impidió prestar una adecuada asistencia por no establecer la adecuada activación y puesta en marcha del Plan de Emergencias Extracentro.

3.8.3. Hospitales en la UE que han sido objeto de desastres, incluso de ataques terroristas:

1. Hospital Clínico de Zaragoza, España (2010): Un incendio se desató en el hospital debido a un fallo eléctrico, obligando a la evacuación de pacientes y personal médico.
2. Hospital Universitario de Oslo, Noruega (2011): Un hombre detonó una bomba cerca del edificio del hospital como parte de los ataques terroristas en Noruega en 2011, causando daños materiales significativos e hiriendo a varias personas como consecuencia del hecho.
3. Hospital Universitario de Lieja, Bélgica (2011): Un hombre armado abrió fuego en el hospital, matando a varias personas e hiriendo a otras antes de ser detenido por la policía.
4. Hospital Universitario de Charleroi, Bélgica (2015): un hombre armado tomó como rehenes a varias personas en el hospital antes de ser abatido por la policía.
5. Hospital de la Trinidad, Dublín, Irlanda (2017): un hombre armado con un cuchillo ingresó al hospital y apuñaló a varias personas, incluido el personal médico, antes de ser detenido por la policía.
6. Hospital Universitario de Helsinki, Finlandia (2017): un hombre armado entró en el hospital y disparó contra el personal médico antes de ser reducido por la policía.
7. Hospital de Dublín, Irlanda (2017): un hombre armado con un cuchillo ingresó al hospital y apuñaló a varias personas, incluido el personal médico, antes de ser detenido por la policía.
8. Hospital Universitario de Uppsala, Suecia (2018): un hombre condujo un coche robado contra la entrada principal del hospital e intentó provocar una explosión al prender fuego al vehículo. El atacante murió posteriormente por las lesiones sufridas durante el incidente.
9. Hospital Universitario de Uppsala, Suecia (2018): un hombre condujo un coche robado contra la entrada principal del hospital e intentó provocar una explosión al prender

fuego al vehículo. El atacante murió posteriormente por las lesiones sufridas durante el incidente.

10. Hospital Sint-Elisabeth, Uccle, Bélgica (2018): un hombre armado entró en el hospital y tomó como rehenes a dos personas antes de ser detenido por la policía.
11. Hospital Central de Málaga, España (2020): un incendio afectó a la planta baja del hospital, causando daños materiales, pero sin víctimas.
12. Hospital Universitario de Montpellier, Francia (2021): un incendio se declaró en el hospital, obligando a la evacuación de pacientes y provocando daños materiales importantes.
13. El Hospital Clínic de Barcelona fue víctima de un ciberataque el 5 de marzo de 2023. El ataque, de tipo *ransomware*, afectó a los servicios sanitarios del hospital, incluyendo urgencias, laboratorio y farmacia

3.8.4. Hospitales en Oriente Medio que han sido objeto de ataques terroristas:

1. Hospital Hadassah, Jerusalén, Israel (2002): durante la Segunda Intifada, un atacante suicida se hizo estallar en la entrada del hospital, matando a varios civiles e hiriendo a muchos más.
2. Hospital Al-Nasiriyah, Irak (2003): durante la Guerra de Irak, un camión bomba explotó en las afueras del hospital, causando una gran cantidad de muertes y heridos entre el personal médico y los pacientes.
3. Hospital Central de Bagdad, Irak (2003-presente): ha sido objetivo de ataques terroristas, bombardeos y ataques con cohetes desde la invasión de Irak en 2003. Estos ataques han causado un gran número de víctimas y han dificultado la prestación de servicios médicos.
4. Hospital Dar Al-Shifa, Gaza (2009): durante el conflicto entre Israel y Hamas en la Franja de Gaza, el hospital fue alcanzado por ataques aéreos israelíes, resultando en la muerte y lesiones de personal médico y pacientes.
5. Hospital Jinnah, Pakistán (2010): fue atacado por un grupo de terroristas armados que tomaron rehenes y llevaron a cabo un tiroteo dentro del hospital, resultando en varias muertes y heridos.
6. Hospital Norteño de Alepo, Siria (2013-2016): durante la guerra civil siria, el hospital fue blanco de repetidos ataques aéreos y bombardeos, causando la muerte y lesiones a pacientes y personal médico.

7. Hospital de Al-Aqsa, Gaza (2014): durante el conflicto entre Israel y Hamas en la Franja de Gaza, el hospital fue alcanzado por ataques aéreos israelíes, lo que provocó la muerte y lesiones de personal médico y pacientes.
8. Hospital de Kunduz, Afganistán (2015): las fuerzas estadounidenses llevaron a cabo un ataque aéreo contra el hospital administrado por Médicos Sin Fronteras, matando a al menos 42 personas, incluyendo personal médico y pacientes. Se alegó que el ataque fue un error.
9. Hospital Público de Quetta, Pakistán (2016): fue blanco de un ataque suicida perpetrado por un grupo terrorista, que resultó en múltiples muertes y heridos entre los pacientes y el personal médico.
10. Hospital Pediátrico Banzai, Afganistán (2017): un ataque suicida perpetrado por el Estado Islámico golpeó el hospital, matando e hiriendo a un gran número de personas, incluyendo niños y personal médico.
11. Hospital Universitario de Mosul, Irak (2017): durante la batalla por Mosul contra ISIS, el hospital sufrió bombardeos y ataques por parte de las fuerzas en conflicto, resultando en daños significativos y la interrupción de los servicios médicos.
12. Hospital General de Kabul, Afganistán (2020): un ataque con bomba dirigido contra el hospital materno-infantil de Dasht-e-Barchi en Kabul mató a decenas de personas, incluidos recién nacidos, madres y personal médico.

3.9. SEGURIDAD DE LOS DATOS Y SEGURIDAD HOSPITALARIA.

Prevalecen, en materia de Protección de Datos de Carácter Personal y Seguridad Hospitalaria, principalmente dos normas de importancia sobre la que dimanan el resto en materia de Protección de Datos de Carácter Personal. La primera, conocida coloquialmente como el RGPD 679/2016 y que hace referencia al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como en nuestro país la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018. En el primero de los textos legales expuestos establece:

1. Política de Privacidad y Protección de Datos: los hospitales deben desarrollar y mantener una política detallada que establezca los principios rectores para el tratamiento de datos personales, incluyendo la información sobre los derechos de los

individuos y los procedimientos para ejercerlos. los principios relativos al tratamiento de datos personales deben ser transparentes y justos. La información debe ser proporcionada de manera clara, concisa y comprensible.

Todo ello a tenor del RGPD (679/2016), en relación a los principios relativos al tratamiento de datos personales, cuyo tenor literal expresa que serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con esos fines; de acuerdo con el artículo 89, apartado 1, estos fines determinados no incluirán el tratamiento ulterior con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, en la medida en que esté sujeto a las medidas técnicas y organizativas adecuadas previstas en el presente Reglamento con miras a garantizar los derechos y libertades del interesado («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas adecuadas previstas en el presente Reglamento con miras a garantizar los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). (Art. 5).

2. Designación de un Delegado de Protección de Datos (DPD): deben designar un DPD encargado de supervisar el cumplimiento de la normativa de protección de datos, actuar como punto de contacto para las autoridades de control y el público en general, y brindar asesoramiento dentro de la organización. En el sentido referenciado, los hospitales, deben designar un DPD con el objeto supervisar el cumplimiento legal y reglamentario en materia de protección de datos de carácter persona. Por ello, tanto el responsable de los datos como el encargado del tratamiento, en atención a lo expuesto, el RGPD 679/2016, recoge que:

   > (…) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala; o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales. (Art. 37).

3. Análisis de Riesgos y Evaluaciones de Impacto de Protección de Datos (DPIA): los hospitales deben llevar a cabo evaluaciones de riesgos y DPIA para identificar y mitigar posibles riesgos para la seguridad de los datos personales, especialmente en casos de tratamiento de datos sensibles, como información médica. Por el motivo expuesto, se establece la obligación de llevar a cabo una DPIA cuando el tratamiento de datos personales pueda entrañar un alto riesgo para los derechos y libertades de las personas. En relación a lo expuesto, en lo que respecta al epígrafe Evaluación de impacto relativa a la protección de datos, a tenor del RGPD 679/2016):

   > Cuando sea probable que un tipo de tratamiento, en particular cuando utilice nuevas tecnologías, y teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento llevará a cabo, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento previstas sobre la protección de datos personales. (Art. 35).

4. Seguridad de la Información: implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los datos personales, incluyendo la encriptación de datos, la gestión de accesos, la monitorización de la red y la capacitación del personal en seguridad de la información.

   En el sentido expuesto, se la establece la obligación de implementar tales medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo la pseudonimización.

5. Consentimiento Informado: obtener el consentimiento informado de los pacientes o sus representantes legales para el tratamiento de sus datos personales, explicando claramente los fines y la base legal del tratamiento.

   En ese sentido, el consentimiento debe ser siempre libre, específico, informado e inequívoco. Los hospitales deben obtener el consentimiento de los pacientes para el tratamiento de sus datos personales de manera clara y explícita.

   Por todo ello y, en relación a las condiciones para el consentimiento, según el RGPD (679/2016):

   > Cuando el tratamiento se base en el consentimiento del interesado, el responsable del tratamiento podrá solicitar el consentimiento para uno o varios fines específicos. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta el hecho de que la ejecución de un contrato, incluida la prestación de un servicio, está supeditada al consentimiento del interesado al tratamiento de datos personales que no sean estrictamente necesarios («consentimiento inequívoco»). (Art. 7).

6. Derechos de los Individuos: garantizar la capacidad de los individuos para ejercer sus derechos de protección de datos, como el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos y oposición al tratamiento. Aumenta los conocidos derechos ARCO, de la Ley 15/99, ya derogada, tales derechos incluyen el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos y oposición al tratamiento.

7. Transferencias Internacionales de Datos: cumplir con las restricciones y requisitos para transferir datos personales fuera del Espacio Económico Europeo, incluyendo la selección de mecanismos de transferencia legalmente válidos, como las cláusulas contractuales tipo o el Escudo de Privacidad UE-EE. UU.

   En el sentido que se expone, ha de considerarse las adecuadas condiciones para la transferencia de datos personales a países fuera del Espacio Económico Europeo, asegurando que se proporcionen garantías debidas para la protección de los datos.

   En lo que respecta a lo que hemos referenciado, el RGPD 679/2016, establece las condiciones y los mecanismos para la transferencia de datos personales fuera del Espacio Económico Europeo. (Arts. 44-50).

8. Registro de Actividades de Tratamiento: mantener un registro detallado de todas las actividades de tratamiento de datos personales llevadas a cabo por el hospital, incluyendo la base legal del tratamiento, las categorías de datos personales involucrados y cualquier transferencia internacional de datos, deben de incluir, la información sobre los fines del tratamiento y las categorías de datos involucrados. En relación a lo expuesto y según el RGPD (679/2016), en relación con el Registro de Actividades de Tratamiento y según su tenor literal:

   > Cada responsable y encargado del tratamiento llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Ese registro contendrá toda la información a que se refieren los apartados 2 y 3. 2.
   >
   > El responsable y el encargado del tratamiento pondrán a disposición de la Autoridad de Control toda la información necesaria para demostrar el cumplimiento de lo dispuesto en el presente artículo y permitirán su examen. (Art. 30).

9. Notificación de Brechas de Seguridad: establecer procedimientos para detectar, investigar y notificar las violaciones de seguridad de datos personales a las autoridades de control y a los individuos afectados dentro de los plazos establecidos por la normativa. Se establece, por tanto, la obligación de notificar a la autoridad de control competente cualquier violación de la seguridad de los datos personales dentro de las 72 horas posteriores a su descubrimiento, a menos que la brecha no represente un riesgo para los derechos y libertades de los individuos. En ese sentido y en relación al

epígrafe que lleva por título Notificación de una violación de la seguridad de los datos personales a la autoridad de control, el RGPD (679/2016), establece que:

> En caso de violación de la seguridad de los datos personales, el responsable del tratamiento lo comunicará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a no ser que sea improbable que dicha violación de la seguridad de los datos personales represente un riesgo para los derechos y libertades de las personas físicas. (Art. 33).

10. Auditorías y Revisiones Regulares: realizar auditorías periódicas y revisiones internas para garantizar el cumplimiento continuo de la normativa de protección de datos y la eficacia de las medidas de seguridad implementadas. Realmente, no está específicamente delineado o incorporado en un artículo de manera específica, el principio de responsabilidad establecido en el artículo 5 del GDPR implica que las organizaciones, incluidos los hospitales, deben realizar auditorías internas y revisiones periódicas para garantizar el cumplimiento continuo de la normativa de protección de datos.

Al considerar estos elementos detallados y aplicarlos de manera rigurosa, los hospitales pueden garantizar la seguridad y protección adecuadas de los datos de carácter personal en cumplimiento con el Reglamento Europeo de Protección de Datos y la legislación nacional aplicable. No debemos de olvidar que los hospitales manejan datos sensibles, del nivel más alto, relativos a la salud de las personas y que han de protegerse adecuadamente.

Si se incumple *grosso modo* con la legislación en materia de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales, las Infraestructuras Críticas podrían enfrentarse a:

- ✓ Sanciones Administrativas: las autoridades de control, como la Agencia Española de Protección de Datos (AEPD), pueden imponer sanciones administrativas en caso de incumplimiento del GDPR y la legislación nacional de protección de datos. Estas multas pueden ser significativas y pueden alcanzar hasta el 4% del volumen de negocio anual global del hospital o una cantidad monetaria considerable, dependiendo de la gravedad de la infracción.

- ✓ Acciones Judiciales: los individuos afectados por un incumplimiento de la normativa de protección de datos pueden emprender acciones judiciales contra el hospital en cuestión. Esto podría dar lugar a demandas por daños y perjuicios, así como a la adopción de medidas correctivas ordenadas por los tribunales, todo ello por las distintas responsabilidades jurídicas que se derivan.
- ✓ Reputación Institucional Dañada: el incumplimiento de la normativa de protección de datos puede socavar la confianza del público en el hospital y su reputación institucional. La divulgación pública de violaciones de datos o de prácticas de tratamiento de datos poco éticas puede afectar negativamente la percepción del hospital por parte de pacientes, personal médico y la comunidad en general.
- ✓ Pérdida de Clientes y Prestigio: los pacientes pueden optar por buscar servicios médicos en otros hospitales que consideren más respetuosos con la privacidad y la seguridad de sus datos personales. Además, los proveedores de seguros y otros socios comerciales pueden reconsiderar sus relaciones con el hospital si perciben un alto riesgo de violaciones de datos o incumplimientos de la normativa de protección de datos.
- ✓ Daño a la Marca: el escándalo relacionado con el incumplimiento de la protección de datos puede dañar la imagen de marca del hospital a largo plazo. La pérdida de confianza del público puede afectar negativamente a la capacidad del hospital para atraer y retener pacientes, así como para atraer talento médico y personal cualificado.

El incumplimiento de los preceptos reseñados en materia de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales en hospitales puede tener graves implicaciones legales y reputacionales. Por lo tanto, es fundamental que los hospitales cumplan rigurosamente con las normativas de protección de datos para evitar estas consecuencias negativas, además de no garantizarse la ciberseguridad y el ciberterrorismo, podría comprometerse la seguridad de los datos y la prestación de servicios médicos asistenciales debido a que pueden favorecer los siguientes ciberataques:

1. Ataques de *Ransomware*: las Infraestructuras Críticas Hospitalarias, como se ha demostrado recientemente, son el blanco de ataques de *ransomware*, donde los ciberdelincuentes cifran los sistemas informáticos y exigen un rescate para restaurar el acceso. Esto puede comportar la interrupción de los distintos servicios asistenciales y

médicos, la pérdida de datos, así como la exposición de información confidencial del paciente.

2. Acceso No Autorizado a Sistemas: los ciberdelincuentes pueden intentar acceder de forma no autorizada a los sistemas informáticos del hospital para robar información confidencial, como registros médicos, datos de tarjetas de crédito o información personal de los pacientes y el personal médico.
3. *Phishing* e Ingeniería Social: los ataques de *phishing* y la ingeniería social pueden utilizarse para engañar al personal del hospital y obtener acceso no autorizado a sistemas o datos confidenciales. Esto puede ocurrir a través de correos electrónicos de *phishing*, llamadas telefónicas fraudulentas u otros métodos de manipulación.
4. Vulnerabilidades de *Software* y Dispositivos Médicos Conectados: los hospitales suelen utilizar una amplia gama de dispositivos médicos conectados a redes informáticas, que pueden ser vulnerables a ataques si no se mantienen actualizados y seguros. Las vulnerabilidades de software también pueden ser explotadas por ciberdelincuentes para acceder a sistemas hospitalarios.
5. Ataques de Denegación de Servicio (DDoS): los ataques DDoS pueden dirigirse contra los sistemas informáticos del hospital, sobrecargándolos con un tráfico malicioso y causando la interrupción de los servicios médicos y la disponibilidad de los sistemas.
6. Robo de Identidad y Fraude: los ciberdelincuentes pueden robar identidades de pacientes o personal médico para cometer fraudes, como la falsificación de recetas médicas o la presentación de reclamaciones falsas a compañías de seguros.
7. Violaciones de Privacidad y Confidencialidad: la exposición no autorizada de información médica confidencial puede violar la privacidad de los pacientes, generar problemas y responsabilidades legales de diversa índole y reputacionales, en relación a la merma de la imagen corporativa, cuyo daño es intangible para el hospital.

Estas brechas en la ciberseguridad pueden ser la puerta de entrada a los ciberataques y al ciberterrorismo pueden tener consecuencias graves para la seguridad de los datos y la prestación de servicios asistenciales y médicos en los hospitales. Por lo tanto, es fundamental implementar medidas sólidas de seguridad cibernética y estar preparado para detectar, prevenir y responder a posibles amenazas. Por lo tanto, es fundamental implementar medidas sólidas de seguridad cibernética y estar preparado para detectar, prevenir y responder a posibles amenazas.

En relación a lo expuesto y, según González, M. (2019):

> En materia de Protección de Datos, los principales problemas que surgen en los hospitales en el día a día son los siguientes:
>
> - La no verificación de la identidad del paciente al que se va a prestar asistencia sanitaria conjuntamente con la tarjeta sanitaria (indistintamente si es del Servicio Público de Salud, de MUGEJU, ISFAS, MUFACE o compañías de seguros privadas).
> - Inexistencia de un protocolo que contemple el deber de conservar la documentación clínica el tiempo necesario para prestar asistencia al paciente.
> - Ausencia de información o de señalética informativa en aquellas áreas donde se recaban los datos personales como pueden ser: Admisión de Urgencias, Admisión de Hospitalización, Admisión de Radiología y Pruebas Diagnósticas complementarias a través de la imagen.
> - Carencia de información a los usuarios y pacientes sobre los derechos que la ley Orgánica en materia de Protección de Datos confiere.
> - Falta de Concienciación del personal y de la organización.
> - Información y formación adecuada a todos los trabajadores del hospital, independientemente de su categoría profesional en relación al deber de secreto y de confidencialidad en relación a los datos de los pacientes y usuarios del hospital.
> - Ausencia de privilegios personalizados para el acceso a la historia clínica d los pacientes en atención a los distintos perfiles profesionales.
> - No se restringe o limita el acceso a la historia clínica para algunos perfiles profesionales (…).
> - Generalmente existen privilegios generalizados que el personal utiliza indistintamente (…).
> - (…). (p. 37).

En tal sentido y en aras de evitar las brechas de seguridad relacionadas con la ciberseguridad y el ciberterrorismo en hospitales, es necesario implementar una serie de medidas de seguridad y protocolos. Es capital la considerar el siguiente decálogo que establecemos con el objeto de evitar los referenciados riesgos, consistente en:

1. Política de Seguridad de la Información: debe de desarrollarse e implementarse una política de seguridad de la información que establezca directrices claras y

procedimientos para proteger los sistemas y datos del hospital contra amenazas cibernéticas.

2. Capacitación del Personal: proporcionar formación regular en seguridad informática y concienciación sobre ciberseguridad a todo el personal del hospital para que estén alerta ante posibles amenazas y sepan cómo responder adecuadamente.
3. Actualización de *Software* y Parches: mantener actualizado el *software* y los sistemas operativos en todos los dispositivos médicos y computadoras del hospital para mitigar vulnerabilidades conocidas y asegurar que se apliquen los parches de seguridad pertinentes.
4. Control de Acceso y Autenticación Multifactorial: implementar medidas de control de acceso, como contraseñas robustas y autenticación multifactorial, para proteger los sistemas y datos del hospital contra accesos no autorizados.
5. Encriptación de Datos: encriptar los datos sensibles almacenados y transmitidos dentro del hospital para protegerlos contra el acceso no autorizado en caso de brechas de seguridad.
6. Auditorías de Seguridad y Pruebas de Penetración: realizar auditorías periódicas de seguridad y pruebas de penetración en los sistemas del hospital para identificar y corregir vulnerabilidades antes de que puedan ser aprovechadas por ciberdelincuentes.
7. Respuesta a Incidentes y Plan de Continuidad del Negocio: debe de desarrollarse un plan de respuesta a incidentes cibernéticos que establezca procedimientos claros para detectar, contener y mitigar las brechas de seguridad, así como un plan de continuidad del negocio para garantizar la prestación de servicios médicos durante y después de un incidente.
8. Seguridad de Dispositivos Médicos Conectados: implementar medidas de seguridad específicas para dispositivos médicos conectados, como sistemas de gestión de parches, segmentación de red y controles de acceso para protegerlos contra ataques cibernéticos.
9. Monitorización y Detección de Amenazas: implementar sistemas de monitorización y detección de amenazas en tiempo real para identificar y responder rápidamente a actividades sospechosas en la red del hospital.

10. Colaborar y compartir Información: colaborar con otras instituciones de salud, agencias gubernamentales, Comunidad de Inteligencia [61] y organizaciones de ciberseguridad para compartir información sobre amenazas y mejores prácticas de seguridad cibernética.

    Todos los elementos destacados son cuestiones que refuerzan la ciberseguridad en los distintos centros e Infraestructuras Críticas hospitalarias. La implementación ISO/IEC 27001 - Sistemas de gestión de la seguridad de la información para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información dentro del contexto de los riesgos generales de la organización, es una herramienta adecuada para reforzar el nivel de seguridad. En el entorno hospitalario, proteger la información del paciente y garantizar la confidencialidad de los registros médicos o cualquier otra información de la Historia Clínica es fundamental.

En relación a lo expuesto, hemos de considerar el reciente ataque a una Infraestructura Crítica Hospitalaria, el sufrido por El Hospital Clínic de Barcelona, víctima de un ciberataque el 5 de marzo de 20231. Este ataque, de tipo *ransomware*, afectó a los servicios sanitarios del hospital, que incluyó al Servicio de Urgencias, laboratorio y la Farmacia Hospitalaria.

El ciberataque se realizó fuera de España, se utilizó un *ransomware*, un tipo de malware que cifra los archivos y exige un rescate para desbloquearlos. El sistema informático del hospital se colapsó debido al ataque. Sus consecuencias más relevantes fueron:

- ✓ Suspensión temporal de intervenciones quirúrgicas: el ataque afectó la programación de cirugías, poniendo en riesgo la salud de los pacientes.
- ✓ Trámites manuales: el hospital tuvo que realizar trámites informáticos a mano debido a la inaccesibilidad de los sistemas.
- ✓ Complicaciones en el acceso a historiales médicos: el *ransomware* dificultó el acceso a los registros de pacientes.

Las medidas que se adoptaron para paliar sus efectos fueron:

- ✓ Coordinación con el Servicio de Emergencias Médicas (SEM): se evitó el traslado de enfermos al centro y se derivaron a otros hospitales.

[61] La comunidad de inteligencia es un término que se refiere a la red de organizaciones, agencias y profesionales dedicados a la recopilación, análisis y difusión de información relacionada con la seguridad nacional, la defensa, el orden público y otros aspectos relevantes para la toma de decisiones gubernamentales.

- ✓ Reactivación parcial de sistemas informáticos: el hospital logró restablecer parte de sus sistemas y reanudó las consultas externas con un 10 % de actividad.
- ✓ Trabajo de servicios técnicos: se implementaron medidas para resolver la incidencia y proteger los sistemas.

El ataque informático al Hospital Clínic de Barcelona tuvo consecuencias significativas, pero se adoptaron medidas reactivas y de contingencia para mitigar los efectos y proteger la seguridad de los pacientes y la integridad de los datos médicos. En cualquier caso, sirve de ejemplo en relación a la importancia de establecer cuántas medidas preventivas y de seguridad son necesarias.

3.10. INSTRUCCIÓN IS-41[62] Y SEGURIDAD HOSPITALARIA.

La referenciada norma fue aprobada por el Consejo de Seguridad Nuclear (CSN). Es una norma de suma importancia para aquellos hospitales que traten enfermedades oncológicas a través de la radioterapia, todo ello por la utilización de distintas fuentes radioactivas. Su implementación tiene implicaciones importantes para las instituciones de salud que utilizan fuentes radiactivas en sus prácticas médicas. La instrucción pretende fortalecer la seguridad y la protección de las distintas fuentes radioactivas, lo que contribuye en los hospitales a lograr un entorno más seguro, tanto para las visitas, pacientes, personal sanitario, técnico, contratas y subcontratas.

Su implementación para elevar el nivel de seguridad hospitalaria es trascendental, para ello han de considerarse los siguientes aspectos cruciales al efecto:

1. Seguridad en el Manejo de Fuentes Radiactivas: los hospitales que emplean fuentes radiactivas para diagnóstico, tratamiento o investigación deben cumplir con los requisitos de seguridad establecidos en la instrucción. Lo que incluye medidas para la prevención del hurto o del robo, así como la retirada no autorizada de las distintas fuentes radioactivas.

2. Protección contra Actos Malévolos: la instrucción se centra en proteger las fuentes radiactivas contra actos malévolos, como el robo o la manipulación indebida. Para

[62] Instrucción que emana del Consejo de Seguridad Nuclear (CSN). El Consejo de Seguridad Nuclear es el organismo regulador en España encargado de la protección radiológica y nuclear, así como de la seguridad de las instalaciones nucleares y radiactivas. Su función principal es garantizar que estas instalaciones sean operadas de manera segura y proteger a las personas y al medio ambiente de los riesgos asociados con la radiación ionizante.

garantizar una mayor seguridad, los hospitales deben de implementar una serie de medidas que eviten que las fuentes caigan en manos equivocadas y puedan utilizarse de manera ilícita. Para ello la instrucción establece la obligatoriedad de implementar Departamentos de Seguridad Hospitalarios con un Director de Seguridad debidamente habilitado por el Ministerio del Interior que deberá de realizar el Plan de Protección Física frente a fuentes radioactivas.

3. Formación y Capacitación del Personal: los hospitales deben capacitar a su personal en los procedimientos de seguridad relacionados con las fuentes radiactivas. Estas acciones deben de incluir la detección temprana de cualquier tipo de circunstancia anómala, así como la adecuada respuesta de carácter reactiva en caso de incidentes.

4. Colaboración con Autoridades Competentes: El CSN colabora en la elaboración de criterios para los planes de emergencia exterior y de protección física de instalaciones radiactivas. Para ello, los hospitales tendrán que coordinarse con las autoridades competentes para la implementación efectiva de cuantas disposiciones y medidas de seguridad sean preceptivas a tenor de la referenciada norma.

En el entorno hospitalario, la protección física frente a fuentes radiactivas es crucial para garantizar la seguridad de los pacientes, el personal médico y el público en general. A continuación, se detallan los aspectos relevantes relacionados con esta protección:

1. Fuentes Radiactivas en Hospitales:

   - ✓ Los hospitales utilizan equipos de rayos X y fuentes radiactivas para el diagnóstico y tratamiento de diversas enfermedades.

   - ✓ Los trabajadores expuestos (como los de radiología, medicina nuclear y oncología radioterápica) tienen una preparación específica en el uso seguro de estas máquinas y fuentes.

   - ✓ Sin embargo, otros trabajadores del hospital también pueden estar expuestos a la radiación en su entorno laboral (enfermeras, personal de mantenimiento, seguridad, administrativos, etc.).

2. Medidas de Protección Radiológica:

   - ✓ Es necesario aplicar medidas de protección radiológica para protegerse frente a la radiación y contaminación originada por las sustancias o fuentes radiactivas.

- ✓ Estas medidas incluyen el uso adecuado de equipos de protección personal, la limitación del tiempo de exposición y la distancia segura de las fuentes radiactivas.

Especial referencia al Plan de Protección Física frente a Fuentes Radioactivas de la IS-41, del Consejo de Seguridad Nuclear: El plan de protección física es un documento que describe el sistema de seguridad física de una instalación o fuente radiactiva.

En él se establecen todas las medidas necesarias para la protección de todo tipo de fuentes, en función a su clase frente a cualquier tipo de acto delictivo, en los que el director de seguridad en el hospital desempeña un papel fundamental en la implementación y supervisión de este plan, ya no sólo porque así lo establece la referenciada Instrucción sino por las competencias legalmente establecidas que ya se referenciaron en el capítulo precedente a la presente investigación. El director de seguridad es responsable de coordinar y supervisar todas las actividades relacionadas con la seguridad en el hospital. En el contexto de protección física frente a fuentes radiactivas, sus funciones incluyen:

- ✓ Elaboración del Plan: trabaja con expertos para desarrollar un plan de protección física específico para el hospital, considerando las áreas de uso de fuentes radiactivas.
- ✓ Implementación: asegura que las medidas del plan se apliquen correctamente en todas las áreas relevantes.
- ✓ Formación y Capacitación: garantiza que el personal esté capacitado en las prácticas seguras relacionadas con la radiación.
- ✓ Supervisión y Evaluación: realiza inspecciones regulares para verificar el cumplimiento y la eficacia del plan.

No debemos de obviar que la seguridad debe ser parte de la cultura de la organización, en lo que respecta a la protección física frente a fuentes radiactivas en hospitales es una responsabilidad compartida entre los trabajadores, el director de seguridad y las autoridades competentes. La colaboración y la formación continua son esenciales para mantener un entorno seguro y protegido

3.11. NORMAS ISO Y SU RELACIÓN CON EL INCREMENTO DE LA SEGURIDAD HOSPITALARIA

Las normas[63] ISO son estándares internacionales desarrollados y publicados por la Organización Internacional de Normalización (ISO, por sus siglas en inglés).

La ISO es una organización no gubernamental compuesta por representantes de organismos de normalización de diversos países, en un contexto mundial en el que cada vez hay más países representados.

El objetivo principal de la organización es promover la estandarización para facilitar el intercambio de bienes y servicios a nivel global.

Las normas ISO abarcan una amplia variedad de áreas, incluyendo calidad, medio ambiente, seguridad de la información, gestión de riesgos, sistemas de gestión, entre otras. Estas normas están diseñadas para establecer requisitos, especificaciones, directrices o características que pueden ser aplicadas de manera voluntaria o exigida por regulaciones en diferentes industrias y sectores.

A continuación, por su relevancia en materia de seguridad en general, así como por su posible integración en el sector hospitalario con el objeto de aumentar la gestión de la seguridad, y por ende, el aumento de su índice de seguridad, aunque no son normas imperativas con carácter legal, una vez que las distintas organizaciones asumen su integración en su política institucional, generan un valor intangible a la imagen corporativa y reputacional. Recogemos aquellas que nos han parecido más pertinentes, por ser de consideración.

1. ISO 45001- Sistemas de gestión de la seguridad y salud en el trabajo: esta norma establece los requisitos para los sistemas de gestión de la seguridad y salud en el trabajo. Es aplicable a cualquier organización que desee establecer, implementar y mantener un sistema de gestión de la seguridad y salud en el trabajo para mejorar el desempeño en esta área.

2. ISO 31000 - Gestión del riesgo: Proporciona principios, marcos y procesos para la gestión del riesgo en cualquier tipo de organización. En el contexto de la seguridad

[63] Las Normas ISO son conjuntos de directrices, reglas o especificaciones técnicas aceptadas internacionalmente que buscan mejorar la calidad, la seguridad, la eficiencia y la interoperabilidad de productos, servicios y sistemas en todo el mundo.

hospitalaria, esta norma sería relevante para identificar, evaluar y tratar los riesgos asociados con la prestación de servicios de salud.

3. ISO/IEC 27001- Sistemas de gestión de la seguridad de la información: especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información dentro del contexto de los riesgos generales de la organización. En el entorno hospitalario, proteger la información del paciente y garantizar la confidencialidad de los registros médicos es fundamental.

4. ISO 22301- Seguridad y resiliencia - Gestión de la continuidad del negocio: Esta norma proporciona un marco para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la gestión de la continuidad del negocio.

   En el ámbito hospitalario, la continuidad del negocio puede implicar mantener la prestación de servicios de atención médica incluso en situaciones de crisis o emergencia.

5. ISO 19600- Sistemas de gestión de *compliance* - Directrices: ofrece pautas para establecer, implementar, mantener, revisar y mejorar un sistema de gestión de *compliance* efectivo en una organización. En un entorno hospitalario, esto se relacionaría con garantizar el cumplimiento de las regulaciones y estándares de atención médica.

   En el sentido apuntado, según González, M. (2023):

   > El Director de Seguridad no sólo ha de ser un verdadero gerente de riesgos, ha de ser un verdadero analista de inteligencia, además de un *Compliance officer*, neologismo que hace referencia a un oficial de cumplimiento legal y normativo en materia de prevención, seguridad y protección integral de la propia organización. Para poder dirigir, gestionar, asesorar en cualquiera de las materias que les son propias, implica su conocimiento y dominio. A contrario *sensu*, la organización queda altamente comprometida y desprotegida en relación a las distintas responsabilidades de las que podrían ser objeto. (p. 104-105).

6. ISO 28000- Gestión de la seguridad para la cadena de suministro: Proporciona un marco para implementar un sistema de gestión de la seguridad de la cadena de suministro, asegurando que los bienes se muevan de manera segura a lo largo de la

cadena de suministro. En hospitales, esto puede aplicarse a la gestión de suministros médicos críticos.

7. ISO 21001- Sistemas de gestión para organizaciones educativas: Aunque no está directamente relacionada con la seguridad hospitalaria, esta norma podría ser relevante para hospitales que ofrecen capacitación y educación médica, ya que proporciona un marco para mejorar la calidad educativa y la satisfacción del estudiante.

Estas son algunas de las normas ISO más relevantes para la seguridad en general y para la seguridad hospitalaria en particular.

Es importante que las organizaciones, incluidos los hospitales, evalúen sus necesidades específicas y seleccionen las normas ISO que mejor se ajusten a sus objetivos y contexto operativo en relación a cuántas debilidades o vulnerabilidades en materia de seguridad, en cualquiera de sus áreas, sean necesarias reforzar.

La adecuada implantación de las referenciadas normas, si se hace de manera adecuada hacen de ellas herramientas valiosas y pertinentes para buscar la excelencia en las materias en las que se implementen si se hace dentro de una cultura que llegue a todos los estamentos de la organización y no sólo como un mérito a efectos de imagen.

Las Normas ISO proporcionan un marco sólido para abordar la seguridad de la información, la gestión ambiental y la preparación para emergencias en entornos hospitalarios, lo que contribuye a garantizar la seguridad y el bienestar de los pacientes, el personal y el medio ambiente.

A continuación, dentro del amplísimo abanico existente y tras su ulterior lectura referenciamos aquellas que realmente pueden ser de interés en el entorno sanitario hospitalario al efecto de incrementar su seguridad.

1. ISO/IEC 27001- Sistemas de gestión de la seguridad de la información: esta norma establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. En el contexto hospitalario, proteger la confidencialidad, integridad y disponibilidad de la información del paciente es crucial.

2. ISO 27799- Tecnología de la información en salud: proporciona directrices para el manejo seguro y efectivo de la información de salud utilizando sistemas de

información. En un entorno hospitalario, esta norma es esencial para garantizar que los datos médicos sensibles se manejen de manera segura y se protejan contra amenazas cibernéticas.

3. ISO 22301- Seguridad y resiliencia - Gestión de la continuidad del negocio: Aunque no está específicamente dirigida a la seguridad de la información, esta norma es relevante para los hospitales en términos de garantizar la continuidad operativa en situaciones de emergencia, lo que incluye la protección de la información crítica.

4. ISO 14001- Sistemas de gestión ambiental: establece los requisitos para un sistema de gestión ambiental que una organización puede utilizar para mejorar su desempeño ambiental. En hospitales, esto implica la gestión adecuada de residuos médicos, consumo de recursos (agua, energía) y la reducción de la contaminación.

5. ISO 14031- Evaluación del desempeño ambiental: proporciona pautas para evaluar el desempeño ambiental de una organización. Los hospitales pueden utilizar esta norma para medir y mejorar su impacto ambiental, lo que incluye la evaluación de la eficacia de las medidas tomadas para mitigar emergencias medioambientales.

6. ISO 22320- Seguridad y resiliencia - Gestión de emergencias: esta norma proporciona orientación sobre la preparación y la capacidad de respuesta ante emergencias, incluidas las emergencias medioambientales. Es particularmente relevante para los hospitales, ya que necesitan estar preparados para responder eficazmente a situaciones como accidentes químicos, desastres naturales, entre otros.

7. ISO 45001- Sistemas de gestión de la seguridad y salud en el trabajo: aunque no está específicamente relacionada con la seguridad de la información o el medio ambiente, esta norma es relevante para los hospitales en términos de garantizar la seguridad y salud de su personal en todas las actividades, incluidas las relacionadas con la gestión de la información y la respuesta a emergencias medioambientales.

3.12. LA *JOINT COMMISSION*[64] Y LA SEGURIDAD HOSPITALARIA:

La *Joint Commission* es una organización independiente y sin fines de lucro en los Estados Unidos. Organización que se dedica a la acreditación y certificación de organizaciones de salud y programas de atención médica.

Aunque no son normas ISO tal y como apuntamos con anterioridad, las pautas y estándares establecidos por la *Joint Commission* son ampliamente reconocidos y seguidos por hospitales y centros de atención médica en los Estados Unidos. A continuación, referenciamos sus características más importantes y lo que supone para los hospitales y su seguridad:

1. Estándares de calidad: establece estándares rigurosos de calidad y seguridad para la atención médica. Estos estándares abarcan una amplia gama de áreas, incluida la gestión de riesgos, la seguridad del paciente, la calidad de la atención y la seguridad de la información.

2. Acreditación voluntaria: acreditación de la *Joint Commission* no es obligatoria, muchos hospitales y centros de atención médica buscan obtenerla para demostrar su compromiso con la excelencia en la atención médica. La acreditación de la *Joint Commission* es ampliamente reconocida como un sello de aprobación de calidad y seguridad.

3. Evaluaciones periódicas: para obtener y mantener la acreditación de la *Joint Commission*, los hospitales deben someterse a evaluaciones periódicas de cumplimiento de los estándares establecidos. Estas evaluaciones pueden incluir auditorías e inspecciones en el lugar, revisiones de documentos y entrevistas con el personal.

4. Enfoque en la mejora continua: la *Joint Commission* promueve un enfoque de mejora continua en la atención médica. Esto implica identificar áreas de mejora, implementar cambios para abordar deficiencias y monitorear continuamente el desempeño para garantizar que se cumplan los estándares de calidad y seguridad.

[64] Representa un compromiso con la calidad, la seguridad y la mejora continua en la atención médica. Para los hospitales, significa cumplir con estándares rigurosos y mantener un enfoque constante en la seguridad y el bienestar de los pacientes.

5. Énfasis en la seguridad del paciente: uno de los principales objetivos de la *Joint Commission* es mejorar la seguridad del paciente y prevenir eventos adversos. Los estándares de la *Joint Commission* incluyen medidas para reducir errores médicos, prevenir infecciones nosocomiales y mejorar la comunicación entre los profesionales de la salud.

6. Orientación hacia las mejores prácticas: la *Joint Commission* proporciona orientación y recursos para ayudar a los hospitales a cumplir con sus estándares. Esto puede incluir herramientas de evaluación, capacitación en línea y publicaciones que destacan las mejores prácticas en atención médica.

La *Joint Commission* establece estándares y requisitos específicos relacionados con la autoprotección y la preparación para emergencias en hospitales y centros de atención médica. Cumplir con estos estándares garantiza que los hospitales estén preparados para responder de manera efectiva a una amplia gama de situaciones de emergencia y proteger la seguridad y el bienestar de los pacientes, el personal y el público en general. En el sentido apuntado es de consideración que en relación al referido estándar de calidad y seguridad hospitalaria que, según Istúrtitz, J.J., (2018) es:

> (…) el estándar de calidad de mayor prestigio en el ámbito hospitalario como es la acreditación de la «Joint Commission International» dedica un amplio apartado a «la administración y seguridad de instalaciones», desde un punto de vista totalmente funcional teniendo en cuenta políticas e indicadores clave de la seguridad. (p. 51).

Destacamos algunos aspectos que se relacionan directamente con la seguridad y las emergencias por considerarlos de gran interés:

1. Planes de emergencia: los hospitales deben desarrollar, implementar y mantener planes de emergencia integrales que aborden una variedad de escenarios, incluidos desastres naturales, emergencias médicas, incendios, y situaciones de seguridad. Estos planes deben incluir procedimientos claros para la evacuación, la comunicación de emergencia, la atención a los pacientes y el manejo de recursos.

2. Capacitación y ejercicios: la *Joint Commission* requiere que los hospitales proporcionen capacitación regular a su personal en materia de seguridad y emergencias. Esto puede incluir la capacitación en la ejecución de planes de emergencia, el manejo de equipos de seguridad, la evacuación de pacientes y la comunicación durante crisis. Además, se

espera que los hospitales realicen ejercicios periódicos de simulacros de emergencias para evaluar la eficacia de sus planes y procedimientos y, si fuese preciso modificarlos para hacerlos más funcionales.

3. Evaluación de riesgos y vulnerabilidades: los hospitales deben realizar evaluaciones regulares de riesgos y vulnerabilidades para identificar posibles amenazas y debilidades en su capacidad de respuesta ante emergencias. Estas evaluaciones pueden ayudar a los hospitales a tomar medidas proactivas para mitigar riesgos y fortalecer su preparación para emergencias.

4. Gestión de recursos: la *Joint Commission* requiere que los hospitales dispongan de planes para gestionar recursos durante emergencias, incluidos suministros médicos, personal, equipo de protección personal y equipo de respuesta a emergencias. Esto garantiza que los hospitales estén preparados para responder de manera efectiva incluso en situaciones de crisis que puedan afectar a sus recursos habituales.

5. Comunicación de emergencia: es crucial que los hospitales establezcan sistemas de comunicación robustos y redundantes para garantizar la coordinación efectiva durante emergencias. Esto puede incluir la implementación de sistemas de comunicación por radio, sistemas de alerta temprana y protocolos para la comunicación interna y externa durante situaciones de crisis.

6. Revisión y mejora continua: la *Joint Commission* enfatiza la importancia de la revisión y la mejora continua, de los planes y procedimientos de emergencia. Los hospitales deben realizar análisis posteriores a la emergencia para identificar lecciones aprendidas y oportunidades de mejora, y actualizar sus planes en consecuencia para garantizar una preparación óptima para futuras emergencias.

En Europa, aunque no existe una organización equivalente a la *Joint Commission* que establezca estándares de acreditación para hospitales a nivel continental, hay varias iniciativas y normativas que abordan la autoprotección y la preparación para emergencias en el ámbito de la atención médica. Estas pueden variar según el país y la región. Algunas de las normativas y directrices relevantes en Europa incluyen:

1. Directiva 2008/114/CE de la Unión Europea sobre la identificación y designación de Infraestructuras Críticas europeas y la evaluación de la necesidad de mejorar su protección: esta directiva establece un marco para la identificación y protección de

Infraestructuras Críticas, que podrían incluir hospitales y centros de atención médica. Si bien su enfoque es más amplio que solo los hospitales, puede proporcionar pautas sobre la importancia de la preparación para emergencias en instalaciones de atención médica.

2. Directiva 2010/63/UE sobre el cuidado y el uso de animales utilizados con fines científicos: si bien esta directiva se centra en el cuidado y uso de animales en investigación científica, también establece requisitos para la protección de la salud y la seguridad del personal que trabaja con animales. Esto puede ser relevante para la autoprotección en instituciones médicas donde se realizan investigaciones que involucran animales.

3. Normas nacionales: muchos países europeos tienen sus propias normativas y regulaciones relacionadas con la seguridad y la preparación para emergencias en hospitales y centros de atención médica. Estas normas pueden variar según el país y pueden abordar aspectos como la gestión de riesgos, la seguridad del paciente, la planificación de emergencias y la respuesta a desastres.

4. Organizaciones de acreditación y certificación: en algunos países europeos, existen organizaciones nacionales o regionales encargadas de la acreditación y certificación de hospitales y centros de atención médica. Estas organizaciones pueden establecer estándares y requisitos específicos relacionados con la autoprotección y la preparación para emergencias como parte del proceso de acreditación.

En España, la gestión de emergencias en hospitales está regulada por una serie de documentos legales y reglamentarios. De entre los más destacados recogemos los siguientes:

1. Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud: esta ley establece el marco general para la organización y funcionamiento del Sistema Nacional de Salud en España. Si bien no aborda específicamente la gestión de emergencias en hospitales, sienta las bases para la prestación de servicios de salud de calidad y la protección de la salud pública.

2. Real Decreto 2393/2004, de 30 de diciembre, por el que se aprueba el Reglamento de la estructura, organización y funcionamiento de los hospitales: este reglamento establece las disposiciones generales para la organización y funcionamiento de los hospitales en España. Si bien no especifica directamente los procedimientos para la

gestión de emergencias, establece los requisitos generales para la prestación de servicios de salud y la seguridad del paciente en hospitales.

3. Plan Nacional de Protección Civil ante el Riesgo Sísmico: este plan, elaborado por la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, establece las medidas y procedimientos para la prevención, preparación y respuesta ante eventos sísmicos en España. Si bien su enfoque principal es la Protección Civil en general, incluye disposiciones relevantes para la gestión de emergencias en hospitales.

4. Normativa autonómica: además de la legislación estatal, cada comunidad autónoma en España puede tener su propia normativa y regulaciones específicas en materia de gestión de emergencias en hospitales, así como las específicas frente a todo tipo de riesgos en atención a sus competencias delegadas. Estas normativas pueden abordar aspectos como la planificación de emergencias, la activación de planes de emergencia y la coordinación con otras agencias y organizaciones.

5. Planes de emergencia hospitalaria[65]: los hospitales en España están obligados a desarrollar y mantener planes de emergencia hospitalaria que describan los procedimientos para responder a una amplia gama de situaciones de emergencia. Estos planes deben estar en consonancia con la normativa estatal y autonómica y pueden incluir disposiciones para la activación de un plan de emergencia extracentro en caso de que se vea afectada la capacidad de atención médica del hospital.

Es importante que los hospitales en España estén familiarizados con la legislación y regulaciones aplicables en su comunidad autónoma y que mantengan sus planes de emergencia actualizados para garantizar una respuesta efectiva ante situaciones de crisis. La formación y la realización de ejercicios de simulacro son elementos clave para asegurar la preparación y la capacidad de respuesta del personal del hospital en caso de emergencia.

Las Infraestructuras Críticas hospitalarias implementan una serie de medidas de seguridad para proteger a pacientes, personal médico y activos importantes. De entre las más relevantes destacamos:

1. Control de acceso físico: se establecen puntos de entrada controlados y se implementan sistemas de control de acceso para regular quién puede ingresar a

[65] En relación a la gestión de las Emergencias Intracentro, viene dado por los distintos Planes de Autoprotección que establece la Norma Básica de Autoprotección. Se recoge en la actualidad por el Capítulo 6 del referenciado Plan que, establece las distintas medidas a adoptar en Emergencias.

diferentes áreas del hospital. Esto ayuda a prevenir intrusiones no autorizadas y protege áreas sensibles como salas de operaciones, salas de cuidados intensivos y farmacias.

2. Identificación y autenticación de personal: se han de utilizar tarjetas de identificación con tecnología de proximidad o sistemas biométricos (como huellas dactilares o reconocimiento facial) para verificar la identidad del personal sanitario y limitar el acceso a áreas restringidas solo a aquellos autorizados.

3. Vigilancia por video: se deben de instalar cámaras de seguridad en áreas clave del hospital, como entradas, pasillos, salas de espera y estacionamientos, para monitorear y registrar actividades. Esto ayuda a disuadir el comportamiento delictivo, proporciona evidencia en caso de incidentes y contribuye a la seguridad general del entorno hospitalario.

4. Protección de datos y sistemas informáticos: se implementan medidas de seguridad cibernética para proteger la información confidencial de los pacientes y garantizar la integridad y disponibilidad de los sistemas informáticos hospitalarios. Esto puede incluir *firewalls*, sistemas de detección de intrusiones, cifrado de datos y políticas de acceso seguro.

5. Gestión de emergencias y planificación de respuesta: se desarrollan y practican planes de respuesta a emergencias para abordar una variedad de situaciones, como desastres naturales, incidentes de seguridad, brotes de enfermedades infecciosas y ataques terroristas.

   Esto incluye la capacitación del personal en procedimientos de evacuación, triaje de pacientes y coordinación con servicios de emergencia externos. En el sentido apuntado hay que considerar los aspectos que de importancia tiene la formación en el aspecto que se apunta, «La formación es fundamental, porque dota de las herramientas necesarias para trazar los planes que nos ayudan a conseguir los objetivos». Ponce, T., (2016, p80).

   En la misma línea la planificación en materia de autoprotección es importante saber que «de nada sirve tener un plan de autoprotección si quienes deben ponerlo en práctica no lo conocen». Ponce, T., (2016, p80).

6. Control de infecciones y bioseguridad: se establecen protocolos rigurosos de control de infecciones para prevenir la propagación de enfermedades dentro del hospital. Esto puede incluir prácticas de higiene estrictas, uso de equipo de protección personal (EPP), desinfección regular de superficies y aire, y segregación de pacientes con enfermedades contagiosas.

7. Protección física de activos críticos: se implementan medidas de seguridad física para proteger equipos médicos costosos, suministros farmacéuticos y otros activos críticos contra robos, vandalismo y daños accidentales. Esto puede incluir sistemas de seguridad para equipos, almacenamiento seguro de medicamentos y protocolos de control de inventario.

8. Educación y concienciación del personal: se brinda capacitación regular al personal hospitalario sobre seguridad, privacidad de datos, manejo de emergencias y procedimientos de respuesta. Esto ayuda a aumentar la conciencia sobre los riesgos de seguridad y promueve una cultura de seguridad en todo el hospital.

3.13. INTELIGENCIA ARTIFICIAL Y SEGURIDAD HOSPITALARIA:

Podría decirse y así está aceptado por todos que estamos inmersos en la llamada IV Revolución Industrial, todo ello debido a que estamos en una nueva era digital del alza de la utilización de las distintas tecnologías, al respecto y en palabras de Oliver, N., (2018):

> Finalmente, la Cuarta Revolución Industrial[66] se apoya en avances de la Revolución Digital, pero incorpora la ubiquidad de la tecnología digital tanto en nuestra sociedad como en nuestro cuerpo y la unión creciente entre el mundo físico y el mundo digital. Los avances tecnológicos que hacen que esta nueva revolución sea posible incluyen a la robótica, la Inteligencia Artificial, el Big Data, la nanotecnología, la biotecnología, el internet de las cosas, los vehículos autónomos, las impresoras en tres dimensiones y la computación cuántica. (p. 37).

La inteligencia artificial (IA) se refiere a la capacidad de las máquinas o programas de computadora para imitar el comportamiento humano inteligente. Esto incluye la capacidad de aprender, razonar, resolver problemas, percibir y entender el lenguaje natural. La IA se basa en

[66] El concepto fue presentado internacionalmente en el Foro Económico Mundial en el año 2016 por ideador, Klaus Schwab. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-itmeans-and-how-to-respond/

algoritmos y modelos matemáticos complejos que permiten a las máquinas realizar tareas que normalmente requerirían la intervención humana.

En relación al uso tan generalizado que la Inteligencia Artificial se hace en la actualidad por todos, es destacable en palabras de Oliver, N., (2018) que:

> (…) la presencia de la IA en nuestras vidas y su capacidad para tener impacto positivo en la sociedad son innegables. Por ello, las grandes potencias mundiales —tanto empresas como gobiernos— han comprendido que el liderazgo en la Inteligencia Artificial conllevará un liderazgo no solo a nivel económico sino también político y social, dado su papel central en la Cuarta Revolución Industrial. (p. 40).

El término de inteligencia artificial fue acuñado por John McCarthy en 1956 durante una conferencia en Dartmouth College. McCarthy, junto con otros pioneros como Marvin Minsky, Allen Newell y Herbert Simon, es considerado uno de los padres de la inteligencia artificial.

Sin embargo, la idea de máquinas que puedan realizar tareas cognitivas data de mucho antes. Por ejemplo, el matemático y lógico británico Alan Turing formuló la famosa Prueba de Turing, en el año 1950, que propuso evaluar la inteligencia de una máquina al someterla a una conversación y determinar si sus respuestas eran indistinguibles de las de un humano. En el sentido referenciado y en palabras de Lamb, L., (2020), citado por la *NATO*, (2023).

> *We have to improve scientific understanding amongst AI paradigms so as to build AI that benefits humanity and the planet. The world will need a principled AI education for all, since AI will be the key technology of the next decades, if not the XXI century.* [Tenemos que mejorar la comprensión científica entre los paradigmas de la inteligencia artificial para construir IA que beneficie a la humanidad y al planeta. El mundo necesitará una educación en IA basada en principios para todos, ya que la IA será la tecnología clave de las próximas décadas, si no del siglo XXI.] (p. 26).

En el mismo sentido, la Comisión Europea (2019), expone:

> *AI refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely softwarebased, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems). Alternatively, AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).* [La Inteligencia

> Artificial se refiere a sistemas que muestran un comportamiento inteligente al analizar su entorno y tomar acciones, con cierto grado de autonomía, para lograr objetivos específicos. Los sistemas basados en IA pueden ser puramente *software*, actuando en el mundo virtual (por ejemplo, asistentes de voz, software de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento de voz y rostro). Alternativamente, la IA puede estar incorporada e dispositivos de *hardware* (como robots avanzados, vehículos autónomos, drones o aplicaciones del Internet de la cosas)]. (p. 26).

Características relevantes de la inteligencia artificial incluyen:

> Aprendizaje automático: los sistemas de IA pueden aprender de los datos y mejorar su rendimiento a medida que se exponen a más información. En el sentido expuesto, cabe destacar «la importancia de la gestión de los datos porque la IA, se nutre precisamente de datos». (Martínez, R., 2018).
>
> Realmente no somos conscientes de la vulnerabilidad que generamos en las distintas Redes Sociales (RRSS) en relación a la cantidad de datos ingentes de carácter general que facilitamos, al exponernos de una manera irreflexiva e inconsciente. De suma importancia lo referido por Martínez, R., (2018) que expone que:
>
> > El análisis, la vigilancia y la acumulación masiva y pormenorizada de datos a través de sistemas inteligentes están conduciendo a cambios en la gobernanza y daños en el núcleo de la sociedad civil. (…) Monopolios globales como Facebook o Google, que poseen y manejan la información más privada de dos mil millones de ciudadanos. Vivimos y no nos damos cuenta en un Estado policial artificialmente inteligente. (pp. 18-19).

1. Razonamiento y resolución de problemas: la IA puede utilizar algoritmos para analizar situaciones, tomar decisiones y resolver problemas de manera similar a como lo haría un ser humano.

2. Procesamiento del lenguaje natural: la capacidad de comprender y generar lenguaje humano es fundamental para muchas aplicaciones de IA, como asistentes virtuales, traducción automática y análisis de sentimientos en redes sociales.

3. Visión por computadora: la IA puede analizar imágenes y videos para reconocer patrones, objetos y rostros, lo que es útil en aplicaciones como la seguridad, la medicina y la conducción autónoma.

4. Robótica: la IA se utiliza en el diseño y control de robots para realizar tareas físicas y cognitivas en entornos diversos, desde la fabricación hasta la exploración espacial.

La Inteligencia Artificial presenta características de transversalidad, así como de invisibilidad, esto supone en palabras de Oliver, N., (2018) que:

> Las técnicas de Inteligencia Artificial pueden utilizarse en un sinfín de aplicaciones en áreas como la biología, la física, la medicina, la química, la energía, el transporte, la educación, los sistemas de producción, la logística y el transporte, los servicios digitales y la prestación de servicios públicos y privados. Además, la gran mayoría de sistemas de Inteligencia Artificial que se utilizan hoy en día son invisibles, es decir, consisten en software en el corazón de los sistemas y servicios inteligentes cotidianos. Estas dos propiedades —transversalidad e invisibilidad— posicionan a la Inteligencia Artificial en el corazón de la Cuarta Revolución Industrial, con un papel similar al que jugó la electricidad en la Segunda Revolución Industrial. (p. 38).

En cualquier caso, la Inteligencia artificial ha de actualizarse permanentemente con el objeto de que su uso no pierda eficacia y pueda ser funcional a cualquier ámbito que la demande, según Oliver, N., (2018):

> Los sistemas actuales de Inteligencia Artificial basados en modelos de aprendizaje profundo son complejos, con cientos de capas de neuronas y millones de parámetros. Esta complejidad dificulta la capacidad para interpretar los modelos que en ciertos casos de uso —por ejemplo, en la medicina o en la educación— es condición necesaria para poder aplicar un sistema de IA. Al mismo tiempo, esta complejidad permite que los sistemas de Inteligencia Artificial puedan procesar cantidades ingentes de datos —que de otra manera sería inviable— y realizar tareas con niveles de competencia superiores a los de los humanos. Es decir, dotan a los sistemas de IA de gran escalabilidad. En muchos de los casos de uso del Big Data, sólo podemos extraer conocimiento y valor de tales cantidades de datos a través del uso de sistemas de Inteligencia Artificial, ya que los métodos tradicionales no escalan a volúmenes de datos tan grandes que, además, son variados, no estructurados y generados a gran velocidad. Asimismo, los sistemas de Inteligencia Artificial son altamente escalables al consistir fundamentalmente en software, que, además, puede estar conectado con miles o millones de otros sistemas de IA, dando lugar a una red colectiva de inteligencia artificial. (p. 39).

También es destacable la capacidad de la Inteligencia Artificial en relación a sus distintos algoritmos para predecir, en ese sentido también destaca lo apuntado por Oliver, N., (2018) que apunta que:

> Los sistemas de Inteligencia Artificial pueden utilizarse para la toma de decisiones automáticas y para predecir situaciones futuras. De hecho, la aspiración es que las decisiones algorítmicas basadas en IA entrenada con datos carezcan de las limitaciones de las decisiones humanas (por ejemplo, conflictos de interés, sesgos, intereses propios, corrupción…) y por tanto sean más justas y objetivas. (p. 39).

Por todo lo expuesto por los distintos autores de relevancia en la materia, la Inteligencia Artificial a aumentar los niveles de seguridad en las Infraestructuras Críticas y en especial a las Infraestructuras Críticas hospitalarias en el entorno de la unión europea contra las distintas amenazas y especialmente contra el terrorismo de corte *yihadista*, debido principalmente a que pueden contribuir a:

1. Detección de amenazas: los sistemas de IA pueden analizar grandes volúmenes de datos, incluidas imágenes de videovigilancia, transmisiones de redes sociales, datos de sensores y registros de entrada de personas, para identificar patrones y comportamientos sospechosos. Esto puede ayudar a detectar posibles amenazas y actividades terroristas en las proximidades de las Infraestructuras Críticas, como los hospitales.

2. Análisis de inteligencia: los algoritmos de IA pueden procesar y analizar información de diversas fuentes para generar inteligencia accionable sobre posibles amenazas terroristas. Esto incluye el análisis de comunicaciones en línea, sitios web extremistas, informes de inteligencia y datos de fuentes abiertas para identificar actividades *yihadistas* y planificación de ataques.

3. Vigilancia avanzada: la IA puede mejorar la capacidad de vigilancia de las Infraestructuras Críticas, como los hospitales, mediante la implementación de sistemas de vigilancia avanzados basados en análisis de video y reconocimiento facial. Estos sistemas pueden alertar sobre comportamientos sospechosos o intrusos no autorizados y mejorar la seguridad del perímetro y el acceso restringido.

4. Protección cibernética: la IA puede desempeñar un papel crucial en la protección de las Infraestructuras Críticas hospitalarias contra ataques cibernéticos, que representan

una amenaza cada vez mayor. Los sistemas de IA pueden monitorear y analizar continuamente el tráfico de red en busca de actividades maliciosas, detectar anomalías y vulnerabilidades en los sistemas informáticos y prevenir o mitigar ataques cibernéticos antes de que causen daños.

5. Respuesta rápida y coordinación: los sistemas de IA pueden facilitar una respuesta rápida y coordinada a incidentes de seguridad en las Infraestructuras Críticas al proporcionar análisis de datos en tiempo real, coordinación de recursos y recomendaciones para la toma de decisiones. Esto puede ayudar a minimizar el impacto de los ataques terroristas y garantizar una recuperación eficiente de las operaciones.

La inteligencia artificial puede ser una herramienta poderosa para fortalecer la seguridad de las Infraestructuras Críticas, incluidos los hospitales, en el entorno de la Unión Europea, ayudando a prevenir y mitigar amenazas como el terrorismo de corte *yihadista*. Sin embargo, es importante tener en cuenta los desafíos éticos, legales y de privacidad asociados con el uso de la IA en el ámbito de la seguridad y garantizar que se implementen medidas adecuadas para proteger los derechos individuales y la integridad de los datos.

En el sentido apuntado ha de considerarse a los conocidos como Sistemas Expertos, con el objeto de la adecuada toma de decisiones ante fenómenos meteorológicos adversos, estos sistemas arrojan una validez importante en el uso de las metodologías de Lógica Difusa que se han aplicado en investigaciones previas en el ámbito de los Riesgos de Carácter Natural. En palabras de Santacreu, L., (2015), la Lógica Difusa la define como:

> (…) una metodología del área de la Inteligencia Artificial que es eficaz cuando se trabaja con imprecisión o ambigüedad, datos erróneos o ausencia de éstos, algo a lo que los servicios de emergencia están acostumbrados. "Llueve mucho" y "hace mucho viento" son respuestas típicas dadas por los alertantes a los Centros 1-1-2. (p.67).

Cuestión que hace extrapolable a la Inteligencia Artificial (IA) frente a cualquier tipo de Riesgo Antrópico, indistintamente del carácter del riesgo. Para ello, en atención a la Lógica Difusa, habrá de utilizarse, en palabras de Santacreu, L., (2015):

> (…) la inferencia entre conjuntos difusos con un sistema de reglas. Un conjunto difuso A en un dominio D viene caracterizado por una función de pertenencia que asocia a

cada elemento del dominio, un valor en el intervalo (0 1), lo que determina su grado de pertenencia al conjunto. (p. 67).

3.13.1. Principales riesgos de la inteligencia artificial:

Si bien la inteligencia artificial (IA) ofrece numerosos beneficios para mejorar la seguridad y la eficiencia de las Infraestructuras Críticas, incluidos los hospitales, también plantea ciertos riesgos y desafíos que deben abordarse adecuadamente. Algunos de los principales riesgos asociados con el uso de IA en Infraestructuras Críticas, especialmente en entornos hospitalarios, por tanto, los riesgos más importantes que la IA puede presentar para las Infraestructuras Críticas en general y las infraestructuras hospitalarias en particular son:

1. Vulnerabilidades de seguridad: los sistemas de IA pueden ser susceptibles a vulnerabilidades de seguridad, como ataques cibernéticos, intrusiones y manipulación de datos. Si los sistemas de IA no están adecuadamente protegidos, podrían ser comprometidos y utilizados para acceder a información confidencial, interrumpir operaciones críticas o causar daños.

2. Sesgos algorítmicos: los algoritmos de IA pueden estar sujetos a sesgos inherentes basados en los conjuntos de datos utilizados para su entrenamiento. Si estos conjuntos de datos contienen sesgos o representan de manera inadecuada ciertos grupos de población, los sistemas de IA pueden tomar decisiones discriminatorias o injustas, especialmente en entornos críticos como la atención médica.

3. Falta de transparencia y explicabilidad: algunos sistemas de IA, como las redes neuronales profundas, pueden ser difíciles de entender y explicar cómo llegan a sus decisiones. Esta falta de transparencia puede ser problemática en contextos críticos donde es importante comprender el razonamiento detrás de las decisiones tomadas por los sistemas de IA, como en el diagnóstico médico o la gestión de emergencias.

4. Dependencia excesiva: una dependencia excesiva de los sistemas de IA sin redundancias adecuadas o planes de contingencia puede hacer que las Infraestructuras Críticas sean más vulnerables a interrupciones y fallos. Es importante mantener una combinación equilibrada de tecnología y recursos humanos capacitados para garantizar la resiliencia y la continuidad operativa.

5. Privacidad y ética: el uso de IA en entornos hospitalarios plantea preocupaciones sobre la privacidad de los datos de los pacientes y la ética de la recopilación, el

almacenamiento y el análisis de información médica sensible. Es fundamental garantizar que se implementen medidas adecuadas de privacidad y seguridad de datos para proteger la confidencialidad y la integridad de la información del paciente.

6. Escalabilidad y mantenimiento: la implementación exitosa de sistemas de IA en Infraestructuras Críticas requiere recursos significativos en términos de infraestructura, personal capacitado y mantenimiento continuo. La falta de recursos adecuados puede obstaculizar la escalabilidad y la efectividad a largo plazo de los sistemas de IA, lo que podría aumentar la vulnerabilidad de las Infraestructuras Críticas.

7. También la Inteligencia Artificial puede provocar un impacto negativo en la sociedad, en lo que al mercado laboral se refiere, en tal sentido, Oliver, N., (2018) apunta que:

> En particular, todo lo que pueda automatizarse o sustituirse con el uso de tecnología, será automatizado total o parcialmente. En consecuencia, la demanda laboral está experimentando un sesgo en beneficio de habilidades profesionales especializadas, y en perjuicio de habilidades u ocupaciones rutinarias y mecánicas. Esta tendencia pronostica un cambio completo en la estructura ocupacional que probablemente conlleve riesgos para la sociedad si no somos capaces de adaptarnos a dicho cambio. (p. 43).

Como puede desprenderse, la inteligencia artificial ofrece numerosos beneficios para mejorar la seguridad y la eficiencia de las Infraestructuras Críticas, es importante abordar los riesgos y desafíos asociados de manera proactiva para garantizar su implementación segura y efectiva, especialmente en entornos hospitalarios donde la vida y la salud de las personas están en juego.

En ese sentido, el Consejo de la Unión Europea, consciente de los riesgos de la utilización de la Inteligencia Artificial ha propiciado un borrador de una Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.

Desde la anterior orientación y, a tenor del documento 8115/21, del consejo, en el apartado de su introducción, 2021/0106 (COD), recoge en su tenor literal que:

> La Comisión adoptó la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) el 21 de abril de 2021 La propuesta de la Comisión tiene por objeto garantizar que los sistemas de inteligencia artificial (IA) comercializados en el mercado de la Unión y utilizados en ella sean seguros y respeten la legislación vigente relativa a los derechos fundamentales y los valores de la Unión, garantizar la seguridad jurídica para facilitar la inversión y la innovación en IA y mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y seguridad, así como facilitar el desarrollo de un mercado único de aplicaciones de inteligencia artificial que sean legales, seguras y fiables y evitar la fragmentación del mercado. (Art. 1.1).

Tal propuesta de borrador recoge los siguientes apartados de interés:

- ✓ Definición de un sistema de IA, prácticas de IA prohibidas, lista de supuestos de utilización de sistemas de IA de alto riesgo en el anexo III y clasificación de sistemas de IA como de alto riesgo. (Art. 4.1).
- ✓ Requisitos de los sistemas de IA de alto riesgo y responsabilidades de diversos agentes de la cadena de valor de la IA. (Art. 4.2).

(pp. 1-6).

3.14. *BIG DATA* Y SEGURIDAD HOSPITALARIA:

El término *Big Data* se refiere a conjuntos de datos extremadamente grandes y complejos que superan la capacidad de los sistemas tradicionales de procesamiento de datos para gestionarlos y analizarlos de manera efectiva. Estos conjuntos de datos suelen tener tres características principales, conocidas como las "3V": Volumen (gran cantidad de datos), Velocidad (alta tasa de generación o cambio de datos) y Variedad (diversidad de tipos y fuentes de datos).

Por tanto, hace referencia al procesamiento y análisis de grandes volúmenes de datos, tanto estructurados como no estructurados, que no pueden ser gestionados con herramientas de procesamiento de datos tradicionales. Esta disciplina implica extraer información valiosa, patrones y tendencias significativas de conjuntos de datos extremadamente grandes y complejos.

En relación a los distintos retos o desafíos que presenta el *Big Data*, y según la *NATO*, (2023), expone literalmente en su epígrafe *Big Data, Information and Communication Technologies*:

> *Data describes Big Data (raw digital data) that presents significant volume, velocity, variety, veracity and visualisation challenges. Increased digitalisation, a proliferation of new sensors, new communication modes, the internet-of-things and the virtualisation of socio-cognitive spaces (e.g. social media) have contributed significantly to the development of Big Data. Advanced (Data) Analytics describes advanced analytical methods for making sense of and visualising large volumes of such information. These techniques span various approaches drawn from research areas across the data and decision sciences, including artificial intelligence, optimisation, modelling & simulation (M&S), human factors engineering and operational research. Two additional aspects are essential in considering the big data challenge: Information and Communication Technologies, and sensors and sensing. This systemof-systems is necessary for an effective multi-domain C4ISR*[67] *framework, reflecting the collection, processing, exploitation and dissemination of information supporting decision-making and C2*[68]. [Los datos describen el *Big Data* (datos digitales sin procesar) que presenta desafíos significativos en términos de volumen, velocidad, variedad, veracidad y visualización. La creciente digitalización, la proliferación de nuevos sensores, los nuevos modos de comunicación, el Internet de las cosas y la virtualización de espacios socio-cognitivos (por ejemplo, las redes sociales) han contribuido significativamente al desarrollo del *Big Data*. La Analítica Avanzada describe métodos analíticos avanzados para dar sentido y visualizar grandes volúmenes de esta información. Estas técnicas abarcan varios enfoques extraídos de áreas de investigación en las ciencias de datos y de decisiones, incluyendo inteligencia artificial, optimización, modelado y simulación (M&S), ingeniería de factores humanos e investigación operativa. Dos aspectos adicionales son esenciales al considerar el desafío del *big data*: las Tecnologías de la Información y la Comunicación, y los sensores y la detección. Este sistema de sistemas es necesario para un marco C4ISR multi-dominio efectivo, que refleje la recolección, procesamiento, explotación y diseminación de información que respalda la toma de decisiones y el C2]. (P.16).

En relación con las Infraestructuras Críticas y su seguridad en general, el *Big Data* puede desempeñar un papel fundamental en la mejora de la seguridad, la eficiencia y la resiliencia.

[67] El comando que utiliza la NATO para hacer referencia al control, inteligencia, vigilancia y reconocimiento

[68] Es lo que la NATO define como comando de "Mando y Control" en cualquier estructura de mando en relación a un organigrama y responsabilidad.

Algunas formas en que el *Big Data* se relaciona con las Infraestructuras Críticas incluyen:

1. Análisis de riesgos y amenazas: el análisis de grandes conjuntos de datos puede ayudar a identificar patrones y tendencias que indiquen posibles riesgos y amenazas para las Infraestructuras Críticas, permitiendo una mejor preparación y mitigación de riesgos.

2. Monitorización y mantenimiento predictivo: el uso de datos en tiempo real y análisis predictivos puede ayudar a prevenir fallas y mejorar la eficiencia operativa al anticipar y abordar problemas de mantenimiento antes de que ocurran.

3. Gestión de la demanda y planificación de recursos: el análisis de grandes volúmenes de datos puede proporcionar información valiosa sobre la demanda de servicios y recursos, permitiendo una planificación más efectiva y una asignación eficiente de recursos para satisfacer las necesidades cambiantes.

4. Optimización de la logística y la cadena de suministro: el *Big Data* puede mejorar la eficiencia de la logística y la cadena de suministro al permitir un seguimiento en tiempo real de los activos, la optimización de rutas y la gestión de inventarios.

En el caso específico de las Infraestructuras Críticas hospitalarias y su seguridad, el *Big Data* también puede desempeñar un papel clave en la mejora de la atención médica y la seguridad de los pacientes. Algunas aplicaciones del *Big Data* en Infraestructuras Críticas hospitalarias incluyen:

1. Diagnóstico y tratamiento personalizado: el análisis de grandes conjuntos de datos de pacientes puede ayudar a identificar patrones y correlaciones entre síntomas, tratamientos y resultados, lo que permite un diagnóstico y tratamiento más precisos y personalizados.

2. Monitorización de pacientes y atención remota: el uso de dispositivos médicos conectados y datos de monitorización en tiempo real puede permitir una atención más efectiva y personalizada para los pacientes, especialmente aquellos con condiciones crónicas o que requieren cuidados intensivos.

3. Gestión de recursos y planificación de servicios: el análisis de datos puede ayudar a los hospitales a optimizar la gestión de camas, recursos humanos y suministros médicos para garantizar una atención eficiente y oportuna a los pacientes.

4. Investigación médica y desarrollo de medicamentos: el *Big Data* puede facilitar la investigación médica al permitir el análisis de grandes conjuntos de datos genómicos, clínicos y epidemiológicos para identificar nuevas terapias, medicamentos y tratamientos para enfermedades.

Por lo tanto, hemos de considerar que, el *Big Data* es una herramienta importante que puede beneficiar a las Infraestructuras Críticas en general, y a las Infraestructuras Críticas hospitalarias en particular, al permitir un análisis más profundo y significativo de los datos para mejorar la seguridad, la eficiencia y la calidad de los servicios prestados.

3.14.1 Principales riesgos del *Big Data*:

Si bien el *Big Data* ofrece numerosos beneficios para las Infraestructuras Críticas hospitalarias, también conlleva ciertos riesgos y amenazas que deben abordarse adecuadamente para garantizar la seguridad, la privacidad y la integridad de los datos y la atención médica. Algunos de los principales riesgos y amenazas del *Big Data* en las Infraestructuras Críticas hospitalarias son:

1. Privacidad y seguridad de los datos: el *Big Data* implica el manejo de grandes volúmenes de datos sensibles y personales de pacientes, que pueden incluir información médica confidencial, historias clínicas, datos genéticos y de salud mental. La violación de la privacidad de estos datos o su compromiso por parte de terceros puede tener consecuencias graves para la seguridad y la confianza del paciente.

2. Vulnerabilidades de seguridad cibernética: las Infraestructuras Críticas hospitalarias son cada vez más objetivos de ataques cibernéticos debido a la cantidad de datos valiosos que manejan y a la creciente interconexión de sistemas y dispositivos médicos. Los ataques cibernéticos pueden comprometer la integridad y la disponibilidad de los datos, interrumpir las operaciones y poner en riesgo la seguridad de los pacientes.

3. Sesgos y discriminación algorítmica: el uso de algoritmos de *Big Data* en la toma de decisiones médicas puede estar sujeto a sesgos inherentes en los datos utilizados para entrenar los modelos, lo que podría llevar a decisiones discriminatorias o injustas en el diagnóstico, tratamiento y asignación de recursos.

4. Falta de transparencia y explicabilidad: los algoritmos de *Big Data*, especialmente los modelos de aprendizaje automático y, la inteligencia artificial, pueden ser difíciles de

entender y explicar cómo llegan a sus decisiones. Esto puede dificultar la supervisión y la rendición de cuentas sobre las decisiones médicas tomadas con el apoyo de sistemas de *Big Data*.

5. Cumplimiento normativo y legal: las Infraestructuras Críticas hospitalarias están sujetas a estrictas regulaciones y normativas en materia de privacidad, seguridad de datos y cumplimiento médico. El uso inadecuado o no autorizado de datos de pacientes en iniciativas de *Big Data* puede resultar en multas significativas y sanciones legales.

6. Pérdida de confianza del paciente: la falta de seguridad, privacidad y transparencia en el manejo de datos de pacientes puede erosionar la confianza del paciente en las Infraestructuras Críticas hospitalarias y en el sistema de atención médica en general, lo que puede tener consecuencias negativas para la salud y el bienestar de los pacientes.

El *Big Data*, por tanto, ofrece variadas e importantes oportunidades para mejorar la atención médica y la eficiencia operativa en las Infraestructuras Críticas hospitalarias, es crucial abordar adecuadamente los riesgos y amenazas asociados para garantizar la seguridad, la privacidad y la confianza del paciente en el uso de datos médicos sensibles.

3.15. ANÁLISIS RELACIONAL ENTRE LA IA Y EL *BIG DATA*:

La inteligencia artificial (IA) y el *Big Data* están estrechamente relacionados y se complementan entre sí en numerosos aspectos. Mostramos a continuación, algunas formas relacionales en los que la inteligencia artificial y el *Big Data,* están interconectados:

1. Procesamiento de datos: el *Big Data* proporciona grandes volúmenes de datos que pueden ser utilizados como entrada para los algoritmos de inteligencia artificial. La IA puede analizar y procesar estos datos de manera eficiente para extraer información valiosa, identificar patrones, realizar predicciones y tomar decisiones informadas.

2. Aprendizaje automático: el aprendizaje automático es una subdisciplina de la inteligencia artificial que se basa en la capacidad de las máquinas para aprender de los datos. El *Big Data* proporciona conjuntos de datos masivos que son fundamentales para entrenar y mejorar los modelos de aprendizaje automático, permitiendo que los sistemas de IA reconozcan patrones complejos y tomen decisiones más precisas.

3. Personalización y recomendaciones: la inteligencia artificial puede utilizar el análisis de *Big Data* para personalizar experiencias y ofrecer recomendaciones precisas a los usuarios. Por ejemplo, los motores de recomendación de plataformas de *streaming* de video utilizan algoritmos de IA que se basan en grandes cantidades de datos de visualización para sugerir contenido relevante a los usuarios.

4. Predicción y optimización: la inteligencia artificial puede utilizar técnicas de modelado avanzado para predecir tendencias futuras y optimizar procesos en función de datos históricos y en tiempo real. Esto puede ser especialmente útil en la planificación de la atención médica en hospitales, donde se pueden utilizar datos de pacientes para prever la demanda de servicios y asignar recursos de manera más eficiente.

5. Análisis de sentimientos y procesamiento del lenguaje natural: la inteligencia artificial puede analizar grandes cantidades de datos de texto, como comentarios en redes sociales, revisiones de productos o registros médicos, para comprender el sentimiento, extraer información relevante y generar *insights*[69] significativos. Esto puede ser útil para comprender la opinión pública, detectar tendencias emergentes o identificar problemas de salud pública.

En atención a lo expuesto, la inteligencia artificial y el *Big Data* están estrechamente entrelazados, ya que el análisis de grandes volúmenes de datos es fundamental para alimentar y mejorar los modelos de inteligencia artificial. Juntos, la IA y el *Big Data* tienen el potencial de transformar numerosos aspectos de la sociedad, desde la atención médica y el comercio electrónico hasta la seguridad y la gestión de recursos.

En el sentido expuesto, cabe destacar las conclusiones de la OTAN, al respecto de la Inteligencia Artificial y el Big Data, en definitiva cualquier tipo de tecnologías emergentes y disruptivas, del inglés *emerging and disruptive technologies (EDT),* en ese sentido, *NATO*, (2023), recoge que:

> *(…) Such characteristics of modern technologies are drivers of the current evolution and revolution in data, AI, autonomy, space, quantum, hypersonics, biotechnologies, materials, energy and electronics. Alone or in combination, they define the*

[69] Término que se utiliza comúnmente para referirse a percepciones, entendimientos o conocimientos profundos que se obtienen a partir de la observación, análisis o experiencia. Son percepciones profundas que proporcionan una comprensión significativa y valiosa sobre un tema específico, lo que puede conducir a acciones o decisiones informadas.

technological edge necessary for NATO's operational and organisational effectiveness. How quickly, in what order, and ultimately how successful these technologies will be, or what threats they will present, is yet to be determined. However, long-term forecasts of military technologies provide a useful exercise while offering a guide to prioritising capability and technology investments. The techno-policy, legal and ethical challenges that they present to NATO cannot be overstated. Understanding why they present a problem or opportunity, how they are expected to 103 manifest, and what this will mean to the Alliance is an excellent first step and will ensure NATO remains technologically prepared and operationally relevant. [Tales características de las tecnologías modernas son impulsores de la evolución y revolución actuales en datos, IA, autonomía, espacio, cuántica, hipersónica, biotecnologías, materiales, energía y electrónica. Solas o en combinación, definen la ventaja tecnológica necesaria para la efectividad operativa y organizativa de la OTAN. Qué tan rápido, en qué orden y, en última instancia, qué tan exitosas serán estas tecnologías, o qué amenazas presentarán, aún está por determinarse. Sin embargo, las previsiones a largo plazo de las tecnologías militares son un ejercicio útil al ofrecer una guía para priorizar las inversiones en capacidades y tecnología. Los desafíos tecnopolíticos, legales y éticos que presentan a la OTAN no pueden ser exagerados. Comprender por qué representan un problema, u oportunidad, cómo se espera que se manifiesten y qué significará esto para la Alianza es un excelente primer paso y asegurará que la OTAN permanezca tecnológicamente preparada y operativamente relevante]. (p. 103).

3.15.1. Relación directa de la IA y el Big Data en la seguridad de las Infraestructuras Críticas hospitalarias.

La relación entre la inteligencia artificial (IA) y el *Big Data*, es fundamental para fortalecer la seguridad, la protección integral y la resiliencia de las Infraestructuras Críticas hospitalarias. La relación directa se produce en atención a las siguientes características:

1. Detección y prevención de amenazas: la IA puede analizar grandes volúmenes de datos generados por sistemas de seguridad, monitorización y registros médicos para detectar patrones anómalos que podrían indicar amenazas potenciales, como intrusiones físicas, ciberataques o eventos médicos inusuales. Esta capacidad de análisis avanzado puede ayudar a prevenir y mitigar amenazas antes de que causen daños significativos.

2. Análisis de seguridad cibernética**:** el *Big Data* proporciona la cantidad masiva de datos necesaria para identificar y analizar ciberamenazas en tiempo real. La IA puede utilizar estos datos para desarrollar modelos de detección de intrusiones y anomalías más sofisticados, mejorar la respuesta a incidentes y fortalecer las defensas cibernéticas de las Infraestructuras Críticas hospitalarias contra ataques informáticos maliciosos.

3. Optimización de la gestión de riesgos: la combinación de IA y *Big data* puede permitir una evaluación más completa y precisa de los riesgos potenciales para las Infraestructuras Críticas hospitalarias. Mediante el análisis de datos históricos y en tiempo real, la IA puede identificar áreas de vulnerabilidad, anticipar posibles escenarios de riesgo y recomendar acciones preventivas para mitigar los impactos negativos.

4. Gestión de crisis y respuesta a emergencias: la IA puede facilitar la gestión de crisis y la respuesta a emergencias en entornos hospitalarios mediante la integración y análisis de datos provenientes de múltiples fuentes, como sistemas de monitorización de pacientes, comunicaciones de emergencia y registros médicos electrónicos. Esto permite una toma de decisiones más rápida y precisa durante situaciones críticas, como desastres naturales, accidentes graves o eventos terroristas.

5. Mejora de la resiliencia operativa: la capacidad de la IA para analizar grandes volúmenes de datos en tiempo real puede ayudar a mejorar la resiliencia operativa de las Infraestructuras Críticas hospitalarias al anticipar y mitigar interrupciones y fallas en los sistemas de energía, comunicaciones, suministro de agua y otros servicios esenciales.

Podríamos concluir que la combinación de inteligencia artificial y *Big Data* es esencial para fortalecer la seguridad, la protección integral y la resiliencia de las Infraestructuras Críticas hospitalarias al permitir una detección más temprana de amenazas, una gestión más eficaz de riesgos, una respuesta más rápida a emergencias y una mejora general de la capacidad de recuperación frente a eventos adversos, desastres, catástrofes o calamidad pública.

La inteligencia artificial y el *Big Data* ofrecen herramientas poderosas para mejorar la seguridad y protección integral en las Infraestructuras Críticas hospitalarias al permitir una detección temprana y una respuesta más eficiente ante amenazas, así como una gestión más efectiva de crisis y recursos.

Reforzamiento con Inteligencia Artificial (IA):

1. Detección de anomalías: los sistemas de IA pueden analizar continuamente los datos generados por los sistemas de seguridad, como cámaras de vigilancia y sensores, para identificar patrones o comportamientos anómalos que podrían indicar posibles amenazas.

2. Predicción de riesgos: mediante el uso de algoritmos de aprendizaje automático, la IA puede analizar grandes conjuntos de datos históricos para identificar tendencias y predecir posibles riesgos de seguridad en el futuro, permitiendo una mejor preparación y prevención.

3. Respuesta automatizada a emergencias: los sistemas de IA pueden ser programados para tomar decisiones automáticas y activar respuestas de emergencia ante situaciones críticas, como la detección de intrusos o la activación de alarmas en caso de incendios o desastres naturales.

4. Optimización de recursos de seguridad: la IA puede optimizar el uso de recursos de seguridad, como personal de vigilancia y equipos de seguridad, al proporcionar análisis en tiempo real sobre dónde se requiere mayor atención y supervisión.

Reforzamiento con *Big Data*:

5. Análisis predictivo: el análisis de *Big Data* puede identificar patrones y correlaciones entre diferentes variables, lo que permite predecir posibles incidentes de seguridad y tomar medidas preventivas para mitigar riesgos.

6. Gestión de datos masivos: el *Big Data* proporciona la capacidad de almacenar, procesar y analizar grandes volúmenes de datos generados por sistemas de seguridad y dispositivos conectados, lo que permite una visión más completa y detallada de la seguridad de la infraestructura hospitalaria.

7. Identificación de vulnerabilidades: mediante el análisis de *Big Data*, es posible identificar vulnerabilidades en la seguridad de la infraestructura hospitalaria al correlacionar datos de diferentes fuentes, como registros de acceso, patrones de comportamiento y datos ambientales.

8. Mejora continua: el análisis de *Big Data* permite retroalimentar los sistemas de seguridad con información en tiempo real sobre incidentes y amenazas, lo que facilita

la mejora continua de los sistemas de seguridad y la adaptación a nuevos riesgos y desafíos.

Por todo ello y en conjunto, la inteligencia artificial y el *Big Data* pueden proporcionar un enfoque integral y proactivo para reforzar la seguridad y protección en Infraestructuras Críticas hospitalarias, permitiendo una detección temprana de amenazas, una respuesta más rápida a emergencias y una gestión más eficiente de los recursos de seguridad.

3.16. PROYECTO *PHIRMA* [70] PARA GARANTIZAR LA SEGURIDAD HOSPITALARIA EN EL ENTORNO DE LA UE.

En los últimos 20 años, las pérdidas y los daños causados por las catástrofes mundiales siguen aumentando. Los sistemas de Infraestructuras Críticas (IC) deben protegerse contra las catástrofes, tanto naturales como provocadas por el hombre, para garantizar el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad y el bienestar económico o social de las personas.

No cabe duda de que los Servicios de Salud (SS) se ajustan a la definición de IC y varias directivas de la UE y otros documentos oficiales, como la Directiva NIS de 2016, enumeran dichos servicios entre los activos y servicios esenciales que deben protegerse frente a ataques cibernéticos y/o físicos.

Por otra parte, aunque la Directiva de 2008 sobre protección de Infraestructuras Críticas [DIR1], menciona la sanidad en la definición de las Infraestructuras Críticas, según los resultados del *proyecto THREATS [TP1]* (hasta ahora, el único proyecto de seguridad de referencia de la UE sobre el tema de la protección del sistema sanitario es evidente que, entre las Infraestructuras, la sanidad, incardinada en el sector salud, dista mucho de estar adecuadamente considerada.

De hecho, los dispositivos de seguridad protectores dentro del sector sanitario no están integrados a nivel operativo y las metodologías para la protección de activos críticos desarrolladas principalmente para otras Infraestructuras Críticas, (principalmente transporte, energía, información y comunicación), aunque adaptables, para apoyar los programas de

[70] *Protection of Health Infraestructures, Resilece, Management and Adaptatation,* cuyo significado es Protección de Infraestructuras de Salud, Resiliencia, Gestión y Adaptación. Proyecto de la UE. Centrado en fortalecer la infraestructura de salud en Europa, haciendo énfasis en la resiliencia ante diferentes desafíos, la gestión eficaz de recursos y la adaptación a cambios en el entorno, como pueden ser pandemias, desastres naturales u otros eventos que afecten la capacidad de los sistemas de salud para funcionar adecuadamente.

protección y reducción de la vulnerabilidad dentro del sector sanitario, aún no se aplican. Además, la falta de financiación, la escasa prioridad con respecto a otros sectores de las Infraestructuras Críticas y los escasos conocimientos y competencias en el ámbito de la seguridad son señalados por el personal sanitario como los principales obstáculos para la aplicación de programas de seguridad en el sector de la salud.

En el ámbito de la presente investigación, es fundamental destacar que concebir los Servicios de Salud como Infraestructuras Críticas significa implementar programas de seguridad profundamente interconectados con la esfera humana.

El objetivo principal de los Servicios de Salud es proporcionar tratamiento médico de calidad y seguro a la población.

En este sentido, no se puede restringir en exceso el acceso a los tratamientos, aunque los distintos Servicios Autonómicos de Salud suelen ser el blanco de los conflictos y los más vulnerables en caso de crisis.

Por lo tanto, garantizar la continuidad de las actividades de los Servicios de Salud críticos, es fundamental para maximizar la resiliencia de las comunidades afectadas, garantizando al menos las funciones básicas incluso en caso de interrupción de las infraestructuras físicas y cibernéticas. En esta línea, dentro de las Infraestructuras Críticas de los Servicios de Salud (ICS), el Sistema de Emergencias Médicas (SEM) -actividades pre hospitalarias y hospitales insertos en una red- es reconocido como el servicio de salud más crítico. Se ocupa de funciones de misión crítica dependientes del tiempo, organizado como una red «multi actor», que presta un servicio 24-7/365, y forma parte de los Primeros Respondedores o intervinientes, sosteniendo el mayor peso de la respuesta en caso de accidentes graves que afecten a la población. Por lo tanto, es esencial para la comunidad que el SME sea capaz de resistir a ataques, tanto no intencionales como intencionales, continuando con la prestación de los servicios esenciales de salud a la comunidad, y hacer frente a cualquier situación de aumento repentino de la demanda de atención médica, como durante los grandes incidentes y desastres, posiblemente aumentando su capacidad operativa, eventualmente reconfigurando y ampliando las instalaciones y procesos.

Es igualmente esencial, señalar cómo el sector sanitario está evolucionando rápidamente con la introducción de las tecnologías de la información y la comunicación, lo que aumenta la capacidad del sector para prestar mejores servicios a los ciudadanos, al tiempo que también

puede mejorarse la respuesta del sector en situaciones de crisis. Sin embargo, esta mayor penetración de las tecnologías de la información y la comunicación introduce vulnerabilidades adicionales, como demuestran los recientes ataques con *ramsomware*s a los servicios de atención sanitaria y, por tanto, requiere tecnologías eficaces de prevención, detección y mitigación. Estas cuestiones son especialmente relevantes cuando se consideran las nuevas formas de amenazas emergentes que se dirigen a los sistemas físicos cibernéticos, por ejemplo, los sistemas de gestión de edificios (BMS), dentro de la Infraestructura Crítica como una fácil «puerta trasera» en la red de TI de una organización. Por desgracia, muchos de estos activos están expuestos debido a una mala configuración y se convierten en un blanco fácil para robar datos, desplegar *ransomware*, lograr el control de los dispositivos y construir ataques de denegación de servicio (DoS). Otras amenazas emergentes incluyen la combinación de ataques físicos y cibernéticos para comprometer HSCI, este aspecto suele ocurrir cuando se compromete la seguridad física se para atacar la red de TI y viceversa.

Tradicionalmente, la principal estrategia para proteger el HSCI contra este tipo de amenazas era confiar en las medidas de prevención. Esto se ha convertido en un enfoque inadecuado y arriesgado, ya que se ha demostrado que las intrusiones se producirán, independientemente de lo buenas que sean las contramedidas. Por estas razones, *PHIRMA* no sólo se centra en la prevención de amenazas, sino que la complementa con un marco de conocimiento activo de la situación para la predicción de amenazas, la detección y la respuesta a incidentes.

Una dimensión importante de la protección de las ICSS es el intercambio de información entre organizaciones sanitarias para empezar a intercambiar conocimientos y lecciones aprendidas en materia de ciberseguridad, como se subraya en un reciente informe de ENISA sobre cibersalud, (aunque la cibersalud es sólo un subconjunto de los problemas que se plantean en el sector sanitario). Esto debería ampliarse con el objeto de abarcar toda la cadena de valor de los servicios sanitarios y cubrir también las amenazas no cibernéticas. Para ello, consideramos oportuna la creación de tales estructuras.

Coherentemente, el proyecto *PHIRMA* está concebido para abordar las necesidades de protección de la HSCI para evitar la destrucción o interrupción de sus instalaciones físicas y servicios cibernéticos, y asegurar las conexiones con todas las demás Infraestructuras Críticas (IC), adoptando un enfoque holístico y teniendo como activo principal a las «personas».

El proyecto *PHIRMA* tiene como objetivo aumentar la seguridad y la resistencia en la IC de Salud de la UE mediante las siguientes medidas (es decir: Objetivos Principales - O.M.):

- ✓ O.M.1: crear un marco global, integrado y escalable para la protección de las Infraestructuras Críticas de los servicios sanitarios (marco HSCIP) para el sistema sanitario europeo a nivel de centros y sistemas.
- ✓ O.M.2: crear una Plataforma centrada en el usuario (compuesta por un conjunto de herramientas analíticas, organizativas, de diseño y operativas innovadoras) para apoyar la aplicación efectiva de un Marco HSCIP y la ejecución en tiempo real de las funciones clave de protección. La Plataforma será diseñada y validada por los usuarios finales y será adecuada tanto para los nuevos sistemas de infraestructura de los Servicios de Salud como para los existentes.
- ✓ O.M.3: construir una red europea de referencia para la protección de la HSCI, con el fin de crear una cultura común y reforzar la cooperación dentro de los Estados miembros.

3.17. Relación entre el Índice de Seguridad Hospitalaria de la OMS con el Proyecto PHIRMA de la UE.

El Índice de Seguridad Hospitalaria, desarrollado por la Organización Mundial de la Salud (OMS) y la Organización Panamericana de la Salud (OPS), es una herramienta que evalúa la seguridad de los hospitales en términos de su infraestructura, capacidad de gestión de emergencias y preparación para desastres. La propia guía para evaluadores proporciona un enfoque paso a paso para utilizar una lista de verificación y clasificar la seguridad estructural y no estructural de los hospitales, así como su capacidad de respuesta ante emergencias y desastres.

> Se puede decir que, en cuanto a la seguridad hospitalaria, en la actualidad ya empieza a crearse un clima favorable y como tema transcendental, sobre todo, en algunos países latinoamericanos, donde se ha creado hasta un índice de seguridad hospitalaria (Organización Panamericana de la Salud, 2018), que permite clasificar a los centros hospitalarios por niveles. (Istúritz, J.J., 2018, p. 51).

Por otro lado, el proyecto *PHIRMA* de la Unión Europea (UE) tiene como objetivo mejorar la preparación y respuesta de los hospitales ante emergencias y crisis de salud pública. Aunque no existe una relación directa entre el Índice de Seguridad Hospitalaria y el proyecto *PHIRMA*, ambos comparten el objetivo común de fortalecer la seguridad y la capacidad de respuesta de los establecimientos de salud.

Para relacionar estas dos iniciativas, se podría considerar lo siguiente:

1. Intercambio de buenas prácticas: los resultados y las lecciones aprendidas del Índice de Seguridad Hospitalaria podrían compartirse con los hospitales y sistemas de salud involucrados en el proyecto *PHIRMA*. Esto permitiría identificar áreas de mejora y aplicar estrategias efectivas para fortalecer la seguridad hospitalaria.

2. Capacitación y formación: el Índice de Seguridad Hospitalaria podría servir como base para desarrollar programas de capacitación y formación dirigidos a los profesionales de la salud y al personal hospitalario en el marco del proyecto *PHIRMA*. Estos programas podrían abordar temas como la gestión de emergencias, la seguridad estructural y la preparación para desastres.

3. Coordinación y colaboración: las autoridades sanitarias y los responsables de la implementación del proyecto *PHIRMA* podrían colaborar con las instituciones que han utilizado el Índice de Seguridad Hospitalaria para compartir experiencias y trabajar juntos en la mejora de la seguridad hospitalaria.

Podemos concluir por tanto que, aunque no hay una conexión directa entre el Índice de Seguridad Hospitalaria y el proyecto *PHIRMA*, existe un terreno común en el objetivo de fortalecer la seguridad y la capacidad de respuesta de los hospitales. La colaboración y el intercambio de conocimientos podrían enriquecer ambas iniciativas y contribuir a un sistema de salud más seguro y resiliente.

RESUMEN DEL CAPÍTULO:

Aunque no es objeto del presente capítulo ahondar en todos los aspectos que afectan a la seguridad hospitalaria, que sin duda alguna sería objeto de otra tesis doctoral, el capítulo intenta contextualizar la importancia de los hospitales, su seguridad, su idiosincrasia, tipos de hospitales, así como cuántos aspectos son de interés para garantizar su seguridad y protección integral para poder comprender los aspectos de relevancia.

En el presente capítulo se han incluido temas de interés que han integrado aspectos de la búsqueda de una nueva taxonomía para los riesgos, el Convenio de Ginebra para garantizar su seguridad frente a cualquier tipo de conflicto, la Instrucción IS-41 del Consejo de Seguridad Nuclear, así como el Plan de Protección Física frente a Fuentes Radioactivas. Todo lo que vuelve a confluir en la enorme importancia que nuevamente entraña la creación de un Departamento de Seguridad en las que al frente debe de estar un Director de Seguridad debidamente habilitado por el Ministerio del Interior.

Aspectos de proyectos europeos en relación con la seguridad y gobernanza de los hospitales, tales como el Proyecto *PHIRMA*, así como su relación con el Índice de Seguridad Hospitalario creado por la Organización Mundial de la Salud se han incorporado al capítulo con el objeto de entender con mayor claridad el instrumento de la Organización Mundial de la Salud que se utilizará en el ulterior capítulo en relación con el Marco Empírico de la presente investigación.

CAPÍTULO IV

Marco empírico y Metodológico

«**Es extraño que sólo las personas extraordinarias hagan descubrimientos que luego aparecen de manera fácil y sencilla**».
Georg Lichtenberg

Capítulo IV

Marco Empírico

4. CAPÍTULO IV. METODOLOGÍA Y PROCEDIMIENTOS

El presente Marco Metodológico queda incardinado en una metodología de carácter mixto, en la que queda integrada, de una parte, por una exhaustiva Revisión Bibliográfica a través de la adecuada recopilación de información en relación al Terrorismo y, especialmente al *Yihadismo*, así como una revisión legislativa al respecto de cuántas disposiciones legales son transversales y de aplicación con el fenómeno terrorista, las Infraestructuras Críticas y la protección de las Infraestructuras Críticas Hospitalarias como Servicios Estratégicos, especialmente sensibles, como centros complejos, a la par que esenciales para la sociedad y, de otra parte, con una metodología exploratoria en la que se ha aplicado un estudio transversal, por medio de una auditoría observacional, en la que además se utilizan técnicas de carácter cuantitativas con la aplicación del Cuestionario Índice de Seguridad Hospitalaria (ISH), en atención al grado de seguridad y protección funcional, en consonancia con el objeto de la presente investigación que realizamos a través de la presente Tesis Doctoral.

El Formulario utilizado ha sido validado con anterioridad por la Organización Mundial de la Salud (OMS), a través de la Organización Panamericana de la Salud (OPS), en relación al instrumento conocido como Índice de Seguridad Hospitalaria, contrastado y aplicado tan solo en hospitales de América del Sur, lo que nos permitirá resaltar y diferenciar las singularidades específicas y distintas al marco de los hospitales de la Unión Europea.

En el presente marco metodológico incardinado en el marco empírico, intentaremos establecerla adecuada relación de aquellos aspectos relevantes que habrían de implementarse en futuras investigaciones para que, el ISH pueda arrojar una respuesta global en la seguridad y la protección integral de los hospitales de los distintos países que integran la Unión Europea de la que España forma parte desde el año 1985, con la firma del Tratado de Adhesión en Madrid y la integración efectiva en la Comunidad Económica el 1 de enero de 1986, en la que aportaremos el adecuado análisis o juicio crítico de toda la información obtenida, en relación con el objeto de la presente Tesis doctoral.

Hemos de manifestar con claridad y de manera taxativa que, la investigación en el ámbito concreto, de cuántos aspectos han sido necesarios recabar para la cumplimentación de los

datos relativos a los distintos hospitales de referencia en España, se torna muy ardua y compleja por la casi imposibilidad de profundizar en obras, artículos y tratados que supongan un respaldo a la presente realización de la presente Tesis Doctoral, todo ello por dos cuestiones bien diferenciadas, la primera es que nunca se ha realizado fuera del contexto de los países de América del Sur y, la segunda, por la dificultad por la propia idiosincrasia de la investigación, de obtener los distintos datos de los hospitales evaluados, todo ello atendiendo que muchos son de Iure y de facto, Infraestructuras Críticas, designados sus distinto servicios autonómicos de salud, Operadores Críticos y, por ello, la información debe de ser de carácter confidencial y reservada. Por tal motivo, aunque hagamos una relación detallada de los hospitales estudiados, sus datos se pondrán con distintas claves o acrónimos para salvaguardar la información de sus datos, en este sentido, hemos de destacar con rotundidad la afirmación de Walters (1976) el cual afirmaba que:

> La información relacionada con el poder, los recursos, capacidades e intenciones de potencias extranjeras o grupos terroristas que puedan afectar a nuestras vidas y a la seguridad de nuestro país, no siempre es ni está disponible para el dominio público.

De la misma manera, hemos también de manifestar que no se ha utilizado el paquete estadístico «Producto de Estadística y Solución de Servicio» (SPSS) de la compañía IBM, para la generación de estadísticas avanzadas. Hemos mantenido el formulario originario con el Modelo Matemático trazable directamente y diseñado por la Organización Mundial de la Salud al considerar que, el Formulario ISH no es un cuestionario propiamente dicho. Representa una Escala de tipo Descriptivo[71] de situaciones o de verificación, con lo que las pruebas estadísticas del SPSS no se pueden aplicar como si se tratara de un «cuestionario al uso».

En relación a la hipótesis de partida hemos de decir que los hospitales en la Unión Europea y, por tanto, los hospitales de nuestro país, que han implementado medidas específicas de seguridad y gestión de riesgos estarán mejor preparados para enfrentarse a posibles emergencias y desastres, lo que se reflejará en un mayor puntaje en el Índice de Seguridad Hospitalaria.

[71] Instrumento utilizado para recopilar datos sobre variables que se pueden describir mediante categorías, atributos o características específicas. Estas escalas se utilizan para medir características observables y mensurables en sujetos de estudio, como actitudes, comportamientos, opiniones, preferencias, habilidades, sobre variables específicas, lo que contribuye a una comprensión más profunda y completa del fenómeno estudiado.

La hipótesis planteada sugiere que existe una relación entre las acciones tomadas por los hospitales para fortalecer su seguridad y su capacidad para responder eficazmente a situaciones críticas. Al evaluar los hospitales utilizando el formulario del Índice de Seguridad Hospitalaria, podríamos investigar si esta relación es válida y cómo se manifiesta en la realidad.

En relación con la Hipótesis Nula, (denotada como **H0**), o afirmación a la que sometemos nuestra investigación en relación con el Índice de Seguridad Hospitalaria en los hospitales del entorno de la Unión Europea.

La hipótesis nula la planteamos de la siguiente manera:(**H0**): «No hay diferencia significativa en los puntajes del Índice de Seguridad Hospitalaria entre los hospitales que han implementado medidas específicas de seguridad y aquellos que no lo han hecho en la Unión Europea».

En otras palabras, la hipótesis nula sugiere que cualquier diferencia observada en los puntajes del índice podría deberse al azar y no a una relación real entre las acciones de seguridad y la preparación para emergencias en los hospitales.

Para probar esta hipótesis, se recopilarían datos de varios hospitales, se calcularían los puntajes del índice y se realizaría un análisis estadístico para determinar si la diferencia, (si existe) es estadísticamente significativa. Si el valor p (probabilidad) resultante es menor que un nivel de significancia predefinido (por ejemplo, 0.05), se rechazaría la hipótesis nula en favor de la hipótesis alternativa.

Es importante recordar que la hipótesis nula no afirma que no haya relación entre las variables; simplemente establece que cualquier diferencia observada podría ser atribuible al azar. La investigación académica busca evidencia para respaldar o refutar esta hipótesis. Aspectos relacionales y diferenciadores entre las dos hipótesis que hemos planteado en nuestra Tesis Doctoral:

Para ello hemos de manifestar que, la hipótesis de partida y la hipótesis nula son conceptos fundamentales en la investigación que hemos planteado. En sus cuestiones relacionales entre ambas hemos de destacar:

4.1. OBJETIVOS:

En relación a los objetivos que hemos establecido en la presente investigación hemos de considerar:

4.1.1 Objetivo general:

Estudiar la pertinencia del Formulario Índice de Seguridad Hospitalaria en el contexto de los hospitales en España y por extensión en el marco de la Unión Europea, todo ello en atención a la idiosincrasia de los riesgos específicos de nuestro entorno, así como a la legislación.

4.1.2 Objetivos específicos:

- ✓ Comprobar la viabilidad del Formulario Índice de Seguridad Hospitalaria en atención a su validez frente a todo tipo de riesgos que garanticen la Seguridad Hospitalaria, así como su prestación de servicio asistencial y su gobernanza frente a cualquier tipo de emergencia o catástrofe.
- ✓ Estudiar su validez frente a los Riesgos Antrópicos de Carácter Antisocial y, especialmente frente al riesgo o amenaza terrorista.
- ✓ Comprobar las distintas vulnerabilidades más representativas de la muestra objeto de estudio para su ulterior análisis.
- ✓ Tener un punto de partida con el que seguir investigando y si fuese el caso preparar y elaborar un cuestionario al efecto en el que se amplíe la matriz de riesgos si fuese preciso, todo ello con un grupo de expertos que pueda dar lugar a futuras investigaciones.
- ✓ Valorar otros aspectos en nuestro contexto europeo que haya de implementarse para su mejora en una nueva edición, o si fuese necesario diseñar otra herramienta al efecto.

4.2. HIPÓTESIS DE PARTIDA[72] (HIPÓTESIS ALTERNATIVA):

En el contexto de nuestro estudio sobre el Índice de Seguridad Hospitalaria, planteamos la hipótesis de partida de la siguiente manera: «Los hospitales que han implementado medidas específicas de seguridad estarán mejor preparados para enfrentar emergencias y desastres, lo que se reflejará en un mayor puntaje en el Índice de Seguridad Hospitalaria». Esta hipótesis sugiere una relación positiva entre las acciones de seguridad y la preparación hospitalaria.

[72]La hipótesis de partida (también conocida como hipótesis alternativa) es la afirmación que se busca probar o respaldar mediante la investigación.

4.3. HIPÓTESIS NULA[73] (H0):

En nuestro caso, la hipótesis nula planteada es que: «No hay diferencia significativa en los puntajes del Índice de Seguridad Hospitalaria entre los hospitales que han implementado medidas específicas de seguridad y aquellos que no lo han hecho en la Unión Europea».

La hipótesis nula, por lo tanto, nos sugiere que cualquier diferencia observada en los puntajes podría deberse al azar y no a una relación real entre las acciones de seguridad y la preparación de los distintos hospitales evaluados.

4.4. RELACIÓN[74] ENTRE AMBAS:

- ✓ La relación entre la hipótesis de partida y la hipótesis nula, por lo tanto es de contraste. Las hemos comparado para determinar si existe evidencia suficiente para rechazar la hipótesis nula a favor de la hipótesis de partida.
- ✓ Durante el análisis estadístico, se calcula un valor p (probabilidad). Si este valor es menor que un nivel de significancia predefinido (por ejemplo, 0.05), se rechaza la hipótesis nula.
- ✓ Si tras la investigación rechazamos la hipótesis nula, aceptamos íntegramente la hipótesis de partida, lo que nos sugerirá que hay evidencia para respaldar la relación propuesta que hemos establecido.

La utilización de la presente metodología está más asociada a un proceso de generación de respuesta a la pregunta a través de métodos matemáticos, métodos de comprobación que nos permitan validar hipótesis, e incluso realizar una comprobación de lo que nosotros consideramos que pueda sucederse en cualquier aspecto de interés que genere la propia idea de la presente investigación.

Además de la utilización de las distintas técnicas metodológicas de carácter cuantitativo que hemos referenciado previamente en atención a que:

- ✓ Utilizamos un modelo matemático, ya realizado, implementado y validado por la Organización Mundial de la Salud, así como la obtención de unos datos tras el

[73] La hipótesis nula (**H0**) es una afirmación que contradice la hipótesis de partida y la hemos planteado como elemento de contraposición a la hipótesis alternativa.

[74] La hipótesis de partida y la hipótesis nula son dos caras de la misma moneda en la investigación científica. La primera busca afirmar una relación, mientras que la segunda plantea la posibilidad de que no haya relación.

cálculo previo con las que puede generarse una estadística en función de los planteamientos previos.

- ✓ Esta pequeña base de datos a través de distintas herramientas como es el Formulario del Índice de Seguridad Hospitalaria, a través de preguntas cerradas, de carácter descriptivo, pueden conllevar la validación de las hipótesis planteadas, sí como generar una estadística si fuese necesario para nuestra investigación.
- ✓ Siempre se ha de considerar que el investigador tenga una base sólida en el estudio de la estadística, de las matemáticas, estudios correlacionales, creación de variables con un formato cerrado para su interpretación con posibilidad de acercarse a la formulación de hipótesis, etc.
- ✓ Aunque el instrumento por excelencia en el presente tipo de investigaciones son las encuestas, en el caso que nos ocupa estamos ante un formulario de carácter descriptivo.

Todo ello sin descontextualizar que el método cuantitativo tiene su objetivo «en la descripción, explicación, predicción y control objetivo de sus causas y la predicción de su ocurrencia». (Sánchez, 2019, p. 104).

La metodología que utilizada, reiteramos de carácter cuantitativa y el instrumento que utiliza en la investigación es un formulario de carácter cerrado, de tipo descriptivo que está integrado por una serie de cuestiones o preguntas cerradas, homogéneas para evitar los sesgos y, por consecuencia, la falta de rigor científico en los resultados, así como tras el adecuado tratamiento estadístico, a través del Modelo Matemático que la Organización Mundial de la Salud ha diseñado. Nos permite obtener unos datos fiables que, tras una ulterior discusión puedan arrojar unos resultados que puedan corroborar o no, las distintas hipótesis de partida planteadas, resultados que hacen que, si el instrumento se ha pasado de manera adecuada y en las condiciones idóneas, con la información precisa y necesaria de las distintas cuestiones que se plantean en el formulario, hacen que no presenten sesgos.

En relación con los sesgos y la pérdida de rigor vienen a ser considerados «(…) interpretaciones erróneas generadas sistemáticamente a partir de la información disponible.» (Prada, et al., 2022).

En el contexto de la presente investigación académica, es fundamental comprender las variables que se desprenden del formulario de este índice (Ver Anexo V).

A continuación, se exponen, grosso modo, las principales variables que se evalúan en el Formulario o Escala de Valoración:

Infraestructura y Servicios:

- ✓ Estado de las instalaciones: evalúa la resistencia y capacidad de las estructuras físicas del hospital para soportar situaciones de emergencia.
- ✓ Disponibilidad de servicios esenciales: considera la existencia y funcionamiento de servicios críticos como electricidad, agua, comunicaciones y suministros médicos.

Gestión de Riesgos:

- ✓ Planificación y preparación: evalúa la existencia y efectividad de planes de emergencia, capacitación del personal y simulacros.
- ✓ Identificación y mitigación de riesgos: analiza las medidas tomadas para prevenir y reducir riesgos, como la gestión de desechos, la seguridad contra incendios y la protección ante amenazas naturales.

Preparación y Respuesta ante Emergencias:

- ✓ Capacidad de respuesta: evalúa la preparación del personal para enfrentar emergencias, incluyendo la disponibilidad de recursos humanos y materiales.
- ✓ Comunicación interna y externa: considera la efectividad de los sistemas de comunicación dentro del hospital y con otras instituciones.

Coordinación y Colaboración:

- ✓ Coordinación interinstitucional: evalúa la colaboración entre el hospital y otras entidades (como servicios de emergencia, administraciones, así como el resto de y organizaciones hospitalarias y de salud).
- ✓ Participación comunitaria: analiza la integración de la comunidad en la planificación y respuesta ante emergencias hospitalarias.

4.5. ASPECTOS RELACIONADOS CON LA REVISIÓN BIBLIOGRÁFICA DESCRIPTIVA

En primer lugar, hemos seleccionado con anterioridad una serie de palabras claves recogidas con anterioridad, tales como: Terrorismo; Ciberterrorismo, Inteligencia; Prevención; Seguridad Hospitalaria; Infraestructuras Críticas, Índice de Seguridad Hospitalaria, así como términos relacionados para centrar la búsqueda y poder delimitar el alcance de la revisión realizada de

la literatura relevante y transversal con el objeto de la investigación y que finalmente hemos utilizado en los distintos buscadores de referencia.

En el sentido de lo expuesto y según Sampieri (2018):

> El presente método se construye en relación con el contexto en el que la investigación se desarrolla, generalmente, estructurales o situacionales, que han de apoyarse con la observación, encuestas o entrevistas guiadas, bibliografía, etc.

Realización de la Revisión de Investigaciones relacionadas, para ello hemos utilizado los siguientes Motores de Búsqueda y Bases de Datos en línea especializados *Google Scholar, Scopus, Dialnet, Web of Science, JSTOR, IEEE Xplore, Pro Quest, Science Direct,* Teseo, y Acceda entre otros.

Se intentó en un principio establecer criterios en relación a las fechas de publicaciones recientes, cuestión que al final se obvió debido a la escasa literatura por una cuestión obvia de confidencialidad de cuántos aspectos están relacionados con el objeto la presente investigación, reiteramos que muchos de los hospitales evaluados, en su defecto, los distintos sistemas autonómicos de salud, han sido declarados Operadores Críticos por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC).

Evaluación de la pertinencia y calidad de los artículos y literatura académica encontrada. Para ello se han revisado los títulos, resúmenes y contenidos de los artículos y estudios identificados para determinar su relevancia y calidad. Todo ello sin olvidar que durante la evaluación de los artículos encontrados que, en una investigación, y en palabras de Ballesteros (2014):

> Las personas perciben, comparan y recuerdan patrones visuales y objetos mientras tratan de ignorar información irrelevante que acompaña a la información relevante. (p. 8).

Lectura, análisis, extracción y toma de notas de cuántas cuestiones fueron de interés para la realización de la presente Tesis Doctoral e implementación de la relación de la revisión bibliográfica.

Además de la utilización del referenciado método de investigación, hemos querido reforzar la investigación, además de la revisión bibliográfica y legislativa, con la implementación del instrumento que se corresponde con el Formulario Índice de Seguridad Hospitalaria, en los que

se ha asegurado a los distintos hospitales participantes objeto de la muestra del estudio, que los datos que se nos faciliten, así como los datos obtenidos se tratarán en la presente investigación con la confidencialidad que merecen, anonimizándolos convenientemente.

En relación con el citado aspecto se detalla a continuación el material y el método utilizado.

4.6. MATERIAL Y MÉTODO EN EL DISEÑO Y LA APLICACIÓN DEL FORMULARIO.

Estos aspectos del «Material y Método» en relación con el Formulario son importantes para proporcionar una visión clara y detallada de cómo se llevó a cabo su realización, así como describir, cual fue el proceso de obtención de los datos necesarios para analizar y responder a las preguntas de investigación planteadas.

Los aspectos del marco metodológico que se corresponden con el «Material y Método» en la Escala o Formulario incluyen los siguientes elementos y las siguientes fases que hemos realizado en la investigación:

Primera Fase

Realización del Curso Virtual[75] de Evaluación de Establecimientos de Salud a través del Índice de Seguridad Hospitalaria en su segunda versión (ISHv2). Es un curso de carácter gratuito que incide en el autoaprendizaje, además abierto a todos los interesados en los que su realización también es «auto administrada», se realiza en línea, en la plataforma educativa virtual *Moodle* del Campus Virtual de Salud Pública de la Organización Panamericana de la Salud perteneciente a su vez a la Organización Mundial de la Salud.

Los módulos cuentan con abundante y diverso material, tales como presentaciones resolución de casos, las distintas actividades se muestran a través de un recorrido en imágenes de 360° de un hospital.

El curso tiene como objetivo principal proporcionar a los profesionales relacionados con el sector salud las habilidades necesarias para evaluar la seguridad hospitalaria. Se centra en la aplicación del Índice de Seguridad Hospitalaria (ISH).

Como objetivos secundarios que el evaluador pueda conocer los distintos elementos con los que cuenta cualquier hospital que ha de ser evaluado con el ISH, tales como que:

[75] El Curso Virtual de Evaluación de Establecimientos de Salud a través del Índice de Seguridad Hospitalaria (ISHv2) es una valiosa herramienta para evaluar y mejorar la seguridad en los hospitales durante emergencias y desastres.

- ✓ Pueda de una manera clara identificar aquellas amenazas que puedan materializarse en un daño al poner en peligro la seguridad y la protección integral del hospital.
- ✓ Pueda de una manera sistematizada y estandarizada calificar cuántos aspectos estructurales y no estructurales se correspondan con el ISH.
- ✓ Pueda identificar aquellos aspectos que son vitales para la gestión de cualquier emergencia, desastre, catástrofe o calamidad pública.
- ✓ Pueda a través de un único procedimiento sistematizar la evaluación y el análisis de los resultados que obtenga.

Estructura del Curso. Con relación a su estructura hemos de indicar que, la realización del curso supone el estudio y la superación de sus distintos módulos permiten conocer lo diferentes elementos de un establecimiento de salud que se evalúan mediante el ISH. Consta de cinco módulos con carácter secuencial que han de superarse y que a su vez cuenta en su totalidad con una carga lectiva total de 40 horas. Los distintos contenidos modulares son:

- ✓ Módulo 1: estudio de las amenazas que afectan la seguridad del hospital y la función de éste en la gestión de emergencias y desastres Se enseña a identificar las amenazas que ponen en riesgo la seguridad, en sus distintas vertientes de un hospital.
- ✓ Módulo 2: estudio y comprensión de la Seguridad estructural Se califican de forma estandarizada los aspectos estructurales con el objeto de servir e integrar el cálculo final del Índice de Seguridad Hospitalaria.
- ✓ Módulo 3: Estudio de la Seguridad no estructural que, igualmente redundará e integrará el cálculo del índice de seguridad hospitalario.
- ✓ Módulo 4: Estudio de la Gestión de emergencias y desastres. Se abordan en el presente apartado cuántos aspectos y elementos necesarios para la gestión de emergencias, desastres o catástrofes en cualquier centro hospitalario.
- ✓ Módulo 5: Estudio del procedimiento de la evaluación y presentación de resultados. Se sistematiza el procedimiento para la evaluación hospitalaria y el análisis de los distintos resultados obtenidos.

En relación a los distintos destinatarios. El curso está dirigido a profesionales relacionados con el sector salud, incluyendo ingenieros, arquitectos, personal médico, de enfermería, administrativo y otros especialistas, en Europa y en España, esos destinatarios son los expertos en gestión, dirección y gerentes de Riesgos, tales como los directores de Seguridad. También

es relevante para aquellos capacitados en la planificación integral de la gestión de riesgos de desastres.

En lo que respecta a su modalidad, hemos de destacar que el curso se realiza en línea, en la plataforma educativa virtual Moodle del Campus Virtual de Salud Pública de la Organización Panamericana de Salud y de la Organización Mundial de la Salud (OPS/OMS).

Segunda Fase

Una vez superado el curso se ha leído detenidamente el Índice de Seguridad Hospitalaria. Guía para evaluadores, tanto su primera como su segunda edición.

La Guía del evaluador del Índice de Seguridad Hospitalaria[76] es una herramienta de gran funcionalidad y trascendental para determinar y mejorar la seguridad en los hospitales durante emergencias y desastres. Los aspectos de mayor relevancia que presenta son:

- ✓ Objetivo: la guía se utiliza para evaluar y clasificar la seguridad hospitalaria. Proporciona instrucciones paso a paso sobre cómo utilizar la lista de verificación y cómo evaluar la seguridad estructural, no estructural y la capacidad de gestión de emergencias y desastres del hospital.
- ✓ Enfoque integral: la evaluación abarca varios aspectos, incluyendo procesos, sistemas, procedimientos y comportamientos. El objetivo es que pueda servir para prevenir daños que puedan preverse, así como reducir a la mínima expresión el riesgo que los hospitales puedan sufrir y materializarse en distintos daños.
- ✓ Aspectos positivos a la hora de estudiar y conocer la Guía del Evaluador: al conocer el evaluador todos los detalles de los aspectos que identifica o evalúa en relación a los distintos riesgos, ayuda a mejorar la seguridad hospitalaria, se puede lograr ya no sólo un gran ahorro de tipo económico, sino a mejorar esa imagen intangible de la organización, al garantizar un entorno asistencial seguro.

En relación a los objetivos específicos, considera de la Guía del Evaluador, OMS/OPS, (2018), los siguientes:

- ✓ Proporcionar a los evaluadores un método objetivo y estandarizado para aplicar la lista de verificación de la seguridad hospitalaria, a fin de que puedan realizar una

[76] Documento que se ha utilizado para formar a los directores de seguridad de los distintos hospitales para ulteriormente pasar los distintos formularios para poder calcular el Índice de Seguridad Hospitalaria con una formación previa.

determinación inicial si el hospital podrá funcionar o no por las consecuencias inmediatas de emergencias y desastres;

- ✓ establecer criterios uniformes para los elementos que serán evaluados en diferentes circunstancias, de manera que haya una base común para examinar la seguridad y las necesidades de muchos hospitales;
- ✓ simplificar el registro y la clasificación de los datos sobre las fortalezas y las debilidades encontradas en un hospital, tanto de manera individual como dentro de una red de servicios de salud, así como la capacidad de la comunidad para gestionar emergencias y desastres;
- ✓ recomendar actividades y medidas para mejorar la seguridad y la preparación del hospital.

La Guía del evaluador también ofrece orientación a los grupos de especialistas de diversas disciplinas que están comprometidos a reducir los riesgos para la seguridad de los hospitales y fortalecer la preparación, la respuesta y la recuperación de dichos establecimientos en casos de desastre

(p. 11).

Tercera Fase

Contactar con los Directores de Seguridad de los distintos hospitales que configuran la muestra, tan sólo en aquellos en los que no he podido acudir de manera presencial, con el objeto de que realicen el curso, así como explicarles de manera rigurosa y sistemática cómo han de cumplimentar el Instrumento que hemos utilizado en la investigación, para que se pase la herramienta de manera homogénea y no pueda alterarse por los sesgos del evaluador, garantizando de esa manera la objetividad y homogeneidad en relación a las condiciones de aplicación. Se les recomienda que realicen previamente El Curso Virtual de Evaluación de Establecimientos de Salud a través del Índice de Seguridad Hospitalaria referenciado con anterioridad.

Se realiza a través de la Plataforma TEAMS[77] vídeo llamada para la cumplimentación de cuántos aspectos de relevancia puedan generar duda

[77]*TEAMS* es una plataforma de colaboración, a través de una nube, que integra parte del conjunto de herramientas de productividad de Microsoft 365. La mencionada plataforma permite comunicarse, compartir recursos de manera funcional desde los distintos sitios en los que se encuentren los asistentes a la reunión a través de un sistema de «Telepresencia». Su versatilidad es múltiple al permitir, reuniones virtuales a través de Videoconferencias, chat y mensajería instantánea, áreas de trabajo personalizadas, entre otras.

Cuarta Fase

Aplicación del formulario que consta de las siguientes dimensiones, con los factores asociados correspondientes de interés para la obtención de los resultados (Ver Anexo V):

- ✓ Aspectos relacionados con la Ubicación Geográfica del establecimiento de salud.
- ✓ Aspectos relacionados con la seguridad estructural.
- ✓ Aspectos relacionados con la seguridad no estructural del hospital.
- ✓ Aspectos relacionados con la seguridad y la capacidad funcional.

Quinta Fase

Introducción de los distintos datos obtenidos en el «Modelo Matemático»[78] de la OMS (ver Anexo VI), consistente en una hoja Excel en las que se integran las distintas fórmulas matemáticas, Después de evaluar los hospitales utilizando una Lista de Verificación, se aplica un modelo matemático (los modelos matemáticos son herramientas de importancia para analizar, predecir y comprender el mundo que nos rodea), de la OMS para calcular el ISH. El ISH se clasifica en tres categorías:

- ✓ C: Medidas urgentes (0 - 0.35).
- ✓ B: Medidas a corto plazo (0.36 - 0.65).
- ✓ A: Medidas a medio y largo plazo (0.66 – 1).

Este enfoque busca fortalecer la resiliencia de los hospitales y garantizar que puedan seguir prestando los diferentes servicios asistenciales, así como atención médica específica, incluso en situaciones de emergencia.

Sexta Fase

[78] En la investigación científica de carácter académico, se utilizan diversos tipos de modelos matemáticos para comprender y representar fenómenos del mundo real, entre los que destacamos: 1. Modelos Empíricos o Teóricos: a) Empíricos: Estos modelos se basan en datos observados y recopilados de la realidad. Utilizan información de la experimentación real y se ajustan a los resultados empíricos. Teóricos: Los modelos teóricos se construyen a partir de principios y suposiciones fundamentales. No necesariamente se basan en datos empíricos, sino en conceptos y teorías. 2. Modelos Estocásticos o Deterministas: a) Estocásticos: Estos modelos incorporan la aleatoriedad y la incertidumbre. Se utilizan cuando los fenómenos no son completamente predecibles y están sujetos a variabilidad. B) Deterministas: Los modelos deterministas son completamente predecibles y no contienen elementos aleatorios. Siguen reglas fijas y se basan en ecuaciones matemáticas. 3. Modelos Estáticos o Dinámicos: a) Estáticos: Los modelos estáticos representan situaciones en un solo punto en el tiempo. No consideran cambios a lo largo del tiempo. b) Dinámicos: Estos modelos capturan la evolución de un fenómeno a lo largo del tiempo. Incluyen variables que cambian con el tiempo y se expresan mediante ecuaciones diferenciales. 4. Modelos Agregados o Distribuidos: a) Agregados: Los modelos agregados simplifican la complejidad al agrupar elementos similares en categorías generales. Son útiles para obtener una visión general. B) Distribuidos: Los modelos distribuidos consideran la heterogeneidad y las diferencias individuales. Representan la variabilidad espacial y temporal de los fenómenos.

Obtención de los datos y resultados para su discusión, análisis y ulteriores conclusiones, todo ello comparándolo con cuántos aspectos son de obligado cumplimiento en la Unión Europea.

Para ello se ha transformado los decimales en números enteros con la intención que en la representación gráfica pueda entenderse mejor. Aunque las gráficas son suficientemente representativas.

Implementación de la herramienta. Para ello hemos sintetizado los aspectos que consideramos de interés en que se exponen a continuación.

Consistencia y validez del Formulario. La validez del presente cuestionario se refiere a la medida en que el instrumento realmente mide lo que pretende medir.

Obviando métodos más fiables de carácter estadístico como el Coeficiente de *Alfa de Crombach*[79], no hemos medido la evaluación completa de la validez, tales como la validez de constructo o la validez concurrente, todo ello por lo expuesto con anterioridad, el ISH en lo que representa una Escala de tipo Descriptivo[80]de situaciones o de verificación, con lo que las pruebas estadísticas del SPSS no se pueden aplicar como si se tratara de un cuestionario convencional. Por lo que nos hemos decantado por el análisis de la validez del contenido, para ello, hemos seleccionado la fórmula para calcular la validez del cuestionario mediante el índice de validez de contenido (IVC) que es la siguiente:

IVC = (Nv / Nt) x 100

Dónde:

- ✓ Nv es el número de expertos que coinciden en la pertinencia y relevancia de cada ítem del cuestionario.
- ✓ Nt es el número total de expertos que participaron en la evaluación.

[79] El coeficiente *alfa de Cronbach* es una medida de confiabilidad o consistencia interna utilizada en la psicometría para evaluar la fiabilidad de una escala o cuestionario. Fue desarrollado por el psicólogo estadounidense Lee Cronbach. Es una medida de fiabilidad interna. varía entre 0 y 1, donde un valor más cercano a 1 indica una mayor consistencia interna de los ítems de la escala o del formulario.

[80] Instrumento utilizado para recopilar datos sobre variables que se pueden describir mediante categorías, atributos o características específicas. Estas escalas se utilizan para medir características observables y mensurables en sujetos de estudio, como actitudes, comportamientos, opiniones, preferencias, habilidades, sobre variables específicas, lo que contribuye a una comprensión más profunda y completa del fenómeno estudiado.

La fórmula del IVC proporciona un porcentaje que indica la validez de contenido del cuestionario. Un valor más alto de IVC indica una mayor concordancia entre los distintos miembros o expertos en seguridad hospitalaria en cuanto a la pertinencia y relevancia de los ítems del formulario.

El Índice de Validez de Contenido (IVC) se refiere a la evaluación de la calidad y relevancia de las preguntas o ítems en un cuestionario o formulario. En el contexto del Índice de Seguridad Hospitalaria (IVC) se aplicaría a las cuestiones contenidas en dicho formulario.

Fórmula para el cálculo del IVC:

Definición del IVC:

- ✓ El IVC mide la concordancia entre los expertos sobre la relevancia y pertinencia de cada ítem en el formulario.
- ✓ Los expertos evalúan cada ítem y asignan una puntuación que indica cuán relevante consideran que es.

Cálculo del IVC:

- ✓ El IVC se calcula para cada ítem individualmente.
- ✓ Los expertos proporcionan una puntuación para cada ítem:
  - 1.0: Muy relevante.
  - 0.8: Relevante.
  - 0.6: Moderadamente relevante.
  - 0.4: Poco relevante.
  - 0.2: No relevante.
  - 0.0: Irrelevante.
- ✓ El IVC se obtiene como el promedio de las puntuaciones de todos los expertos para ese ítem.

Interpretación del IVC:

- ✓ Un IVC alto (cerca de 1) indica que los expertos están de acuerdo en que el ítem es relevante y pertinente.
- ✓ Un IVC bajo (cerca de 0) sugiere que hay discrepancias en la percepción de relevancia.

Por lo tanto, el IVC proporciona información sobre la calidad de las preguntas en el formulario del Índice de Seguridad Hospitalaria. Un alto IVC garantiza que las cuestiones sean apropiadas y útiles para evaluar la seguridad hospitalaria.

4.7. MUESTRA:

Describir la población objetivo de estudio y especificar cómo se seleccionó la muestra de participantes, ya sea a través de un muestreo aleatorio, intencional u otro método. Es importante tener en cuenta la selección de la muestra de manera adecuada a los objetivos de la investigación, así mismo la determinación de la muestra representativa, que en nuestro caso no ha sido posible, dado que nos vemos condicionados por la muestra disponible y adecuada. En el sentido que se apunta es importante destacar según Snedecory (1967) que:

> (…) a mayor precisión deseada se requerirá un tamaño de muestra mayor; pero inversamente proporcional al valor de la precisión; es decir, que a mayor precisión de la muestra será menor. (p.78).

Tabla 1

Descripción de los Centros Hospitalarios Evaluados

	Año de Construcción/ inauguración					EQUIPAMIENTO TECNOLÓGICO a 31/12/2022												
Hospital		Superficie (m^2)	Camas	Quirófanos	Consultas	TAC	RM	GAM	HEM	ASD	LIT	BCO	ALI	SPECT	PET	MAMOS	DO	DIAL
Hospital General Universitario Gregorio Marañón de Madrid	1968	194000	1140	41	77	4	3	0	5	3	1	0	3	2	1	3	1	45
Hospital Universitario de la Paz de Madrid	1964	250000	966	50	180	7	4	3	3	4	1	0	4	1	1	4	3	49
Vithas Hospital Nisa Pardo de Aravaca de Madrid	1990	30000	88	10	25	1	2	0	1	1	0	0	0	0	0	1	1	0
Hospitales San Roque Las Palmas	1920	100000	162	30	80	1	3	1	1	1	1	0	1	1	1	1	1	1
Hospital Clínico Universitario Virgen de la Arrixaca de Murcia	1975	180000	920	45	120	5	3	2	3	5	0	0	3	2	1	3	1	36
Clínica Cajal de Las Palmas	1988	20000	136	8	15	1	1	0	0	0	0	0	0	0	0	0	1	0
Vithas Hospital Santa Catalina	1934	40000	157	15	30	1	2	0	1	0	1	0	0	0	0	0	1	1
Hospital Nisa del Rey Don Jaime de Castellón de La Plana	1998	25000	96	12	26	2	1	1	0	0	1	0	3	1	1	1	1	0
Hospital Insular Materno Infantil de Las Palmas	1972	60000	916	20	35	4	3	1	1	2	1	0	0	2	1	3	1	35
Hospital San Roque Meloneras Las Palmas	2008	15000	147	6	10	1	1	0	0	0	0	0	0	0	0	1	1	12
Hospital Universitario Son Espases de Mallorca	2010	300000	839	70	200	4	4	2	2	2	1	0	3	2	1	2	1	36
Complejo Universitario Hospital Doctor Negrín	1971	100000	652	30	80	3	2	2	3	5	1	0	6	2	1	1	1	118

TAC: Tomografía Axial Computarizada
RM: Resonancia Magnética
GAM: Gammacámara
HEM: Sala de Hemodinámica
ASD: Angiografía por Sustracción Digital
LIT: Litotricia Extracorpórea por Ondas de Choque
BCO: Bomba de Cobalto
ALI: Acelerador de Partículas
SPECT: Tomografía por emisión de fotones
PET: Tomografía por emisión de positrones
MAMOS: Mamógrafo
DO: Densitómetros Óseos
DIAL: Equipos de Hemodiálisis

4.8. CONSIDERACIONES ÉTICAS:

Hemos de mencionar las consideraciones éticas aplicadas durante el proceso de investigación, como el consentimiento informado de los participantes, la confidencialidad y la protección de datos personales, el respeto a los principios éticos y normativas aplicables, entre otros.

1. Consentimiento informado: los Directores de Seguridad proporcionaron su consentimiento antes de participar en la investigación. Fueron plenamente informados sobre su propósito, los procedimientos involucrados, cualquier riesgo potencial y, su derecho a su no participación.

2. Confidencialidad: se garantizó la confidencialidad de la información recopilada. Al garantizar la identidad de los directores de seguridad participantes la identidad de los participantes, así como garantizar su anonimato.

3. Protección de datos: se ha considerado la legislación específica en la materia. Cuestión que incluye el almacenamiento seguro de la información recopilada.

4. Se ha explicado que el estudio puede tener un beneficio potencial para la sociedad si se sigue con las distintas líneas de investigación.

5. No maleficencia: se ha pasado cuidadosamente el formulario de índice de Seguridad Hospitalaria y se ha evitado realizar preguntas al margen de la herramienta para evitar preguntas que puedan ser intrusivas en relación a la intimidad o el honor.

6. *Debriefing*[81]: se ha informado a los participantes de la muestra los resultados del estudio y se han atendido sus distintas sugerencias en atención a las actuaciones de mejora que ellos pueden implementar en sus hospitales con el objeto de aumentar el Índice de Seguridad Hospitalaria.

[81] Viene a significar un «informe o análisis posterior». Se refiere a una reunión o sesión en la que se revisa y analiza un evento, situación o experiencia después de que ha ocurrido. El propósito del *debriefing* es discutir lo que sucedió, evaluar el desempeño, identificar lecciones aprendidas y proporcionar retroalimentación constructiva para mejorar en el futuro. El *debriefing* es comúnmente utilizado en contextos como el militar, la aviación, la medicina, los equipos de emergencia y otras áreas donde la revisión y el análisis de las acciones son cruciales para mejorar el rendimiento y la seguridad.

4.9. RESULTADOS

En el procedimiento de análisis de los datos pretendemos describir cómo se procesaron y analizaron los datos recopilados. Esto puede implicar el uso de software de análisis cualitativo o cuantitativo, la aplicación de técnicas estadísticas o de codificación de datos, la identificación de patrones o temas emergentes, etc.

A continuación, se recogen las distintas gráficas obtenidas con los resultados que se desprende del «Modelo Matemático»[82] *creado exprofeso* para evaluar el Índice de Seguridad Hospitalaria. En cualquier caso, En atención a cómo se ha secuenciado y realizado la presente investigación que se corresponde con la Tesis Doctoral que se presenta, consideramos la fiabilidad de los resultados y la pertinencia de la técnica de investigación utilizada utilizando como instrumento o herramienta el Formulario Índice de Seguridad Hospitalaria.

Se han seguido todas y de manera secuencial los distintos estadios o fases, siempre en atención al método científico y los resultados obtenidos, así como las conclusiones son precisas al estar debidamente cuantificadas, según Hernández (2014):

> (…) por el uso de la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías. (p. 4).

Se identifican y objetivan, por tanto, los resultados que, cada hospital de referencia, en su área de influencia arroja tras la adecuada aplicación del formulario.

Los resultados se exponen a través de las siguientes gráficas que se obtienen con el objeto de que visualmente puedan ser mucho más clarificadoras, en cualquier caso, se presenta con una breve explicación de los datos obtenidos antes de pasar a su adecuada y pertinente discusión de los datos de la investigación sobre variables específicas, lo que contribuye a una comprensión más profunda y completa del fenómeno estudiado.

Los resultados que han arrojado tras pasar el Formulario del Índice de Seguridad Hospitalaria se han plasmado en orden en relación a los mejores criterios de seguridad a los hospitales que menor puntuación han obtenido, es decir en relación de la mayor puntuación a la menor, de manera decreciente. Curiosamente los hospitales con peor Índice de Seguridad Hospitalaria

[82] Hemos de referenciar que el Modelo Matemático está protegido por la propia Organización Mundial de la Salud con el objeto de que las fórmulas utilizadas al efecto no puedan alterarse y producir sesgos en el resultado de la evaluación final del hospital objeto de estudio.

están Madrid y pertenecen a dos grandes hospitales que son referentes en su área de influencia, en contraposición a otros dos hospitales de la propia geografía de nuestro estado, que han obtenido los mejores resultados, paradójicamente son los dos hospitales de referencia de las dos Comunidades Isleñas de nuestro país, la Comunidad Canaria, seguida de la Comunidad Balear.

Figura 20

Resultados tras la aplicación del Formulario en el Hospital Universitario Doctor Juan Negrín, 2023

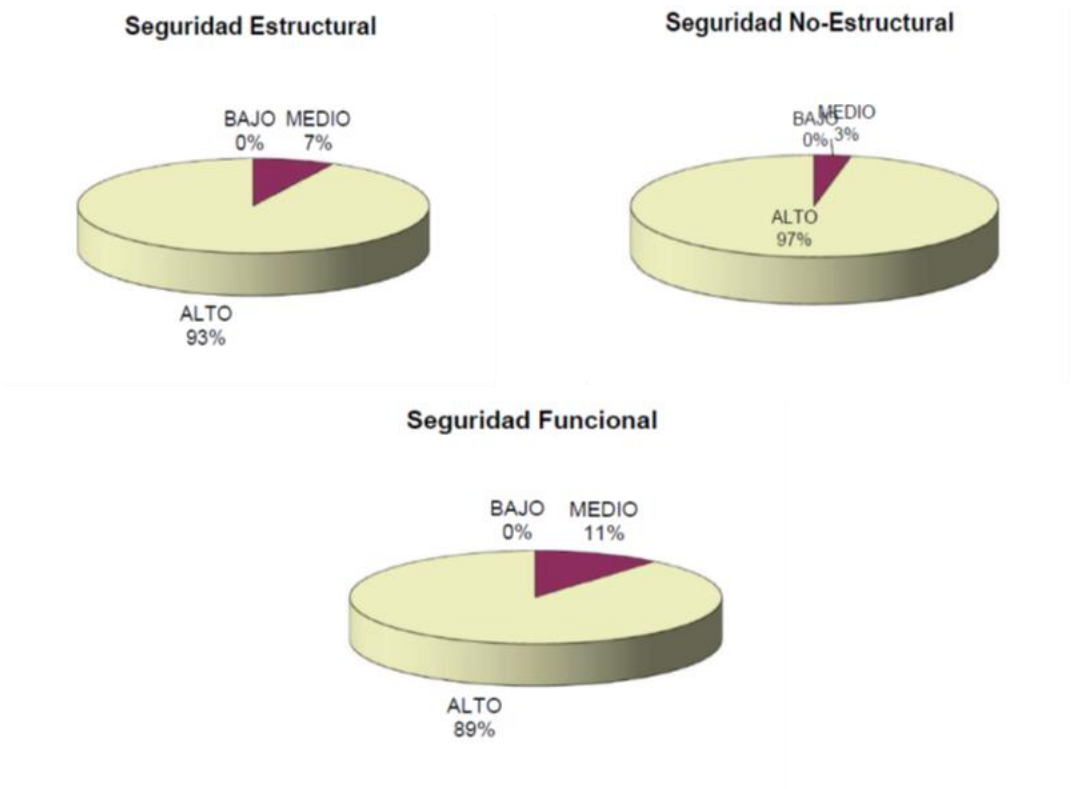


Figura 21

Índice de Seguridad Hospitalaria en el Hospital Universitario Doctor Juan Negrín, 2023

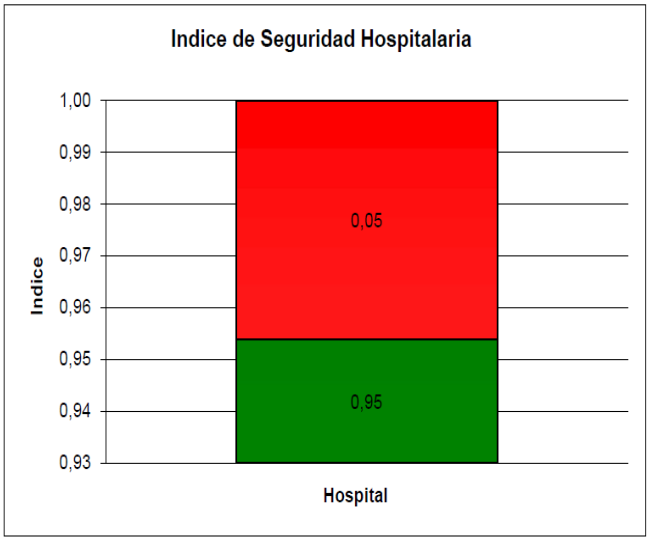


Figura 22

Resultados alcanzados por el Hospital Universitario Son Espases, Mallorca, Islas Baleares, 2023

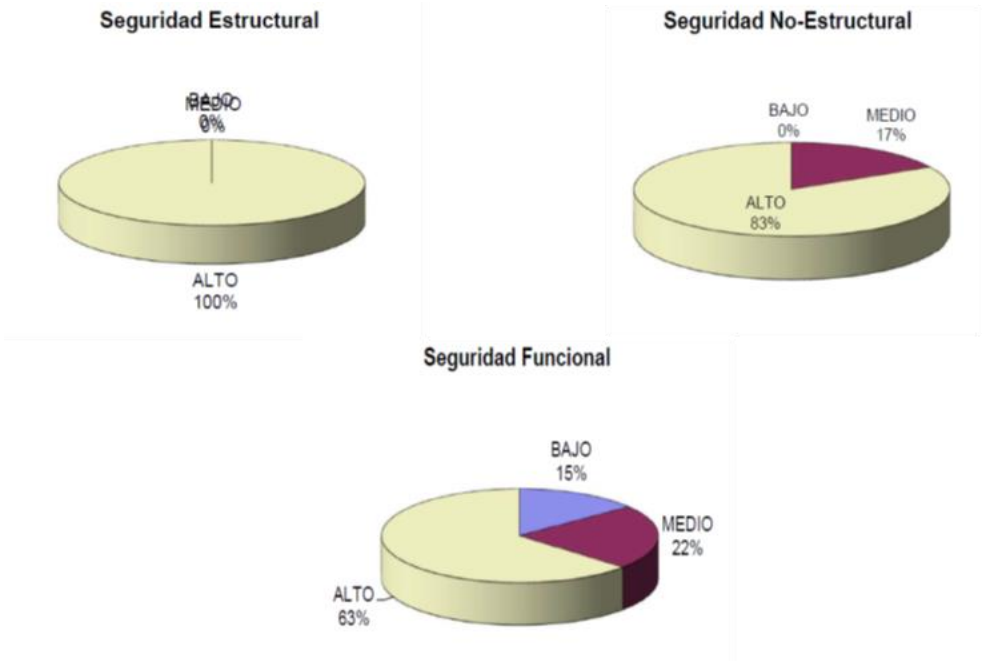


Figura 23

Índice de Seguridad Hospitalaria en el Hospital Universitario Son Espases, Mallorca, Islas Baleares, 2023

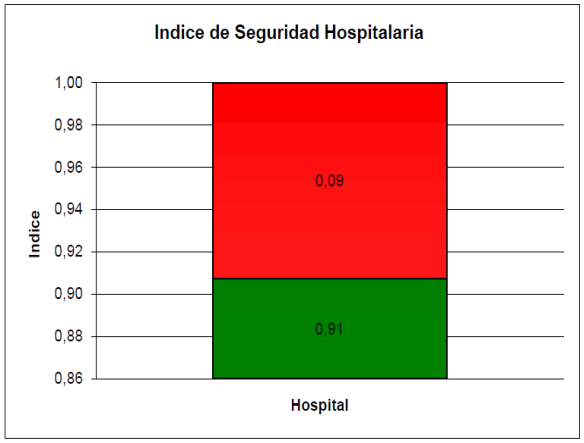


Figura 24

Resultados alcanzados en el Hospital San Roque de Meloneras, Gran Canaria, 2023

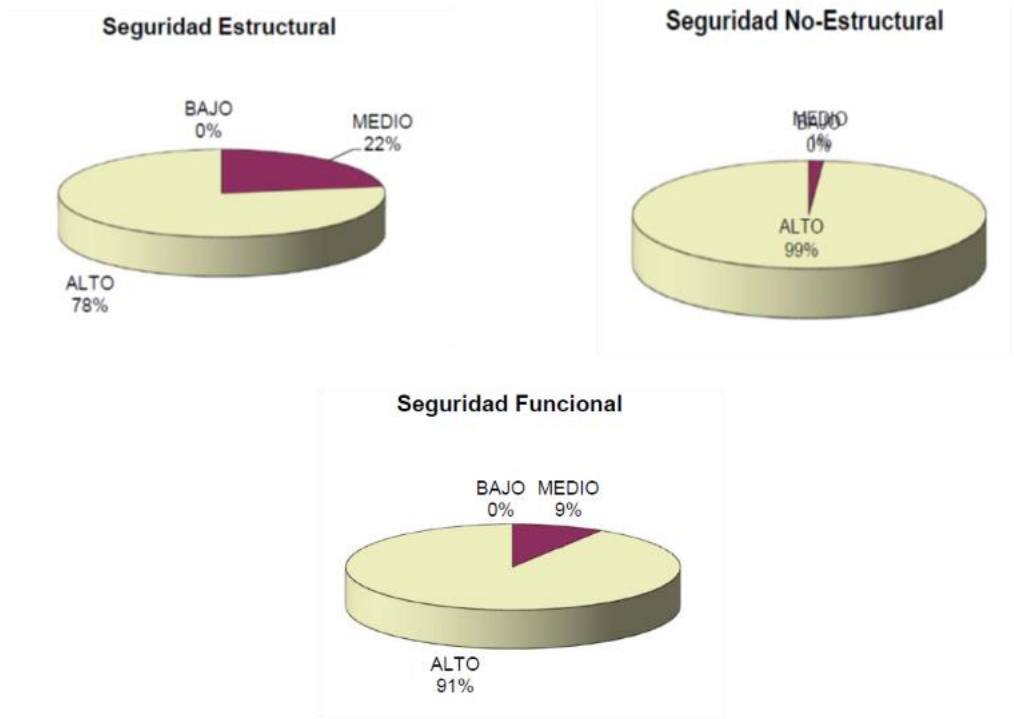


Figura 25

Representación del Índice de Seguridad Hospitalaria en el Hospital San Roque de Meloneras, Gran Canaria, 2023

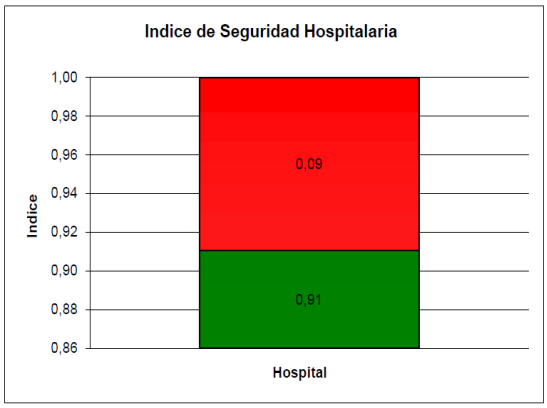


Figura 26

Resultados alcanzados en el Hospital Universitario Materno-Infantil de Gran Canaria, 2023

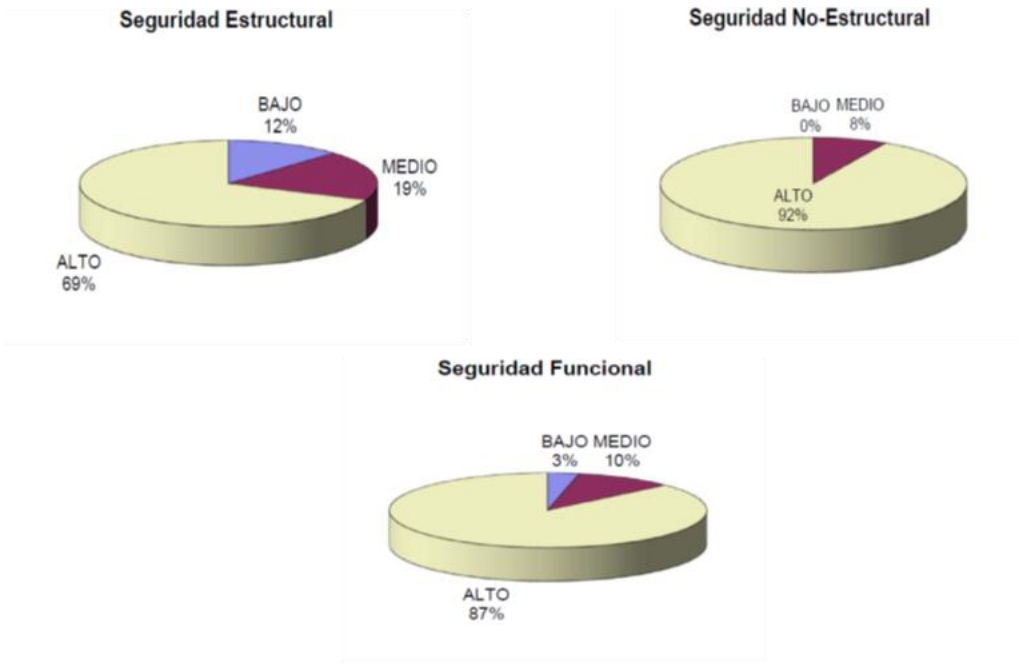


Figura 27

Representación del Índice de Seguridad Hospitalaria en el Hospital Universitario Materno-Infantil de Gran Canaria, 2023

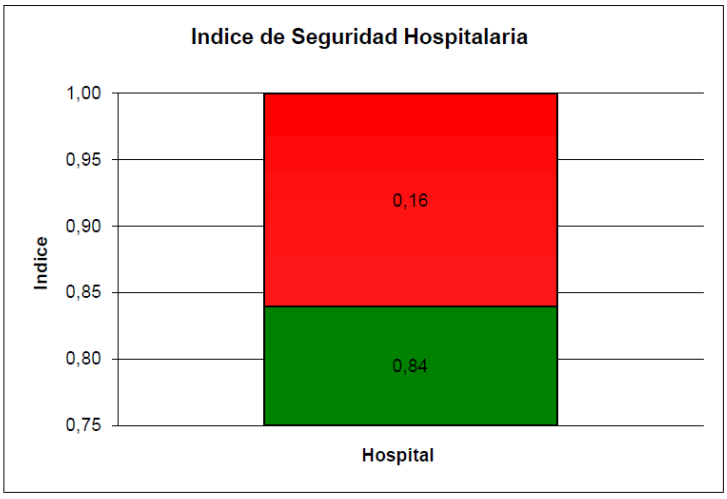


Figura 28

Resultados alcanzados en el Hospital Nisa del Rey Don Jaime, Castellón de La Plana, 2023

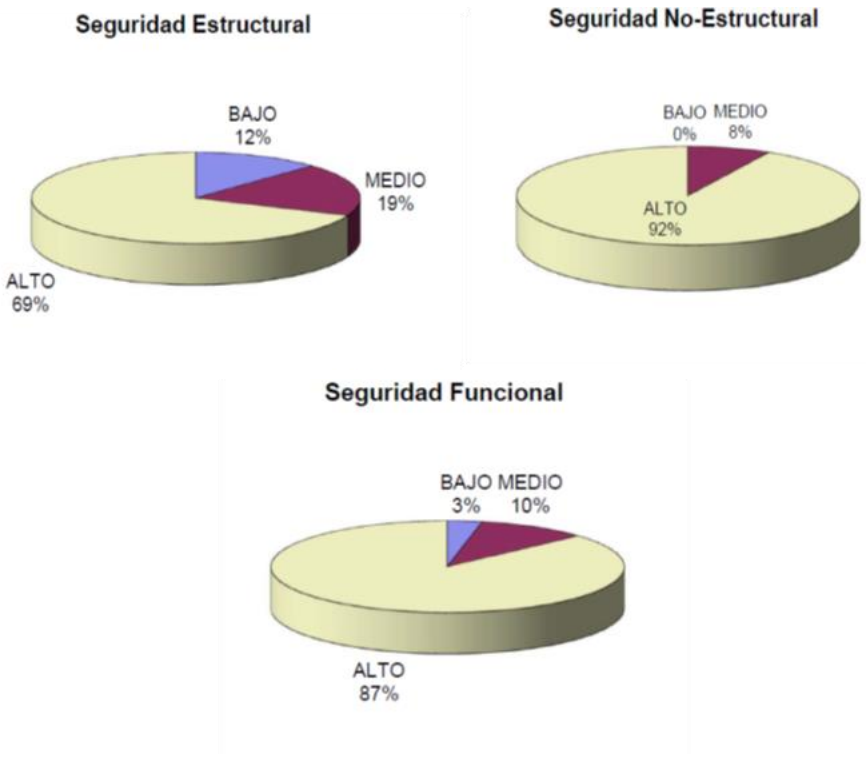


Figura 29

Representación del Índice de Seguridad Hospitalaria en el Hospital Nisa del Rey Don Jaime, Castellón de La Plana, 2023

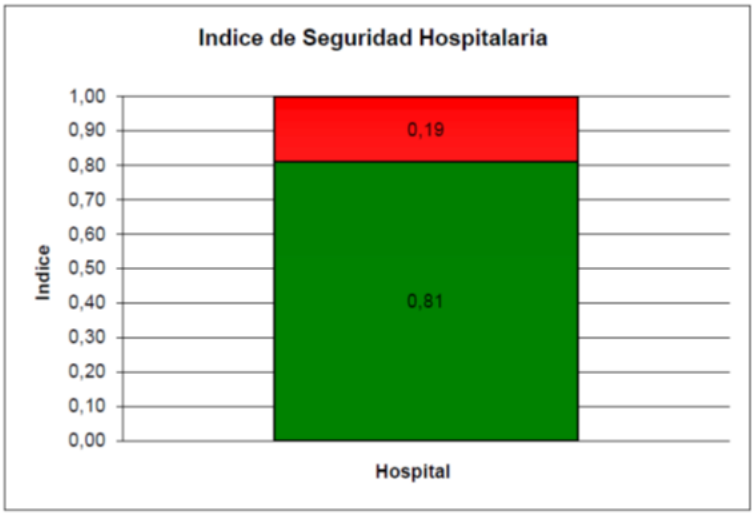


Figura 30

Resultados alcanzados en Vithas Hospitales de Las Palmas de Gran Canaria, 2023

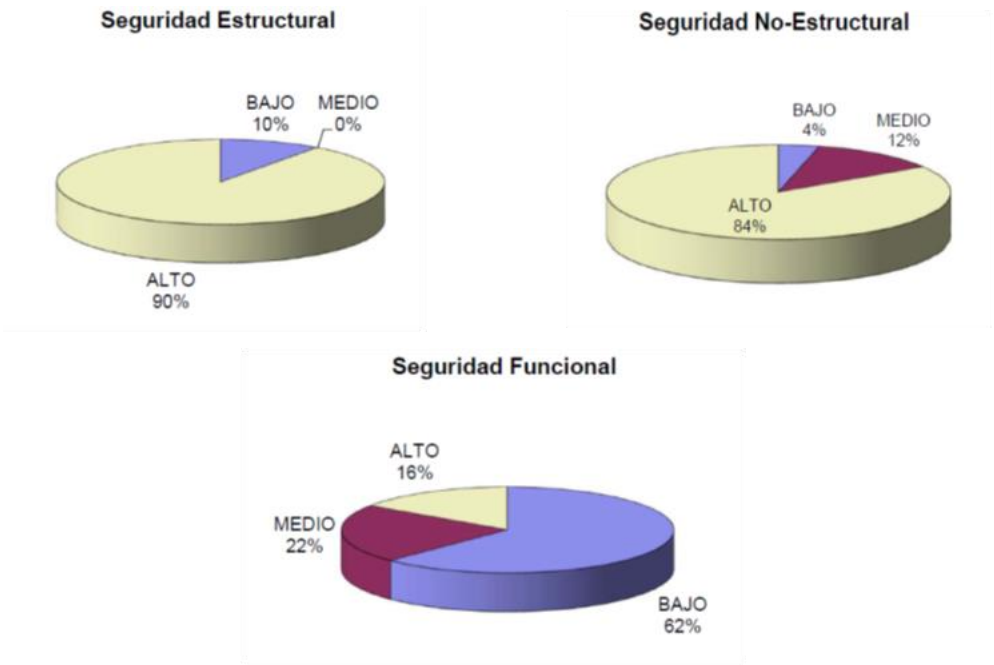


Figura 31

Índice de Seguridad Hospitalaria en Vithas Hospitales de Las Palmas de Gran Canaria, 2023

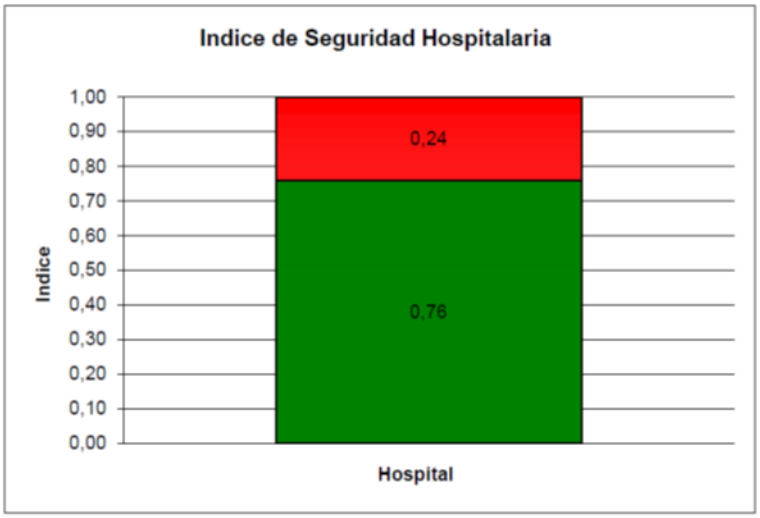


Figura 32

Resultados alcanzados en Clínica la Cajal, Las Palmas de Gran Canaria, Islas Canarias, 2023

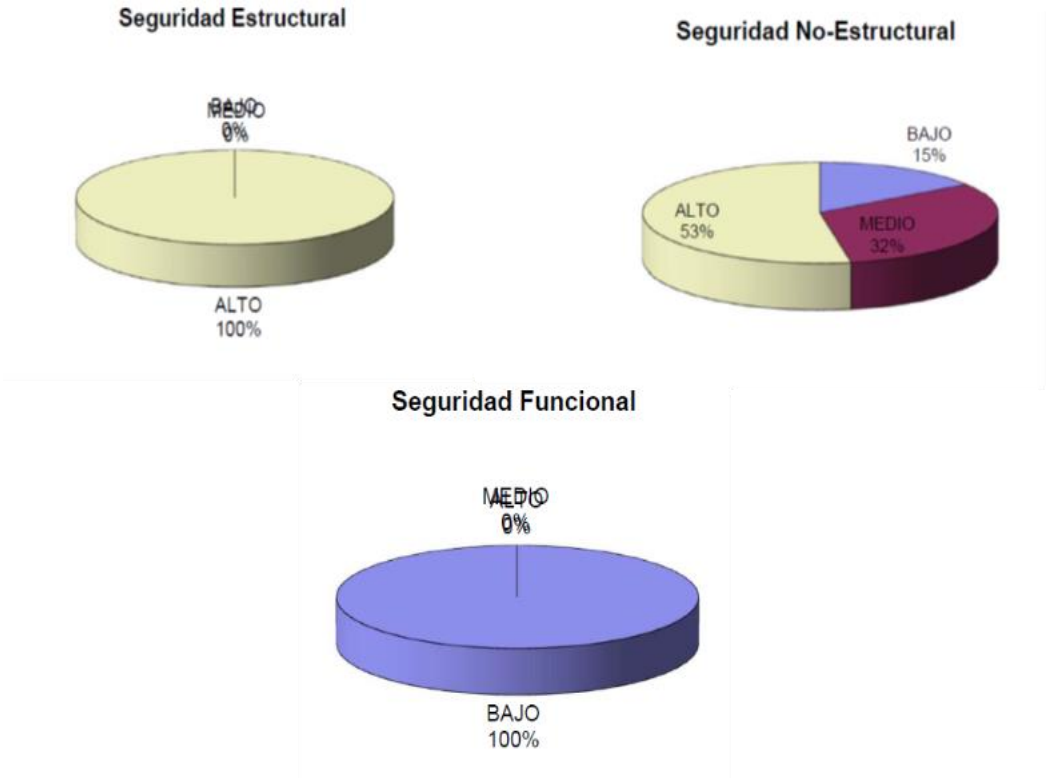


Figura 33

Representación del Índice de Seguridad Hospitalaria en Clínica la Cajal, Las Palmas de Gran Canaria, Islas Canarias, 2023

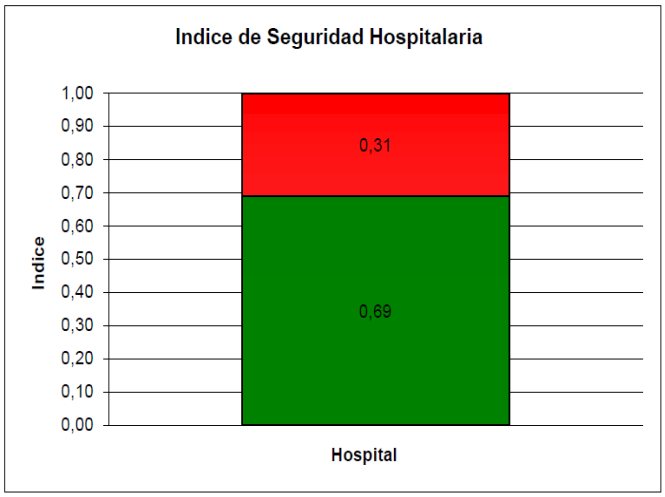


Figura 34

Resultados alcanzados en el Hospital Clínico Universitario Virgen de la Arrixaca, El Palmar, Murcia, 2023

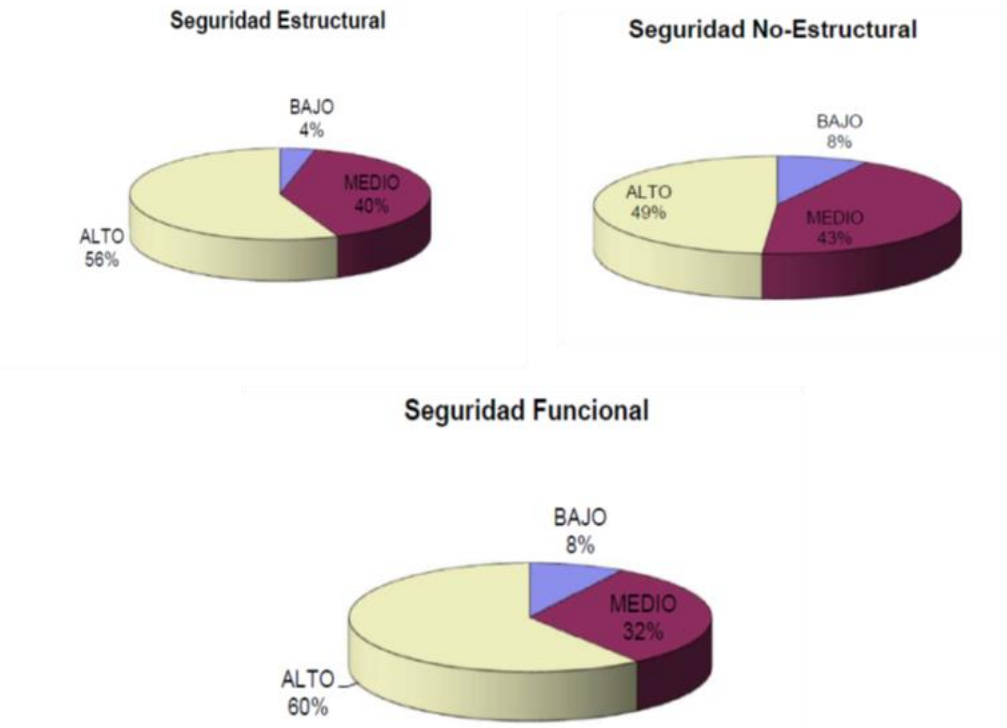


Figura 35

Representación del Índice de Seguridad Hospitalaria en el Hospital Universitario Virgen de Arrixaca, El Palmar, Murcia, 2023

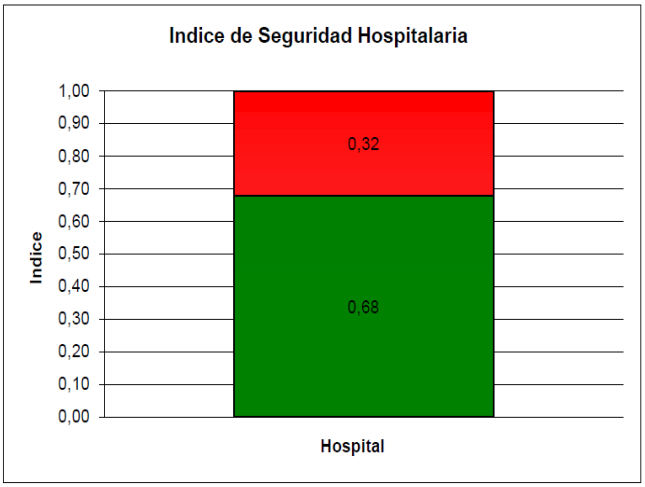


Figura 36

Resultados alcanzados en Hospitales San Roque, Las Palmas de Gran Canaria, Islas Canarias, 2023

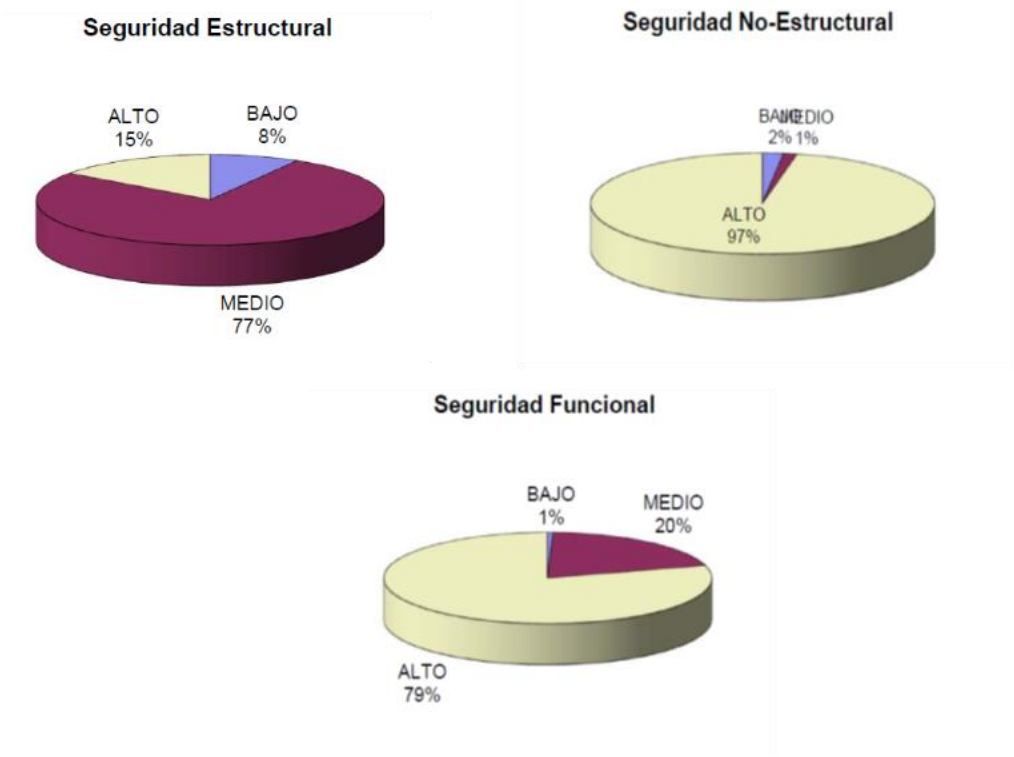


Figura 37

Representación del Índice de Seguridad en Hospitales San Roque, Las Palmas de Gran Canaria, Islas Canarias, 2023

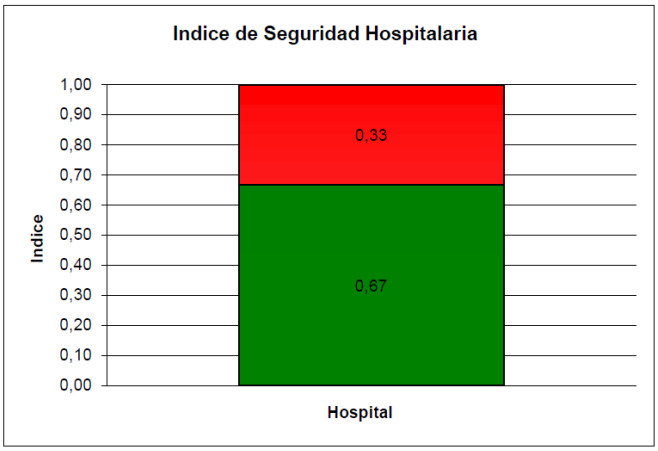


Figura 38

Resultados alcanzados en Vithas Hospital Nisa Pardo de Aravaca, Madrid, 2023

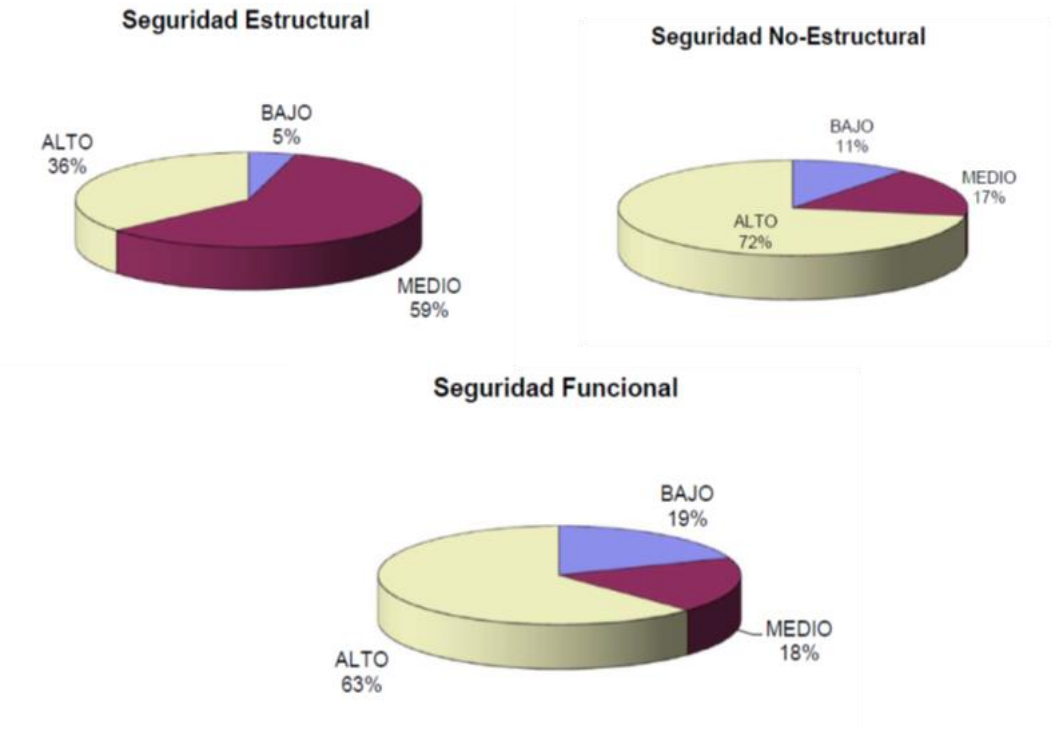


Figura 39

Representación del Índice de Seguridad en Vithas Hospital Nisa Pardo de Aravaca, Madrid, 2023

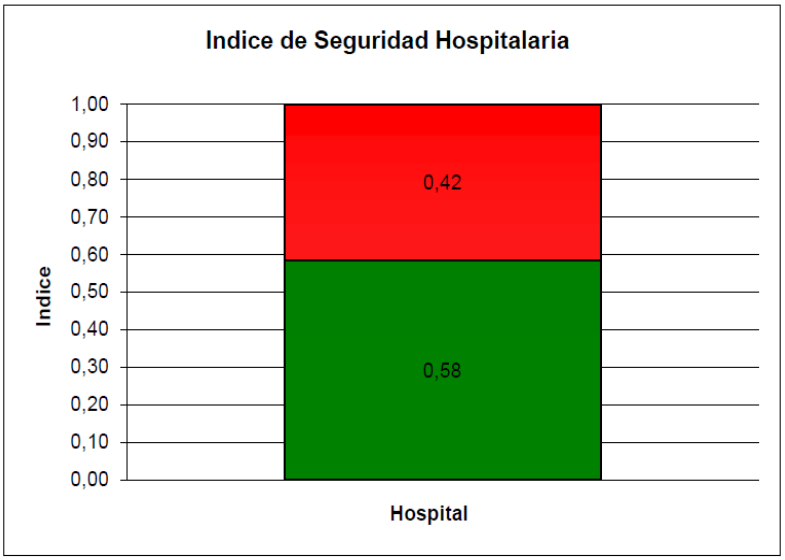


Figura 40

Resultados alcanzados en el Hospital Universitario de la Paz, Madrid, 2023

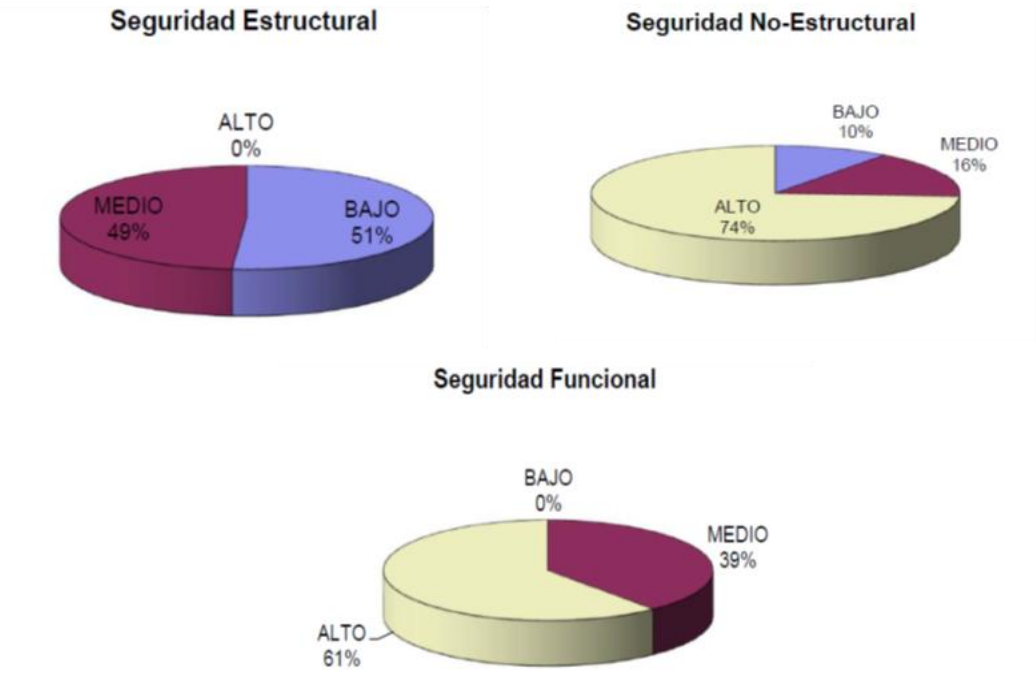


Figura 41

Representación del Índice de Seguridad Hospitalaria en el Hospital Universitario de la Paz, Madrid, 2023

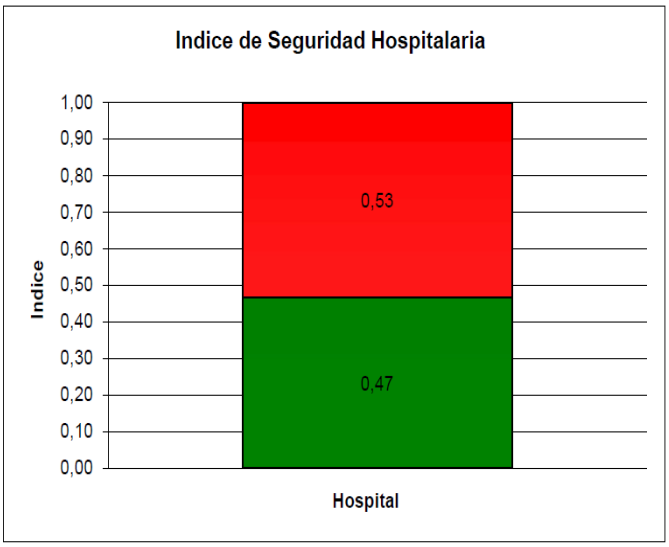


Figura 42

Resultados alcanzados del Hospital General Universitario Gregorio Marañón, Madrid, 2023

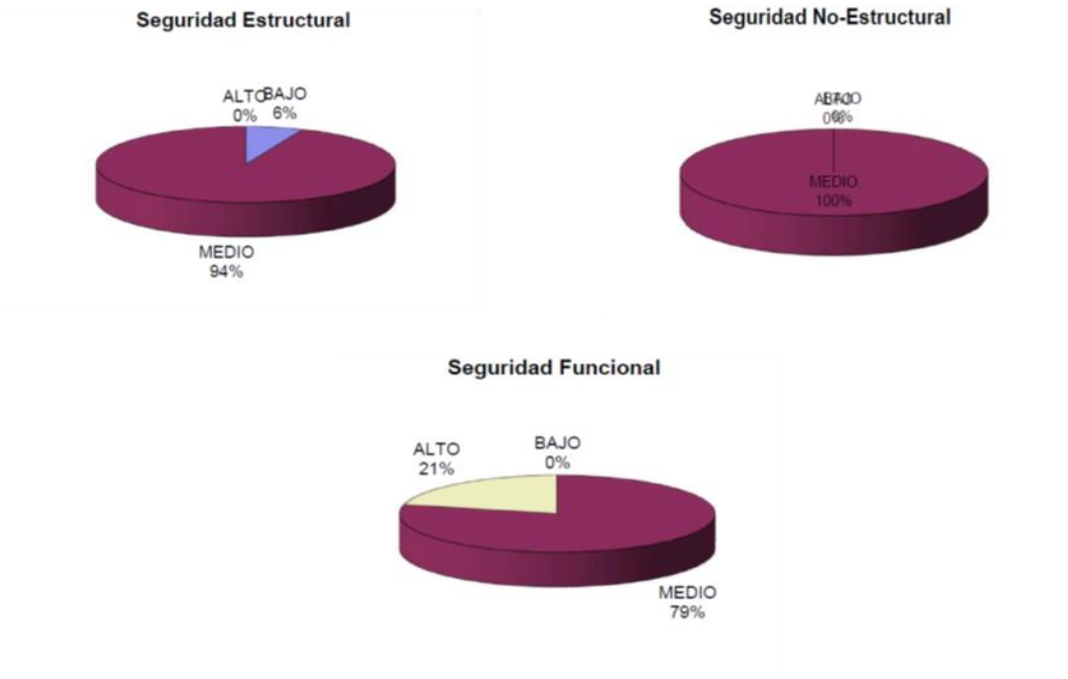
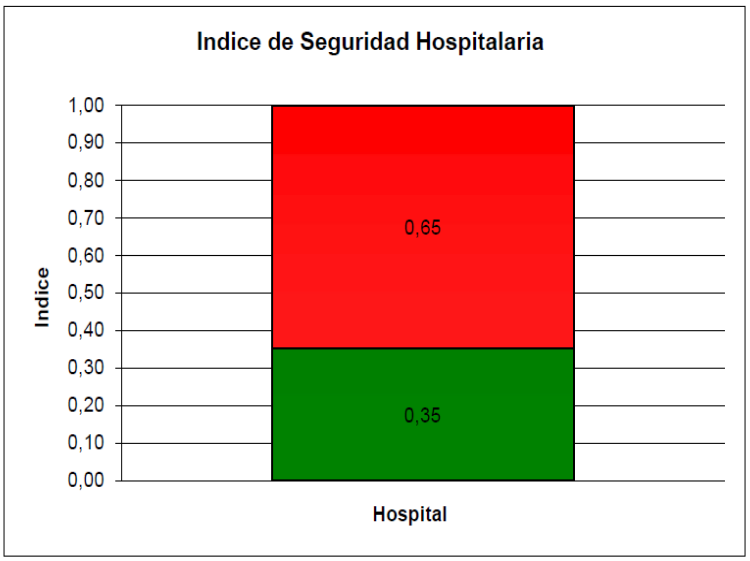


Figura 43

Representación del Índice de Seguridad Hospitalaria en el Hospital General Universitario Gregorio Marañón, Madrid, 2023



Representados los diferentes Niveles alcanzados sobre la Seguridad Hospitalaria, en los gráficos anteriores, bajo el criterio de Bajo, Medio y Alto, se observa los índices alcanzados en cada Hospital.

Con el objetivo de disponer de una visión global de los Resultados registrados, a modo de resumen presentamos las tablas con las puntuaciones porcentuales de cada uno de ellos, a la vez que hemos realizado el cálculo de los estadísticos Media y Desviación Estándar, para observar el estado de la cuestión (Tabla 2).

Tabla 2

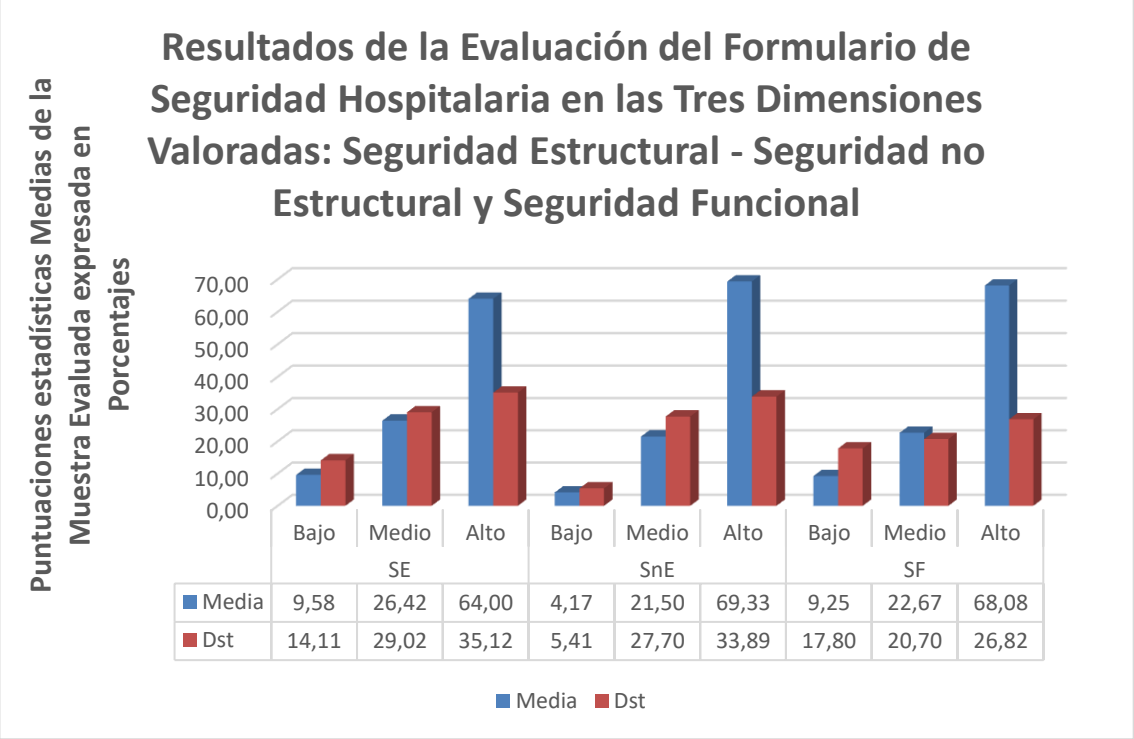
Datos de los Hospitales Participantes

	Análisis de datos de los Hospitales participantes en la Muestra Disponible									
	Niveles de Seguridad Hospitalaria	SE			SnE			SF		
N	Hospitales Participantes	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
1	Hospital Universitario Doctor Juan Negrín	0	7	93	0	3	97	0	11	89
2	Hospital Universitario Son Espases, Mallorca	0	0	100	0	17	83	15	22	63
3	Hospital San Roque de Meloneras, Gran Canaria	0	22	78	0	1	99	0	9	91
4	Hospital Universitario Materno-Infantil de Gran Canaria	12	19	69	0	8	92	3	10	87
5	Hospital Nisa del Rey Don Jaime, Castellón de La Plana	12	19	69	0	8	92	3	10	87
6	Vithas Hospitales de Las Palmas de Gran Canaria	10	0	90	4	12	84	62	22	16
7	Clínica la Cajal, Las Palmas de Gran Canaria	0	0	100	15	32	53	0	0	100
8	Hospital Clínico Universitario Virgen de la Arrixaca, El Palmar	4	40	56	8	43	49	8	32	60
9	Hospitales San Roque, Las Palmas de Gran Canaria	15	8	77	2	1	97	1	20	79
10	Hospital Nisa Pardo de Aravaca, Hospital Universitario Vithas	5	59	36	11	17	12	19	18	63
11	Hospital Universitario de la Paz, Madrid	51	49	0	10	16	74	0	39	61
12	Hospital General Universitario Gregorio Marañón	6	94	0	0	100	0	0	79	21
	Media	9,58	26,42	64,00	4,17	21,50	69,33	9,25	22,67	68,08
	Dst	14,11	29,02	35,12	5,41	27,70	33,89	17,80	20,70	26,82
	N	12	12	12	12	12	12	12	12	12

En ocasiones, una representación de la información, ilustra un poco mejor los datos anteriores, es lo que presentamos en la Figura 44.

Figura 44

Niveles Medios de la Seguridad Hospitalaria en Seguridad Estructural (SE), Seguridad no Estructural (SnE) y Seguridad Funcional (SF).



Interesante observar que en su conjunto son los Niveles no Estructurales y los Funcionales de Seguridad los que más destacan, aun cuando no podemos considerar que las diferencias sean significativas, para ello se hace necesario otro tipo de análisis estadísticos, en esta ocasión nos limitamos a presentar datos descriptivos solamente.

Con respecto a los Valores calculados para los Índices de Seguridad Hospitalaria, hemos registrado las puntuaciones en la Tabla 3.

Tabla 3

Valores del Índice de Seguridad en los Hospitales Evaluados

	Valores del Índice de Seguridad en los Hospitales Evaluados	Indice de Seguridad Hospitalario		
N	Nombre del Hospital	Inseguridad	Seguridad	Diferencia
1	Hospital Universitario Doctor Juan Negrín	5	95	90
2	Hospital Universitario Son Espases, Mallorca	9	91	82
3	Hospital San Roque de Meloneras, Gran Canaria	9	91	82
4	Hospital Universitario Materno-Infantil de Gran Canaria	16	84	68
5	Hospital Nisa del Rey Don Jaime, Castellón de La Plana	19	81	62
6	Vithas Hospitales de Las Palmas de Gran Canaria	24	76	52
7	Clínica la Cajal, Las Palmas de Gran Canaria	31	69	38
8	Hospital Clínico Universitario Virgen de la Arrixaca, El Palmar	32	68	36
9	Hospitales San Roque, Las Palmas de Gran Canaria	33	67	34
10	Hospital Nisa Pardo de Aravaca, Hospital Universitario Vithas	42	58	16
11	Hospital Universitario de la Paz, Madrid	53	47	-6
12	Hospital General Universitario Gregorio Marañón	65	35	-30
	Media	**28,17**	**71,83**	**43,67**
	Std	**18,42**	**18,42**	**36,84**
	N	**12**	**12**	12

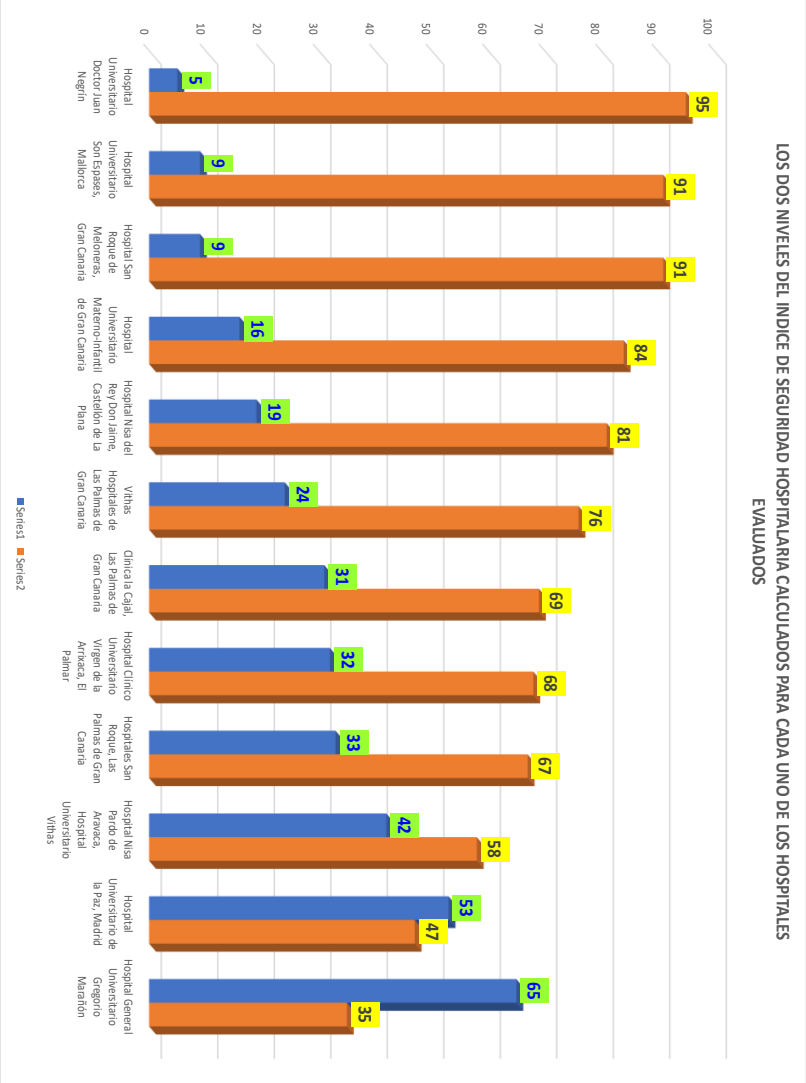
Del cálculo realizado en la Tabla anterior presentado, con valores enteros, entendiendo que son Índices Calculados, según la Fórmula aplicada en el Formulario del Modelo Matemático de la Organización Mundial de la Salud, para tener una imagen más comprensible de dichos datos.

Se observan comportamientos curiosos en los valores de los Hospitales Evaluados. Hemos puesto en orden cada uno de ellos, considerando dichos valores de manera decreciente con respecto a la Seguridad en General, destacando la gran mayoría como seguros y descubriendo dos de ellos con señales indicadoras de necesidad de actuación.

La representación gráfica de las puntuaciones medias de los Índices de Seguridad Hospitalaria es lo que presentamos en la Figura 45.

Figura 45

Valoración Media de los Índices de Seguridad Hospitalaria en el grupo de Hospitales Evaluados.



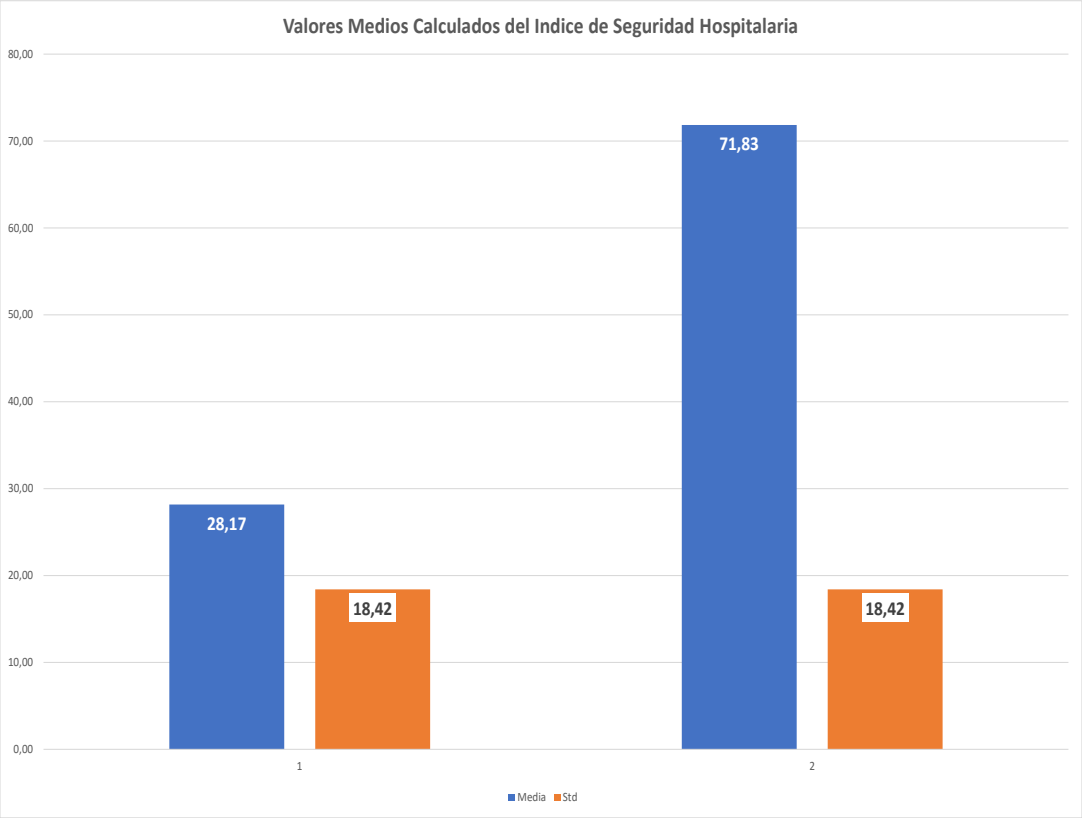
A partir de los Resultados conseguidos con el Formulario aplicado, se observa que en general hay un Índice de Seguridad Hospitalaria notable, con niveles de Seguridad Funcional, No Estructural y Estructural, por este orden adecuado, desde una orientación global. Pero lo interesante de nuestra investigación, reside en disponer de una herramienta útil para llevar a cabo evaluaciones precisas e identificar las fortalezas y debilidades en cuestiones de Seguridad Hospitalaria.

Las representaciones gráficas se han obtenido a través de las puntuaciones medias globales de todos los casos evaluados, valoración media de interés en atención a futuras investigaciones.

Es precisamente el modelo médico de evaluación el que no puede orientar para llevar a cabo las intervenciones precisas y para ello hay que llevar a cabo el diagnóstico pertinente de cada Centro Hospitalario Evaluado, como se puede observar en la siguiente Figura 46.

Figura 46

Evaluación de Seguridad Hospitalaria por Centros



Es a partir de los datos, cuando estamos en condiciones de llevar a cabo la discusión objetiva de los Resultados, a la luz de las investigaciones previas analizadas en la primera parte de la presente Tesis. Cuestión que pasamos a describir en el siguiente apartado.

4.10. DISCUSIÓN Y REFLEXIONES

En relación a los resultados hemos de considerar el bajo porcentaje extrapolable al índice de Seguridad Hospitalaria que en general los distintos hospitales evaluados se trazaban con los elementos estructurales, lo que sugiere una infraestructura obsoleta, o en su caso con un inadecuado mantenimiento.

En relación a los resultados que se trazan directamente con los factores no estructurales sus resultados han sido mucho mejor lo que incide positivamente en el resultado al alza del Índice de Seguridad Hospitalaria, concretamente en aspectos tales como las distintas instalaciones (sistema eléctrico, abastecimiento de agua, telecomunicaciones y gases medicinales), denominados en el Modelo Matemático como Líneas vitales. En cualquier caso, las líneas vitales han de ser elementos de minuciosa consideración, todo ello porque pueden incrementar la vulnerabilidad y magnificar ante cualquier tipo de daño sus efectos.

También arrojan un resultado favorable los distintos sistemas de calefacción, ventilación, aire acondicionado en Áreas Críticas.

En relación al mobiliario de oficinas, equipos de oficinas y almacenes, equipos médicos de laboratorios y suministros utilizados para el diagnóstico y tratamiento, también tienen una ponderación bastante aceptable, así como los elementos arquitectónicos, tales como las condiciones de las puertas, escaleras, ascensores, protección contra incendios, iluminación, tanto externa como interna.

En relación a los aspectos relacionados con la seguridad en base a la capacidad funcional, son valorados positivamente en atención a sus resultados, pero de manera genérica, salvo algún hospital.

Se hace necesaria la realización de simulacros, ya no sólo los relacionados con la Autoprotección de los distintos hospitales, al preguntárseles por estos aspectos, en relación a su implementación periódica, se constata que, algunos hospitales no lo han hecho en varios años. Máxime cuando hay una norma que obliga como mínimo a su realización anual con carácter mínimo.

En relación a las emergencias externas, nunca se ha realizado una actuación coordinada en la que todos los hospitales de una zona o región activen dicho procedimiento con el objeto de establecer las distintas sinergias de colaboración y poder atender, ya no sólo a los distintos pacientes que estaban ingresados, sino a aquellos que sufren alguna patología o lesión a

causas de la emergencia, indistintamente de sus causas. La formación global para aunar en el concepto de coordinación de todos los equipos de emergencia internos como externos se hace imprescindible para garantizar la seguridad hospitalaria y por ende, de cuántas personas se encuentren en esas Infraestructuras Críticas.

4.11. PERSPECTIVAS FUTURAS Y PROPUESTAS DE INVESTIGACIÓN

En relación con posibles líneas de investigación científica proponemos buscar un consenso internacional a la hora de la clasificación de los riesgos, por una cuestión de coherencia conceptual y por una mejor y más objetiva evaluación de los distintos riesgos tras su identificación.

Implementar en el Formulario aspectos de relevancia que no se consideran en el actual para incorporarlo plenamente en el contexto específico, legal y geoestratégico de la Unión Europea, con el objeto de integrar una matriz de riesgos mucho más completa en base a una adecuada taxonomía de los riesgos, tanto generales como específicos.

Ahondar en investigaciones específicas en relación a la piedra angular en cualquier tipo de situación de Emergencia o Catástrofe, la Coordinación, tango de los distintos equipos internos de emergencias de las distintas organizaciones sanitarias hospitalarias, como a los Equipos Externos de Emergencia como la adecuada coordinación de toda la Red de Hospitales, para su adecuada activación del Plan de Emergencias Extra hospitalarias.

Investigar en las adecuadas estrategias que ayuden al cumplimiento legal en materia de formación y simulacros de emergencia en los hospitales, en especial aquellos de titularidad pública, para que deje de ser un mero requerimiento y un mero cumplimiento documental, todo ello a través de auditorías específicas externas en la materia para, de esa manera estudiar si existe un mayor cumplimiento de los aspectos referenciados y comprobar si produce una mejora en la respuesta y así poder garantizar que los hospitales en España y por ende en el resto del marco de la Unión Europea, son ciertamente, a tenor de las herramientas que hemos presentado en la presente investigación, «Hospitales Seguros».

Investigar sobre la mejora de la Resiliencia y continuidad de la prestación de los Servicios asistenciales hospitalarios en el diseño de hospitales seguros que se articulen y se planifiquen a modo de Campus Hospitalario, con lo que esa separación o disgregación de los distintos servicios en módulos hospitalarios favorecerá su gobernanza durante la gestión de cualquier tipo de contingencia, emergencia, catástrofe, desastre o calamidad pública.

Entendemos que se ha de seguir profundizando en estos asuntos, considerados de vital importancia y orientados siempre por una filosofía preventiva, de ahí la importancia que le hemos dado a la utilización de instrumentos, en nuestro caso el Formulario aplicado. Por tanto tenemos la necesidad de adaptar dicho instrumento a la realidad de España, en un primer momento, para disponer de una herramienta válida y fiable que se llegue a estandarizar y sea adecuada para aplicar en múltiples situaciones y contextos hospitalarios y que a la vez participen todos los agentes implicados y pueda, por ende ser de utilidad en todo el contexto de Europa.

Es nuestra intención seguir investigando en esta línea y por ello incluimos en los Anexos de esta Tesis, un borrador nuestra nueva propuesta investigadora, que hemos acuñado con el nombre de Escala de Valoración del Índice de Seguridad Hospitalaria (EVISH). Escala que hemos incluido como compromiso de investigaciones futuras, ya no individual, sino cooperativa y colaborativa para aportar datos que nos lleven a comprender, explicar y predecir[83] cuestiones relacionadas con la Seguridad Hospitalaria a nivel europeo.

Para ello se ha cogido el mismo modelo del Formulario del Índice de Seguridad Hospitalaria y hemos realizado una primera propuesta de adaptación para que pueda ser utilizado en un futuro en el contexto de la Unión Europea. Recoge las mismas cuestiones y factores. En esa adaptación se llevarán a cabo todas las actuaciones y cálculos, que incluyen las pruebas de validez y fiabilidad, sino también el análisis factorial con el objeto de comprobar si los factores, dimensiones y las matices que existen y se han definido para estandarizarlo en un contexto europeo global, para hacer un análisis estructural si las cuestiones que se plantean están agrupadas según las categorías que el Modelo Matemático ha definido.

El EVISH, inicialmente está creado en una tabla Excel en el que pueden incorporarse las distintas respuestas a través de una pestaña en cada casilla celda correspondiente en la que a través de un desplegable puede establecerse la respuesta considerada. El rango de respuestas comprende:

(M) = Muy probable.

(B) = Bastante probable.

(R) = Regular.

[83] Tal y como establece Mario Bunge en su obra «El Método Científico».

(P) = Poco probable.

(N) = Nada probable.

CONCLUSIONES

En el presente apartado recogemos aquellas conclusiones que nos parecen significativas en la investigación que hemos desarrollado entre las que destacan:

1. En relación a la pertinencia del Formulario hemos de decir que significa una sólida y buena base, pero que ha de adaptarse con contexto hospitalario europeo en atención a los distintos riesgos específicos y al resto de la legislación que en la materia pueda afectar.

   Todo ello puede materializarse de dos maneras posibles, la primera adaptándolo a riesgos específicos, en especial aquellos relacionados con la ciberseguridad, Protección de Datos, así como en el contexto de cualquier acción terrorista, bien a través del ciberespacio, o bien atacando áreas críticas de los hospitales (ya estudiadas con anterioridad en su capítulo correspondiente) que, magnificaría el efecto del daño causado.

   Con el objeto de garantizar la gobernanza es imprescindible preparar con ejercicios, formación y simulacros ante las distintas emergencias que puedan producirse por cualquier riesgo, indistintamente de su naturaleza.

   Es imperativo que en la realización de los distintos simulacros se active el Plan de Emergencias extra centro para que el resto de hospitales pueda también establecer una respuesta coordinada que, a su vez les sirva de preparación, todo ello relacionado con la seguridad funcional. Tal aspecto debe de materializarse en una ley que establezca tal obligatoriedad, con el objetivo de ahondar en el concepto de coordinación, aspecto de especial relevancia y la piedra angular de cualquier actuación en emergencias.

   Todas y cada una de las cuestiones que afectan a las Infraestructuras Críticas en general, así como a las Infraestructuras Críticas Hospitalarias en particular, afectan directa y transversalmente al concepto integral de Seguridad Humana como cuestión que integra todas y cada una de las seguridades, o si se prefiere, el resto de «subseguridades».

2. Es imprescindible una taxonomía de riesgos estandarizada y universal para poder planificar las adecuadas respuestas con el objeto de su mitigación, neutralización, reducción o control.

3. El Formulario Índice de Seguridad Hospitalaria podría ser válido ante los distintos Riesgos Antrópicos de Carácter Antisocial, también frente al fenómeno o al riesgo terrorista, pero habría que modificarse para su incorporación, o bien realizar una nueva edición integradora, en la que además, se realice el cálculo estadístico, no con un Modelo Matemático en una hoja de Excel, sino con paquetes o *softwares* estadísticos muchos más potentes en el campo de la investigación científica, con los que, una vez adaptados, o generada una nueva versión, contemplando un nuevo diseño desde el origen, pueda estudiarse su validez, consistencia, así como los distintos factores correlacionales.

4. En relación a las principales vulnerabilidades detectadas en la investigación, hemos de considerar que los distintos hospitales tendrían que hacer un mayor esfuerzo en el diseño, así como el adecuado mantenimiento de los aspectos relacionados con la seguridad estructural, de gran importancia para que no colapsen, así como que sean lo más resistentes posibles ante cualquier tipo de riesgo que pueda materializarse.

   Lo propio en lo que respecta a la seguridad funcional, tales como institucionalizar, dar formación específica a los miembros integrantes de los distintos comités para desastres, adecuar zonas específicas debidamente dotada de medios para que los distintos centros de operaciones de emergencias sean operativos desde el pragmatismo, actualizar y realizar la formación periódica y simulacros correspondientes al Plan Operativo para desastres internos (Plan de Autoprotección), así como los externos, trabajar racionalmente sobre los distintos planes de contingencia, facilitar la disponibilidad de medicamentos, insumos, instrumental y equipos específicos para desastres.

5. El presente Formulario Índice de Seguridad Hospitalaria es un buen punto de partida con el que poder seguir investigando en el contexto de las Infraestructuras Críticas Hospitalarias en el entorno europeo de la que España forma parte.

6. Es imprescindible la constitución de un Comité de Expertos de carácter multidisciplinar con los que pueda mejorarse, en el contexto Europeo el formulario o bien diseñar un instrumento al efecto que, se adapte a la realidad geoestratégica, socioeconómica, legal y política de la Unión Europea. El EVISH que hemos propuesto en la presente investigación también podría ser un punto de partida para futuras investigaciones.

7. La evaluación del índice de seguridad hospitalaria de la OMS, en el contexto de las Infraestructuras Críticas Hospitalarias, frente a cualquier tipo de riesgo, indistintamente de su naturaleza, y se creara una nueva matriz de riesgos, tras el establecimiento de una taxonomía con rigor científico, y se adaptara convenientemente el ISH, o se diseñara una herramienta similar desde el origen, con un enfoque integrador e integrado, en el que participen un comité de expertos en seguridad hospitalaria y sus diferentes áreas, así como otros actores y expertos en Infraestructuras Críticas. Sin duda alguna, proporcionaría información valiosa para mejorar la seguridad, la protección integral y la resiliencia de los hospitales europeos que, a nuestro juicio, podría tener implicaciones más amplias a nivel internacional.

8. La creación de un Grupo de Investigación Reconocido (GIR) en materia de terrorismo, Infraestructuras Críticas y seguridad hospitalaria, como vector de transmisión del conocimiento a través de la investigación científica, tendría una serie de importantes implicaciones y beneficios que redundarían a la sociedad, fundamental para avanzar en la comprensión y protección contra las amenazas terroristas, así como para fortalecer la gobernanza y por ende la resiliencia de las comunidades y las instituciones ante estos y cualquier tipo de riesgos, todo ello por:

   - ✓ Enfoque especializado: entendemos que un GIR dedicado a la presente área de conocimiento permitiría concentrar recursos humanos, financieros y tecnológicos en la investigación específica de terrorismo, Infraestructuras Críticas y seguridad hospitalaria. Esto facilitaría un enfoque más especializado y profundo en un área de importancia crítica para la seguridad pública.
   - ✓ Generación de conocimiento: el GIR contribuiría significativamente a la generación de conocimiento en este campo. Investigaciones innovadoras y análisis rigurosos podrían producir información valiosa sobre las amenazas actuales y emergentes relacionadas con el terrorismo, así como sobre las mejores prácticas para proteger las Infraestructuras Críticas, incluidos los hospitales.
   - ✓ Desarrollo de herramientas y metodologías: el grupo tendría la capacidad de desarrollar herramientas, metodologías y marcos de evaluación específicos para la protección de Infraestructuras Críticas y la seguridad hospitalaria. Esto incluiría la adaptación y mejora de índices de seguridad existentes, como el índice de seguridad hospitalaria de la OMS, para abordar las necesidades específicas en el contexto del terrorismo.

- ✓ Asesoramiento y consultoría: el GIR podría proporcionar asesoramiento y consultoría especializada a gobiernos, organizaciones de salud y otras entidades interesadas en mejorar su capacidad para hacer frente a amenazas terroristas y proteger Infraestructuras Críticas, como los hospitales. Esto podría incluir la evaluación de riesgos, la planificación de seguridad y la capacitación del personal.
- ✓ Colaboración multidisciplinar: la creación de un GIR fomentaría la colaboración multidisciplinaria entre investigadores de diversas áreas, como la seguridad, la medicina, la ingeniería, la psicología, así como profesionales de prestigio. Esta colaboración interdisciplinaria es fundamental para abordar la complejidad de las amenazas terroristas y desarrollar soluciones efectivas y holísticas, en el que la universidad ha de ser vanguardia y punta de lanza al liderar la investigación con Personal Docente e Investigador (PDI) expertos en la materia.
- ✓ Fortalecimiento de la resiliencia y la gobernanza de las Infraestructuras Críticas: al investigar y desarrollar estrategias para proteger las Infraestructuras Críticas, incluidos los hospitales, el GIR contribuiría al fortalecimiento de la resiliencia de la sociedad frente a las amenazas terroristas. Esto incluiría medidas para prevenir ataques, mitigar impactos y facilitar la recuperación rápida y efectiva en caso de incidentes.

REFERENCIAS

REFERENCIAS BIBLIOGRÁFICAS

A., D. F. (2013). *Diccionario Inteligencia y Seguridad*. Ministerio de la Presidencia.

A., D. F. (2013). *Diccionario LID Inteligencia y Seguridad*. Ministerio de Presidencia.

AEI Seguridad. (2012). *Protección de Infraestructuras Críticas: Guía para la elaboración de planes de seguridad del operador y Planes de protección específica*. Recuperado de: https://www.aeiciberseguridad.es/GuiaPIC.pdf

Alcalde, J. J. (2008). *Los Servicios Secretos en España*. Madrid: E-books UCM.

Alonso, J. (mayo 2018). Protección frente a nuevas amenazas. *Cuadernos de Seguridad,* (333), 30-31. www.cuadernosdeseguridad.com

Amorós, A. (2019). *El papel de los medios de comunicación españoles durante los conflictos armados.* [Trabajo de fin de grado]. Facultad de Periodismo de la Universidad de Sevilla. Material sin publicar.

Anabalón, J., & Donders, E. (2014). Una revisión de ciberdefensa de Infraestructura Crítica . *Revista Estudios de Seguridad y Defensa, 3*, 131- 164.

Annan, K.A. (2000). *Millenium Report of the secretary-General of the UN We the Peoples-The role of the United Nations in the 21 Century*. United Nations Departament of Public Information. New York.

Aparicio, P. (julio-agosto 2019). Debemos avanzar en la homogeneización de las normas de seguridad en todos los centros sanitarios. *Seguritecnia,* (466), 70-72. www.seguritecnia.es

Aparicio-Ordaz, L.A. (2012). Enfrentamientos asimétricos. La respuesta del estado español frente a la amenaza del terrorismo: Asimetría y Simetría en el conflicto. *Saberes Revista de estudios jurídicos, económicos y sociales, vol.10.*

Aprimatc (abril 2018).Seguridad, control de accesos y soluciones antiterrorista. *Cuadernos de Seguridad,* (332), 88-89. www.cuadernosdeseguridad.com

Aragonés, L. M. (1998). Medios de comunicación social. Influencia en los conflictos armados. *Boletín de Información*, (255), 7.

Ariza, D. (2021, 15 septiembre). Tácticas, Técnicas y Procedimientos (TTP). *AFS Informática.*https://www.afsinformatica.com/tacticas-tecnicas-y-procedimientos-ttp/

Art.1 Ley 11/2002. (s.f.). Obtenido de Ley 11/2002, de 6 de mayo, reguladora del CentroNacional Inteligencia: https://www.boe.es/buscar/pdf/2002/BOE-A-2002-8628-consolidado.pdf

Austral, J. y Labrado, E. (2021). *Dos grados centígrados más. Una aproximación al cambio climático como vector y acelerante de tendencias que puede convertirse en una amenaza a la seguridad nacional y europea*. Documento Marco. ieee.es

Ballbé, M. (2006). "Seguridad Humana: del Estado anómico al Estado regulador", Prólogo a Hood, C., et al., El gobierno del riesgo, Ariel.

Ballbé, M. (2007). "El futuro del derecho administrativo en la globalización: entre la americanización y la europeización", RAP, 174.

Ballbé, M. & Martínez, R. (2010). *"Law and globalization: between the United States and Europe",* en J. Robalino y J. Rodriguez-Arana (eds.): Global administrative law, Londres, Cameron May. Pag. 137.

Ballesteros, S. (2014). La Atención Selectiva Modula El Procesamiento De La Información Y La Memoria Implícita. *Acción Psicológica*, 11(1), 7–20. https://doi.org/10.5944/ap.1.1.13788

Bargués, P. (2022). Conflicto híbrido, guerra total. *Opinión CIDOB, 5.* Recuperado de: https://n9.cl/za65b

Berntsen, G. y Pezzullo, R. (2014). *Human Intelligence: Counter terrorism and National Leadership" (Inteligencia Humana: Contraterrorismo y Liderazgo Nacional)* Editorial: Potomac Books.

Bilbao, J.V. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 156, 157, 165, 166.

Blanco, M.M. (22 de abril de 2020). *Las implicaciones del agua como recurso estratégico: escasez hídrica y conflicto en el Sahel.* Bie 3: Boletín IEEE. https://dialnet.unirioja.es/servlet/articulo?codigo=7552071

Blas, L. E. (2020). *Ciberguerra desde el Kremlin: Las capacidades cibernéticas rusas como herramienta para mantener su esfera de influencia.* Universidad Pontificia Comillas. [Trabajo fin de Grado]. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/40796/TFG%20-%20Blas%20Barba%2c%20Luis%20Enrique.pdf?sequence=1&isAllowed=y

Blog Think Big, (2022, 11 mayo). *OSINT: en qué consiste la open source intelligence*. https://blogthinkbig.com/open-source-inteligence-que-hay-detras-de-osint

Blum I. & Williams H. (2018). Obtenido de *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise:* https://www.rand.org/pubs/research_reports/RR1964.html

Bonilla, D. (2009). El alma de la victoria. Estudios sobre inteligencia estratégica. Madrid: Plaza y Valdés.

Borrell, J. (2022). *La nueva Europa de la Defensa y la Brújula Estratégica.* Fundación Feindef. Ministerio de Defensa. https://publicaciones.defensa.gob.es/media/downloadable/files/links/l/a/la_nueva_europa_defensa_y__brujula_estrategica.pdf

Bradford, W. H. (1997). *Internacional Journal of Intelligence and Counter intelligence*.

Bruneau, T. y. (2007). *Reforming Intelligence. Obstacles to Democratic Control and Effectiveness.* Estados Unidos: University of Texas Press.

Bustamante, J. (2 de febrero de 2022). Obtenido de ¿Qué es el nombre de dominio y cómo elegirlo correctamente?: https://www.presteamshop.com/blog/que-es-un-nombre-dedominio/

Calvo, J.L. (2020). Implicaciones del ámbito cognitivo en las Operaciones Militares. Documento de trabajo. *Centro Superior de Estudios de la Defensa Nacional (CESEDEN, IEEE).* https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf

Canadian Land Force. (2004). *Intelligence, Surveillance, Target Acquisition and Reconnaissance* (Istar) (English).B-Gl-352-001/Fp-001, 113.

Cano, M. A. (2011). *El binomio Internet/terrorismo islamista*. Iter Criminis.

Caro Bejarano, M. J. (2011). La protección de las Infraestructuras Críticas. *Documento de Análisis. Instituto Español de Estudios Estratégicos, 21.*

Castillo Arranz, J. (2022). PwC Digital Trust Insights 2023. Conclusiones de la encuesta mundial sobre el presente y futuro de la ciberseguridad. *Revista SIC: ciberseguridad, seguridad de la información y privacidad, 31(152),* 176-179.

CCN. (09 de junio de 2023). *Defensa frente a las ciberamenazas. Detección temprana de amenazas en Sistemas de Control Industrial*. Recuperado de: https://n9.cl/02shfo

CCN. (2020). *Guía Nacional de Gestión y Notificación de Ciberincidentes*. Recuperado de: https://n9.cl/hs1sg

CCN. (2020). La ciberseguridad y su relevancia en el sector público. El papel del Centro Criptológico Nacional. *Revista Española de Control Externo, 22 (64),* 66-87.

CCN. *(s. f.). ENS. Esquema Nacional de Seguridad.* Recuperado 2 de mayo de 2023, de https://ens.ccn.cni.es/es/

Ceseden. (2018). *Instituto Español de Estudios Estratégicos*; Centro Superior de Estudios de la Defensa Nacional. http://www.ieee.es/Galerias/fichero/docs_trabajo/2018/DIEEET01-2018_Futuro_PCSD_ VisionDesdeSur.pdf

Chávez, R.M. (2019).*El papel de los medios de comunicación españoles durante los conflictos armados*. [Trabajo de fin de grado]. Universidad de Sevilla. https://idus.us.es/bitstream/handle/11441/92701/tfg%20%c3%81ngela%20Amor%c3%b3s%20Aguaded.pdf?sequence=1&isAllowed=y

Cherepanov, A. (2016, 11 enero). Black Energy by the SSH Bear Door: attacks against Ukrainian news media and electric industry. *We Live Security*. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

CIS. (2015). *Centro de Investigaciones Sociológicas*. Obtenido de Encuesta Social General Española: https://www.cis.es/cis/opencm/ES/1_encuestas/estudios/ver.jsp?estudio=14252.

Clark, R.M. (2012). *Intelligence Analysis: A Target-Centric Approach" (Análisis de Inteligencia: Un Enfoque Centrado en el Objetivo.)* CQ Press.

CNI. Inteligencia, C. N. (s.f.). *El Ciclo de la Inteligencia.* Obtenido de https://www.cni.es/la-inteligencia/direccion

Cohen, J., López, G., Pouy, J.L., y Urmeneta, M. (julio-agosto 2018). Las noticias falsas: un problema de siempre para combatir entre todos. *Cuadernos de Seguridad,* (335), 16-17. www.cuadernosdeseguridad.com

Collins. (2017). Obtenido de "*How the Collins Tesaurus is compiled*": https://www.collinsdictionary.com/word-lovers-blog/new/how-the-collins-thesaurusis-compiled,352,HCB.html

Consejo de Seguridad Nacional. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado*, de 30 de abril de 2019, núm. 103, pp. 43437-43455.

Cook, T. D., & Campbell, D. T. (1979*). Quasi-experimentation: Design and analysis issues for field settings.* Houghton Mifflin.

Corral, P. (2021, 17 septiembre). *El arma del fin del mundo.* La Razón. https://www.larazon.es/tecnologia/20210917/umsfdesa4jcq3ktdfke5oqmbaa.html

Correa-Henao, G. J. &Yusta-Loyo, J.M. (2013). Seguridad Energética y Protección de Infraestructuras Críticas, *Lámpsakos, 10,* 92-108.

Crumpton, H.A. (2012). *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service (El Arte de la Inteligencia: Lecciones de una vida en el Servicio Clandestino de la CIA).* Penguin Press.

CSOComputerworld.es. (9 de enero de 2023). Obtenido de *Gasto en Ciberseguridad y dificultades económicas en 2023*: https://cso.computerworld.es/tendencias/gasto-en-ciberseguridad-y-dificultades-economicas-en-2023

Cussac, J. G. (2012). Coordinador: *Inteligencia.* Valencia: Tirant lo Blanc.

Cussac, J. L. (2006). *Retos de la política criminal actual. Nuevas amenazas a la seguridad nacional: los desafíos del nuevo terrorismo*. Castellón: REGASP.

Cyware (2022). What *is Cyber Threat Intelligence Sharing? And Why Should You Care?* Cyware Educational Guides. Cyware Labs.https://cyware.com/security-guides/cyber-threat-intelligence/what-is-cyber-threat-intelligence-sharing-and-why-should-you-care-cfdc

Delgado, L. F. (2018). Dialnet.unirioja.es. Obtenido de *España y la Ciberseguridad: Hora de remangarse.* https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf

Deyimar, A. (15 de febrero de 2023). Obtenido de ¿Cómo funciona el SSH?: https://www.hostinger.es/tutoriales/que-es-ssh

Díaz Cuesta, J. F., Gómez López, J., & Quiñones de la Iglesia, J. (2023). La desinformación y la guerra híbrida: Instrumentalización de las narrativas informativas para entender la guerra del siglo XXI. *Comunicación y Hombre, 19*, 223- 232.

Díaz, E. (abril 2018).Garantizar la seguridad de los procesos es fundamental para nuestra actividad. *Cuadernos de Seguridad,* (332), 26-27. www.cuadernosdeseguridad.com

Díaz, G. (2008). *Hacia una definición inclusiva de Inteligencia*. Inteligencia y Seguridad.

Díez, E. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 203, 205.

Directiva NIS. EUR-Lex - 32016L1148 - EN - EUR-Lex. (n.d.). *Diario Oficial De La Unión Europea.* Retrieved January 21, 2023, from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016L1148

Dodge, C., & Burness, G. (2019). Policing Cybercrime: Responding to the growing problem and considering future solutions, *Human Factor of Cybercrime*, 339–358.

Dulles, A.W. (2006). *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World (El Arte de la Inteligencia: El Maestro de Espionaje Legendario de América sobre los Fundamentos de la Recopilación*

de Inteligencia para un Mundo Libre) Harper Perennial (originalmente publicado en 1963).

El Consejo de Seguridad Nacional DSN. (n.d.). *El Consejo de Seguridad Nacional*. DSN. Retrieved January 21, 2023, from: https://www.dsn.gob.es/es/sistema-seguridad-nacional/consejo-seguridad-nacional#collapseFour

España, H. (8 de febrero de 2022). CiberSeguritynews.es. Obtenido de *Cuatro consejos para desplegar una estrategia de ciberseguridad eficaz en las empresas*: https://cybersecuritynews.es/cuatro-consejos-para-desplegar-una-estrategia-de-ciberseguridad-eficaz-en-las-empresas/

Espinosa, O. (2023). *Redes Zone*. Obtenido de "Qué es y para qué sirve un Honeypot": https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/ Estrategia de Seguridad Nacional 2019.

Esteban, P. (2021). *Inteligencia compartida* [Grabado por S. s. Defensa.]. Madrid,España.

Esteve- Domínguez, M. (2020). *Aplicación de SIEMs a la protección de las Infraestructuras Críticas*. Universidad Politécnica de Valencia [Trabajo final de Grado]. Recuperado de: https://n9.cl/jkisd

Estratégicos, I. E. (2009). *LA INTELIGENCIA, FACTOR CLAVE FRENTE AL TERRORISMO INTERNACIONAL*. Madrid: Ministerio de Defensa.

Estratégicos., pp 7-36.

Étienne, B. (1996). *El islamismo radical.* Madrid: Siglo XXI.

Europea., C. E. (2022). consilium.europa.eu. Obtenido de *Ciberseguridad: cómo combate la UE las amenazas cibernéticas*: https://www.consilium.europa.eu/es/policies/cybersecurity/#defence

Fernández Pereira, J.P. (2005). *Seguridad Humana* [Tesis doctoral, Universidad Autónoma de Barcelona]. Programa de doctorado en Seguridad y prevención. https://www.iidh.ed.cr/multic/UserFiles/Biblioteca/IIDHSeguridad/12_2010/d540f1cb-719b-4b49-95b1-f61a7faa7ab2.pdf

Fernando, C. G. (2016). *Estado Islámico en España*. Madrid: Real Instituto Elcano.

Ferrero, J. (2013). La Ciberguerra. Génesis y evolución. *Revista General de Marina*, 86.

Fogelman, F. (2008) Mining Massive Data Sets for Security: Advances un Data Minning, Search, Social Networks and Text Minning, and Their Applications to Security. Página 58 de 67.

Fondón, A. (julio-agosto 2019). La seguridad en el entorno hospitalario. *Seguritecnia,* (466), 82-83. www.seguritecnia.es

Fondón, A. (septiembre 2017). Seguridad corporativa en constante evolución. *Seguritecnia,* (445), 100-101. www.seguritecnia.es

Fontaine, E. R. (2008). *Evaluación social de proyectos* .Pearson Educación. https://economicas.unsa.edu.ar/iie/archivos/syc/Fontaine.pdf

Formigo, J.C. (abril 2018). La perfecta coordinación entre las medidas de seguridad y el personal operativo es clave para una seguridad satisfactoria. *Cuadernos de Seguridad,* (332), 16-20. www.cuadernosdeseguridad.com

Galán, C. (2018). Amenazas híbridas: nuevas herramientas para viejas aspiraciones. *Real Instituto El Cano, Documento de Trabajo, 20*. Recuperado de: https://n9.cl/ulhyq

Galeano, S. (27 de enero de 2023). *marketing4ecommerce.net*. Obtenido de Cuáles son las redes sociales con más usuarios del mundo (2023): https://marketing4ecommerce.net/cuales-redes-sociales-con-mas-usuarios-mundoranking/

Galvache, F. (2004). *La Inteligencia Compartida en Estudios sobre Inteligencia.* EnF. Galvache Valero. Madrid: Instituto Español de Estudios Estratégicos.

Galván, J. (julio-agosto 2019). El director de Seguridad de un hospital no puede ser el responsable de mantenimiento. *Seguritecnia,* (466), 60-64. www.seguritecnia.es

Gálvez, L. (2019). *Ciberseguridad en las redes eléctricas*. Universidad Carlos III de Madrid. [Trabajo fin de Grado]. https://docs.google.com/viewerng/viewer?url=https://e-archivo.uc3m.es/bitstream/handle/10016/30475/TFG_Lucia_Galvez_Fernandez.pdf.

Gamero-Garrido, A. (2007), *Cyber Conflicts in International Relations*. Boston Massachusetts: Massachusetts Institute of Technology.

García de Enterría, E., Fernández, T.R., (2022). *Curso de Derecho Administrativo I.* Editorial Aranzadi Civitas.

García, F. R. (2013). *Los yihadistas en España: perfil sociodemográfico de condenados por actividades terroristas o muertos en acto de terrorismo suicida entre1996 y 2012.* En R. I. Elcano.

García, M.J. (2002) Mecanismos básicos de la propaganda de guerra en los medios informativos. El ejemplo de Kosovo. *Revista Internacional de Comunicación*. Nº 7-8. https://revistascientificas.us.es/index.php/Ambitos/article/view/9469.

García, S. (mayo 2016). Cambio de paradigma en la gestión de emergencias en hospitales. *Seguritecnia,* (431), 86-89. www.seguritecnia.es

García, S. (septiembre 2017). Instrucciones 3/2017 sobre agresiones al personal sanitario: un cambio de enfoque. *Seguritecnia,* (445), 90-92. www.seguritecnia.es

García, S. y Liguori, M. (julio-agosto 2019). Gestión de riesgos sobre personas con interés policial. *Seguritecnia,* (466), 66-69. www.seguritecnia.es

Germán, I. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco.

Gill, P. (2012). *Intelligence in an Insecure World (Inteligencia en un Mundo Inseguro).* Polity.

Gobierno de España, (2014). La Moncloa. *Francisco Martínez afirma en Luxemburgo ante la industria de Internet que la «colaboración público-privada es una herramienta clave en la lucha contra el yihadismo» en la Red*. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2014/101014jailuxemburgo.aspx

Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad*. Departamento de Seguridad Nacional. Ministerio de la Presidencia relaciones con las Cortes e Igualdad.

Gobierno de España. (2021). *Estrategia de Seguridad Nacional 2021*. Recuperado de https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2021/290121_SeguridadNacional.pdf

Gobierno de España. (2022). *España digital 2026.* Next Generation EU.https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

Gobierno de España. (2023). *Departamento de Seguridad Nacional*. Obtenido de Seguridad Nacional: https://www.dsn.gob.es/.

Gomes, C. (2017). *The new era of information as power and the field of CyberIntelligence*. Revista Latinoamericana de Estudios de Seguridad, No. 20, pp. 94-109

Gómez- Llinás, D. A. (2017). *Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo: Stuxnet, el virus informático*. Universidad del Rosario [Trabajo Final de Grado]. Recuperado de: https://n9.cl/c54is

González, M. (2009). *Tácticas Policiales en Protección de Personas y Técnicas de Escolta.* Editorial AC.

González, M. (mayo 2016). Actos antisociales en hospitales: actuaciones frente a las agresiones al personal hospitalario. *Seguritecnia,* (431), 90-94. www.seguritecnia.es

González, M. (septiembre 2017). El departamento de seguridad debe pertenecer a la máxima línea jerárquica del hospital. *Cuadernos de Seguridad,* (325), 34-37. www.cuadernosdeseguridad.com

González, M. (septiembre 2017). La gestión de la seguridad y la protección integral en los hospitales como centros complejos e Infraestructuras Críticas. *Seguritecnia,* (445), 94-97. www.seguritecnia.es

González, M. (diciembre 2018). La bioseguridad en áreas críticas hospitalarias: Actuaciones técnicas preventivas y reactivas que la garanticen. Especial referencia al área quirúrgica. *Ingeniería del mantenimiento en Canarias,* (11), 50-60

González, M. (julio-agosto 2019). La gestión y dirección de seguridad con químicos peligrosos. *Seguritecnia,* (466), 75-78. www.seguritecnia.es

González, M. (septiembre 2019). Dirección y gestión de la seguridad y la protección de datos en hospitales. *Cuadernos de Seguridad,* (346), 36-37. www.cuadernosdeseguridad.com

González, M. (septiembre-octubre 2022). El director de seguridad en entornos patrimoniales corporativos. Seguritecnia, (497), 84-88. www.seguritecnia.es

Gutiérrez, A. (septiembre 2017). Máximo control en entornos hospitalarios. *Cuadernos de Seguridad,* (325), 38-39. www.cuadernosdeseguridad.com

Hall, W.M. y Citrenbaum, G. (2009). *Intelligence Analysis: How toThink in Complex Environments" (Análisis de Inteligencia: Cómo Pensar en Entornos Complejos)* Praeger.

Hassan H. & Hijazi R. (2018). *Open-Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence (1st ed)*. Apress.

Haq, M.U. (1998). Human rights, security, and governance. *Peace & Policy of the Toda Institute for Peace and Policy Research: Dialogue of Civilizations for World Citizenship*, Vol3, Nº2.

Hayden, M. (2007). *Prepared Remarks at the Council of Foreign Relations*. Obtenido de https://www.cia.gov/news-information/speeches-testimony/2007/generalhaydens-remarks-at-the-council-on-foreign-relations.html

Hendrix, C.S. (2018). *Búsqueda de vínculos entre conflictos climáticos*. Naturaleza Cambio Climático 8, 190-191

Herman, M. (2003). *Counter-Terrorism, Information Technology and Intelligence Change.* Londres: Orión. Página 78 de 85

Hernández García, N. (2020). *La seguridad humana: del concepto al enfoque. Causas de la reducción de su uso como concepto*. Relaciones Internacionales, nº 43, pp. 33-48.https://revistas.uam.es/relacionesinternacionales/article/view/relacionesinternacionales2020.43.002/11881

Hernández, R., Fernández, C. & Baptista, P. (2010). *Metodología de la Investigación. 6ª edición*. Mc Graw Hill Education 1914.

Herraiz, F.J. (septiembre 2017). Ciberseguridad en hospitales: defensa ante ataques. *Seguritecnia,* (445), 98-99. www.seguritecnia.es

Herrera, F. P. (2016). *Ensanchando el Pensamiento: La comunidad ampliada de inteligencia.* Notes internationals.

Hidalgo- Cisneros, R. (2022). Buenas prácticas en la implantación de SIEM en las Infraestructuras Críticas. *Revista Nuclear, 384*, 29- 32.

Hoffman, B. (1999). A mano armada. Historia del terrorismo. Madrid: Espasa Calpe.

Hoffman, B. y. (2004). *Terrorism, Signaling, and Suicide Attack. Studies in Conflict & Terrorism,* vol. 27.

Hoffman, M. J., & Oliver-Smith, A. (2018). *Climate change and insecurity: Mapping vulnerability in Africa.* International Journal of Terrorism and Political Hotspots, 13(2), 91-107.

Holt, R. (2022). Sand worm: una historia de ciberataques disruptivos atribuidos a este grupo. We live security. https://www.welivesecurity.com/la-es/2022/03/22/sandworm-historia-ciberataques-atribuidos-este-grupo/.

Huguet, M. (2001). *Los procesos de descolonización y los nuevos protagonistas*. Madrid: Crítica.

Hull, R. Belluck, D. &Lipchin, C. (2006). *A framework for multi-criteria decision making with special reference to critical infrastructure: policy and risk management working group summary and recommendations*. Ecotoxico-logy, Ecological Risk Assessment and Multiple Stressors. Springer.

IBM. (07 de marzo de 2023). Obtenido de *¿Qué es el phishing y cuáles son sus consecuencias?*: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataquesinformaticos/que-es-el-phishing-y-cuales-son-sus-consecuencias.html.

Incibe (abril 2018). El INCIBE dio respuesta a 123.064 ciberincidentes durante 2017. *Cuadernos de Seguridad,* (332), 81. www.cuadernosdeseguridad.com

INCIBE-CERT. (28 de mayo de 2014). Obtenido de OSINT - La información es poder: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Instrucción núm. 1/2016, de la Secretaria de Estado de Seguridad, por la que se actualiza el Plan Nacional de Protección las Infraestructuras Críticas.

Instrucción núm. 10/2015 de la Secretaría de Estado de Seguridad, por la que se regula el proceso de implantación del sistema de protección de Infraestructuras Críticas a nivel territorial

Interior, M. d. (s.f.). Real Decreto 400/2012, de 17 de febrero, *por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.* Obtenido de

https://intelpage.info/real-decreto-400-2012-de-17-de-febrero-por-el-que-se-desarrolla-la-estructura-organica-basica-del-ministerio-del-interior.html

Ionut, L. y González, L. (julio-agosto 2018). Oportunidades y amenazas de la cuarta revolución industrial. *Cuadernos de Seguridad,* (335), 28. www.cuadernosdeseguridad.com

Irene P., Daniel A. & Abril A. (2022). ¿Psicólogos y psicólogas sesgados? Sesgos de confirmación y representatividad en estudiantes universitarios de psicología. *Revista Wimb Lu,* 17(2). https://doi.org/10.15517/wl.v17i2.52724.

Istúritz, J.J. (junio 2014). La formación en seguridad hospitalaria. *Cuadernos de Seguridad,* (290), 46-48. www.cuadernosdeseguridad.com

Istúritz, J.J. (junio 2014). Directores y departamentos de Seguridad. *Cuadernos de Seguridad,* (290), 86-89. www.cuadernosdeseguridad.com

Istúritz, J.J. (noviembre 2015). Reflexiones sobre la nueva Ley del Sistema Nacional de Protección Civil. *Securitecnia,* (425), 68-69. www.seguritecnia.es

Istúritz, J.J. (septiembre 2018). La Dirección de Seguridad desde la perspectiva de la Gerencia Hospitalaria. *Cuadernos de Seguridad,* (336), 50-51. www.cuadernosdeseguridad.com

Istúritz, J.J. & Istúritz, N. (enero-febrero 2022). La transformación digital en seguridad corporativa (I) *Cuadernos de Seguridad,* (362), 109. www.cuadernosdeseguridad.com

Istúritz, J.J., González, M., Miranda, D. & Rubio, G. (2023). *Manual de Seguridad Corporativa en Edificios Administrativos.* Gobierno de Canarias.

Istúritz, J.J. (2023). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 26. https://www.gobiernodecanarias.org/hpae/

Johnson, L. (2007). Manual de estudios de inteligencia. Routledge.

Jones, I. (2008). *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture (El Factor Humano: Dentro de la Cultura Disfuncional de la Inteligencia de la CIA.)* En Counter Books.

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Granada: Grupo de Estudios en Seguridad Internacional.

Joyanes, L. (2011). Estado del arte de la ciberseguridad. *Cuadernos de Estrategia, 149,* 11- 46.

Joyanes, L. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0), *Cuadernos de Estrategia, 185,* 19-64.

Kamboj, R. (28 de octubre de 2022). *Noticias ONU*. Obtenido de El Comité contra el Terrorismo apoya el uso de las nuevas tecnologías para combatir esa lacra: https://news.un.org/es/interview/2022/10/1516452

Keegan, J. (2003). *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda (Inteligencia en la Guerra: Conocimiento del Enemigo desde Napoleón hasta Al-Qaeda)* Vintage.

Kent, S. (2019). *Strategic Intelligence for American World Policy.* Princeton Legacy Library,2377.

Kocsis, M.L. (2015). *Intelligence Operations: Understanding Data, Tools, Tactics, and Techniques (Operaciones de Inteligencia: Comprender Datos, Herramientas, Tácticas y Técnicas)* Wiley.

Laborde, J.P. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 25.

Laqueur, W. (1987). The Age of Terrorism. Boston: Little Brown.

Legido, J. M. (2015). *Ciberseguridad en las Infraestructuras Críticas*. La Vanguardia. Recuperado de: https://n9.cl/q6ngu

LejarzaIllaro, E. (2014). CIBERGUERRA, LOS ESCENARIOS DE CONFRONTACIÓN. IEEE. Documento Opinión. https://www.ieee.es/contenido/noticias/2014/02/DIEEEO18-2014.html

Lengua, R. A. (2022). RAE.es. Obtenido de https://www.rae.es/

León, B. G. (2019). El concepto de lo híbrido: de las estrategias híbridas a la zona gris. Amenaza híbrida. La guerra imprevisible., 32-33.

Lesaca, J. (2017). Armas de seducción masiva. Barcelona: Península (1ª edición).

Ley 36/2015, *de Seguridad Nacional*. (28 de septiembre de 2015). Obtenido de Agencia Estatal Boletín Oficial del Estado: https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas. *Boletín Oficial del Estado*, de 29 de abril de 201, núm. 1092, pp. 71548-71586

Ley PIC. EUR-Lex - 32008L0114 - EN - EUR-Lex. (n.d.). *Diario Oficial De La Unión Europea*. Retrieved January 21, 2023, from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32008L0114

Lisa Institute (20 de mayo de 2021). *Infraestructuras Críticas, definición, planes, riesgos, amenazas y legislación*. Recuperado de: https://n9.cl/mb4h3

López, J. (julio-agosto 2019). Hay que seguir invirtiendo en seguridad e integrarla de manera trasversal en las estructuras de los hospitales. *Seguritecnia,* (466), 79-81. www.seguritecnia.es

López, N., Sandoval, I. (2016). *Métodos y técnicas de investigación cuantitativa y cualitativa.*

Lowenthal, M. (2003). *Preface to a theory of strategic Inteligence*. Washinton DC: CQ Press.

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy*. Washinton DC: CQ Press.

MALDITA.ES. (2022, 9 marzo). Videojuegos, falsas portadas y subtítulos. Así se mueve la desinformación en la guerra iniciada por Rusia en*. www.20minutos.es* - Últimas Noticias. https://www.20minutos.es/noticia/4967603/0/los-formatos-en-los-que-semueve-la-desinformacion-de-la-guerra-iniciada-por-rusia-en-ucrania/

Maras, M. (2017). *Cibercriminología*. Londres: Oxfor University Press.

Martín, D. (28 de Enero de 2015). Publico.es. Obtenido de *La yihad no es guerra y mucho menos santa*: https://www.publico.es/internacional/yihad-no-guerra-y-mucho.html

Martín, J. M. (2019). *La comunidad de inteligencia española, presente y futuro.* Monografías 153 XIX CEMFAS. Escuela Superior de las Fuerzas Armadas.

Martín, L. E. (2013). *El cambio climático como constante amenaza biológica. Nuevo terrorismo: ¿estamos preparados? Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=7531310*

Martín, L.-C. P. (2016). Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide, Part 1. *Royal Canadian Air Force Journal*, 5(3), 43-69.

Martín, R. (2022). *Ciberguerra, elemento decisivo en la invasión de Rusia a Ucrania*. Canal Informática y TICS. https://www.inesem.es/revistadigital/informatica-y tics/ciberguerra/ Martínez de Castro, M. M. (2022). La respuesta a incidentes en un escenario global y con protagonismo del ransomware. *Revista de Unidades de Información, 19.*

Martínez, D. (julio-agosto 2018). La gestión ágil, esencial para hacer frente a las nuevas ciberamenazas. *Cuadernos de Seguridad,* (335), 30. www.cuadernosdeseguridad.com

Martínez Quirante, R. & Rodríguez, J. (2018). *Inteligencia artificial y armas letales autónomas*, TREA, pág. 108 y 109.

Martínez, R. (2022). Estrategias nacionales de seguridad, una herramienta del S.XXI. *Papeles de relaciones sociosociales y cambio global. (157) pág. 157. file:///C:/Users/User/Desktop/Papeles-relaciones-ecosociales-cambio-global-157.pdf*

Matey, G. D. (2008). *Hacia una definición inclusiva de Inteligencia. Inteligencia y Seguridad*.

Matey, G. D. (2016). El papel de la inteligencia en la lucha contra el terrorismo salafista yihadista. *Revista CIDOB dáfers Internacionals*, 208.

Matthews, R. (29 de Marzo de 2023). Obtenido de ¿Qué es spam y cómo evitarlo?: https:// nordvpn.com/es/blog/que-es-spam/

McDowell, D. (2013). *Strategic Intelligence: A Hand bookf or Practitioners, Managers, and Users (Inteligencia Estratégica: Un Manual para Profesionales, Gerentes y Usuarios).* Scarecrow Press.

McMillan, R. (14 de septiembre de 2010). *Siemens: Stuxnet worm his industrial systems. Computerworld*. Recuperado de: https://n9.cl/ch91j

McNamara, R. S. (2011). *Anthropologist in the Security Scape: Practice, and Professional Identity.* Routledge.

Medina Llinás, M. (2022). Ataques híbridos a infraestructuras híbridas. *CIDOB Report, 8.* Recuperado de: https://n9.cl/43j4z

Melucci, A. (1999). *Acción colectiva, vida cotidiana y democracia*. México: Centro de Estudios Sociológicos.

Méndez, M. Á. (2022, 21 mayo). El 'virus' ruso que inutiliza miles de 'routers' en segundos e inquieta a Occidente. elconfidencial.com. https://www.elconfidencial.com/tecnologia/2022-05-20/acidrain-malware-viasat-satelite-hackers-ciberseguridad_3426592/

Mercado, J. M. M. (2017). Evolución histórica de la gestión de la información en conflictos bélicos. bie3: Boletín IEEE, (8), 1030-1052.https://dialnet.unirioja.es/servlet/articulo?codigo=6361709

Merlos García, J. A. (2006). *Al Qaeda. Raíces y metas del terror global*. Madrid: Biblioteca Nueva.

Ministerio de Asuntos Económicos y Transformación Digital. (2021). *España Digital 2025*. Recuperado de: https://acortar.link/WhCywG

Ministerio de Defensa. (2022). *Ciberamenazas y tendencias. Análisis de las ciberamenazas nacionales e internacionales de su evolución y tendencias futuras*. Centro Criptológico Nacional. Recuperado de: https://n9.cl/lc84r

Ministerio del Interior (mayo 2018). Las Infraestructuras Críticas, blanco de los ciberdelincuentes. *Cuadernos de Seguridad,* (333), 80. www.cuadernosdeseguridad.com

Ministerio del Interior. Secretaria de Estado de Seguridad (s. f.). *Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV). Un marco para el respeto y el entendimiento común*. https://www.interior.gob.es/opencms/es/servicios-al-ciudadano/plan-estrategico-nacional-de-lucha-contra-la-radicalizacion-violenta/documentacion-del-plan/estrategia-interior/

Ministerio del Interior. (s. f.). *Uno de cada cinco delitos. 1 de cada 5 delitos se comenten en la red*[vídeo]. Recuperado 3 de marzo de 2023, de https://unodecadacincodelitos.com/

Miranda, D. (2003). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 33. https://www.gobiernodecanarias.org/hpae/

Miranda, D. (2003). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 34. https://www.gobiernodecanarias.org/hpae/

Miranda, D. (2003). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 48. https://www.gobiernodecanarias.org/hpae/

MIT(2022).*Cyber Defense Index.* https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/

Moncloa. (08 de febrero de 2023). *Grande-Marlaska presenta la campaña de Interior contra la ciberdelincuencia*. Página web oficial de La Moncloa. Recuperado de: https://n9.cl/ezap2

Moncloa. (25 de abril de 2023). *La Secretaria de Estado de Seguridad establece el dispositivo de seguridad para las elecciones del 28M*. Página web oficial de La Moncloa. Recuperado de: https://n9.cl/r50ez

Montero. A. (2006). Doctrina de infiltración para inteligencia contraterrorista. *Estudios para la Seguridad y Defensa,* Vol. 1, (1), 31-49.

Montesinos, F. A. (2011). *La Ecuación de la Guerra*. Barcelona: Montesinos Editor.

Monzó, C. C. (24 de abril de 2011). Obtenido de ¿Qué son las redes sociales profesionales?: http://uncommunitymanager.es/redes-profesionales/

Morales, S. (2019). *Guerra informativa: llenar la información de desinformación*. Documento de opinión IEEE.

Morán, F. (septiembre 2017). Retos y soluciones en el control de accesos de los hospitales. *Cuadernos de Seguridad,* (325), 54-55. www.cuadernosdeseguridad.com

Moreno, C. (julio-agosto 2018). La amenaza actual del terrorismo sobre los eventos. *Cuadernos de Seguridad,* (335), 81-85. www.cuadernosdeseguridad.com

Moreno, J. D. (2017). *Terrorismo Yihadista y los nuevos delitos de captación, adiestramiento y adoctrinamiento tras la LO 2/2015*. Quaderns de ciènciessocials, (35), 4-37.https://roderic.uv.es/bitstream/handle/10550/76332/4.pdf?sequence=1

Naciones Unidas. (1986, 4 diciembre). *Declaración sobre el derecho al desarrollo.* https://www.ohchr.org/es/instruments mechanisms/instruments/declaration-right-development

National, D. (2006). National Defense Authorization Act for Fiscal Public Law 109-163, section 931. Página 59 de 67.

Nato. (2002). Nato OSINT Hanbook V1. 2.

Nato. (2023). *Science & Technology Trends 2023-2043*, NATO Science & Technology Organization VOLUME 1: Overview. pág. 16, 101, 103.

Nato. (2023). *Science & Technology Trends 2023-2043*, NATO Science & Technology Organization VOLUME 2: Analysis. pág. 26

ODIN. (s. f.). Odin - *OSINT y ciber inteligencia*. Recuperado 8 de marzo de 2023, de https://odint.net/

Oliver, N (2018). *Inteligencia artificial: Ficción, realidad y …sueños.* Real Academia de Ingeniería, pág. 37, 39, 40.

Olivier, E. (2023). Obtenido de Hashtag: *Para qué Sirven y Cómo Usarlos Correctamente:* https://www.genwords.com/blog/hashtag/

OMS, OPS; 2018., (2018). *Índice de Seguridad Hospitalaria, Guía para Evaluadores*. Segunda edición.

ONU. (2020, 17 junio). *Cambio climático. Desarrollo Sostenible*. https://www.un.org/sustainabledevelopment/es/climate-change-2/

OTAN, AJP.-2. (2003). Doctrina Conjunta aliada para Inteligencia, Contrainteligencia y Seguridad. OTAN.

OTAN. (2001). Allied Joint Intelligence de la OTAN, documento AJP-2.0.2001.

OTAN. (2008). Center of Excellence Defence Against Terrorism. Sub-series E: Human and societal dynamics. IOS Press.

Otero, L. E. M. (2013). *El cambio climático como constante amenaza biológica. Nuevo terrorismo: ¿estamos preparados?* Pre-bie3, (5), 36. https://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO97-2013_CambioClimatico-NuevoTerrorismo_MartinOtero.pdf

Page, D. (19 de abril de 2023). *Seguridad Nacional alerta de 15.500 ciberataques contra Infraestructuras Críticas en el año de la guerra*. Diario Activos. Recuperado de: https://n9.cl/1kex3

Palacios, J. (08 de marzo de 2017). Blog Mosaico. Obtenido de GESI, *Enseñanza de la inteligencia: errores sobre el ciclo*.https://global-strategy.org/ensenanza-de-la-inteligencia-errores-sobre-el-ciclo/

Pastor Galindo, J. Nespoli, P., Gómez Mármol, F., Martínez Pérez, G. (2020). IEEE Access nº 8. Obtenido de *La mina de oro aún no explotada de OSINT: oportunidades, desafíos abiertos y tendencias futuras*: https://ieeexplore.ieee.org/document/8954668

Pastor, N. (2022 Abril 7). *España ya tiene déficit de expertos en Ciberseguridad y la demanda sigue aumentando.* La Vanguardia.https://www.lavanguardia.com/economia/20220401/8161871/espana-deficit-expertos-ciberseguridad-demanda-sigue-aumentando-nuclio-brl.html

Pastrana, A. G. (2015). *Análisis de la Ley Orgánica 2/2015, de reforma del código penal en materia de terrorismo. Seguridad y Ciudadanía*. Seguridad y Ciudadanía. Revista del Ministerio del Interior, 139-153.

Patiño, L. (30 de agosto de 2019). Obtenido de ¿Cuánto valor tiene un 'like' en su vida?: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-significado-de-un-likeen-las-redes-sociales-406570

Patrizio, A. (12 de Diciembre de 2019). Obtenido de ¿Qué es una dirección IP?: https://www.avast.com/es-es/c-what-is-an-ip-address

Payá-Santos, C., y Luque Juárez, J. M. (2021). *El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio.* Revista Científica General José Marta Córdova, 79(36), 1121-1136. https://dx.doi.org/10.21830/19006586.855

Perrino Navas, I. (2022). oa.upm.es. Obtenido de Investigación y extracción de datos con técnicas OSINT: https://oa.upm.es/72302/1/TFG_IRENE_PERRINO_NAVAS.pdf

Pineda, F. (2002). La guerra de la desinformación en la era de la información. *Revista OSAL: Observatorio Social de América Latina, 2 (6)*, 35- 40.

PNUD (Programa de las Naciones Unidas para el Desarrollo) (1994). *Informe sobre desarrollo humano 1994: Nuevas dimensiones de la seguridad humana.* Fondo de Cultura Económica. México.

Pollitt, M. (1998). Cyberterrorismo: Realidad o Fantasía. Computer Fraud & Security 2.

Ponce, T. (mayo 2016). De nada sirve tener un plan de autoprotección si quienes deben ponerlo en práctica no lo conocen. *Seguritecnia,* (431), 80-85. www.seguritecnia.es

Portillo, I. (s. f.). *Monta la NSA en casa: Inteligencia aplicada al mundo ciber*. GINSEG. https://ginseg.com/es/noticias/36-monta-la-nsa-en-casa-inteligencia-aplicada-al-mundo-ciber.html

Presidencia del Gobierno. (2021). *Estrategia de Seguridad Nacional*. Recuperado de: https://www.dsn.gob.es/sites/dsn/files/ESN2021%20Accesible_1.pdf

Puime, J. (2009). El ciberespionaje y la ciberseguridad. *La violencia del siglo XXI. Nuevas dimensiones de la guerra*, 45- 76.

Ramphele, M. (2004). *Reply. Seminnar at the National Council for Research on Women*. www.ncrw.org/interest/bernstein_remarks.htm

Random, R. (2010). *Studies in Intelligence.* Página 79 de 85

Real A. E. (2021). Real Academia Española. Obtenido de Asociación de Academias de la Lengua Española: https://dle.rae.es/terrorismo

Real Academia Española (2014). Diccionario de la lengua española(23a edición). Madrid: RAE.

Recio, M. (20 de enero de 2018). *CSO Computerworl.es*. Obtenido de *En lucha contra la ciberdelincuencia.* https://cso.computerworld.es/alertas/en-lucha-contra-la-ciberdelincuencia

Recomendación del Consejo de 8 de diciembre de 2022 sobre un enfoque coordinado en toda la Unión para reforzar la resiliencia de las Infraestructuras Críticas. *DOUE, 20*.

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad en las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº. 526/2013 (Reglamento sobre la Ciberseguridad). *Diario Oficial de la Unión Europea*, núm. 151, de 7 de junio de 2019, pp. 15-65.

Rey, M. (11 de marzo de 2023*). De la culpabilidad rusa a las sospechas sobre Ucrania: ¿qué se sabe del sabotaje al Nord Stream?*. Radio Televisión Española. Recuperado de: https://n9.cl/t74aq

RGPD. *Diario Oficial De La Unión Europea*. Retrieved January 21, 2023, from: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

Rivas, A. (septiembre 2017). La importancia de los estándares de atención sanitaria. *Cuadernos de Seguridad,* (325), 44-45. www.cuadernosdeseguridad.com

Rodríguez, P. (2011). *El necesario refuerzo de la cooperación bilateral en la lucha contra el Terrorismo yihadista*. UNISCI Discussion Papers nº27. Octubre 2011.

Rodríguez, Y. (2019). Grupo de Estudios de Seguridad Internacional. Obtenido de INTELIGENCIA DE FUENTES ABIERTAS (OSINT): CARACTERÍSTICAS, DEBILIDADES Y ENGAÑO: https://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertasosint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1oPágina 60 de 67.

Romero, J.L. (septiembre 2017). Seguridad en hospitales y centros de salud. *Cuadernos de Seguridad,* (325), 40-42. www.cuadernosdeseguridad.com

Rubio, G. (2003). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 51. https://www.gobiernodecanarias.org/hpae/

Rubio, G. (2003). Manual de Seguridad Patrimonial en Edificios Administrativos. Gobierno de Canarias. Pág. 58. https://www.gobiernodecanarias.org/hpae/

Ruiz de Azcárate, J. (3 de agosto 2015). Islam, Terrorismo y Medios de Comunicación*. Ieee.es Documento de Opinión*, (83), 1-14.

Sahagún, F. (2015). *Panorama Estratégico. Introducción*. En Instituto Español de estudios

Salazar J. & Silvestre S. (2016). Obtenido de INTERNET DE LAS COSAS: https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

Sampieri, R. H. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw Hill.

Sánchez Gómez, F. J. (2014). Las políticas de protección de las Infraestructuras Críticas en España. *Seguridad y Ciudadanía: Revista del Ministerio del Interior, 11,* 15-77.

Sánchez, F.A. (2019). *Fundamentos Epistémicos de la Investigación Cualitativa y Cuantitativa: Consensos y Disensos.* Revista Digital de Investigación En Docencia Universitaria, 13 (1). https://doi.org/10.19083/ridu.2019.644

Sánchez-Torres, B., Rodríguez-Rodríguez, J. A., Rico-Bautista, D. W., & Guerrero, C. D. (2018). Campus inteligente: Tendencias en ciberseguridad y desarrollo futuro. *Revista Facultad de Ingeniería, 27(47).*

Santos, L. (2021). *Ciberseguridad e Infraestructuras Críticas*. Universidad Europea. ABACUS. Repositorio de Producción científica.

Sardá, J. F. (1992). *La gestión de fuentes abiertas por los servicios de Inteligencia y los equipos de investigación.* El estado de la cuestión. Valencia.

Shakarian, P. (2012). *Stunext: Revolución de ciberguerra en los asuntos militares. Air and Space Power Journal*. Recuperado de: https://n9.cl/e43nt

Sierra, F. (1998). *Función y sentido de la entrevista cualitativa en investigación social*. México D.F.: Pearson.

Sistema de Seguridad Nacional, DSN. (2019). Obtenido de *Contrainteligencia*: https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad nacional/contrainteligencia#:~:text=La%20Estrategia%20de%20Seguridad%20Nacional%20plantea%20como%20objetivo,est%C3%A9n%20dirigidas%20a%20la%20obtenc

Sociedad Argentina de Estudios Estratégicos y Globales (SAEEG). (2021). CONFLICTOS HÍBRIDOS Y LA DOCTRINA GERASIMOV. https://saeeg.org/index.php/2021/07/10/conflictos-hibridos-y-la-doctrina-gerasimov/

Soto, K. (2005). Análisis crítico del actual régimen jurídico aplicable al terrorismo internacional. Memoria. Universidad Austral de Chile. Facultad de Ciencias Jurídicas y Sociales.

Soto, J. M. (2017). Impacto de la regulación administrativa en la fase prehospitalaria del programa de coordinación "Código Infarto Agudo de Miocardio" en Cataluña. [Tesis Doctoral, UAB. (p. 30).

Steele, R. (1997). 6th International Conference & Exhibit Global Security & Global. Open-Source Solutions. Subijana, I. J. (diciembre de 2008). Cuaderno del Instituto Vasco de Criminología, 22. pp. 169-187. Obtenido de EL CIBERTERRORISMO: UNA PERSPECTIVA LEGAL Y JUDICIAL: https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf.

The EU's Cybersecurity Strategy for the Digital Decade. (2020). Shaping Europe's Digital Future. Retrieved January 21, 2023, from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0?pk_source=ec_newsroom&pk_medium=email&pk_campaign=dae%20Newsroom

Times, T. N. (20 de septiembre de 2002). *Full Text: Bush´s Nacional Security Strategy*.

Torres Soriano, M. (2009). *El eco del terror. Ideología y propaganda en el terrorismo yihadista*. Madrid: Plaza y Valdés.

Torres, H. (2010). *El concepto de terrorismo, su inexistencia o inoperancia: La apertura a la violación de derechos humanos.* Fundación Dialnet, Informes de Investigación, Diálogo de Saberes nº 32. https://dialnet.unirioja.es/servlet/articulo?codigo=3295663

Torres, M. (2007). *La dimensión propagandística del terrorismo yihadista global*. Granada: Universidad de Granada. Tesis Doctoral.

Torres, M. R. (2011). Guerras Youtube: el impacto de las nuevas tecnologías de la información en el tratamiento mediático de los conflictos armados*. Cuadernos de estrategia,* (148), 129-157.

Torres, M.R.T. (2017). *Concepto y niveles de la ciber-inteligencia*. Revista de Aeronáutica y Astronáutica, 862, 316-320. https://www.researchgate.net/publication/316036648_Concepto_y_niveles_de_la_ciberinteligencia_Revista_de_Aeronautica_y_Astronautica_n_862_abril_2017_pp_316-320

Tovar, A. (mayo 2018).El director de Seguridad debe desarrollar una estrategia global de defensa de la compañía. *Cuadernos de Seguridad,* (333), 10-12. www.cuadernosdeseguridad.com

Tovar, H. (2011). *Guerra de Información: ¿el arma es el mensaje?.* Caracas: UCV. Cap. 1.

Treverton, G.F. (2009). *Intelligence for an Age of Terror (Inteligencia para una Era de Terror)* Cambridge University Press.

Tsang, S. (2008). *Intelligence and Human Rights in the Era of Global Terrorism (Inteligencia y Derechos Humanos en la Era del Terrorismo Global)* Stanford University Press.

UK Army.(2007). *Field Army ISTAR Handbook.*

Un proyecto compartido. (2013). Obtenido de: https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesibl ebpdf.pdf.

US Army.(1998). *Fm 34-8-2 Intelligence Officer's Handbook*. Distribution.

US Army.(2004). *FM 2-0 Intelligence*. Intelligence, May.

US Army.(2010). *CoISTTactics, Techniques and Procedures*.

US Army.(2019). *ADP 2-0 Intelligence*.

Val, T. F. (2014). *La Inteligencia Militar, una constante histórica*. Instituto Español de Estudios Estratégicos.

Valero, V. M. (2016). *Monografías 148. Inteligencia, Un enfoque integral*. Madrid: ESFAS.

Valverde, A. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 145, 154.

Vázquez, N. (2021). Obtenido de Operadores Booleanos: https://bayamonweb.azurewebsites.net/cai/wp/content/uploads/sites/6/2021/10/OperadoresBooleanos.pdf.

Villar García, A. (2018). TFG. Universidad de Zaragoza. Obtenido de Uso de redes sociales: captación y creación de imagen de marca: https://zaguan.unizar.es/record/86069/files/TAZ-TFG-2018-1780.pdf

Villena, J. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 103.

VV.AA. (2002). Terrorismo Internacional en el Siglo XXI (X CURSO INTERNACIONAL DE DEFENSA JACA): Ministerio de Defensa.

Walters, V. (1976). *Strategic Studies Institute of the US Army War College*.

Warren J. K., & Green, M. C. (2009). *Marketing Internacional* (5a. ed.).Pearson Educación.https://eds.s.ebscohost.com/eds/pdfviewer/pdfviewer?vid=12&sid=c928241c-dead-4b2e-bf96-1ff9122cb407%40redis

WatchGuard Technologies. (2021). *Cómo los MSPs pueden protegerse frente a nuevas TTPs de los estados*. https://www.watchguard.com/es/wgrd-news/blog/como-los-msps-pueden-protegerse-frente-nuevas-ttps-de-los-estados.

Wringht, J. (1985). *Terrorismo: una forma de guerra*. En Military Rewiew.

Zaragoza, J.I. (2021). *Terrorismo Yihadista: Aproximación criminológica y victimológica.* Servicio Editorial de la Universidad del País vasco, pág. 143.

REFERENCIAS LEGALES Y NORMATIVAS

ÁMBITO DE LA SEGURIDAD PRIVADA

Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, modificado por el Real Decreto 195/2010, de 26 de febrero. *Boletín Oficial del Estado núm. 8, de 10 de enero de 1995*.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín *Oficial del Estado núm. 281, de 24 de noviembre de 1995.*

Orden de 23 de abril de 1997, por la que se concretan determinados aspectos en materia de empresas de seguridad, en cumplimiento de la Ley y el Reglamento de Seguridad Privada. Boletín *Oficial del Estado núm. 108, de 10 de mayo de 1997.*

Real Decreto 862/2009, de 14 de mayo, por el que se aprueban las normas técnicas de diseño y operación de aeródromos de uso público y se regula la certificación de los aeropuertos de competencia del Estado. Boletín *Oficial del Estado núm. 132, de 1 de junio de 2009.*

Real Decreto 195/2010, de 26 de febrero, por el que se modifica el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, para adaptarlo a las modificaciones introducidas en la Ley 23/1992, de 30 de julio, de Seguridad Privada, por la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre el libre acceso a las actividades de servicios y su ejercicio. Boletín *Oficial del Estado núm. 60, de 10 de marzo de 2010.*

Orden INT/315/2011, de 1 de febrero, por la que se regulan las Comisiones Mixtas de Coordinación de Seguridad Privada. Boletín *Oficial del Estado núm. 42, de 18 de febrero de 2011.*

Orden INT/314/2011, de 1 de febrero, sobre empresas de Seguridad Privada. Boletín *Oficial del Estado núm. 42, de 18 de febrero de 2011.*

Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la Seguridad Privada. Boletín *Oficial del Estado núm. 42, de 18 de febrero de 2011.*

Orden INT/317/2011, de 1 de febrero, sobre medidas de Seguridad Privada. Boletín *Oficial del Estado núm. 42, de 18 de febrero de 2011.*

Orden INT/318/2011, de 1 de febrero, sobre personal de Seguridad Privada. Boletín *Oficial del Estado núm. 42, de 18 de febrero de 2011.*

Ley 5/2014, de 4 de abril, de Seguridad Privada. *Boletín Oficial del Estado núm. 83,*

de 5 de abril de 2014.

Ley 11/2019, de 25 de abril, de Patrimonio Cultural de Canarias. Boletín *Oficial del Estado núm. 140, de 12 de junio de 2019.*

Ley 11/2019, de 25 de abril, de Patrimonio Cultural de Canarias. Boletín *Oficial del Estado núm. 140, de 12 de junio de 2019*

Orden INT/826/2020, de 3de septiembre, por la que se modifican en los plazos de adecuación de medidas de seguridad electrónica, la Orden INT7316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, y la Orden INT/317/2011, de 1 de febrero, sobre medidas de Seguridad Privada. Boletín *Oficial del Estado núm. 241, de 9 de septiembre de 2020*

ÁMBITO DE LA PROTECCIÓN CIVIL

Real Decreto 1378/1985, de 1 de agosto, sobre medidas provisionales para la actuación en situaciones de emergencia en los casos de grave riesgo, catástrofe o calamidad pública. Boletín *Oficial del Estado núm. 191, de 10 de agosto de 1985.*

Real Decreto 407/1992, de 24 de abril, Norma Básica de Protección Civil. Boletín *Oficial del Estado núm. 105, de 1 de mayo de 1992.*

Resolución de 31 de enero de 1995, de la Secretaría de Estado de Interior, por la que se dispone la publicación del Acuerdo del Consejo de Ministros por el que se aprueba la Directriz Básica de Planificación de Protección Civil ante el riesgo de inundaciones. *Boletín Oficial del Estado núm. 38, de 14 de febrero de 1995.*

Resolución de 21 de febrero, de 1996, de la Secretaría de Estado de Interior, por la que se dispone la publicación del Acuerdo del Consejo de Ministros por el que se aprueba la Directriz Básica de Planificación de Protección Civil ante el riesgo volcánico. *Boletín Oficial del Estado núm. 55, de 4 de marzo de 1996.*

Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil. Boletín *Oficial del Estado núm. 164, de 10 de julio de 2015.*

Real Decreto 842/2002, de 2 de agosto, por el que se apruebe el reglamento electrotécnico para baja tensión. Boletín *Oficial del Estado núm. 224, de 18 de septiembre de 2002.*

Resolución de 17 de septiembre, de 2004, de la Secretaría de Estado de Interior, sobre riesgo sísmico. *Boletín Oficial del Estado núm. 238, de 2 de octubre de 2004.*

Real Decreto 314/2006, de 17 de marzo, por el que se aprueba el Código Técnico de la Edificación. Boletín *Oficial del Estado núm. 74, de 28 de marzo de 2006.*

Decreto 186/2006, de 19 de diciembre, por el que se aprueba el Plan Específico de Protección Civil y Atención de Emergencias de la Comunidad Autónoma de Canarias por riesgos de fenómenos meteorológicos adversos (**PEFMA**). *Boletín Oficial de Canarias núm. 17, de 23 de enero de 2007.*

Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia. Boletín *Oficial del Estado núm. 239, de 3 de octubre de 2008.*

Ley 9/2007, de 13 de abril, del Sistema Canario de Seguridad y Emergencias. Boletín *Oficial del Estado núm. 124, de 24 de mayo de 2007.*

Real Decreto 1468/2008, de 5 deseptiembre, por el que se modifica el Real Decreto 393/2007, y aprueba la norma básica de autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan originar situaciones de emergencia. Boletín *Oficial del Estado núm. 239, de 3 de octubre de 2008.*

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín *Oficial del Estado núm. 25, de 29 de enero de 2010.*

Decreto 86/2013, de1de agosto, por el que se aprueba el Reglamento de Actividades Clasificadas y Espectáculos Públicos. Boletín *Oficial de Canarias núm. 156, de 14 de agosto de 2013.*

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Boletín *Oficial del Estado núm. 233, de 29 de septiembre de 2015.*

Decreto 67/2015, de 30 de abril, por el que se aprueba el Reglamento de Autoprotección exigible a determinadas actividades, centros o establecimientos que puedan dar origen a situaciones de emergencia en la Comunidad Autónoma de Canarias. *Boletín Oficial de Canarias núm. 98, de 25 de mayo de 2015.*

Real Decreto 513/2017, de22 de mayo, por el que se aprueba el Reglamento de Instalaciones de Protección Contra incendios. Boletín *Oficial del Estado núm. 139, de 12 de junio de 2017.*

Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. Boletín *Oficial del Estado núm. 309, de 21 de diciembre de 2017.*

Orden PRA/116/2017, de 9 de febrero, por la que se publica el acuerdo del Consejo

de Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. *Boletín Oficial del Estado núm. 38, de 14 de febrero de 2017.*

Orden INT/1149/2018, de 29 de octubre, por la que se regula la organización y el funcionamiento de la Red Nacional de Radio de Emergencia. *Boletín Oficial del Estado núm. 263, de 31 de octubre de 2018.*

UNE 23500:2021. Sistemas de abastecimiento de agua contra incendios*. Norma Española de septiembre de 2021. Versión corregida, Febrero 2022*

Real Decreto 524/2023, de 20 de junio, por el que aprueba la Norma Básica de Protección Civil. *Boletín Oficial del Estado núm. 147, de 21 de junio de 2023.*

ÁMBITO DE LA SEGURIDAD CIUDADANA

Ley Orgánica 2/1986 de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. *Boletín Oficial del Estado núm. 63, de 14 de marzo de 1986.*

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado núm. 281, de 24 de noviembre de 1995*

Ley Orgánica 4/2015 de 30 de marzo, de Protección de la Seguridad Ciudadana. *Boletín Oficial del Estado núm. 77, de 31 de marzo de 2015.*

Real Decreto 726/2020, de 4 de agosto, por el que se modifica el Reglamento de Armas, aprobado por el Real Decreto 137/1993, de 29 de enero. *Boletín Oficial del Estado núm.211, de 5 de agosto de 2020*

ÁMBITO DE LA SEGURIDAD CONTRAINCENDIOS

Real Decreto 314/2006, de 17 de marzo, por el que se aprueba el Código Técnico de la Edificación. *Boletín Oficial del Estado núm. 74, de 28 de marzo de 2006.*

- ✓ Documentos. Básicos de Seguridad Contra Incendios **(DB-SI)**.
- ✓ Documentos Básicos de Seguridad de utilización y accesibilidad. **(DB-SUA).**

UNE-23007-14-2014. Sistemas de detección y alarma de incendios. *Norma Española de 2014.*

Real Decreto 513/2017, de 22 de mayo, por el que se aprueba el Reglamento de Instalaciones de Protección contra incendios**. (RIPCI 2017).** *Boletín Oficial del Estado núm. 139, de 12 de junio de 2017.*

Real Decreto 656/2017, de 23 de Junio, por el que se aprueba el Reglamento de Almacenamiento de Productos Químicos y sus Instrucciones Técnicas

Complementarias MIE APQ 0 a 10. *Boletín Oficial del Estado núm. 176, de 25 de julio de 2017.*

ITC MIE-APQ-5**:** Almacenamiento y utilización de botellas y botellones de gases comprimidos, licuados y disueltos a presión. *Boletín Oficial del Estado núm. 176, de 25 de julio de 2017.*

Real Decreto 809/2021, de 21 de septiembre, por el que se aprueba el Reglamento de equipos a presión y sus instrucciones técnicas complementarias (en vigor desde el 2 de enero del 2022). *Boletín Oficial del Estado núm. 243, de 11 de octubre de 2021.*

ÁMBITO DE LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas. *Boletín Oficial del Estado núm. 102, de 29 de abril de 2011.*

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas. *Boletín Oficial del Estado núm. 121, de 21 de mayo de 2011.*

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. *Boletín Oficial del Estado núm. 224, de 18 de septiembre de 2015.*

https://eur-lex.europa.eu/eli/dir/2022/2555, Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo. *Official Journal of the European Union. L333/80 27/12/2022.*

ÁMBITO DE LA PROTECCIÓN DE DATOS

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. (Actualización del 02 de Julio de 2021). *Boletín Oficial del Estado núm. 106, de 4 de mayo de 1993.*

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos. *Diario Oficial de la Unión Europea, L119/1 de 27 de abril de 2024.*

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado núm. 294, de 6 de diciembre de 2018.*

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. *Boletín Oficial del Estado núm. 126, de 27 de mayo de 2021.*

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado núm. 106, de 4 de mayo de 2022.*

ÁMBITO DE LA CIBERSEGURIDAD

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. *Boletín Oficial del Estado núm. 109, de 7 de mayo de 2022.*

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *Boletín Oficial del Estado núm. 166, de 12 de julio de 2002.*

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. *Boletín Oficial del Estado núm. 251, de 19 de octubre de 2007.*

Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. *Boletín Oficial del Estado núm. 230, de 25 de septiembre de 2007.*

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. *Boletín Oficial del Estado núm. 25, de 29 de enero de 2010.*

Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración. *Boletín Oficial del Estado núm. 271, de 10 de noviembre de 2011.*

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *Boletín Oficial del Estado núm. 114, de 10 de mayo de 2014.*

Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social. *Boletín Oficial del Estado núm. 117, de 14 de mayo de 2014*

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. *Boletín Oficial del Estado núm. 233, de 29 de septiembre de 2015.*

Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. *Boletín Oficial del Estado núm. 309, de 21 de diciembre de 2017.*

Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. *Boletín Oficial del Estado núm. 38, de 14 de febrero de 2017.*

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. *Boletín Oficial del Estado núm. 218, de 8 de septiembre de 2018*

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. *Boletín Oficial del Estado núm. 20, de 23 de enero de 2018.*

Ley 1/2019, de 20 de febrero, de Secretos Empresariales. *Boletín Oficial del Estado núm. 45, de 21 de febrero de 2019.*

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado núm. 103, de 30 de abril de 2019*

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. *Boletín Oficial del Estado núm. 24, de 28 de enero de 2021*

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado núm. 106, de 4 de mayo de 2022.*

ÁMBITO DE LA PREVENCIÓN DE RIESGOS LABORALES

Real Decreto 2291/1985 de 8 de noviembre, por el que se aprueba el Reglamento de Aparatos de Elevación y Manutención de los mismos. *Boletín Oficial del Estado núm. 296, de 11 de diciembre de 1985.*

Ley 31/1995 de 8 de noviembre, de Prevención de Riesgos Laborales. *Boletín Oficial del Estado núm. 269, de 10 de noviembre de 1995.*

Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención. *Boletín Oficial del Estado núm. 27, de 31 de enero de 1997*

Real Decreto 485/1997, de 14 de abril, sobre disposiciones mínimas de señalización de Seguridad y Salud en el Trabajo. *Boletín Oficial del Estado núm. 97, de 23 de abril de 1997.*

Real Decreto 486/1997, de 14 de abril, sobre disposiciones mínimas de Seguridad y Salud en los Lugares de Trabajo. *Boletín Oficial del Estado núm. 97, de 23 de abril de 1997.*

Real Decreto 664/1997, del 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo. *Boletín Oficial del Estado núm. 124, de 24 de mayo de 1997.*

Real Decreto 773/1997, de 30 de mayo, sobre disposiciones mínimas de seguridad y salud relativas a la utilización por los trabajadores de equipos de protección individual. *Boletín Oficial del Estado núm. 97, de 12 de junio 1997.*

NTP[84] 361: Planes de Emergencia en lugares de pública concurrencia. *Instituto Nacional de Seguridad e Higiene en el trabajo. Año 1999.*

NTP 368: Extinción de Incendios: Plan de revisión de equipos. *Instituto Nacional de Seguridad e Higiene en el trabajo. Año 1999.*

NTP 436: Cálculo estimativo de vías y tiempos de evacuación. *Instituto Nacional de Seguridad e Higiene en el trabajo. Año 1999.*

NTP 404: Escaleras fijas. *Instituto Nacional de Seguridad e Higiene en el trabajo. Año 1999.*

Real Decreto 374/2001, de 6 de abril, sobre la protección de la salud y seguridad de los trabajadores contra los riesgos relacionados con los agentes químicos durante el trabajo. *Boletín Oficial del Estado núm. 104, de 1 de mayo de 2001.*

Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la Prevención de Riesgos Laborales. *Boletín Oficial del Estado núm. 298, de 13 de diciembre de 2003.*

Real Decreto 171/2004, de 30 de enero, por el que se desarrolla el artículo 24 de la Prevención de Riesgos Laborales, en materia de coordinación de actividades empresariales. *Boletín Oficial del Estado núm. 27, de 31 de enero de 2004*

NTP 888: Señalización de emergencia en los centros de trabajo. *Instituto Nacional de Seguridad e Higiene en el trabajo. Año 2010*

Real Decreto 88/2013, de 8 de febrero, por el que se aprueba la Instrucción Técnica Complementaria AEM 1 "Ascensores" del Reglamento de aparatos de elevación y manutención, aprobado por Real Decreto 2291/1985, de 8 de noviembre. *Boletín Oficial*

[84]Las Notas Técnicas de Prevención (NTP), son Guías de buenas prácticas. Sus indicaciones no son obligatorias, salvo que estén recogidas en una disposición normativa vigente. A efectos de valorar la pertinencia de las recomendaciones contenidas en una NTP concreta es conveniente tener en cuenta su fecha de edición. Estas Notas Técnicas de Prevención son publicadas por el Instituto Nacional de Seguridad e Higiene en el Trabajo.

del Estado núm. 46, de 22 de febrero de 2013

ITC MIE-APQ-5 Almacenamiento y utilización de botellas y botellones de gases comprimidos, licuados y disueltos a presión". *Boletín Oficial del Estado núm. 176, de 25 de julio de 2017.*

ÁMBITO DE LA BIOSEGURIDAD

Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública. *Boletín Oficial del Estado núm. 102, de 29 de abril de 1986.*

Ley 14/1986, de 14 de abril, General de Sanidad. *Boletín Oficial del Estado núm. 102, de 29 de abril de 1986.*

Ley 1/1999, de 29 de enero, de Residuos de Canarias. *Boletín Oficial del Estado núm. 46, de 23 de febrero de 1999.*

Real Decreto 486/1997, de 14 de abril, sobre disposiciones mínimas de Seguridad y Salud en los Lugares de Trabajo. *Boletín Oficial del Estado núm. 97, de 23 de abril de 1997.*

Real Decreto 664/1997, del 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo. *Boletín Oficial del Estado núm. 124, de 24 de mayo de 1997.*

Real Decreto 773/1997, de 30 de mayo, de disposiciones mínimas de seguridad y salud relativas a la utilización de los trabajadores de equipos de protección individual. *Boletín Oficial del Estado núm. 140, de 12 de junio de 1997.*

Decreto 104/2002, de 26 de julio, de ordenación de la gestión de residuos sanitarios de Canarias. *Boletín Oficial de Canarias núm. 109, de 14 de agosto de 2002.*

UNE EN 100012, Higienización de Sistemas de Climatización. *Norma Española de 19 de enero de 2005.*

Real Decreto 1027/2007, de 20 de julio, por el que se aprueba el Reglamento de Instalaciones Térmicas en los Edificios. *Boletín Oficial del Estado núm. 207, de 29 de agosto de 2007.*

Directiva 2008/98/CE, de residuos. *Diario Oficial de la Unión Europea. L312/3 de 22 de noviembre de 2008.*

Ley 42/2010, de 30 de diciembre, por la que se modifica la Ley 28/2005, de 26 de diciembre, de medidas sanitarias frente al tabaquismo y reguladora de la venta, el

suministro, el consumo y la publicidad de los productos del tabaco. *Boletín Oficial del Estado núm. 318, de 31 de diciembre de 2010.*

Ley 33/2011, de 4 de octubre, General de Salud Pública. *Boletín Oficial del Estado núm. 240, de 5 de octubre de 2011.*

Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la crisis sanitaria por el Covid-19. *Boletín Oficial del Estado núm. 67, de 14 de marzo de 2020*

Real Decreto 926/2020, de 25 de octubre, por el que se declara el estado de alarma para contener la propagación de infecciones causadas por el SARS-COV-2. *Boletín Oficial del Estado núm. 282, de 25 de octubre de 2020.*

Real Decreto 487/2022, de 21 de junio, por el que se establecen los requisitos sanitarios para la prevención y el control de la legionelosis. *Boletín Oficial del Estado núm. 148, de 22 de junio de 2022.*

ÁMBITO DE LA IMAGEN INSTITUCIONAL.

Real Decreto 1465/1999, de 17 de septiembre, por el que se establecen criterios de imagen institucional y se regula la producción documental y el material impreso de la Administración General del Estado. *Boletín Oficial del Estado núm. 230, de 25 de septiembre de 1999.*

Decreto 184/2004, de 21 de diciembre, por el que se aprueba la identidad corporativa del Gobierno de Canarias y se establecen las normas para su tratamiento y utilización. *Boletín Oficial de Canarias núm. 4, de 7 de enero de 2005.*

ANEXO I

Glosario de Términos

ANEXO I

GLOSARIO DE TÉRMINOS Y DEFINICIONES SINGULARES

- ✓ **Activo**: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (*software*), equipos (*hardware*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (ENS, 2022, p. 76).
- ✓ **Acto Terrorista:** Acción violenta o amenaza de violencia llevada a cabo con el objetivo de generar miedo, pánico o causar daño a una población civil o instituciones gubernamentales.
- ✓ **Acto Terrorista:** Acción violenta o amenaza de violencia llevada a cabo con el objetivo de generar miedo, pánico o causar daño a una población civil o instituciones gubernamentales.
- ✓ **Administrador del sistema:** persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo. (ENS, 2022, p. 76).
- ✓ **AGE*:*** Administración General del Estado.
- ✓ ***Al-Fatah*:** Término árabe para "la conquista", a menudo utilizado por grupos yihadistas para referirse a la expansión del islam por medios militares.
- ✓ ***Al-Hijra*:** Migración o emigración en nombre del islam, a veces utilizada por yihadistas para justificar la lucha en territorios extranjeros.
- ✓ ***Al-Qaeda*:** Organización terrorista fundada por Osama bin Laden, responsable de numerosos ataques terroristas a nivel mundial, incluidos los ataques del 11 de septiembre de 2001 en Estados Unidos.
- ✓ ***Al-Wala' Wal-Bara'*:** Concepto yihadista que promueve la lealtad exclusiva a los musulmanes y el rechazo absoluto de los no musulmanes.
- ✓ **Amenaza:** Cualquier evento, acto o fenómeno que tiene el potencial de causar daño a una entidad o sistema.
- ✓ **Análisis de riesgos:** proceso de evaluación y comprensión de los riesgos mediante la identificación de amenazas, la evaluación de vulnerabilidades y la estimación de

consecuencias. Supone, por tanto, Proceso de reconocimiento y descripción de amenazas potenciales que podrían afectar a una entidad o sistema. Eestudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra. (ENS, 2022, p. 76).

- ✓ **Análisis de Vulnerabilidades:** Evaluación sistemática de las debilidades de un sistema que podrían ser explotadas por amenazas.
- ✓ **Apología del Terrorismo:** Promoción o justificación pública de actos terroristas o de sus ideologías, ya sea verbalmente, por escrito o a través de medios de comunicación.
- ✓ **Área controlada:** zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella. (ENS, 2022, p. 76).
- ✓ **Arquitectura de seguridad:** conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas. (ENS, 2022, p. 76).
- ✓ **Auditoría de la seguridad:** es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios. (ENS, 2022, p. 76).
- ✓ **Autenticación multifactor:** exigencia de dos o más factores de autenticación para ratificar una autenticación como válida. (ENS, 2022, p. 76).
- ✓ **Autenticación:** ratificación de la identidad de un usuario, proceso o dispositivo. (ENS, 2022, p. 76).
- ✓ **Autenticador**: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios. (ENS, 2022, p. 76).
- ✓ **Autenticidad**: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. (ENS, 2022, p. 76).
- ✓ **Biometría** (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento. (ENS, 2022, p. 76).
- ✓ **Bioterrorismo:** Uso de agentes biológicos o toxinas para causar enfermedades o muertes en humanos, animales o plantas con fines terroristas.

- ✓ ***Boko Haram:*** Grupo islamista radical nigeriano.
- ✓ **Cadena de suministro:** conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final. (ENS, 2022, p. 76).
- ✓ **Cadena de Suministro Resiliente:** Una red de proveedores y recursos que están diseñados para resistir y recuperarse de interrupciones o perturbaciones.
- ✓ **Califato:** Un estado islámico gobernado por la ley islámica, según la interpretación *yihadista* radical.
- ✓ **Capacidad de Adaptación:** La capacidad de ajustar y modificar las operaciones, políticas y procedimientos de una entidad o sistema para hacer frente a cambios en el entorno o en las condiciones de riesgo.
- ✓ **Capacidad de Recuperación:** La habilidad de una entidad o sistema para recuperarse rápidamente después de un incidente o crisis.
- ✓ **Capacidad de Respuesta:** La habilidad de un hospital para movilizar recursos y tomar acciones efectivas durante una emergencia o desastre para proteger a pacientes, personal y activos.
- ✓ **Capacitación en Seguridad:** Entrenamiento del personal hospitalario en medidas de seguridad, manejo de emergencias y primeros auxilios para mejorar la preparación y la respuesta ante situaciones críticas.
- ✓ **Capacitación y Educación:** Actividades diseñadas para mejorar el conocimiento y las habilidades del personal hospitalario en materia de seguridad y respuesta a emergencias.
- ✓ **Categoría de seguridad de un sistema:** es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios. (ENS, 2022, p. 76).
- ✓ **Célula terrorista:** Grupo de individuos que trabajan juntos para planificar y llevar a cabo actos terroristas.

- ✓ **Centro de Operaciones de Emergencia (COE):** Unidad centralizada dentro del hospital responsable de coordinar y dirigir la respuesta a emergencias y desastres.
- ✓ **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. (ENS, 2022, p. 76).
- ✓ **Certificado de firma electrónica** (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona. (ENS, 2022, p. 76).
- ✓ **Ciberamenaza**: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. (ENS, 2022, p. 76).
- ✓ **Ciberataque:** cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos. (ENS, 2022, p. 76).
- ✓ **Ciberespacio:** dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual. (ENS, 2022, p. 77).
- ✓ **Ciberincidente**: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio. (ENS, 2022, p. 77).
- ✓ **Ciberseguridad** (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. (ENS, 2022, p. 77).
- ✓ **Ciberterrorismo:** Uso de tecnología informática y redes de computadoras para llevar a cabo ataques terroristas o promover objetivos terroristas.
- ✓ ***CiberYihad*:** Uso de Internet y redes sociales por parte de yihadistas para reclutar, radicalizar y coordinar ataques.

- ✓ **Comité de Seguridad Hospitalaria:** Grupo multidisciplinario encargado de supervisar y coordinar las actividades relacionadas con la seguridad en un hospital.
- ✓ **Compromiso de la seguridad:** incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado. (ENS, 2022, p. 77).
- ✓ **Comunicación de Crisis:** proceso para transmitir información precisa, oportuna y comprensible durante una emergencia, garantizando una coordinación efectiva entre todas las partes involucradas.
- ✓ **Comunicación de Riesgos:** El intercambio de información sobre riesgos entre partes interesadas para facilitar la toma de decisiones informadas y la acción coordinada.
- ✓ **Comunidad de Práctica:** Grupo de profesionales que comparten conocimientos, experiencias y mejores prácticas en gestión de riesgos.
- ✓ **Confidencialidad**: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. (ENS, 2022, p. 77).
- ✓ **Conformidad Regulatoria:** Cumplimiento de leyes, regulaciones y estándares relacionados con la gestión de riesgos y la seguridad.
- ✓ **Contrainteligencia:** Actividades y medidas para detectar, prevenir y neutralizar las amenazas a la seguridad de una organización o país provenientes de servicios de inteligencia enemigos o actividades de espionaje.
- ✓ **Contraseña de un solo uso** (*One-Time Password –OTP-*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado. (ENS, 2022, p. 77).
- ✓ **Contraseña**: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta. (ENS, 2022, p. 77).
- ✓ **Control de Acceso:** Medidas para regular y restringir el acceso a áreas sensibles del hospital, como salas de operaciones, farmacias y salas de almacenamiento de medicamentos.
- ✓ **Control de Acceso:** Medidas para regular y restringir el acceso a áreas sensibles del hospital, como salas de operaciones, farmacias y salas de almacenamiento de medicamentos.

- ✓ **Control de Infecciones:** Medidas para prevenir y controlar la propagación de enfermedades infecciosas dentro del hospital, incluyendo prácticas de higiene, desinfección y aislamiento de pacientes.
- ✓ **Control de Infecciones:** Medidas para prevenir y controlar la propagación de enfermedades infecciosas dentro del hospital, incluyendo prácticas de higiene, desinfección y aislamiento de pacientes.
- ✓ **Control de Riesgos:** Implementación de medidas preventivas o correctivas para gestionar y reducir los riesgos a niveles aceptables.
- ✓ **Control de rondas:** sistema por el cual el profesional, de manera dinámica, pasa por diversos puntos, previamente establecidos para detectar de manera preventiva determinados elementos de protección y funcionamiento, dejando constancia de su estado funcional-operativo, siendo proactivo para su resolución.
- ✓ **Crisis:** Una situación de emergencia o desastre que pone en peligro la vida, la propiedad o el bienestar de las personas y que requiere una respuesta inmediata.
- ✓ **Daño:** Los efectos negativos resultantes de una amenaza materializada, que pueden ser físicos, financieros, sociales o emocionales.
- ✓ ***Dawah*:** Proselytismo islámico, a veces utilizado por grupos yihadistas para reclutar seguidores y simpatizantes.
- ✓ **Desradicalización:** Proceso de reintegración de individuos radicalizados en la sociedad, a menudo mediante programas de rehabilitación y desvinculación ideológica.
- ✓ **Disponibilidad**: propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. (ENS, 2022, p. 77).
- ✓ **Dispositivo de autenticación (*token*):** autenticador físico. (ENS, 2022, p. 77).
- ✓ **Distintivo de Certificación de Conformidad con el ENS:** documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate. (ENS, 2022, p. 77).
- ✓ **Distintivo de Declaración de Conformidad con el ENS:** documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un

enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate. (ENS, 2022, p. 77).

- ✓ **Doctrina Terrorista:** Conjunto de creencias, principios y estrategias que guían las acciones de un grupo terrorista.
- ✓ **Dominio de seguridad:** colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo: a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles. b) Servidor central (*host*), frontal *Unix* y equipos administrativos. c) Seguridad física, seguridad lógica. (ENS, 2022, p. 77).
- ✓ **Eco-terrorismo:** Uso de acciones violentas o amenazas de violencia para promover objetivos ambientales o proteger el medio ambiente.
- ✓ **Edificio e instalación:** se refiere al inmueble y las instalaciones que este contenga y que es objeto de la vigilancia y protección.
- ✓ **Efectividad:** La medida en que las acciones tomadas para gestionar un riesgo logran sus objetivos previstos.
- ✓ **Equipos de Intervención Rápida:** Grupos de personal entrenado y equipado para responder de manera inmediata a emergencias médicas y situaciones críticas en el hospital.
- ✓ **Estado Islámico (ISIS o ISIL):** Grupo terrorista *yihadista* que ha llevado a cabo numerosos ataques terroristas en todo el mundo en nombre del islam radical, estableciendo un "califato" en partes de Irak y Siria.
- ✓ **Estado Islámico (ISIS):** Grupo *yihadista* extremista que busca establecer un califato islámico en varias regiones del mundo.
- ✓ **ETA:** Acrónimo de *Euskadi Ta Askatasuna.* Grupo terrorista vasco.
- ✓ **Evaluación de Impacto en el Negocio:** Análisis de las consecuencias potenciales de un evento adverso en las operaciones y la viabilidad de una organización.
- ✓ **Evaluación de Riesgos:** Análisis sistemático de la magnitud de los riesgos identificados, incluyendo amenazas naturales, tecnológicas y humanas incluyendo la probabilidad de ocurrencia y las consecuencias asociadas.
- ✓ **Evaluación de Vulnerabilidades:** Análisis de los puntos débiles y las áreas de riesgo en un hospital que podrían ser explotados por amenazas internas o externas.

- ✓ **Evento de seguridad:** ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad. (ENS, 2022, p. 77).
- ✓ **Exposición al Riesgo:** La medida en que una entidad o sistema está expuesto a la ocurrencia de un riesgo.
- ✓ **Extremismo:** Adhesión a puntos de vista extremos o radicales, a menudo con disposición a usar la violencia para lograr objetivos políticos o ideológicos.
- ✓ **Factor de autenticación:** hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría. (ENS, 2022, p. 77).
- ✓ **FARC:** Fuerzas Armadas Revolucionarias de Colombia, grupo guerrillero y político colombiano que ha estado involucrado en conflictos armados y actividades terroristas en ese país.
- ✓ ***Fatwa* contra la democracia:** Edicto religioso emitido por líderes yihadistas que prohíbe la participación en sistemas democráticos no islámicos.
- ✓ ***Fatwa*:** Edicto religioso emitido por un líder religioso musulmán, a veces utilizado para justificar acciones violentas en nombre del islam.
- ✓ **Financiaciación del Terrorismo:** Provisión de recursos financieros o materiales a individuos o grupos terroristas para apoyar sus actividades.
- ✓ **Firma electrónica:** los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar. (ENS, 2022, p. 77).
- ✓ **Firma electrónica avanzada:** la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. (ENS, 2022, p. 77).
- ✓ **Firma electrónica cualificada:** una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. (ENS, 2022, p. 77).
- ✓ **Fundamentalismo:** Adhesión rígida y a menudo literal a principios ideológicos o religiosos, asociada con la intolerancia hacia otras creencias y prácticas.

- ✓ **Fusión de Inteligencia:** Integración y análisis de información proveniente de diversas fuentes para producir inteligencia significativa y oportuna, para identificar y prevenir amenazas *yihadistas*.
- ✓ **Gestión de Crisis:** Coordinación de esfuerzos para manejar situaciones críticas o desastres, minimizando su impacto y restaurando la normalidad lo antes posible.
- ✓ **Gestión de Desastres:** Conjunto de actividades coordinadas para prepararse, mitigar, responder y recuperarse de un desastre, minimizando sus impactos en la salud pública y la infraestructura.
- ✓ **Gestión de Incidentes:** Coordinación de acciones para manejar y resolver incidentes de seguridad, minimizando su impacto en la salud y la seguridad de las personas o el funcionamiento de una entidad o sistema. Procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste. (ENS, 2022, p. 77).
- ✓ **Gestión de riesgos:** actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos. (ENS, 2022, p. 78).
- ✓ **Gestión de Riesgos Hospitalarios:** Proceso sistemático para identificar, evaluar y mitigar los riesgos potenciales que pueden afectar la seguridad en un hospital.
- ✓ **Gobernanza de una Infraestructura Crítica :** Marco de políticas, regulaciones y procesos de toma de decisiones que rigen la seguridad, operación y gestión de una Infraestructura Crítica , involucrando a múltiples partes interesadas. Coordinación y supervisión de las actividades y recursos necesarios para proteger y mantener la Infraestructura Crítica de una nación.
- ✓ **Guerra Asimétrica:** Conflicto entre partes desiguales en términos de poder militar, en el que las tácticas no convencionales y la asimetría de fuerzas son características distintivas.
- ✓ ***Hadiz*:** Colección de dichos y acciones del Profeta Mahoma, a menudo citados por yihadistas para respaldar sus acciones y que, junto con el Corán, constituyen la fuente primaria de la ley islámica.
- ✓ ***Hezbollah***: Grupo paramilitar y político chiita libanés, considerado una organización terrorista por varios países occidentales.
- ✓ **Identificación de Riesgos:** Proceso de reconocimiento y descripción de amenazas potenciales que podrían afectar a una entidad o sistema.
- ✓ **Impacto:** El efecto o consecuencia de un evento en términos de daños, pérdidas o interrupciones.

- ✓ **Implicaciones:** Las posibles consecuencias o efectos secundarios de una acción o decisión.
- ✓ **Incidente de seguridad** (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información. (ENS, 2022, p. 78).
- ✓ **Índice de Seguridad Hospitalaria (ISH):** Una herramienta desarrollada por la OMS para evaluar y mejorar la seguridad en los hospitales, centrándose en la preparación y respuesta a emergencias y desastres.
- ✓ **Inspecciones de Seguridad:** Revisiones periódicas de instalaciones, equipos y procedimientos para identificar y corregir deficiencias en la seguridad del hospital.
- ✓ **Integridad**: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. (ENS, 2022, p. 78).
- ✓ **Inteligencia de fuentes abiertas** (*OSINT*): Recopilación de información de fuentes públicas y accesibles, como medios de comunicación, internet o documentos públicos.
- ✓ **Inteligencia de fuentes humanas** (*HUMINT*): Recopilación de información a través de fuentes humanas, como informantes, agentes encubiertos o entrevistas.
- ✓ **Inteligencia de imágenes** (*IMINT*): Recopilación y análisis de imágenes y fotografías para obtener información de inteligencia.
- ✓ **Inteligencia de señales** (*SIGINT*): Recopilación y análisis de información de comunicaciones electrónicas, como interceptación de radio o monitorización de señales.
- ✓ **Inteligencia geoespacial** (*GEOINT*): Utilización de datos y análisis geográficos para obtener información de inteligencia.
- ✓ **Interdependencia de Riesgos:** La relación entre diferentes riesgos y cómo la ocurrencia de uno puede afectar la probabilidad o el impacto de otros.
- ✓ **Investigación Posterior al Incidente:** El análisis de las causas y circunstancias que rodean un incidente o crisis para identificar lecciones aprendidas y oportunidades de mejora.
- ✓ ***Jihad al-Nikah:*** Interpretación radical de la yihad que justifica el uso de la violencia sexual en nombre del islam. Interpretación radical del concepto de "jihad sexual" que justifica la esclavitud sexual de mujeres no musulmanas.
- ✓ ***Jihadismo* Global:** Extensión de la ideología y las actividades *yihadistas* más allá de una región específica, con células y simpatizantes en todo el mundo.

- ✓ ***Jihadista*:** Persona que apoya o participa en la yihad, especialmente de manera violenta.
- ✓ **Legislación Antiterrorista:** Conjunto de leyes y disposiciones jurídicas diseñadas para prevenir, detectar y castigar actos y actividades terroristas.
- ✓ **Legitimación del uso de la violencia:** Justificación o autorización de la violencia en nombre de una causa política, religiosa o ideológica.
- ✓ **Ley de la Abrogación (*Naskh*):** Interpretación radical del islam que justifica la anulación de versículos pacíficos del Corán por versículos violentos.
- ✓ **Lista de componentes *software*:** documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio. (ENS, 2022, p. 78).
- ✓ **Lobo Solitario:** Individuo radicalizado que actúa solo en nombre del *yihadismo*, a menudo llevando a cabo ataques terroristas.
- ✓ **Lucha contra el Terrorismo**: Esfuerzos y acciones coordinadas para prevenir, mitigar y responder a amenazas y actos terroristas.
- ✓ ***Madrassa*:** Escuela islámica, a veces asociada con la radicalización y la formación de militantes yihadistas, que enseña el Corán y la ley islámica.
- ✓ **Mártir (Shaheed):** Persona que muere en la yihad o en el camino de Alá, considerada una figura honorable en la ideología yihadista.
- ✓ **Medidas de seguridad[85]:** conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. (ENS, 2022, p. 78).
- ✓ **Mejora Continua:** Proceso sistemático para identificar oportunidades de mejora en la seguridad hospitalaria e implementar acciones correctivas y preventivas.
- ✓ **Mínimo privilegio:** principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento. (ENS, 2022, p. 78).
- ✓ **Mitigación de Riesgos:** Reducción de las consecuencias adversas de un riesgo que ya ha ocurrido o que no se puede eliminar por completo.
- ✓ **Modelado de Riesgos:** Utilización de técnicas y herramientas para prever y cuantificar la probabilidad y el impacto de eventos adversos futuros.

[85] Ámbito Ciberespacial.

- ✓ **Monitorización continua:** proceso de gestión dinámica de la seguridad, basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información. (ENS, 2022, p. 78).
- ✓ ***Mujahideen*:** Combatientes yihadistas que luchan en nombre del islam, a menudo contra los no creyentes o las fuerzas consideradas enemigas del islam.
- ✓ **Neutralización de Riesgos:** Acciones destinadas a eliminar o reducir la probabilidad de ocurrencia de un riesgo.
- ✓ **Observatorio Digital**: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza. (ENS, 2022, p. 78).
- ✓ **Operativo:** Miembro de un grupo *yihadista* encargado de llevar a cabo operaciones terroristas. También, relacionado con la realización de operaciones, especialmente aquellas de naturaleza táctica o estratégica.
- ✓ **Perfil de cumplimiento específico:** conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN. (ENS, 2022, p. 78).
- ✓ **PIN**: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación. (ENS, 2022, p. 78).
- ✓ **Plan de Contingencia:** Plan detallado de acciones a seguir en caso de que ocurra un evento adverso o una emergencia.
- ✓ **Plan de Continuidad del Negocio:** Estrategias para garantizar la prestación continua, de servicios de salud durante situaciones de crisis o desastres que puedan afectar la operación normal del hospital.
- ✓ **Plan de Seguridad Hospitalaria:** Documento que establece las políticas, procedimientos y responsabilidades para gestionar situaciones de emergencia y proteger la seguridad en un hospital, de los pacientes, el personal y las instalaciones.
- ✓ **Planes de Emergencia y Continuidad del Negocio:** Documentos que establecen los procedimientos y acciones a seguir antes, durante y después de una emergencia para garantizar la continuidad de las operaciones hospitalarias.

- ✓ **Política de firma electrónica**, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos. (ENS, 2022, p. 78).
- ✓ **Política de seguridad** (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. (ENS, 2022, p. 78).
- ✓ **Preparación Hospitalaria:** La capacidad de un hospital para planificar, organizar y desarrollar medidas de seguridad para responder efectivamente a emergencias y desastres.
- ✓ **Prevención del Terrorismo:** Conjunto de medidas y políticas diseñadas para evitar, detectar y mitigar la amenaza del terrorismo, incluyendo la vigilancia, inteligencia, seguridad fronteriza y cooperación internacional, así como prevenir la radicalización y reclutamiento de terroristas.
- ✓ **Principios básicos de seguridad:** fundamentos que deben regir toda acción orientada a asegurar la información y los servicios. (ENS, 2022, p. 78).
- ✓ **Probabilidad:** La medida de cuán probable es que ocurra un evento, generalmente expresado como una frecuencia o porcentaje.
- ✓ **Proceso de seguridad:** método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad. (ENS, 2022, p. 78).
- ✓ **Proceso TIC:** conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC. (ENS, 2022, p. 78).
- ✓ **Proceso**: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado. (ENS, 2022, p. 78).
- ✓ **Producto TIC:** elemento o grupo de elementos de las redes o los sistemas de información. (ENS, 2022, p. 78).
- ✓ **Protocolos de Emergencia:** Procedimientos estandarizados para responder eficazmente a situaciones de emergencia, como incendios, evacuaciones, incidentes químicos o biológicos, entre otros.

- ✓ **Radicales violentos:** Individuos que mantienen creencias extremas y están dispuestos a usar la violencia para promover sus objetivos.
- ✓ **Radicalización:** Proceso por el cual un individuo o grupo adopta creencias extremistas o violentas, a menudo como resultado de la exposición a ideologías extremas en respuesta a factores sociales, políticos o religiosos.
- ✓ **Radicalización en línea:** Proceso de radicalización que ocurre a través de plataformas en línea, redes sociales y otros medios digitales.
- ✓ **Radicalización en prisión:** Proceso de radicalización que ocurre en el entorno carcelario, donde los individuos pueden entrar en contacto con ideologías extremistas.
- ✓ **Radicalización violenta:** Proceso de radicalización que lleva a la participación activa en actos de violencia o terrorismo.
- ✓ **Reducción de Riesgos:** Acciones dirigidas a disminuir la probabilidad de ocurrencia o el impacto de un riesgo en una entidad o sistema.
- ✓ **Requisitos mínimos de seguridad:** exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados. (ENS, 2022, p. 78).
- ✓ **Reserva de Contingencia:** Recursos o fondos reservados para hacer frente a costos imprevistos asociados con eventos adversos o crisis.
- ✓ **Reserva de Riesgo:** Fondos reservados para cubrir costos asociados con riesgos no asegurados o inesperados.
- ✓ Resiliencia Comunitaria: La capacidad de una comunidad para resistir, adaptarse y recuperarse de desafíos y crisis.
- ✓ **Resiliencia:** La capacidad de recuperarse rápidamente de dificultades o adversidades. Capacidad de una Infraestructura Crítica para resistir, adaptarse y recuperarse rápidamente de perturbaciones, crisis o desastres, manteniendo la prestación de servicios esenciales a la sociedad.
- ✓ **Resiliencia Hospitalaria:** La capacidad de un hospital para adaptarse y recuperarse rápidamente de emergencias y desastres, manteniendo la prestación de servicios de salud.
- ✓ **Responsabilidad Civil:** La obligación legal de una entidad de compensar a terceros por daños o pérdidas causadas por sus actividades o productos.
- ✓ **Responsabilidad Corporativa:** La obligación ética y legal de una entidad de gestionar los riesgos de manera responsable y mitigar los impactos negativos en la sociedad, el medio ambiente y las partes interesadas.

- ✓ **Riesgo:** La probabilidad de que ocurra un evento adverso junto con las consecuencias de ese evento.
- ✓ **Riesgo Residual:** El nivel de riesgo que permanece después de que se hayan implementado medidas de mitigación o control.
- ✓ **Riesgo Tolerable**: Nivel de riesgo que una organización está dispuesta a aceptar en función de sus objetivos y tolerancia al riesgo.
- ✓ **Ronda de Seguridad (RS):** visita planificada realizadas por los vigilantes de seguridad, dentro de un rango horario con el objeto de comprobar el estado de los medios de protección y la seguridad del edificio e instalaciones.
- ✓ **Sagrado Corán:** Texto sagrado del islam, a menudo interpretado de manera extremista por grupos *yihadistas* para justificar la violencia.
- ✓ **Secreto memorizado** (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN. (ENS, 2022, p. 78).
- ✓ **Seguridad:** La protección contra riesgos, amenazas o peligros.
- ✓ **Seguridad corporativa:** conjunto de elementos de previsión, prevención, planificación e intervención que analizan y actúan en la gestión de riesgos, abordando el conjunto de seguridades que existen en una organización, tanto aquellas referidas a la protección de personas y bienes, como el patrimonio común, desde un enfoque integral e integrado.
- ✓ **Seguridad de Datos Médicos:** Protección de la información médica confidencial de los pacientes contra accesos no autorizados o pérdidas de datos.
- ✓ **Seguridad de la Información**: Protección de la información contra accesos no autorizados, divulgación, alteración, destrucción o uso no autorizado.
- ✓ **Seguridad Física:** Protección de personas, activos y recursos contra daños físicos, robos o intrusiones.
- ✓ **Seguridad Hospitalaria:** Conjunto de medidas y protocolos diseñados para garantizar la protección y el bienestar de pacientes, visitantes y personal en un entorno hospitalario.
- ✓ **Seguridad Sanitaria:** Medidas para proteger la salud pública y prevenir la propagación de enfermedades infecciosas.
- ✓ **Seguridad y Salud Ocupacional (OSH):** Prácticas y procedimientos para proteger la seguridad y la salud de los trabajadores en el lugar de trabajo.

- ✓ **Seguro de Riesgo:** Un instrumento financiero que proporciona protección contra pérdidas o daños causados por eventos adversos específicos.
- ✓ **Sentido de Comunidad:** Sentimiento de pertenencia, identificación y responsabilidad compartida entre los miembros de una comunidad.
- ✓ ***Shahada*:** Profesión de fe musulmana, a veces utilizada por *yihadistas* antes de llevar a cabo ataques terroristas.
- ✓ **Sharia:** Ley islámica, interpretada de manera radical por grupos *yihadistas* para justificar la violencia y la imposición de su ideología.
- ✓ **Simulacro:** Ejercicio práctico diseñado para simular una situación de emergencia o desastre y evaluar la respuesta y preparación de los participantes.
- ✓ **Sistema de Gestión de Seguridad:** Marco organizativo para gestionar y mejorar la seguridad, que incluye políticas, procedimientos y controles.
- ✓ **Sistema de información (SI):** cualquiera de los elementos siguientes: 1. º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión. 2. º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales. Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1. º y 2. º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos. (ENS, 2022, p. 79).
- ✓ **Sistema de Información de Seguridad:** Sistema de recopilación, análisis y distribución de información sobre amenazas, riesgos y vulnerabilidades.
- ✓ **Sistemas de Alarmas:** Dispositivos electrónicos que emiten señales audibles o visuales para alertar al personal sobre emergencias o situaciones de peligro.
- ✓ **Sistemas de Alerta Temprana:** Mecanismos utilizados para detectar y advertir sobre posibles amenazas o emergencias, permitiendo una respuesta rápida y efectiva.
- ✓ **Supervisión y Auditoría:** La revisión regular y sistemática de las actividades de gestión de riesgos para garantizar el cumplimiento de políticas, estándares y procedimientos establecidos.
- ✓ **Táctica de Golpe y Fuga:** Estrategia utilizada por *yihadistas* para llevar a cabo ataques rápidos y luego escapar de la captura.

- ✓ **Tácticas Terroristas:** Métodos empleados por grupos terroristas para llevar a cabo sus objetivos, como atentados con bombas, secuestros, asesinatos selectivos, toma de rehenes, entre otros.
- ✓ ***Takfirismo*:** Ideología *yihadista* que justifica la violencia contra musulmanes considerados "herejes" o no verdaderos creyentes.
- ✓ **Talibán:** Grupo insurgente *yihadista* que gobernó Afganistán y continúa siendo una fuerza importante en la región, promoviendo una interpretación extremista de la ley islámica.
- ✓ **TEMPEST:** término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones. (ENS, 2022, p. 79).
- ✓ **Terrorismo:** Uso sistemático de la violencia o la amenaza de violencia para intimidar o coaccionar a una población, gobierno o sociedad en general con fines políticos, religiosos o ideológicos.
- ✓ **Terrorismo de Estado:** Uso por parte de un gobierno de tácticas terroristas o represivas contra su propia población o contra otros estados.
- ✓ **Terrorismo de Proximidad:** Actividades terroristas dirigidas contra objetivos cercanos geográficamente, como instalaciones locales o personas prominentes.
- ✓ **Terrorismo Doméstico:** Actividades terroristas llevadas a cabo por individuos o grupos dentro del propio país, con objetivos políticos, ideológicos o sociales.
- ✓ **Terrorismo Económico:** Uso de amenazas o actos terroristas para afectar la economía de un país o región.
- ✓ **Terrorismo Internacional:** Actividades terroristas que trascienden las fronteras nacionales y pueden involucrar a grupos o individuos de diferentes países.
- ✓ **Terrorismo Mediático:** Uso de medios de comunicación, como Internet, televisión o prensa, para difundir propaganda terrorista o promover objetivos terroristas.
- ✓ **Terrorismo Nuclear:** Amenaza o uso de armas nucleares o materiales nucleares con fines terroristas.
- ✓ **Terrorismo Químico:** Uso de sustancias químicas peligrosas para causar daño, lesiones o muertes con fines terroristas.

- ✓ **Terrorismo Religioso:** Uso de la religión como justificación o motivación para cometer actos terroristas.
- ✓ **Terrorismo Transnacional:** Actividades terroristas que trascienden las fronteras nacionales y que a menudo involucran la colaboración entre grupos de diferentes países.
- ✓ **Terrorista:** Persona o grupo que emplea tácticas terroristas para promover sus objetivos políticos, ideológicos o religiosos.
- ✓ **Tolerancia al Riesgo:** El nivel de riesgo que una entidad o sistema está dispuesta a aceptar antes de tomar medidas adicionales para mitigarlo.
- ✓ **Transparencia:** La divulgación clara y accesible de información relevante sobre riesgos, amenazas y medidas de gestión de riesgos.
- ✓ **Trazabilidad**: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad. (ENS, 2022, p. 79).
- ✓ **USO OFICIAL:** designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad. (ENS, 2022, p. 79).
- ✓ **Usuarios de la organización:** personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización. (ENS, 2022, p. 79).
- ✓ **Usuarios externos:** usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados. (ENS, 2022, p. 79).
- ✓ **Valoración de Riesgos Hospitalarios:** Proceso para identificar y evaluar los riesgos específicos asociados con la prestación de servicios de salud en un entorno hospitalario.
- ✓ **Víctima del Terrorismo:** Persona o grupo que sufre daños físicos, psicológicos o materiales como resultado de un acto terrorista.
- ✓ **Vigilancia Epidemiológica:** Recopilación sistemática y análisis de datos sobre enfermedades y condiciones de salud en una población.
- ✓ **Vigilancia Hospitalaria:** Monitorización constante de actividades y eventos dentro y alrededor del hospital para detectar y prevenir posibles amenazas a la seguridad.

- ✓ **Vigilancia y protección:** aquellos aspectos relacionados con la seguridad humana integral, eficiente e integrada, de forma que englobe, tanto la vigilancia, prevención, protección y seguridad de las personas, los bienes y el patrimonio común.
- ✓ **Vulnerabilidad:** Debilidad o fallo en un sistema que puede ser explotado por amenazas para causar daño o interrupción.
- ✓ ***Wahabismo/Salafismo*:** Corriente del islam extremista que promueve una interpretación puritana y radical del islam, a menudo asociada con el *yihadismo*.
- ✓ ***Yihad*:** Literalmente "esfuerzo" o "lucha" en árabe, a menudo se interpreta como la lucha por la causa de Alá, que puede incluir esfuerzos personales, espirituales o militares.
- ✓ ***Yihad* Económica:** Uso de recursos financieros para apoyar actividades *yihadistas*, incluyendo el financiamiento de ataques terroristas.
- ✓ ***Yihadismo*:** Movimiento ideológico y militar asociado con el islam radical, que promueve la yihad (lucha) como medio para alcanzar objetivos políticos o religiosos. Promueve la lucha armada y el uso de la violencia para defender y expandir el islam.
- ✓ ***Yihadista*:** Individuo que participa en la yihad, ya sea de forma militar o ideológica, en nombre del islam extremista.
- ✓ **Zonas de Riesgo:** Áreas identificadas como propensas a amenazas o peligros específicos que pueden afectar a la seguridad de una entidad o población.

ANEXO II

Glosario de Acrónimos

ANEXO II

GLOSARIO DE ACRÓNIMOS

- ✓ **112:** Número de Emergencias.
- ✓ **11-M**: Atentados del 11 de marzo de 2004, acaecidos en Madrid.
- ✓ **11-S**: Atentados acaecidos el 11 de septiembre de 2001 en Nueva York.
- ✓ **17-B**: Atentados del 17 de abril en Barcelona.
- ✓ **AA.PP.:** Administraciones Públicas.
- ✓ **ACL:** Listas de Control de Acceso.
- ✓ **AEI:** Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información.
- ✓ **AGE:** Administración General del Estado.
- ✓ ***AQAP***: Al Qaeda en la Península Arábiga.
- ✓ ***AQIM***: Al Qaeda en el Magreb Islámico.
- ✓ ***ASG***: Grupo *Abu Sayyaf* (Filipinas).
- ✓ **BCIT:** Brigada Central de Investigación Tecnológica.
- ✓ **BIA:** Análisis de Impacto del Negocio.
- ✓ **BIM:** Modelado de Información de Edificios.
- ✓ ***Boko Haram***: *Jama'atu Ahlis Sunna Lidda'awati wal-Jihad* (Grupo para la Predicación y la *Yihad*).
- ✓ **BPI:** Brigada de Información. Es la unidad de la Policía Nacional encargada de recopilar y analizar información relacionada con la delincuencia organizada, el terrorismo y otros delitos graves.
- ✓ **C4ISR:** Comando, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento.
- ✓ **CCN**: Centro Criptológico Nacional.
- ✓ **CCTA:** Centro Conjunto de Análisis de Amenazas Críticas (Australia).
- ✓ **CCTV:** Circuito Cerrado de Televisión.
- ✓ **CDC:** Centro de Coordinación de Desastres.
- ✓ **CDGAI:** Comisión Delegada del Gobierno para Asuntos de Inteligencia.
- ✓ **CECO:** Centro de Coordinación.
- ✓ **CECOPI:** Centro de Coordinación Operativa Integrada.
- ✓ **CEDEX:** Centro de Estudios y Experimentación de Obras Públicas.
- ✓ **CEGAL:** Centro de Gestión de Alertas.

- ✓ **CEIM:** Centro de Información y Mando.
- ✓ **CFATS:** Programa de Seguridad en Instalaciones Químicas de Alto Riesgo (EE. UU.).
- ✓ **CGI**: Comisaria General de Información de la Policía Nacional.
- ✓ **CI:** Contrainteligencia**.**
- ✓ ***CIA*:** Agencia Central de Inteligencia (*Central Intelligence Agency*).
- ✓ **CICO:** Centro de Inteligencia contra el Crimen Organizado.
- ✓ **CICOB:** Centro de Información y Documentación Internacional de Barcelona.
- ✓ **CIEMAT:** Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas.
- ✓ **CIFAS**: Centro de Información de las Fuerzas Armadas.
- ✓ **CIIP:** Protección de Infraestructuras Críticas y Asociadas (Unión Europea).
- ✓ **CIIP *Directive*:** Directiva sobre la Protección de las Infraestructuras Críticas (Directiva UE 2008/114/EC).
- ✓ **CIP:** Protección de Infraestructuras Críticas.
- ✓ **CIPIC:** Comité de Protección de Infraestructuras Críticas (Canadá).
- ✓ **CIRG:** Grupo de Coordinación de la Infraestructura de la Red de la UE.
- ✓ **CISA:** Agencia de Seguridad de Infraestructuras y Ciberseguridad.
- ✓ **CISCE:** Comité de Infraestructuras Críticas de España.
- ✓ **CITCO:** Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.
- ✓ **CIWIN:** Red de la UE para la protección de Infraestructuras Críticas.
- ✓ **CIWIN-N:** Red de la UE para la protección de Infraestructuras Críticas - Nacional.
- ✓ **CMAC:** Centro de Mando Avanzado de Catástrofes.
- ✓ **CME:** Centro de Mando y Control de Emergencias.
- ✓ **CMEI:** Centro de Mando y Control de Emergencias Integrado.
- ✓ **CNCA**: Centro Nacional de Coordinación Antiterrorista.
- ✓ **CNE:** Comisión Nacional de Emergencias.
- ✓ **CNI**: Centro Nacional de Inteligencia.
- ✓ **CNP**: Cuerpo Nacional de Policía.
- ✓ **CNPC:** Comisión Nacional de Protección Civil.
- ✓ **CNPIC:** Centro Nacional para la Protección de Infraestructuras Críticas.
- ✓ **CNPIC-CIAT:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Inteligencia de Amenazas.
- ✓ **CNPIC-CIEN:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Información y Evaluación Nacional.

- ✓ **CNPIC-CIUD:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Información y Urgencias de Defensa.
- ✓ **CNPIC-COACI:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Observación y Análisis de Ciberamenazas Industriales.
- ✓ **CNPIC-COECI:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Observación y Estudio de Ciberamenazas Industriales.
- ✓ **CNPIC-CTIC:** Centro Nacional para la Protección de Infraestructuras Críticas - Centro de Tratamiento y Coordinación de Incidentes de Ciberseguridad.
- ✓ **COE:** Centro de Operaciones de Emergencia.
- ✓ **COS:** Centro de Operaciones de Socorro.
- ✓ **CPNI:** Centro Nacional de Protección de la Infraestructura (Reino Unido).
- ✓ **CRISP:** Programa de Protección de Sistemas de Información Crítica (Canadá).
- ✓ **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática.
- ✓ **CT:** Contraterrorismo.
- ✓ **CTC:** Centro de Coordinación contra el Terrorismo (Australia).
- ✓ ***DAESH*:** *Al Dawla al Islamiya fi al Iraq wa al Sham* que viene a significar Estado Islámico de Irak y el Levante" o "Estado Islámico de Irak y Siria" (EIIS).
- ✓ **DHS:** Departamento de Seguridad Nacional (EE. UU.).
- ✓ **DHS-CISA:** Agencia de Seguridad de Infraestructuras y Ciberseguridad del Departamento de Seguridad Nacional (EE. UU.).
- ✓ **DHS-OEC:** Oficina de Comunicaciones de Emergencia del Departamento de Seguridad Nacional (EE. UU.).
- ✓ **DOT:** Departamento de Transporte (EE. UU.).
- ✓ **DOT-PHMSA:** Administración de Seguridad y Protección del Transporte de Materiales Peligrosos del Departamento de Transporte (EE. UU.).
- ✓ ***DRONE*:** *Dron Remotamente* Operado de Navegación Aérea. Aeronave no tripulada.
- ✓ **DSN**: Departamento de Seguridad Nacional.
- ✓ **DSS:** Seguridad del Suministro de Datos.
- ✓ **EICTIR**: Estrategia Integral contra el Terrorismo Internacional y la radicalización.
- ✓ **ELN**: Ejército de Liberación Nacional (Colombia).
- ✓ **ELN:** Ejército de Liberación Nacional (Colombia).
- ✓ **EMMI:** Equipo Médico de Intervención.
- ✓ **EMT:** Equipo de Manejo de Emergencias.

- ✓ **ENISA:** Agencia de la Unión Europea para la Ciberseguridad.
- ✓ **ENT**: Estrategia Nacional contra el Terrorismo.
- ✓ **EPC:** Equipos de Primeros Auxilios Comunitarios.
- ✓ **EPE:** Estado de Preparación para Emergencias Químicas.
- ✓ **EPF:** Estado de Preparación para Fenómenos Meteorológicos Adversos.
- ✓ **EPG:** Estado de Preparación para Grandes Riesgos.
- ✓ **EPI:** Equipo de Protección Individual.
- ✓ **EPIC:** Centro de Protección de Infraestructuras Críticas y Cibernéticas (Australia).
- ✓ **EPIR:** Equipo de Protección Individual Respiratorio.
- ✓ **EPSAR:** Equipos de Psicología en Situaciones de Alto Riesgo.
- ✓ **ERIE:** Equipo de Respuesta Inmediata en Emergencias.
- ✓ **ETA**: En Euskera, *Euskadi Ta Askatasuna* que, significa País Vasco y Libertad.
- ✓ **EU-CIP:** Plan de Protección de Infraestructuras Críticas de la Unión Europea.
- ✓ **FAA:** Administración Federal de Aviación (EE. UU.).
- ✓ **FARC**: Fuerzas Armadas Revolucionarias de Colombia.
- ✓ **FAS**: Fuerzas Armadas.
- ✓ **FEMA:** Agencia Federal para el Manejo de Emergencias (EE. UU.).
- ✓ **FERC:** Comisión Federal de Regulación de Energía (EE. UU.).
- ✓ **FFCCS**: Fuerzas y Cuerpos de Seguridad.
- ✓ **FFCSE**: Fuerzas y Cuerpos de Seguridad del Estado.
- ✓ **FSA:** Ejército Libre Sirio.
- ✓ **GC:** Guardia Civil.
- ✓ **GCN:** Grupo de Coordinación Nacional.
- ✓ **GEOINT**: Inteligencia geoespacial.
- ✓ **HAMAS:** Movimiento de Resistencia Islámica (Palestina).
- ✓ ***HEZBOLLA*:** Partido de Dios (Líbano).
- ✓ ***HUM*:** *Harkat-ul-Mujahideen* (Movimiento de los Guerreros).
- ✓ ***HUMINT***: Inteligencia de fuentes humanas.
- ✓ **ICN:** Infraestructuras Críticas Nacionales.
- ✓ **ICS:** Sistema de Comando de Incidentes.
- ✓ **ICS-CERT:** Equipo de Respuesta a Emergencias Informáticas y de Control Industrial.
- ✓ ***IMINT***: Inteligencia de imágenes.
- ✓ **IMT:** Movimiento Islámico de Turquestán (China).

- ✓ **IMU:** Movimiento Islámico de Uzbekistán.
- ✓ **IPI:** Información Personal Identificable.
- ✓ **IRA**: Ejército Republicano Irlandés.
- ✓ **IRA:** Ejército Republicano Irlandés.
- ✓ **IS:** Estado Islámico.
- ✓ **ISA:** Análisis de Seguridad de la Infraestructura.
- ✓ **ISAC:** Centro de Análisis de la Información de Seguridad.
- ✓ ***ISIL***: Estado Islámico de Irak y el Levante.
- ✓ **ISIL-KP**: Estado Islámico de Irak y el Levante - Provincia de Jorasán.
- ✓ ***ISIS*****:** Estado Islámico *(Islamic State of Iraq and Syria)*.
- ✓ **IT:** Tecnología de la Información.
- ✓ ***JAN***: *Jama'at Ansar al-Islam* (Siria).
- ✓ ***JeM*****:** *Jaish-e-Mohammed* (Ejército de Mahoma, Pakistán).
- ✓ ***JeM-BaF*****:** *Jaish-e-Mohammed al-Badr* (Ejército de Mahoma - Batallón de Abu Dujana, Pakistán).
- ✓ ***JeM-FT:*** *Jaish-e-Mohammed Fidayeen Tanzeem* (Ejército de Mahoma - Unidad de Comandos Suicidas, Pakistán).
- ✓ ***JeM-MdK:*** *Jaish-e-Mohammed Mufti Aslam Khan* (Ejército de Mahoma - MdK, Pakistán).
- ✓ ***JeM-Qari Saifullah*****:** *Jaish-e-Mohammed Qari Saifullah* (Ejército de Mahoma - Qari Saifullah, Pakistán).
- ✓ **JIGC:** Jefatura de Información de la Guardia Civil.
- ✓ ***JMB*****:** *Jamaat-ul-Mujahideen* Bangladesh (Movimiento de los Guerreros de Bangladés).
- ✓ ***JRTN*****:** *Jaysh Rijal al-Tariq al-Naqshabandi* (Ejército de los Hombres de la Orden *Naqshbandi*, Irak).
- ✓ ***JUI-F:*** *Jamiat Ulema-e-Islam-Fazl* (Partido de los Líderes Religiosos-Islam, Fazlur Rehman).
- ✓ ***JUI-S:*** *Jamiat Ulema-e-Islam-Sami* (Partido de los Líderes Religiosos-Islam, Samiul Haq).
- ✓ ***JUI-T:*** *Jamiat Ulema-e-Islam-Tariq* (Partido de los Líderes Religiosos-Islam, Tariq).
- ✓ ***LEJ*****:** *Lashkar-e-Jhangvi al-Alami* (Ejército de Jhangvi Internacional).
- ✓ ***LET*****:** *Lashkar-e-Taiba* (Ejército de los Puros, Pakistán).
- ✓ ***LJ*****:** *Lashkar-e-Jhangvi* (Ejército de Jhangvi, Pakistán).
- ✓ **LM:** *Lashkar-e-Mustafa* (Ejército de Mustafa, Pakistán).

- ✓ **LRA**: Ejército de Resistencia del Señor (África Central).
- ✓ ***MASINT***: Inteligencia de medidas científicas y técnicas (*Measurement and Signature Intelligence*).
- ✓ **MCCD**: Mando Conjunto de Ciberdefensa.
- ✓ ***MEK*****:** *Mujahedin-e Khalq* (Organización de los Muyahidines del Pueblo de Irán).
- ✓ ***MUJAO*****:** Movimiento por la Unidad y la *Yihad* en África Occidental.
- ✓ **NAAA**: Nivel de Alerta Antiterrorista.
- ✓ **NCIIP:** Plan Nacional de Protección de Infraestructuras Críticas.
- ✓ **NCIIPC:** Centro Nacional de Protección de Infraestructuras Críticas (India).
- ✓ **NCIIPC-EU:** Centro Nacional de Protección de Infraestructuras Críticas - Unión Europea.
- ✓ **NCSC:** Centro Nacional de Ciberseguridad (Reino Unido).
- ✓ **NCSC-CISP:** Programa de Compartición de Información de Seguridad Cibernética del Centro Nacional de Ciberseguridad (Reino Unido).
- ✓ **NCSC-TAF:** Foro de Atribución de Amenazas del Centro Nacional de Ciberseguridad (Reino Unido).
- ✓ **NERC:** Consejo de Fiabilidad de la Red Eléctrica.
- ✓ **NERCCIP:** Plan de Protección de Infraestructuras Críticas del Consejo de Fiabilidad de la Red Eléctrica.
- ✓ **NERIS:** Sistema Nacional de Respuesta de Emergencia (Australia).
- ✓ **NICC:** Centro Nacional de Coordinación de Infraestructuras Críticas.
- ✓ **NICPP:** Programa Nacional de Protección de la Infraestructura Crítica (Australia).
- ✓ **NIPP:** Plan Nacional de Protección de Infraestructuras.
- ✓ **NIS *Directive*:** Directiva sobre la Seguridad de las Redes y los Sistemas de Información (Directiva UE 2016/1148).
- ✓ **NRC:** Comisión Reguladora Nuclear (EE. UU.).
- ✓ **NSTAC:** Comité Asesor del Presidente en Infraestructura de Telecomunicaciones y Ciberseguridad (EE. UU.).
- ✓ **ONIC**: Oficina Nacional de Inteligencia y Contrainteligencia.
- ✓ **ONR:** Oficina Nacional de Riesgos (Francia).
- ✓ **ONS**: Oficina Nacional de Seguridad.
- ✓ **ONU**: Organización de las Naciones Unidas.
- ✓ **OPSEC**: Seguridad operacional (*Operational Security*).
- ✓ ***OSINT***: Inteligencia de fuentes abiertas.

- ✓ **OT:** Tecnología Operativa.
- ✓ **OTAN**: Organización del Tratado del Atlántico Norte.
- ✓ **PAFMEC:** Grupo *Ansar al-Furqan* en Cachemira.
- ✓ ***PAG*:** Grupo de *Abu Sayyaf-Maute* (Filipinas).
- ✓ **PC:** Protección Civil.
- ✓ **PC-CIAE:** Protección Civil - Centro de Información de Asistencia a Emergencias.
- ✓ **PCEM:** Puesto de Control de Emergencias Móvil.
- ✓ **PCIF:** Plan de Contingencia de Incendios Forestales.
- ✓ **PCR:** Punto de Control de Riesgos.
- ✓ **PE:** Protección del Entorno.
- ✓ **PEA:** Plan Especial de Emergencias.
- ✓ **PEDI:** Plan Especial de Protección Civil ante el Riesgo de Inundaciones.
- ✓ **PEIN:** Plan Especial de Protección Civil ante el Riesgo de Accidentes en el Transporte de Mercancías Peligrosas por Carretera y Ferrocarril.
- ✓ **PEN-LCRV**: Plan Estratégico Nacional de lucha contra la Radicalización Violenta.
- ✓ **PERC:** Plan Especial de Protección Civil ante el Riesgo Químico.
- ✓ **PERI:** Plan Especial de Protección Civil ante el Riesgo de Incendios Forestales.
- ✓ ***PHIRMA***: *Protection of Health Infrastructures, Resilience, Management, and Adaptation* (Protección de Infraestructuras de Salud, Resiliencia, Gestión y Adaptación).
- ✓ **PII:** Punto de Información de Incendios.
- ✓ **PIR:** Punto de Información de Riesgos.
- ✓ ***PKK*:** *Partiya Karkerên Kurdistan* (Partido de los Trabajadores del Kurdistán).
- ✓ **PLO:** Organización para la Liberación de Palestina.
- ✓ **PMA:** Puesto de Mando Avanzado.
- ✓ **PMA-CM:** Puesto de Mando Avanzado - Centro de Mando.
- ✓ **PME:** Puesto de Mando Estratégico.
- ✓ **PMI:** Puesto de Mando Integrado.
- ✓ **PMI-CM:** Puesto de Mando Integrado - Centro de Mando.
- ✓ **PMU:** Puesto Médico de Urgencia.
- ✓ **PPPyRA**: Plan de Prevención, Protección y Respuesta Antiterrorista del Ministerio del Interior de España.
- ✓ **PSI:** Iniciativa de Seguridad de los Puertos.

- ✓ ***PYD*: *Partiya Yekîtiya Demokrat*** (Partido de la Unión Democrática, Siria).
- ✓ **SCADA:** Sistema de Control y Adquisición de Datos.
- ✓ **SI**: Servicios de Información.
- ✓ **SIEM:** Gestión de Eventos e Información de Seguridad.
- ✓ ***SIGINT***: Inteligencia de señales.
- ✓ **SN**: Seguridad Nacional.
- ✓ **SPEIS:** Servicio de Prevención, Extinción de Incendios y Salvamento.
- ✓ **SVA:** Servicio de Vigilancia Aérea.
- ✓ ***TAK***: *Teyrêbazên Azadiya Kurdistan* (Halcones de la Libertad de Kurdistán).
- ✓ **TFG:** Gobierno Federal de Transición (Somalia).
- ✓ **TIA:** Evaluación de Impacto de Amenazas.
- ✓ **TIC**: Tecnología de la Información y de las Comunicaciones.
- ✓ **TNSM:** Movimiento de Estudiantes de Pakistán.
- ✓ ***TNSM*-K:** *TNSM Khas* (Movimiento de Estudiantes de Pakistán - Facción Especial).
- ✓ ***TPLF*:** Frente de Liberación del Pueblo Tigray (Etiopía).
- ✓ **TSA:** Administración de Seguridad del Transporte (EE. UU.).
- ✓ ***TTP*:** *Tehrik-i-Taliban Pakistan* (Movimiento de los Talibanes de Pakistán).
- ✓ **UME:** Unidad Militar de Emergencias.
- ✓ **UMEI:** Unidad Médica de Emergencias e Intervención.
- ✓ **UPR:** Unidad de Primeros Auxilios.
- ✓ **USAR:** Búsqueda y Rescate Urbano.
- ✓ **UTN:** Unión de Tribus de Norte Waziristán.
- ✓ **Vulnerabilidad CI:** Vulnerabilidad de Infraestructura Crítica .
- ✓ ***YPG*:** *Yekîneyên Parastina Gel* (Unidades de Protección del Pueblo, Siria).
- ✓ ***YPJ*:** *Yekîneyên Parastina Jin* (Unidades de Protección de la Mujer, Siria).

ANEXO III

Índice de Figuras y Tablas

ANEXO III

ÍNDICE DE FIGURAS Y TABLAS

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

ANEXO IV

Modelo Matemático de la OMS

Indice de Seguridad Hospitalaria

MODELO MATEMATICO

Paso 1: Ingrese el número "1" en la celda correspondiente de cada rubro. Algunas líneas podrán estar en BLANCO sólo si aparece una nota en LETRAS MAYUSCULAS.

2. Aspectos relacionados con la seguridad estructural
Columnas, vigas, muros, losas y otros, son elementos estructurales que forman parte del sistema de soporte de la edificación. Estos aspectos deben ser evaluados por Ingenieros estructurales.

	2.1 Seguridad debido a antecedentes del establecimiento	CONTROL	Grado de seguridad BAJO	MEDIO	ALTO	PESO	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
						25	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
1	**¿El hospital ha sufrido daños estructurales debido a fenómenos naturales?.** Verificar si existe dictamen estructural que indique que el grado de seguridad ha sido comprometido. SI NO HAN OCURRIDO FENOMENOS NATURALES EN LA ZONA DONDE ESTA EL HOSPITAL, NO MARQUE NADA. DEJE ESTA LINEA EN BLANCO, SIN CONTESTAR. *B= Daños mayores; M= Daños moderados; A= Daños menores.*	BLANCO				25	0	0	0	0	0	0
2	**¿El hospital ha sido reparado o construido utilizando estándares actuales apropiados?** Corroborar si el inmueble ha sido reparado, en que fecha y si se realizó con base a la normatividad de establecimientos seguros. *B= No se aplicaron los estándares; M=Estándares parcialmente aplicados; A=Estándares aplicados completamente.*	ERROR				50	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
3	**¿El hospital ha sido remodelado o adaptado afectando el comportamiento de la estructura?** Verificar si se han realizado modificaciones usando normas para edificaciones seguras. *B=Remodelaciones o adaptaciones mayores; M= Remodelaciones y/o adaptaciones moderadas; A= remodelaciones o adaptaciones menores o no han sido necesarias.*	ERROR				25	0	0	0			
							0	0	0			

	2.2 Seguridad relacionada con el sistema estructural y el tipo de material usado en la edificación.	CONTROL	Grado de seguridad BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
						75	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
4	**Estado de la edificación.** *B= Deteriorada por meteorización o exposición al ambiente, grietas en primer nivel y elementos discontínuos de altura; M= Deteriorada sólo por meteorización o exposición al ambiente; A= Sana, no se observan deterioros ni grietas..*	ERROR				20	0	0	0	0	0	0
5	**Materiales de construcción de la estructura.** *B= Oxidada con escamas o grietas mayores a 3mm; M= Grietas entre 1 y 3 mm u óxido en forma de polvo; A= Grietas menores a 1mm y no hay óxido.*	ERROR				5	0	0	0			
6	**Interacción de los elementos no estructurales con la estructura.** *B= Se observa dos o más de lo siguiente: columnas cortas, paredes divisorias unidas a la estructura, cielos rígidos o fachada que interactúa con la estructura; M= Se observa sólo uno de problemas antes mencionados; A= Los elementos no estructurales no afectan la estructura.*	ERROR				10	0	0	0			
7	**Proximidad de los edificios** (martilleo, túnel de viento, incendios, etc.) *B= Separación menor al 0.5% de la altura del edificio de menor altura; M= Separación entre 0.5 – 1.5% de la altura del edificio de menor altura; A= Separación mayor al 1.5% del edificio de menor altura.*	ERROR				5	0	0	0			
8	**Redundancia estructural.** *B= Menos de tres líneas de resistencia en cada dirección; M= 3 líneas de resistencia en cada dirección o líneas con orientación no ortogonal; A= Más de 3 líneas de resistencia en cada dirección ortogonal del edificio.*	ERROR				10	0	0	0			
9	**Detallamiento estructural incluyendo conexiones.** *B= Edificio anterior a 1970; M= Edificio construido en los años 1970 y 1990; A=Edificio construido luego de 1990 y de acuerdo a la norma.*	ERROR				5	0	0	0			
10	**Seguridad de fundaciones o cimientos.** *B= No hay información o la profundidad es menor que 1.5 m; M= No cuenta con planos ni estudio de suelos pero la profundidad es mayor que 1.5 m; A= Cuenta con planos, estudio de suelos, y profundidades mayores a 1.5 m.*	ERROR				5	0	0	0			
11	**Irregularidades en planta** (rigidez, masa y resistencia). *B= Formas no regulares y estructura no uniforme; M= Formas no regulares pero con estructura uniforme; A= Formas regulares, estructura uniforme en planta y ausencia de elementos que podrían causar torsión.*	ERROR				5	0	0	0			
12	**Irregularidades en elevación** (rigidez, masa y resistencia). *B= Pisos difieren por más del 20% de altura y existen elementos discontinuos o irregulares significativos; M= Pisos de similar altura (difieren menos de un 20%, pero más de 5%) y pocos elementos discontinuos o irregulares; A= Pisos de similar altura (difieren por menos del 5%) y no existen elementos discontinuos o irregulares.*	ERROR				5	0	0	0	ESTRUCTURAL		
13	**Adecuación estructural a fenómenos.** (meteorológicos, geológicos entre otros) Valorar por separado y en conjunto, el posible comportamiento del hospital desde el punto de vista estructural ante las diferentes amenazas o peligros excepto sismos. *B= baja resiliencia estructural a las amenazas naturales presentes en la zona donde está ubicado el hospital; M, moderada resiliencia estructural; A, excelente resiliencia estructural.*	ERROR				30	0	0	0	BAJO	MEDIO	ALTO
	TOTAL ESTRUCTURAL	**13**	0	0	0	**0**	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!

3. Aspectos relacionados con la seguridad no estructural del hospital
Elementos que no forman parte del sistema de soporte de la edificación. En este caso corresponden a elementos arquitectónicos, equipos y sistemas necesarios para la operación del establecimiento.

	3.1 Líneas vitales (instalaciones)	CONTROL	Grado de seguridad BAJO	MEDIO	ALTO							
						25						
	3.1.1 Sistema eléctrico					20	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO

14	**Generador adecuado para el 100% de la demanda.** El evaluador verifica que el generador entre en función segundos después de la caída de tensión, cubriendo la demanda de urgencias, cuidados intensivos, central de esterilización, quirófanos, etc. *B = Sólo se enciende manualmente o cubre del 0 – 30% de la demanda; M = Se enciende automáticamente en más de 10 segundos o cubre 31 – 70 % de la demanda; A = Se enciende automáticamente en menos de 10 segundos y cubre del 71 – 100% de la demanda.*	ERROR				25	0	0	0				
15	**Regularidad de las pruebas de funcionamiento en las áreas críticas.** *El evaluador verifica la frecuencia en que el generador es puesto a prueba con resultados satisfactorios. B= > 3 meses; M= 1 a 3 meses; A=< 1 mes.*	ERROR				25	0	0	0				
16	**¿Está el generador adecuadamente protegido de fenómenos naturales?.** *B= No; M= Parcialmente; A= Sí.*	ERROR				8	0	0	0				
17	**Seguridad de las instalaciones, ductos y cables eléctricos.** *B= No; M= Parcialmente; A= Sí.*	ERROR				8	0	0	0				
18	**Sistema redundante al servicio local de suministro de energía eléctrica.** *B= No; M= Parcialmente; A= Sí.*	ERROR				8	0	0	0				
19	**Sistema con tablero de control e interruptor de sobrecarga y cableado debidamente protegido.** Verificar la accesibilidad así como el buen estado y funcionamiento del tablero de control general de electricidad. *B= No; M= Parcialmente; A= Sí.*	ERROR				8	0	0	0				
20	**Sistema de iluminación en sitios clave del hospital.** Realizar recorrido por urgencias, UCI, quirófano etc. Verificando el grado de iluminación y funcionalidad de lámparas. *B= No; M= Parcialmente; A= Sí.*	ERROR				8	0	0	0				
21	**Sistemas eléctricos externos, instalados dentro del perímetro del hospital.** Verificar si existen subestaciones eléctrica o transformadores que proveen electricidad al hospital. *B= No existen subestaciones eléctricas instaladas en el hospital; M= Existen subestaciones, pero no proveen suficiente energía al hospital; A= Subestación eléctrica instalada y provee suficiente energía al hospital.*	ERROR				10	0	0	0				
							0	0	0				
	3.1.2 Sistema de telecomunicaciones					15				BAJO	MEDIO	ALTO	
22	**Estado técnico de las antenas y soportes de las mismas.** Verificar que las antenas, pararrayos cuenten con soportes que eleven el nivel de seguridad del Hospital. *B= mal estado o no existen; M= Regular; A= Buen estado.*	ERROR				10	0	0	0	0	0	0	
23	**Estado técnico de sistemas de baja corriente** (conexiones/cables de Internet). Verificar en áreas estratégicas que los cables estén conectados evitando la sobrecarga. *B= mal estado o no existen; M= Regular; A= Bueno.*	ERROR				10	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	
24	**Estado técnico del sistema de comunicación alterno.** *Verificar el estado de otros sistemas: radiocomunicación, teléfono satelital, Internet, etc. B= mal estado o no existe; M= Regular; A= Bueno.*	ERROR				30	0	0	0				
25	**Estado técnico de anclajes de los equipos y soportes de cables.** Verificar que los equipos de telecomunicaciones (radios, teléfono satelital, video-conferencia, etc.) cuenten con anclajes que eleven su grado de seguridad. SI EL SISTEMA NO NECESITA ANCLAJES O ABRAZADERAS, NO LLENAR. DEJAR LAS TRES CASILLAS EN BLANCO. *B= malo; M= Regular; A= Bueno.*	BLANCO				10	0	0	0				
26	**Estado técnico de sistemas de telecomunicaciones externos, instalados dentro del perímetro del hospital.** Verificar si existen sistemas de telecomunicaciones externos que interfieran con el grado de seguridad del hospital. *B= Telecomunicaciones externas interfieren seriamente con las comunicaciones del hospital; M= Telecomunicaciones externas interfieren moderadamente con las comunicaciones del hospital; A= No existe interferencia a las comunicaciones del hospital.*	ERROR				10	0	0	0				
27	**Local con condiciones apropiadas para sistemas de telecomunicaciones.** *B= malo o no existe; M= Regular; A= Bueno*	ERROR				10	0	0	0				
28	**Seguridad del sistema interno de comunicaciones.** *Verificar el estado de los sistemas de perifoneo, anuncios, altavoces, intercomunicadores y otros, que permitan comunicarse con el personal, pacientes y visitas en el hospital. B= malo o no existe; M= Regular; A= Bueno*	ERROR				20	0	0	0				
							0	0	0				
	3.1.3 Sistema de aprovisionamiento de agua					30				BAJO	MEDIO	ALTO	
29	**Tanque de agua con reserva permanente suficiente para proveer al menos 300 litros por cama y por día durante 72 horas.** Verificar que el depósito de agua cuente con una capacidad suficiente para satisfacer la demanda del hospital por 3 días *B= Cubre la demanda de 24 horas o menos; M = Cubre la demanda de más de 24 horas pero menos de 72 horas; A= Garantizado para cubrir la demanda por 72 horas o más.*	ERROR				36	0	0	0	0	0	0	
30	**Los depósitos se encuentran en lugar seguro y protegido.** Visitar sitio de cisterna y corroborar el área donde está instalada y su grado de seguridad. *B= Si el espacio es susceptible de falla estructural o no estructural; M= Cuando la falla no representa posibilidad de colapso; A= Cuando tiene poca posibilidad de dejar de funcionar.*	ERROR				11	0	0	0				
31	**Sistema alterno de abastecimiento de agua adicional a la red de distribución principal.** Identificar organismos o mecanismos para abastecer o reaprovisionar de agua al hospital en caso de falla del sistema público. *B= Si da menos de 30% de la demanda; M= Si suple valores de 30 a 80% de la demanda; A= Si suple más del 80% de la dotación diaria.*	ERROR				28	0	0	0				
32	**Seguridad del sistema de distribución.** Verificar el buen estado y funcionamiento del sistema de distribución, incluyendo la cisterna,válvula, tuberías y uniones. *B= Si menos del 60% se encuentra en buenas condiciones de operación; M= entre 60 y 80 %; A= más del 80 %.*	ERROR				18	0	0	0				

33	**Sistema de bombeo alterno.** Identificar la existencia y el estado operativo del sistema alterno de bombeo, en caso de falla en el suministro. *B= No hay bomba de reserva y las operativas no suplen toda la demanda diaria; M= Están todas las bombas en regular estado de operación; A= Todas las bombas y las de reserva están operativas.*	ERROR				7	0	0	0			
							0	0	0			
	3.1.4 Depósito de combustible (gas, gasolina o diesel):					20					BAJO	MEDIO	ALTO
34	**Tanques para combustible con capacidad suficiente para un mínimo de 5 días.** Verificar que el hospital cuente con depósito amplio y seguro para almacenaje de combustible. *B= Cuando es inseguro o tiene menos de 3 días; M= Almacenamiento con cierta seguridad y con 3 a 5 días de abastecimiento de combustible; A= Se tienen 5 o más días de autonomía y es seguro.*	ERROR				36	0	0	0		0	0	0
35	**Anclaje y buena protección de tanques y cilindros** *B= No hay anclajes y el recinto no es seguro; M= se aprecian anclajes insuficientes; A= Existen anclajes en buenas condiciones y el recinto o espacio es apropiado.*	ERROR				14	0	0	0			
36	**Ubicación y seguridad apropiada de depósitos de combustibles.** Verificar que los depósitos que contienen elementos inflamables se encuentren a una distancia que afecte el grado de seguridad del Hospital. *B= Existe el riesgo de falla o no son accesibles; M= se tiene una de las dos condiciones mencionadas; A= los depósitos son accesibles y están en lugares libres de riesgos.*	ERROR				14	0	0	0			
37	**Seguridad del sistema de distribución (válvulas; tuberías y uniones).** *B= Si menos del 60% se encuentra en buenas condiciones de operación; M= entre 60 y 80 %; A= más del 80 %.*	ERROR				36	0	0	0			
							0	0	0			
	3.1.5 Gases medicinales (oxígeno, nitrógeno, etc.)					15					BAJO	MEDIO	ALTO
38	**Almacenaje suficiente para 15 días cómo mínimo.** *B= Menos de 10 días; M= entre 10 y 15 días; A= 15 días.*	ERROR				23	0	0	0		0	0	0
39	**Anclaje de tanques, cilindros y equipos complementarios** *B= No existen anclajes; M= Los anclajes no son de buen calibre; A= Los anclajes son de buen calibre.*	ERROR				9	0	0	0			
40	**Fuentes alternas disponibles de gases medicinales.** *B= No existen fuentes alternas o están en mal estado; M= Existen pero en regular estado; A= Existen y están en buen estado.*	ERROR				13	0	0	0			
41	**Ubicación apropiada de los recintos.** *B= Los recintos no tienen accesos; M= los recintos tienen acceso pero con riesgos A= los recintos son accesibles y están libres de riesgos;*	ERROR				9	0	0	0			
42	**Seguridad del sistema de distribución (válvulas, tuberías y uniones).** *B= Si menos del 60% se encuentra en buenas condiciones de operación; M= entre 60 y 80 %; A= más del 80 %.*	ERROR				23	0	0	0			
43	**Protección de tanques y/o cilindros y equipos adicionales.** *B= No existen áreas exclusivas para tanques y equipos adicionales; M= Areas exclusivas para protección de tanques y equipos, pero el personal no está entrenado; A= Áreas exclusivas para este equipamiento y el personal está entrenado.*	ERROR				9	0	0	0		#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
44	**Seguridad apropiada de los recintos.** *B= No existen áreas reservadas para almacén de gases; M= Áreas reservadas para almacenar gases, pero sin medidas de seguridad apropiadas; A= se cuenta con áreas de almacenamiento adecuados y no tienen riesgos*	ERROR				14	0	0	0		#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
							0	0	0			
	3.2 Sistemas de calefacción, ventilación, aire acondicionado en áreas críticas	CONTROL	Grado de seguridad			12	BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO
			BAJO	MEDIO	ALTO								
45	**Soportes adecuados para los ductos y revisión del movimiento de los ductos y tuberías que atraviesan juntas de dilatación.** *B= No existen soportes y tienen juntas rígidas; M=Existen soportes o juntas flexibles; A= Existen soportes y las juntas son flexibles.*	ERROR				16	0	0	0		0	0	0
46	**Condición de tuberías, uniones, y válvulas.** *B= Malo; M= Regular; A= Bueno.*	ERROR				16	0	0	0				
47	**Condiciones de los anclajes de los equipos de calefacción y agua caliente.** *B= Malo; M= Regular; A= Bueno.*	ERROR				19	0	0	0				
48	**Condiciones de los anclajes de los equipos de aire acondicionado.** *B= Malo; M= Regular; A= Bueno.*	ERROR				9	0	0	0				
49	**Ubicación apropiada de los recintos.** *B= Malo; M= Regular; A= Bueno.*	ERROR				8	0	0	0				
50	**Seguridad apropiada de los recintos.** *B= Malo; M= Regular; A= Bueno.*	ERROR				16	0	0	0				
51	**Funcionamiento de los equipos (Ej. Caldera, sistemas de aire acondicionado y extractores, entre otros).** *B= Malo; M= Regular; A= Bueno.*	ERROR				16	0	0	0				
							0	0	0				
	3.3 Mobiliario y equipo de oficina fijo y móvil y almacenes (incluye computadoras, impresoras, etc.)	CONTROL	Grado de seguridad			13	BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO
			BAJO	MEDIO	ALTO								
52	**Anclajes de la estantería y seguridad de contenidos.** Verificar que los estantes se encuentren fijos a las paredes y/o con soportes de seguridad. *B= La estantería no está fijada a las paredes; M= La estantería está fijada, pero el contenido no está asegurado; A= La estantería está fijada y el contenido asegurado.*	ERROR				30	0	0	0		0,00	0,00	0,00
53	**Computadoras e impresoras con seguro.** Verificar que las mesas para computadora estén aseguradas y con frenos de ruedas aplicados. *B= Malo; M= Regular; A= Bueno o no necesita anclaje.*	ERROR				50	0	0	0				
54	**Condición del mobiliario de oficina y otros equipos.** Verificar en recorrido por oficinas el anclaje y/o fijación del mobiliario. *B= Malo; M= Regular; A= Bueno o no necesita anclaje.*	ERROR				20	0	0	0				

						0	0	0				
	3.4 Equipos médicos, de laboratorio y suministros utilizados para el diagnóstico y tratamiento.	**CONTROL**	**Grado de seguridad**			25	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
			BAJO	MEDIO	ALTO							
55	**Equipo médico en el quirófano y la sala de recuperación.** Verificar que lámparas, equipos de anestesia, mesas quirúrgicas se encuentren operativos y con seguros y frenos aplicados. *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0	0	0	0
56	**Condición y seguridad del equipo médico de Rayos X e imagenología.** Verificar que las mesas de Rayos X y el equipo de rayos se encuentren en buenas condiciones y fijos. *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
57	**Condición y seguridad en equipo médico en laboratorios.** *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0			
58	**Condición y seguridad del equipo médico en el servicio de urgencias.** *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0			
59	**Condición y seguridad del equipo médico de la unidad de cuidados intensivos o intermedios.** *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0			
60	**Condición y seguridad del equipamiento y mobiliario de farmacia** *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0			
61	**Condición y seguridad de equipo médico de esterilización.** *B= Cuando el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	ERROR				10	0	0	0			
62	**Condición y seguridad de equipo médico para cuidado del recién nacido.** *B= Cuando el equipo no existe, está en malas condiciones o no está seguro; M= Cuando el equipo está en regulares condiciones o poco seguro; A= El equipo está en buenas condiciones y está seguro*	ERROR				5	0	0	0			
63	**Condición y seguridad de equipo médico para la atención de quemados.** *B= Cuando el equipo no existe, está en malas condiciones o no está seguro; M= Cuando el equipo está en regulares condiciones o poco seguro; A= El equipo está en buenas condiciones y está seguro.*	ERROR				5	0	0	0			
64	**Condición y seguridad de equipo médico de radioterapia o medicina nuclear.** SI EL HOSPITAL NO CUENTA CON ESTOS SERVICIOS, DEJAR EN BLANCO. *B= Cuando no existe o el equipo está en malas condiciones o no está seguro; M= cuando el equipo está en regulares condiciones o poco seguro; A= el equipo está en buenas condiciones y está seguro.*	BLANCO				5	0	0	0			
65	**Condición y seguridad de equipo médico en otros servicios.** *B= Si más del 30 % de los equipos se encuentra en riesgo de pérdida material o funcional y/o si algún equipo pone en forma directa o indirecta en peligro la función de todo el servicio; M= Si entre el 10 y el 30% de los equipos se encuentra en riesgo de pérdida, A=Si menos del 10% de los equipos tiene riesgo de pérdida.*	ERROR				5	0	0	0			
66	**Anclajes de la estantería y seguridad de contenidos médicos.** *B= 20% o menos se encuentran seguros contra el vuelco de la estantería o el vaciamiento de contenidos; M= 20 a 80 % se encuentra seguros contra el vuelco; A= Más del 80 % se encuentra con protección a la estabilidad de la estantería y la seguridad del contenido, o porque no requiere anclaje.*	ERROR				10	0	0	0			
							0	0	0			
	3.5 Elementos arquitectónicos	**CONTROL**	**Grado de seguridad**			25	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
			BAJO	MEDIO	ALTO							
67	**Condición y seguridad de puertas o entradas.** *B= Cuando se daña e impide el funcionamiento de otros componentes, sistemas o funciones; M=Cuando se daña pero permite el funcionamiento de otros componentes; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				3	0	0	0	0	0	0
68	**Condición y seguridad de ventanales.** *B= Cuando se daña e impide el funcionamiento de otros componentes, sistemas o funciones; M=Cuando se daña pero permite el funcionamiento de otros componentes; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				9	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
69	**Condición y seguridad de otros elementos de cierre (muros externos, fachada, etc.).** *B= Cuando se daña e impide el funcionamiento de otros componentes, sistemas o funciones; M=Cuando se daña pero permite el funcionamiento de otros componentes; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				3	0	0	0			
70	**Condición y seguridad de techos y cubiertas.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento de otros componentes; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				9	0	0	0			

71	**Condición y seguridad de parapetos (pared o baranda que se pone para evitar caídas, en los puentes, escaleras, etc.)** *B= Cuando se daña e impide el funcionamiento de otros componentes, sistemas o funciones; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes, sistemas o funciones.*	ERROR				3	0	0	0			
72	**Condición y seguridad de cercos y cierres perimétricos.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes, sistemas o funciones.*	ERROR				3	0	0	0			
73	**Condición y seguridad de otros elementos perimetrales (Cornisas, ornamentos etc.).** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes, sistemas o funciones.*	ERROR				3	0	0	0			
74	**Condición y seguridad de áreas de circulación externa.** *B= Los daños a la vía o los pasadizos impide el acceso al edificio o ponen en riesgo a los peatones; M= Los daños a la vía o los pasadizos no impiden el acceso al edificio a los peatones, pero sí el acceso vehicular; A= No existen daños o su daño es menor y no impide el acceso de peatones ni de vehículos.*	ERROR				3	0	0	0			
75	**Condición y seguridad de áreas de circulación interna (pasadizos, elevadores, escaleras, salidas, etc.).** *B= Los daños a las rutas de circulación interna impiden la circulación dentro del edificio o ponen en riesgo a las personas; M= Los daños a la vía o los pasadizos no impiden la circulación de las personas, pero sí el acceso de camillas y otros; A= No existen daños o su daño es menor y no impide la circulación de personas ni de camillas y equipos rodantes.*	ERROR				3	0	0	0			
76	**Condición y seguridad de particiones o divisiones internas.** *B= Cuando se daña e impide el funcionamiento de otros componentes, sistemas o funciones; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes, sistemas o funciones.*	ERROR				3	0	0	0			
77	**Condición y seguridad de cielos falsos o rasos** SI EL HOSPITAL NO TIENE TECHOS FALSOS O SUSPENDIDOS, NO MARQUE NADA. DEJE LAS TRES CASILLAS EN BLANCO. *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	BLANCO				9	0	0	0			
78	**Condición y seguridad del sistema de iluminación interna y externa.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				9	0	0	0			
79	**Condición y seguridad del sistema de protección contra incendios.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				9	0	0	0			
80	**Condición y seguridad de ascensores.** SI NO EXISTEN ELEVADORES, DEJE LAS TRES CASILLAS EN BLANCO. *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	BLANCO				9	0	0	0			
81	**Condición y seguridad de escaleras.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				9	0	0	0			
82	**Condición y seguridad de las cubiertas de los pisos.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				3	0	0	0			
83	**Condición de las vías de acceso al hospital.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				7	0	0	0	NO-ESTRUCTURAL		
84	**Otros elementos arquitectónicos incluyendo señales de seguridad.** *B= Cuando se daña e impide el funcionamiento de otros componentes o sistemas; M=Cuando se daña pero permite el funcionamiento; A= Cuando no se daña o su daño es menor y no impide su funcionamiento o el de otros componentes o sistemas.*	ERROR				3	0	0	0	BAJO	MEDIO	ALTO
	TOTAL NO-ESTRUCTURAL	71	0	0	0	0	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!

	4. Aspectos relacionados con la seguridad en base a la capacidad funcional Se refiere al nivel de preparación para emergencias masivas y desastres del personal que labora en el hospital así como el grado de implementación del plan hospitalario para casos de desastre.											
	4.1 Organización del comité hospitalario para desastres y centro de operaciones de emergencia. Mide el nivel de organización alcanzado por el comité hospitalario para casos de desastre.	CONTROL	Nivel de organización.			21						
			BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
85	**Comité formalmente establecido para responder a las emergencias masivas o desastres.** Solicitar el acta constitutiva del Comité y verificar que los cargos y firmas correspondan al personal en función. B= No existe comité; M= Existe el comité pero no es operativo; A= Existe y es operativo.	ERROR				15	0	0	0	0,00	0,00	0,00

86	**El Comité está conformado por personal multidisciplinario.** Verificar que los cargos dentro del comité sean ejercidos por personal de diversas categorías del equipo multidisciplinario: director, jefe de enfermería, ingeniero de mantenimiento, jefe de urgencias, jefe médico, jefe quirúrgico, jefe de laboratorio y servicios auxiliares entre otros. B= 0-3; M=4-5; A= 6 o más	ERROR				10	0	0	0		
87	**Cada miembro tiene conocimiento de sus responsabilidades específicas.** Verificar que cuenten con sus actividades por escrito dependiendo de su función específica: B= No asignadas; M= Asignadas oficialmente; A= Todos los miembros conocen y cumplen su responsabilidad.	ERROR				10	0	0	0		
88	**Espacio físico para el centro de operaciones de emergencia (COE) del hospital.** Verificar la sala destinada para el comando operativo que cuente con todos los medios de comunicación (teléfono, fax, Internet, entre otros). B= No existe; M= Asignada oficialmente; A= Existe y es funcional.	ERROR				5	0	0	0		
89	**El COE está ubicado en un sitio protegido y seguro.** Identificar la ubicación tomando en cuenta su accesibilidad, seguridad y protección. B= La sala del COE no está en un sitio seguro; M= EL COE está en un lugar seguro pero poco accesible; A= EL COE está en un sitio seguro, protegido y accesible.	ERROR				5	0	0	0		
90	**El COE cuenta con sistema informático y computadoras.** Verificar si cuenta con intranet e internet. B= No; M=Parcialmente; A= Cuenta con todos los requerimientos.	ERROR				5	0	0	0		
91	**El sistema de comunicación interna y externa del COE funciona adecuadamente**. Verificar si el conmutador (central de redistribución de llamadas) cuenta con sistema de perifoneo y si los operadores conocen el código de alerta y su funcionamiento. B= No funciona/ no existe; M = Parcialmente; A= Completo y funciona.	ERROR				15	0	0	0		
92	**El COE cuenta con sistema de comunicación alterna.** Verificar si además de conmutador existe comunicación alterna como celular, radio, entre otros. B= No cuenta; M= Parcialmente; A= Si cuenta.	ERROR				5	0	0	0		
93	**El COE cuenta con mobiliario y equipo apropiado.** Verificar escritorios, sillas, tomas de corriente, iluminación, agua y drenaje. B= No cuenta; M= Parcialmente; A= Si cuenta.	ERROR				5	0	0	0		
94	**El COE cuenta con directorio telefónico actualizado y disponible.** Verificar que el directorio incluya todos los servicios de apoyo necesarios ante una emergencia (corroborar teléfonos en forma aleatoria). B= No; M= Existe pero no está actualizado; Si cuenta y está actualizado.	ERROR				10	0	0	0		
95	**"Tarjetas de acción" disponibles para todo el personal.** Verificar que las tarjetas de acción indiquen las funciones que realiza cada integrante del hospital especificando su participación en caso de desastre interno y/o externo. *B= No; M= Insuficiente (cantidad y calidad); A= Todos la tienen.*	ERROR				15	0	0	0		
							0	0	0		
	4.2 Plan operativo para desastres internos o externos.	CONTROL	Nivel de implementación BAJO	MEDIO	ALTO	28	BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
96	**Refuerzo de los servicios esenciales del hospital.** El plan especifica las actividades que se deben realizar antes, durante y después de un desastre en los servicios clave del hospital (servicio de urgencias, unidad de cuidados intensivos, esterilización y quirófano, entre otros). *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				6	0	0	0	0,00	0,00	0,00
97	**Procedimientos para la activación y desactivación del plan.** Se especifica cómo, cuándo y quién es el responsable de activar y desactivar el plan. *B= No existe o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				2	0	0	0			
98	**Previsiones administrativas especiales para desastres.** Verificar que el plan considere contratación de personal, adquisiciones en caso de desastre y presupuesto para pago por tiempo extra, doble turno, etc. *B= No existen las previsiones o existen únicamente en el documento; M= Existen previsiones y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				4	0	0	0			
99	**Recursos financieros para emergencias presupuestados y garantizados.** El Hospital cuenta con presupuesto específico para aplicarse en caso de desastre: *B= No presupuestado; M= Cubre menos de 72 horas; A= Garantizado para 72 horas o más.*	ERROR				4	0	0	0			
100	**Procedimientos para habilitación de espacios para aumentar la capacidad, incluyendo la disponibilidad de camas adicionales.** El plan debe incluir y especificar las áreas físicas que podrán habilitarse para dar atención a saldo masivo de víctimas: *B= No se encuentran identificadas las áreas de expansión; M= Se han identificado las áreas de expansión y el personal capacitado para implementarlos; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementar los procedimientos.*	ERROR				4	0	0	0			
101	**Procedimiento para admisión en emergencias y desastres.** El plan debe especificar los sitios y el personal responsable de realizar el TRIAGE. *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				2	0	0	0			
102	**Procedimientos para la expansión del departamento de urgencias y otras áreas críticas.** El plan debe indicar la forma y las actividades que se deben realizar en la expansión hospitalaria (Ej. suministro de agua potable, electricidad, desagüe, etc.): *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				6	0	0	0			

103	**Procedimientos para protección de expedientes médicos (historias clínicas).** El plan indica la forma en que deben ser tratados los expedientes clínicos e insumos necesarios para el paciente: *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				2	0	0	0
104	**Inspección regular de seguridad por la autoridad competente.** En recorrido por el hospital verificar la fecha de caducidad y/o llenado de extintores, extintores e hidrantes. Y si existe referencia del llenado de los mismos así como bitácora de visitas por el personal de protección civil. *B= No existe; M = inspección parcial o sin vigencia; A= Completa y actualizada.*	ERROR				4	0	0	0
105	**Procedimientos para vigilancia epidemiológica intra-hospitalaria.** Verificar si el Comité de Vigilancia Epidemiológica intra-hospitalaria cuenta con procedimientos específicos para casos de desastre o atención a saldo masivo de víctimas: *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				2	0	0	0
106	**Procedimientos para la habilitación de sitios para la ubicación temporal de cadáveres y medicina forense.** Verificar si el plan incluye actividades específicas para el área de patología y si tiene sitio destinado para depósito de múltiples cadáveres: *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				2	0	0	0
107	**Procedimientos para triage, reanimación, estabilización y tratamiento.** *B= No existe el procedimiento; M= Existe el procedimiento y el personal entrenado; A= Existe el procedimiento, personal capacitado y cuenta con recursos para implementarlo.*	ERROR				6	0	0	0
108	**Transporte y soporte logístico.** El hospital cuenta con ambulancias, vehículos oficiales: *B= No cuenta con ambulancias y otros vehículos para soporte logístico; M= Cuenta con vehículos insuficientes; A= Cuenta con vehículos adecuados y en cantidad suficiente.*	ERROR				2	0	0	0
109	**Raciones alimenticias para el personal durante la emergencia.** El plan especifica las actividades a realizar en el área de nutrición y cuenta con presupuesto para aplicarse en el rubro de alimentos. *B= No existe; M= Cubre menos de 72 horas; A= Garantizado para 72 horas o más.*	ERROR				2	0	0	0
110	**Asignación de funciones para el personal movilizado durante la emergencia.** *B= no existe o existe únicamente el documento; M= las funciones están asignadas y el personal capacitado; A= las funciones están asignadas, el personal está capacitado y se cuenta con recursos para cumplir las funciones.*	ERROR				6	0	0	0
111	**Medidas para garantizar el bienestar del personal adicional de emergencia.** El plan incluye el sitio donde el personal de urgencias puede tomar receso, hidratación y alimentos. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas.*	ERROR				2	0	0	0
112	**Vinculado al plan de emergencias local.** Existe antecedente por escrito de la vinculación del plan a otras instancias de la comunidad. *B= No vinculado; M= Vinculado no operativo; A= Vinculado y operativo.*	ERROR				4	0	0	0
113	**Mecanismos para elaborar el censo de pacientes admitidos y referidos a otros hospitales.** El plan cuenta con formatos específicos que faciliten el censo de pacientes ante las emergencias: B= no existe o existe únicamente el documento; M= existe el mecanismo y el personal capacitado; A= existe el mecanismo y el personal capacitado, y se cuenta con recursos para implementar el censo.	ERROR				6	0	0	0
114	**Sistema de referencia y contrarreferencia.** *B= No existe o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				6	0	0	0
115	**Procedimientos de información al público y la prensa.** El plan hospitalario para caso de desastre especifica quien es el responsable para dar información a público y prensa en caso de desastre. (la persona de mayor jerarquía en el momento del desastre): *B= no existe el procedimiento; M= existe el procedimiento y el personal entrenado; A= existe el procedimiento, el personal capacitado y se cuenta con recursos para implementarlo.*	ERROR				6	0	0	0
116	**Procedimientos operativos para respuesta en turnos nocturnos, fines de semana y días feriados.** *B= no existe el procedimiento; M= existe el procedimiento y el personal entrenado; A= existe el procedimiento, el personal capacitado y se cuenta con recursos para implementarlo.*	ERROR				4	0	0	0
117	**Procedimientos para evacuación de la edificación.** Verificar si existe plan o procedimientos para evacuación de pacientes, visitas y personal *B= no existe el procedimiento; M= existe el procedimiento y el personal entrenado; A= existe el procedimiento, el personal capacitado y se cuenta con recursos para implementarlo.*	ERROR				6	0	0	0
118	**Las rutas de emergencia y salida son accesibles.** Verificar que las rutas de salida están claramente marcadas y libres de obstrucción. *B= Las rutas de salida no están claramente señalizadas y varias están bloqueada;. M=Algunas rutas de salida están marcadas y la mayoría están libres de obstrucciones; A=Todas las rutas están claramente marcadas y libres de obstrucciones.*	ERROR				6	0	0	0
119	**Ejercicios de simulación o simulacros.** Verificar que los planes sean puestos a prueba regularmente mediante simulacros o simulaciones, evaluados y modificados como corresponda. *B= Los planes no son puestos a prueba; M= Los planes son puestos a prueba con una frecuencia mayor a un año; A= Los planes son puestos a prueba al menos una vez al año y son actualizados de acuerdo a los resultados de los ejercicios.*	ERROR				6	0	0	0
							0	0	0
	4.3 Planes de contingencia para atención médica en desastres.	CONTROL	Grado de implementación			19			
			BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO

BAJO	MEDIO	ALTO

120	**Sismos, tsunamis, volcanes y deslizamientos.** SI NO EXISTEN ESTAS AMENAZAS EN LA ZONA DONDE ESTA UBICADO EL HOSPITAL, NO MARCAR NADA. DEJAR LAS TRES CASILLAS EN BLANCO. *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	BLANCO				18	0	0	0	0,00	0,00	0,00
121	**Crisis sociales y terrorismo.** *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				7	0	0	0	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
122	**Inundaciones y huracanes.** SI NO EXISTEN ESTAS AMENAZAS EN LA ZONA DONDE ESTA UBICADO EL HOSPITAL, NO MARCAR NADA. DEJAR LAS TRES CASILLAS EN BLANCO. *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	BLANCO				18	0	0	0			
123	**Incendios y explosiones.** *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				15	0	0	0			
124	**Emergencias químicas o radiaciones ionizantes.** *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				7	0	0	0			
125	**Agentes con potencial epidémico.** *B= No existe plan o existe únicamente el documento; M= Existe el Plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				13	0	0	0			
126	**Atención psico-social para pacientes, familiares y personal de salud.** *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				7	0	0	0			
127	**Control de infecciones intra-hospitalarias.** Solicitar el manual correspondiente y verificar vigencia: *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				15	0	0	0			
							0	0	0			

	4.4 Planes para el funcionamiento, mantenimiento preventivo y correctivo de los servicios vitales. Mide el grado de accesibilidad, vigencia y disponibilidad de los documentos indispensables para la resolución de una urgencia.	CONTROL	Grado de implementación			16						
			BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO
128	**Suministro de energía eléctrica y plantas auxiliares.** El área de mantenimiento debe presentar el manual de operación del generador alterno de electricidad, así como bitácora de mantenimiento preventivo: *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				19	0	0	0	0,00	0,00	0,00
129	**Suministro de agua potable.** El área de mantenimiento deberá presentar el manual de operación del sistema de suministro de agua así como bitácora de mantenimiento preventivo y de control de calidad del agua: *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				19	0	0	0			
130	**Reserva de combustible** El área de mantenimiento debe presentar el manual para el suministro de combustible, así como la bitácora de mantenimiento preventivo: *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				12	0	0	0			
131	**Gases medicinales.** El área de mantenimiento deberá presentar el manual de suministro de gases medicinales, así como bitácora de mantenimiento preventivo. *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				19	0	0	0			
132	**Sistemas habituales y alternos de comunicación.** *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				6	0	0	0			
133	**Sistemas de aguas residuales.** El área de mantenimiento garantizará el flujo de estas aguas hacia el sistema de drenaje público evitando la contaminación de agua potable. *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				6	0	0	0			
134	**Sistema de manejo de residuos sólidos.** El área de mantenimiento deberá presentar el manual de manejo de residuos sólidos, así como bitácora de recolección y manejo posterior. *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				6	0	0	0			
135	**Mantenimiento del sistema contra incendios.** El área de mantenimiento debe presentar el manual para el manejo de sistemas contra incendios, así como la bitácora de mantenimiento preventivo de extintores e hidrantes. *B= No existe plan o existe únicamente el documento; M= Existe el plan y el personal capacitado; A= Existe el plan, personal capacitado y cuenta con recursos para implementar el plan.*	ERROR				13	0	0	0			
							0	0	0			

	4.5 Disponibilidad de medicamentos, insumos, instrumental y equipo para desastres. Verificar con lista de cotejo la disponibilidad de insumos indispensables ante una emergencia.	CONTROL	Grado de disponibilidad			16						
			BAJO	MEDIO	ALTO		BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO

136	**Medicamentos.** Verificar la disponibilidad de medicamentos para emergencias. Se puede tomar como referencia el listado recomendado por OMS. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					14	0	0	0			
137	**Material de curación y otros insumos.** Verificar que exista en la central de esterilización una reserva esterilizada de material de consumo para cualquier emergencia (se recomienda sea la reserva que circulará el día siguiente). *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					14	0	0	0			
138	**Instrumental.** Verificar existencia y mantenimiento de instrumental específico para urgencias. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					14	0	0	0			
139	**Gases medicinales.** Verificar teléfonos y domicilio así como la garantía de abastecimiento por parte del proveedor. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					10	0	0	0			
140	**Equipos de ventilación asistida (tipo volumétrico).** El comité de emergencias del hospital debe conocer la cantidad y condiciones de uso de los equipos de ventilación asistida. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					10	0	0	0			
141	**Equipos electro-médicos.** El comité de emergencias del hospital debe conocer la cantidad y las condiciones de uso de los equipos electromédicos: *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					9	0	0	0			
142	**Equipos para soporte de vida.** *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					14	0	0	0			
143	**Equipos de protección personal para epidemias (material desechable).** El hospital debe contar con equipos de protección para el personal que labore en áreas de primer contacto. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					5	0	0	0			
144	**Carro de atención de paro cardiorrespiratorio.** El comité de emergencia del hospital debe conocer la cantidad, condiciones de uso y ubicación de los carros para atención de paro cardiorrespiratorio. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					5	0	0	0			
145	**Tarjetas de triage y otros implementos para manejo de víctimas en masa.** En el servicio de urgencias se difunde e implementa la tarjeta de TRIAGE en caso de saldo masivo de víctimas. Se debe evaluar según la capacidad instalada máxima del hospital. *B= No existe; M= Cubre menos de 72 horas; A= garantizado para 72 horas o más.*	ERROR					5	0	0	0			
		TOTAL FUNCIONAL	**61**	0	0	0	**0**		0	0	0		
		TOTAL	**145**	**0**	**0**	**0**	**0**						

0,00	0,00	0,00

FUNCIONAL

BAJO	MEDIO	ALTO
#¡DIV/0!	**#¡DIV/0!**	**#¡DIV/0!**

Paso 2: Verifique que no existan filas con la palabra "**ERROR**". En caso se muestre el mensaje de "**ERROR**", revise nuevamente la pregunta específica y respóndala de acuerdo al paso 1. Las tablas y las fórmulas no calcularán apropiadamente si hay un mensaje de "**ERROR**" en alguna de las filas.

Paso 3: Tabulación automática de las respuestas de acuerdo a la categoría.

Categoría	Alta probabilidad de no funcionar	Probablemente funcione	Alta probabilidad de funcionar	Total
Estructural	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
No-estructural	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
Funcional	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!

Paso 4: Ingreso de los pesos verticales a ser usados. Abajo se incluyen los pesos acordados por el GAMiD.

Ponderación vertical	
Estructural	0,5
No-estructural	0,3
Funcional	0,2

Categoría	Alta probabilidad de no funcionar	Probablemente funcione	Alta probabilidad de funcionar	Total
Estructural	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
No-estructural	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
Funcional	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!
Total	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!	#¡DIV/0!

Paso 5: Ingreso de los pesos horizontales a ser usados. Abajo se incluyen los pesos acordados por el GAMiD.

Ponderación horizontal		Factores de Seguridad
Alta probabilidad de no funcionar	1	#¡DIV/0!
Probablemente funcione	2	#¡DIV/0!
Alta probabilidad de funcionar	4	#¡DIV/0!

Extremo horizontal inferior

Extremo horizontal superior

Factor de seguridad final: #¡DIV/0!

Paso 6: Cálculo del rango a ser usado para computar los índices de seguridad y vulnerabilidad

NOTA: Para evitar sesgos debido a las cifras concordadas de los pesos usados en las ponderaciones del modelo, se acordó usar un Rango que toma en cuenta ambos extremos de la escala horizontal de peso. En este caso, el nivel mínimo de la seguridad es 1 y la máxima puntuación es 4. El uso de un rango también le permite al evaluador apreciar gráficamente ambos índices y cómo éstos se relacionan entre sí. Se ha sugerido que estos niveles de seguridad podrían verse usando el concepto de un vaso con agua. A medida que el hospital aumenta su factor de seguridad, el vaso se llenará más, es decir, se reducirá la vulnerabilidad.

Rango = Extremo horizontal superior - Extremo horizontal inferior = 4 - 1 = 3

Paso 7: Cálculo del índice de seguridad y el índice de vulnerabilidad

Indice de seguridad $= S =$ $\dfrac{\text{Factor seguridad - extremo horizontal inferior}}{\text{Rango}} =$ #¡DIV/0!

Indice inseguridad $= 1 - S =$ $\dfrac{\text{Extremo horizontal superior - Factor seguridad}}{\text{Rango}} =$ #¡DIV/0!

Indice seguridad	#¡DIV/0!
Indice de vulnerabilidad	#¡DIV/0!

Paso 8: Compare índices de seguridad con recomendaciones base.

Clasificación del establecimiento de salud: #¡DIV/0!

Indice de seguridad	Categoría	¿Qué se tiene que hacer?
0 – 0.35	C	Se requieren medidas urgentes de manera inmediata, ya que los niveles actuales de seguridad del establecimiento no son suficientes para proteger la vida de los pacientes y el personal durante y después de un desastre.
0.36 – 0.65	B	Se requieren medidas necesarias en el corto plazo, ya que los niveles actuales de seguridad del establecimiento pueden potencialmente poner en riesgo a los pacientes, el personal y su funcionamiento durante y después de un desastre.
0.66 – 1	A	Aunque es probable que el hospital continúe funcionando en caso de desastres, se recomienda continuar con medidas para mejorar la capacidad de respuesta y ejecutar medidas preventivas en el mediano y largo plazo, para mejorar el nivel de seguridad frente a desastres.

ANEXO V

Propuesta Cuestionario EVISH

Anexo V

Propuesta Cuestionario EVISH

Tabla A1.

Escala de Valoración del Índice de Seguridad Hospitalaria (EVISH)

Nº	Escala de Valoración del Índice de Seguridad Hospitalaria	RR
1	El Centro ha sufrido daños Estructurales debidos a Fenómenos Naturales	
2	El Centro ha sido Construido según Normativas Vigentes	
2	El Centro ha sido Reparado según Normativas Vigentes	
3	Se han realizado Adaptaciones o Remodelaciones Estructurales en el Centro	
4	Estado actual de la Edificación es correcta	
6	La Interacción Elementos Estructurales es adecuada	
8	Existe Redundancia Estructural	
13	Existe Adecuación Estructural a Fenómenos Naturales (+)	
5	Estado de los Materiales Estructurales (-)	
7	Proximidad de los Edificios (-)	
9	Antigüedad del Edificio (-)	
10	Seguridad de fundaciones y cimientos (+)	
11	Irregularidades en Planta, rigidez, masa y resistencia (-)	
12	Irregularidades en Elevación rigidez, masa y resistencia (-)	
13	Adecuación estructural a fenómenos geológicos y Metereológicos	
14	Sistema Eléctrico dispone de un Generador adecuado a demanda	
15	Sistema Eléctrico es Regular en el funcionamiento en Áreas Críticas	
16	Sistema Eléctrico está Protegido ante Fenómenos Naturales	
17	Sistema Eléctrico está Instalado bajo condiciones de Seguridad	
18	Sistema Eléctrico es Redundante (Repetido) con el Servicio Local de Suministro de Energía	
19	Sistema Eléctrico dispopne de Tablero de Control e Interruptor de Sobrecarga y Cableado	
20	Sistema Eléctrico de Iluminación está situado en lugares Estratégicos y Adecuados	
21	Sistemas Eléctricos Externos instalados dentro del Perímetro del Edificio están correctos	
22	Los Sistema Telecomunicaciones de Antenas y Soportes cumplen normativas de instalación y mantenimiento	
23	Los Sistemas de Baja corriente está en estado Técnico Adecuado	
24	Los Sistema de Comunicación Alterno está en Estado Técnico correcto	
25	En los Sistemas Telecomunicaciones, los Anclajes de Equipos, Soportes y Cables está correctos	
26	Los Sistema Telecomunicaciones Externos está instalados dentro del Perímetro del Centro	
27	Los Sistema Telecomunicaciones está ubicados en un espacio adecuado	
28	Los Sistema Telecomunicaciones Internos están bajo Control de Seguridad	
29	Sistema Suministro de Agua dispone de Tanques de Agua con Reserva Permanente para cubrir necesidades diarias	
30	Sistema Suministro de Agua está situado en el lugar seguro y protegido	
31	Existe un Sistema Suministro de Agua Alterno Adicional a la Red de Distribución Principal	
32	Sistema Suministro de Agua de Distribución está bajo Control de Seguridad	
33	En el Sistema Suministro de Agua existe Bombeo Alterno	
34	Existen Depósitos de Combustibles con capacidad suficiente para disponer de autonomía en cinco días	
35	Los Depósitos de Combustibles están Anclados y disponen de Protección de Tanques y Cilindros	
36	Depósitos de Combustibles están Seguros y situados de forma apropiada y según Normativas	
37	Depósitos de Combustibles tiene mecanismos de Seguridad en el Sistema de Distribución, con válvulas, tuberías y conexiones	
38	Dispone de Almacenamiento de Gases Medicinales para 15 días	
39	Tanques, Cilindros, Equipos de los Gases Medicinales están bien Anclados	
40	Existen Fuentes Alternativas para disponer de Gases Medicinales	
41	Gases Medicinales están situados de forma correcta en el lugar adecuado	
42	Existe Seguridad en el Servicio de Distribución de los Gases Medicinales	
43	Disponen de Protección adecuada los Tanques, Cilindros y Equipos de los Gases Medicinales	
44	La Seguridad de los Gases Medicinales en los Recintos es Apropiada	
45	Los Sistemas de Calefacción tienen Soportes Adecuados para los Ductos y Tuberías que cruzan Juntas de Dilatación	
46	Los Sistemas de Calefacción tienen en perfecto estado las Tuberías, Uniones y Válvulas	
47	Sistemas de Calefacción disponen de Anclajes de los Equipos y Depósitos de Agua Caliente	
48	Los Anclajes del Aire Acondicionado están correctos	
49	Ubicación del Aire Acondicionado está correcta en los Recintos de Áreas Críticas	
50	Existe Seguridad de los Recintos dónde están ubicados los Equipos de las Áreas Críticas	
51	Correcto Funcionamiento de Equipos: caldera, aire acondicionado, extractores	

52	Anclajes adecuado de Estanterías y Seguridad Contenidos	
53	Los Equipos Informáticos están Asegurados	
54	Estado funcional y para uso del Mobiliario de Oficina y Equipos	
55	Quirófano y Sala de Recuperación cumplen las condiciones exigidas	
56	La Sala de Rayos X e Imagenología cumple con la Normativa Vigente	
57	Los Laboratorios están bien dotados	
59	El Servicio de Urgencias dispone de los Recursos necesarios para un funcionamiento eficaz	
60	El Equipamiento y Mobiliario de Farmacia dispone de las existencias básicas	
61	Sistemas de Esterilización está en estado funcional	
62	El Cuidado del Recién Nacido se lleva a cabo con calidad	
63	El Servicio de Atención al Quemado está en perfecto estado funcional	
64	Los Servicios de Radioterapia y Medicina Nuclear están bajo condiciones de Seguridad	
65	Existe un adecuado funcionamiento de Otros Servicios	
66	Anclajes de estanterías y seguridad de los Contenidos	
67	Puertas o Entradas están en perfecto estado de funcionamiento	
68	Las Ventanas están supervisadas y en perfecto funcionamiento	
69	Elementos de Cierre: muros externos, fachadas se encuentran en buen estado	
70	Techos y Cubiertas están controlados y revisados	
71	Parapetos: paredes, barandas en escaleras están en buenas condiciones de uso	
72	Cercos y Cierres perimétricos	
73	Cornisas, ornamentos, etc	
74	Áreas de Circulación Externa	
75	Áreas de Circulación Interna	
76	Particiones o Divisiones Internas	
77	Cielos Falsos o Rasos	
78	Iluminación Externa e Interna	
79	Protección Contra Incendios	
80	Sistemas de Ascensores	
81	Escaleras	
82	Cubiertas de Pisos	
83	Vías de Acceso a la Instalación	
84	Elementos Arquitectónicos, Señales de Seguridad	
85	Comité Formalmente Constituido	
86	Comité Personal Multidisciplinar	
87	Los Miembros conocen sus Responsabilidades	
88	El Centro de Operaciones de Emergencia tiene espacio suficiente	
89	El Centro de Operaciones de Emergencia ubicado en lugar adecuado	
90	El Centro de Operaciones de Emergencia tiene Sistema Informáticos adecuados	
91	El Centro de Operaciones de Emergencia funciona la Comunicación Interna y Externa	
92	El Centro de Operaciones de Emergencia tiene Sistemas Comunicaciones Alternativos	
93	El Centro de Operaciones de Emergencia dispone de Mobiliario y Equipos Adecuados	
94	El Centro de Operaciones de Emergencia dispone de Directorio Telefónico Actualizado	
95	El Centro de Operaciones de Emergencia ha elaborado Tarjetas de Acción para todos los implicados ante situaciones de Emergencias	
96	Refuerzo de Servicios Esenciales	
97	Procedimientos para la Activación y Desactivación del Plan de Emergencias	
98	Previsiones Administrativas Especiales en Desastres	
99	Recursos Financieros Presupuestados y Disponibles	
100	Procedimientos de habilitación de Espacios para aumentar Capacidad	

101	Procedimientos para la Admisión de Emergencias y Desastres	
102	Procedimientos para Expansión del Servicio de Urgencias y Áreas Críticas	
103	Procedimientos para Protección de Expedientes Médicos Historias Clínicas	
104	Inspección Regular de Seguridad por la Autoridad Competente	
105	Procedimientos para Vigilancia Epidemiológica Intra Hospitalaria	
106	Procedimientos para ubicar Temporalmente Cadáveres y Actuaciones Forenses	
107	Procedimientos para Triaje, Reanimaciópn, Estabilización y Tratamiento	
108	Procedimientos y medios para Transporte y Soporte Logístico	
109	Disponer de Raciones Alimenticias para el personal durante las Emergencias	
110	Asignación de Funciones para el Personal en Estado de Emergencias	
111	Medidas para garantizar el Bienestar del Personal Adicional de Emergencias	
112	Existe Vinculación con el Plan de Emergencias Local	
113	Mecanismo paora Elaborar el Censo de Pacientes Admitidos y en otros Hospitales	
114	Existe un Sistemas de Referencia y Contrareferencias	
115	Tiene Procedimientos de Información Pública y Prensa.	
116	Procedimientos Operativos para Organizar los Turnos	
117	Existen Procedimientos para Evacuar el Centro	
118	Nivel de Accesibilidad de Rutas de Emergencias y Salidas	
119	Se llevan a cabo Simulaciones de Emergencias y Desastres en el centro	
120	Desastres Naturales: sismos, volcanes, deslizamientos	
121	Crisis Sociales y Actos Terroristas	
122	Existencia de Inundaciones y Huracanes	
123	Existencia de Incendios y Explosiones	
124	Existencia de Emergencias Químicas o Irradiaciones Ionizantes	
125	Existencia de Agentes con Potencial Epidémico	
126	Existe Atención Psicosocial a Pacientes, Familiares y Personal del Centro	
127	Existen procedimientos para el Control de Infecciones Intrahospitalarias	
128	Estado del Suministro de Energía Eléctrica y Plantas Auxiliares	
129	Nivel de Suministro de Agua Potable	
130	Niveles de Reserva de Combustibles	
131	Nivel de Suministros de Gases Medicinales	
132	Funcionamiento de los Sistemas Habituales y Alternos de Comunicación	
133	Funcionamiento de los Sistemas de Aguas Residuales	
134	Funcionamiento de los Sistema de Residuos Sólidos	
135	Nivel de Mantenimiento de los Sistemas Contra Incendios	
136	Disponibilidad de Medicamentos para Situación de Emergencias	
137	Nivel de Reserva de material de Curas Esterilizado para cualquier Situación de Emergencias	
138	Existencia y Mantenimiento de Instrumental específico para Emergencias	
139	Dispone de datos de Proveedores de Gases Medicinales para contactar en caso de Urgencias	
140	Existen Equipos de Ventilación Asistida para utilizar en caso de Emergencias	
141	Dispone el Centro de Equipos Electro-Médicos en condiciones de uso	
142	Dispone el Centro de Equipos para Soporte de Vida	
143	Hay suficientes Equipos disponibles de Protección para el Personal en caso de Epidemias	
144	Dispone el Centro de Carros de Atención de Paro Cardio Respiratorio	
145	Existen suficientes Tarjetas de Triaje y otros Implementos para el Control de Víctimas en Masa	

Tabla A2.

Escalas de Valoración de Prevención de Riesgos. Seguridad y Control de Riesgos

Dimensiones	Factores	Matices
Ubicación Geográfica del Establecimiento	Amenazas y Fenómenos	Geológicas e Hidrometereológicas Sociales y Culturales Sanitarios y Ecológicos Químicos y Tecnológicos
	Propiedades Geotécnicas del Suelo	Propiedades de los Materiales del Terreno Geometría y Distribución del Terreno Condiciones Hidrogeológicas del Terreno Condiciones de la Construcción

Tabla A3

Seguridad Estructural

Dimensiones	Factores
Seguridad Estructural	Antecedentes del Establecimiento (1-3) Seguridad de los Sistemas Estructurales (4-13) Seguridad del Material de la Construcción (5,7,9,10 Irregularidades Observadas (11 y 12)

Tabla A4

Seguridad no Estructural (primera parte)

Dimensión	Factores	Matices
Seguridad no Estructural	Líneas Vitales en Instalaciones	Sistema Eléctrico Sistema de Telecomunicaciones Sistema de Abastecimiento de Agua Sistemas de Combustibles Sistemas de Gases Medicinales
	Instalaciones en Áreas Críticas	Sistemas de Calefacción Sistemas de Ventilación Sistemas de Aire Acondicionado
	Mobiliario y Equipos	Tipos de Mobiliario y Seguridad Sistemas Informáticos y Ordenadores
	Equipos Médicos	Equipos de Quirófano Equipos de Sala de Recuperación Sala de Radioterapia e Imagenología Equipos de Laboratorio Equipos del Servicio de Urgencias Equipos en Unidad de Cuidados Intensivos Material de Farmacia del Centro Sistemas de Esterilización Condición de Seguridad Recién Nacido Condición de Seguridad Unidad de Quemados Condición de Seguridad de Radioterapia y Nuclear Condición Seguridad en otros Servicios Anclajes y Seguridad de Mobiliario con material

Tabla A5

Seguridad no Estructural (segunda parte)

Dimensiones	Factores	Matices
Seguridad no Estructural	Elementos Arquitectónicos	Puertas o Entradas están en perfecto estado de funcionamiento
		Las Ventanas están supervisadas y en perfecto funcionamiento
		Elementos de Cierre: muros externos, fachadas se encuentran en buen estado
		Techos y Cubiertas están controlados y revisados
		Parapetos: paredes, barandas en escaleras están en buenas condiciones de uso
		Cercos y Cierres perimétricos
		Cornisas, ornamentos, etc
		Áreas de Circulación Externa
		Áreas de Circulación Interna
		Particiones o Divisiones Internas
		Cielos Falsos o Rasos
		Iluminación Externa e Interna
		Protección Contra Incendios
		Sistemas de Ascensores
		Accesos y Escaleras
		Cubiertas de Pisos
		Vías de Acceso a la Instalación
		Elementos Arquitectónicos, Señales de Seguridad

Tabla A6

Seguridad y Capacidad Funcional ante Emergencias y Desastres

Dimensiones	Factores
Seguridad y Capacidad Funcional ante Emergencias y Desastres	Organización y Funcionamiento del Comité
	Plan Operativo de Desastres Internos y Externos
	Plan de Contingencias de Atención Médica
	Planes de Acción Preventiva y Correctiva de los Servicios Vitales
	Disponibilidad de Medios Materiales y Equipos Apropiados