UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

# Normativa y procedimientos de la UE sobre ciberseguridad en redes 5G y su aplicación en la normativa y procedimientos españoles.

Trabajo Fin de Máster

Máster Universitario en Ciberseguridad y Ciberinteligencia

AUTOR/A: Cutanda Mansilla, Ernesto

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2021/2022

PÁGINA INTENCIONADAMENTE EN BLANCO

# ÍNDICE

# TABLA DE ILUSTRACIONES

PÁGINA INTENCIONADAMENTE EN BLANCO

# 1. Introducción

El presente Trabajo Fin de Máster (TFM) se ha considerado como una oportunidad de poder avanzar en un conocimiento más profundo sobre la legislación aplicable en cuanto a los procedimientos de implementación de seguridad en los sistemas de información y telecomunicaciones, sobre la base del actual estado de implementación e integración de sistemas de tecnología 5G en las redes de sistemas de información.

La tecnología 5G supondrá nuevos retos para los integrantes de los Comités de Seguridad de las Tecnologías de la Información y las Comunicaciones (CSEGTIC) de las instituciones o sus equivalentes en el sector privado, estando los roles de sus integrantes definidos en la guía de seguridad **CCN-STIC 201 Organización y Gestión para la Seguridad de las TIC**[1] y sus equivalencias en los entornos de la Unión Europea (UE) y de la Organización del Tratado del Atlántico Norte (OTAN), no siendo estos roles objeto de estudio ni de valoración en el presente TFM

Pero si nos centramos en la legislación, se observa que en la legislación de la UE se ha producido un avance en cuanto a considerar la relevancia de la tecnología 5G junto con el aumento de los riesgos asociados a la misma y sus posibles mitigaciones. Mientras tanto, la transposición a la legislación nacional de los estados miembros se está produciendo a un ritmo menor del deseado. Las implicaciones económicas, dado que afecta al principio de libre mercado dentro de la UE, así como la necesidad de renovación de recursos tanto en el ámbito de la administración pública como en el sector privado, se considera el principal referente para el ritmo de esta transposición. Aún a pesar de que a priori, los riesgos considerados sean asumibles frente a los beneficios que la tecnología 5G proporcionará a los ciudadanos de la Unión.

A nivel legislación del Reino de España, se cuenta en la actualidad con legislación referente a los requisitos necesarios para la implementación de la

[1] TIC: Tecnologías de la Información y las Comunicaciones.

tecnología 5G, pero a falta de definir un Esquema Nacional de Seguridad acorde a dicha tecnología. Este esquema deberá ser el punto de partida para el desarrollo de las distintas guías técnicas que orienten sobre las mejores prácticas en ciberseguridad ante el reto que supone la implementación 5G (y seguramente se actúe de igual manera ante la aparición y puesta en uso de futuras generaciones de tecnología).

# 2. Objeto

El objeto marcado para el presente TFM es el de conocer la legislación aplicable en cuanto a la implementación de las medidas de ciberseguridad en los sistemas de información y telecomunicaciones de los que se fuese responsable, sin descender al rol asignado de la guía de seguridad CCN-STIC 201 anteriormente mencionada.

Se constata que los componentes de los CSEGTIC cuentan con una formación completa en cuanto a concienciación y actuaciones para mejorar las capacidades de ciberseguridad y así reducir las brechas de seguridad en los sistemas implementados/explotados. Por ello se considera oportuno que una vez con los conocimientos suficientes, se proceda a conocer la legislación aplicable en la implementación de dichos requisitos, llegando si fuese posible, hasta la tecnología 5G (el ritmo de aprobación de la legislación y normativa derivada seguramente no vaya a la par que el presente TFM, pero al menos este podría ser un punto de inicio para su continuación y actualización en un posible estudio futuro).

Pero no sólo busca el presente TFM centrarse en la legislación a equivalencia de un vademécum. Busca que cualquiera de los implicados en un CSEGTIC o equivalente, con independencia del rol asignado, sea conocedor de las posibles implicaciones que pudiese llevar una mala praxis por no considerar la relevancia que tiene la implementación de procedimientos de seguridad en las redes y sistemas de información. El seguimiento de un método técnico reconocido, la implementación de unas políticas de seguridad acordes a lo que como mínimo se quiere defender y que las actuaciones, o la carencia de estas, puede acarrear una elevada responsabilidad ética y/o económica dentro del entorno que se viese comprometido, así como judicial.

A su vez, se considera que el presente TFM en ningún momento se podrá considerar definitivo. Las amenazas evolucionan, la tecnología evoluciona, la legislación y normativa derivada (incluidas guías o procedimientos de implementación técnicos) evolucionan, por lo que, a lo igual que está ocurriendo

en el momento de redacción del presente TFM con la implementación e integración de la tecnología 5G, la misma no se produce de manera simultánea. Es decir, no se abandona en un momento concreto y definido la tecnología 4G y anteriores, sino que la tecnología 5G se integra en las anteriores hasta que, en un futuro, en algún momento, todo sea 5G (a no ser que ya se esté integrando tecnología posterior por la capacidad y necesidad de evolución o se mantenga la tecnología anterior, debido a la imposibilidad de evolución de distintos componentes hardware o software). Por lo que, si bien el objeto es la trasposición de la normativa referente a la tecnología 5G de la UE en la legislación española, en ningún momento se podrá suponer una separación total de las generaciones antecedentes con la futura generación (ya casi presente).

Finalmente, siendo las redes y sistemas de información objeto de aplicación de la normativa en vigor las pertenecientes o explotadas por las administraciones públicas y aquellas consideradas esenciales o críticas por su interés nacional, esto no impide que los modelos aplicados para la implementación de las capacidades de ciberseguridad sean empleadas en redes y sistemas de información no obligados a ello por legislación. Esto ocurre principalmente en el entorno privado, cumplimentado esta implementación de capacidades de ciberseguridad con potenciales comunicaciones de ciberincidentes de acuerdo con los procedimientos establecidos.

Y todas estas implementaciones de ciberseguridad motivadas principalmente, sobre la base de las posibles amenazas declaradas para España como nación soberana, como estado miembro de entidades supranacionales o como estado miembro de acuerdos multinacionales.

Llegados este punto, se considera oportuno indicar explícitamente los objetivos. Se considera **objetivo principal** el **conocimiento de la legislación de la UE o nacional aplicable en actuaciones (o carencia de estas) en relación con la ciberseguridad, incluyendo** la tecnología de última generación **5G**, y como **objetivos secundarios**, una vez conocidos el por qué debo implementar medidas de seguridad, conocer **el qué y el cómo se debe implementar, y en su caso, que tomar como referencia o que se pudiese considerar como tal.**

Finalmente, se planteará como el presente TFM cumplimenta determinados objetivos de desarrollo sostenible (ODS), recogidos en Anexo específico.

# 3. Antecedentes

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión, puede ser considerada como el punto de partida de las medidas de ciberseguridad a implementar en las redes de comunicaciones y su evolución hacia la quinta generación (5G) en la UE, si bien con anterioridad a la misma se contaba ya con la Estrategia Europea de Ciberseguridad (2013)[2].

La omnipresencia de los sistemas de información y telecomunicaciones en la sociedad, sobre la que se empiezan a basar las relaciones y actividades económicas y sociales, así como el vertiginoso incremento de incidentes de seguridad o el elevado número de fuga de datos, tanto deliberados como no, ponen en riesgo la estabilidad de la UE y la defensa de los derechos propios del individuo como miembro de esta.

Ello hace que el intercambio de información sobre las buenas prácticas a aplicar en las redes y en los sistemas de información se convierta en una necesidad. Para ello, los países miembros de la UE han optado por la regulación comunitaria de unas capacidades mínimas de seguridad en las redes y en los sistemas de información, con el objeto de elevar el nivel de seguridad en los mismos. El éxito de dicha regulación se sustenta indispensablemente en la participación tanto de los proveedores de servicios sobre dichas redes como de la de los proveedores de los sistemas y equipos, en cuanto a la implementación y cumplimiento de las medidas de seguridad estipuladas, la comunicación de incidentes, una gestión de riesgos acorde con la situación, junto con las necesidades a proteger y las capacidades disponibles.

[2] Unión Europea. Comunicación Conjunta (JOIN 2013) de 7 de febrero de 2013 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *"Estrategia de Ciberseguridad de la Unión Europea: Un Ciberespacio abierto, Protegido y Seguro".* [Consulta 6 de marzo de 2022]. Disponible en: https://data.consilium.europa.eu/doc/document/ST%206225%202013%20INIT/es/pdf

Motivado por el incremento del riesgo en la estabilidad de la UE sobre la base del uso de los sistemas de información y telecomunicaciones, así como con la visión de la popularización en el acceso a Internet, la UE no sintió únicamente la necesidad de empezar a normalizar la implementación de las diferentes medidas de seguridad dentro de sus estados miembros en las redes y en los sistemas de información propiamente dichos. También incrementó y completó diferentes regularizaciones al respecto en cuanto a la accesibilidad física a los diferentes componentes o equipos que los estructuran.

Es decir, empezaron, dentro de las capacidades normativas al amparo del Tratado de Funcionamiento de la Unión Europea[3] (TFUE), a introducir regulaciones de nivel supranacional con el objeto de unificar lo máximo posible las medidas de seguridad que se adoptasen por cada uno de los estados de manera independiente, de acuerdo con el nivel legislativo de cada una de las normas.

Y todo ello debido a que *«el ciberespacio se ha convertido ya en el lugar en el cual se va a decidir en gran medida la prosperidad y seguridad de los países en el futuro próximo»*[4], habiendo sido el mismo un espacio en el que las amenazas y peligros estaban siendo infravalorados (si bien continúan siendo infravalorados por una elevada parte de la sociedad por la dificultad o poca relación que encuentran entre su concienciación de seguridad y las posibilidades de que dichas amenazas o riesgos les puedan afectar a nivel particular).

Pero en relación con el dominio ciberespacial, se debe en primer lugar saber que dicho termino, «ciberespacio» no es un término originariamente técnico. *«El término «ciberespacio» fue acuñado por WILLIAM GIBSON, escritor de ciencia ficción, en el contexto de un relato breve que vio la luz en el año 1982[5]. Su*

[3] Unión Europea. Versión Consolidada del Tratado de Funcionamiento de la Unión Europea. *Diario Oficial de la Unión Europea*, 30 de marzo de 2010, núm C 83, p. 49.
[4] MORET MILLÁS, Vicente. "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español". En *ieee.es Documentos de Opinión* [en línea]. Núm 21/2017. 3 de marzo de 2017 [consulta: 6 de marzo de 2022]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf
[5] El término «ciberespacio» es acuñado por W. Gibson en 1982 por primera vez, pero se popularizó a raíz del éxito internacional de su novela «Neuromante» publicada en 1984.

*creación literaria resultó sorprendentemente profética, erigiéndose hoy como la forma con que se designa al conjunto de aparatos informáticos, redes, cables de fibra óptica, y demás infraestructuras que llevan el internet a miles de millones de personas de todo el mundo»*[6].

La incapacidad de limitar el ciberespacio a un territorio concreto, bajo la actuación y legislación de un único estado, hace que las medidas supranacionales, multinacionales e internacionales se constituyan como la estrategia a seguir en defensa de los intereses nacionales, complementadas con las medidas nacionales particularizadas a las amenazas definidas por cada estado soberano sobre la base de su gestión de riesgos (no únicamente referidos al ciberespacio). Todo ello con el objeto de crear una mayor fortaleza ante las amenazas emergentes que se desarrollan en una dimensión ilimitada, no completamente explotada, conocida o controlada frente a la vulnerabilidad que significaría la aplicación de estrategias nacionales no coordinadas.

Siendo conscientes de que la seguridad absoluta no existe, las medidas que se adopten, dentro de una escalabilidad global, ayudaran a frenar las amenazas y riesgos existentes y emergentes ante los nuevos desarrollos en el uso de las tecnologías (macrodatos, nube, inteligencia artificial, …), si bien quedará pendiente la concienciación del eslabón más débil de la cadena de seguridad, el usuario. Este difícilmente podrá ser regulado en cuanto a uso, no en cuanto a acceso, sobre el que habrá que realizar los mayores esfuerzos en concienciación de los riesgos potenciales en el uso de las redes y de los sistemas de información, en la importancia de las medidas de seguridad implementadas y en

MANSILLA MORALES, José Manuel. "Caminando hacia el futuro. El ciberespacio y el educador social". En: *Educación, sociedad y tecnología.* [en línea]. Madrid: Editorial Universitaria Ramón Areces, p 169 [consulta 18 de mayo de 2022]. Disponible en: https://books.google.be/books?id=m3SUDAAAQBAJ&pg=PA169&dq=fecha+neuromante+william+gibson&hl=es&sa=X&ved=2ahUKEwjh-Oz4yen3AhVDQRoKHRbLCEYQ6AF6BAgLEAI#v=onepage&q=fecha%20neuromante%20william%20gibson&f=false

[6] MARCO CLEMENT, Isabel. "La protección de las infraestructuras críticas en la UE: ¿Ciberseguridad al rescate? Tutora: Susana de Tomás Morales. Trabajo Fin de Grado Derecho Internacional Público. Universidad Pontificia Comillas Madrid. Abril 2017. P 1 [consulta 6 de marzo de 2022]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/17923/TFG%20DERECHO%20-%20Isabel%20Marco%20Clement.pdf?sequence=1&isAllowed=y

las acciones que, a nivel particular, mejorarán la protección no solo de los sistemas, sino también del individuo sobre la base de las acciones que el mismo realice en el ciberespacio.

# 4. Legislación

## 4.1 Unión Europea

4.1.1 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 de las tecnologías de la información y la comunicación por el que se deroga el Reglamento (UE) nº 526/2013 (Reglamento sobre Ciberseguridad)

La definición legal de reglamento se recoge en el TFUE, en su artículo 288, *«El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.»*[7]

Los Reglamentos adquieren automáticamente carácter vinculante en toda la UE a partir de la fecha de su entrada en vigor[8], siendo responsabilidad de las autoridades nacionales que se aplique correctamente.

Siendo el objeto del presente TFM la normativa y procedimientos sobre ciberseguridad de la UE para redes 5G y su aplicación a la normativa y procedimientos españoles, el estudio se centra en los artículos 46 al 65 del Reglamento (UE) 2019/881, considerados como el marco europeo para la certificación de ciberseguridad.

Si bien, y por tratarse de un trabajo en el que se procederá a respetar el orden del grado jerárquico de la normativa de las distintas disposiciones de la Unión Europea o del Reino de España durante su estudio, se considera que la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión (Directiva NIS[9]), es el documento inicial de referencia en cuanto a la necesidad de

[7] Vid nota 3, p. 171.
[8] Unión Europea. "Aplicar la legislación de la UE". En: *ec.europa.eu Legislación Proceso legislativo* [en línea]. [consulta: 6 de marzo de 2022]. Disponible en: https://ec.europa.eu/info/law/law-making-process/applying-eu-law_es
[9] En la actualidad se está a la espera de aprobación definitiva de Directiva que actualizará la considerada como Directiva NIS, recibiendo su actualización el sobrenombre de Directiva NIS 2,

normalización en ciberseguridad de las redes y los sistemas de telecomunicaciones dentro de la legislación comunitaria. Será tratado con posterioridad.

La implementación del marco europeo de certificación de ciberseguridad busca dos objetivos. Por un lado, incrementar la confianza en la seguridad tanto de los procesos de tráfico de datos (información) en las redes y en los sistemas de información como en los datos consecuencia del funcionamiento de los sistemas que conforman las mismas (tráfico de datos de las redes y de los sistemas de información); y por otro, establecer un único esquema de referencia en cuanto a certificaciones en el ámbito supranacional que constituye la UE.

Este esquema de certificación se marca como objetivo el proteger la disponibilidad, autenticidad, integridad y confidencialidad del tráfico de datos, su procesamiento y su almacenamiento. Por ello, en función de la relevancia de estos, se definen tres grados de certificación a alcanzar por las redes y sistemas de información, básico, sustancial y elevado, que se alcanzarán tras pasar la evaluación correspondiente de conformidad.

Los requisitos para dicha evaluación no se encuentran detallados en el Reglamento objeto de estudio, siendo la Agencia de la Unión Europea para la Ciberseguridad (ENISA) la responsable de crear y mantener el marco de certificación europea de la ciberseguridad. Deberá definir los requisitos necesarios a implementar conforme al grado de certificación a obtener en función de la sensibilidad de los datos y de los sistemas a proteger, así como sobre la base de la gestión de riesgos y amenazas de los que pudiesen ser objeto.

El cumplimiento de los requisitos durante la evaluación de seguridad para la obtención del certificado de ciberseguridad será valorado por uno de los organismos de evaluación de la conformidad debidamente autorizado por la

---

sobre la base del documento de la Comisión Europea, *"Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad de las redes y por la que se deroga la Directiva (UE) 2016/1148"* [en línea]. COM (2020) 823 final 2020/0359 (COD). 16 de diciembre de 2022 [consulta: 19 de abril de 2022]. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0012.02/DOC_1&format=PDF

autoridad nacional de certificación de ciberseguridad (el Reglamento permite más de una autoridad nacional por estado miembro), o en carencia de los primeros, por esta última (o estas últimas).

#### 4.1.2 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión

La definición legal de directiva se recoge en el TFUE, en su artículo 288, *«La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios.»*[10]

Las Directivas tienen que ser incorporadas a la legislación nacional por los Estados miembros de la UE[11], de acuerdo con el plazo marcado en las mismas, tanto para su incorporación como para la información de tal hecho a la Comisión de la UE.

La Directiva (UE) 2016/1148 constituye el hito de referencia como inicio de la implementación de un procedimiento para garantizar un cierto nivel, elevado en el momento de su promulgación, en cuanto a la seguridad en las redes y sistemas de información en la UE. Si bien únicamente es aplicable a las administraciones públicas que sean consideradas operadores de servicios esenciales, estas por lo general, se apoyaran en proveedores de servicios digitales de carácter privado.

Para ello, el primer objetivo de esta Directiva ha sido la identificación y unificación de criterios en la UE para considerar a una empresa como operadora de servicios esenciales. Es decir, la Directiva busca focalizar su implementación en sectores muy concretos que aseguren las capacidades básicas de funcionamiento de un estado.

[10] Vid nota 3 p. 172.
[11] Vid nota 8.

El segundo objetivo que se desgrana de la Directiva fue el hecho de implementar la colaboración para intercambiar información, buenas prácticas y apoyarse mutuamente en el desarrollo de herramientas y sistemas de ciberseguridad sobre la base de la prevención, detección, mitigación y respuesta a ciberincidentes. Este «grupo de colaboración» requirió las diferentes actualizaciones de las estrategias de ciberseguridad de los estados, o el desarrollo de estas por los estados carentes de estrategias que regulasen el ciberespacio. Asimismo, requirió la creación a nivel nacional equipos de respuesta ante incidentes de seguridad informática que serían los responsables de gestionar los riesgos, amenazas e incidentes a su nivel, así como cooperar en estos aspectos como representantes nacionales en la comunidad supranacional que supone la UE.

En este concepto de «grupo de colaboración» destaca ENISA, como vértice de este y responsable de velar y promover dichas relaciones de cooperación.

A su vez, la Directiva adopta una medida operativa, como es la creación de una red de equipos de respuesta a incidentes de seguridad informática (CSIRT), compuesta por los CSIRT nacionales de cada uno de los estados miembros de la UE, los cuales constituyen el auténtico nivel de cooperación rápida, eficaz y supranacional ante ciberincidentes.

Finalmente, hay que indicar que lo novedoso de esta Directiva fue la implicación en cuanto a seguridad en redes y en sistema de información, de determinados actores privados, y en concreto, de operadores de los servicios esenciales una vez concretados los mismos, y de los proveedores de servicios digitales. Estos actores privados tienen que implementar una serie de medidas de seguridad, de acuerdo con el nivel de riesgo, para proteger sus redes y sus sistemas de información, así como deben establecer las relaciones con el correspondiente CSIRT en cuanto a la transmisión de información sobre incidentes detectados o sufridos en sus sistemas.

En resumen, a la entrada en vigor de la Directiva se buscaba implementar un grado de seguridad elevado en las redes y en los sistemas de información

empleados para la gestión de las infraestructuras definidas como críticas y el establecimiento de mecanismos de cooperación eficaces a nivel supranacional, *«no es una norma de seguridad en sí misma, sino que establece el mandato y los mecanismos para normalizar la seguridad en cada uno de los Estados miembros de la Unión y los de coordinación entre todos ellos.»*[12]

No obstante, la limitación a redes de uso por las administraciones públicas y de las entidades definidas como de servicios esenciales, no se debe considerar impedimento para que las mejoras que empiezan a introducirse sean a su vez implementadas a título particular por entidades o particulares no administración pública. Y como muestra de ello, la directiva no sólo implica la obligación *ex lege* «*sino que también prevé que aquellas empresas que no se encuentren obligadas por la propia Directiva, pero quieran notificar los incidentes que afecten a la continuidad de sus servicios, puedan hacerlo de forma voluntaria.»*[13]

Finalmente, de la presente directiva se detectan las siguientes carencias:

- No detalla estándares en cuanto a las medidas de seguridad a implementar o los requisitos mínimos que se deben de alcanzar.
- En cuanto a proveedores de software, no se les aplica nada similar a lo aplicado a los proveedores de servicios digitales.
- Tampoco afecta a los proveedores de hardware, pudiendo los componentes fundamentales de cualquier arquitectura de red o de sistemas de información, junto con el software propio de funcionamiento (firmware) de estos componentes, convertirse en el eslabón más débil ante las amenazas y riesgos a los que se pudiesen enfrentar.

La actualización de la Directiva UE 2016/1148, sobre la base de la propuesta (COM 2020) 823 final, 2020/0359 (COD) de 16 de diciembre de 2020 de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a

[12] *"La Transposición de la Normativa NIS al Ordenamiento Jurídico Español: Una Perspectiva empresarial".* Fundación ESYS. Septiembre de 2017 p. 24 [consulta 6 de marzo de 2022]. Disponible en: https://fundacionesys.com/en/system/files/documentos/ESTUDIO%20NIS%2BANEXOS.pdf
[13] Vid nota 4 p. 9.

garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148, surge como consecuencia de la necesaria adaptación a los desarrollos tecnológicos acaecidos desde su aprobación, así como con el espíritu de corregir las deficiencias detectadas para su implementación, dadas las distintas interpretaciones habidas tanto por los estados como por los actores implicados.

La Directiva vigente no recoge servicios digitales que en la actualidad se consideran relevantes (como pueden ser servicios en la nube o las plataformas de redes sociales). La identificación de los proveedores digitales no se realizó de manera inequívoca. No estableció un procedimiento único de comunicación de incidentes. Permite la disparidad en cuanto a las sanciones y obligaciones marcadas por cada estado. No ha mejorado el intercambio de información relevante entre las entidades nacionales responsables de la ciberseguridad y actores privados principalmente por la carencia de un procedimiento sistematizado. Finalmente, no se dimensionó correctamente el potencial humano y económico que su implementación podría suponer para el sector público, por un lado, pero principalmente, el esfuerzo que supondría para el sector privado.

Tratándose por el momento como propuesta la Comunicación referenciada, la misma inicialmente corrige distintas carencias detectadas en la Directiva en vigor, si bien continúa detectándose la carencia de detallar estándares en cuanto a las medidas de seguridad a implementar o requisitos mínimos a cumplir, reflejándose en el artículo 21 de la Directiva propuesta por la Comisión que *«los estados miembros podrán exigir a las entidades esenciales e importantes que certifiquen determinados productos, servicios y procesos de TIC en virtud de un esquema europeo de certificación de la ciberseguridad específico adoptado con arreglo al artículo 49 del Reglamento (UE) 2019/881.»*[14]

[14] Vid nota 9 p. 53.

### 4.1.3 Recomendación (UE) 2019/534 de la Comisión de 26 de marzo de 2019 Ciberseguridad en las redes 5G

La definición legal de decisión, recomendación o dictamen se recoge en el TFUE, en su artículo 288, «*La decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos.*

*Las recomendaciones y los dictámenes no serán vinculantes.»*[15]

La Recomendación (UE) 2019/534 aporta tres ideas principales en cuanto a la relevancia de la importancia de las redes y de los sistemas de información para la UE:

- Por un lado, resalta la importancia que para el comercio interior tendrán las futuras redes, sustentadas en tecnologías 5G, aumentando las capacidades y velocidad, e incrementando a su vez potenciales vulnerabilidades y riesgos.
- Asimismo, resalta la importancia que puede suponer la dependencia para el establecimiento y mantenimiento de dichas redes de servicios y tecnologías no desarrolladas en el seno de la UE, haciendo referencia a la elevada presencia de tecnología china en las redes y en los sistemas de información como ejemplo de una potencial influencia no deseada o no acorde con los principios de la UE, suponiéndolo un riesgo.
- Finalmente, destaca la necesidad de realización de evaluaciones de riesgos a nivel nacional como base de una evaluación coordinada de los riesgos para la entidad supranacional que supone la UE.

Y sobre la base de dicha evaluación de riesgos nacionales y de la Unión, la Recomendación establece la necesidad de establecer un conjunto de herramientas común a la Unión para hacer frente a los mismos, debiendo incluir las mismas un inventario de riesgos de seguridad sobre las redes 5G y un conjunto de posibles medidas mitigadoras.

[15] Vid nota 3 p. 172.

Asimismo, y es de destacar, la Recomendación invita a los estados miembros de la UE a la elaboración de reglamentos técnicos en los que se reflejen los requisitos necesarios para la certificación de los componentes y sistemas constitutivos de las redes y de los sistemas de información, así como a la inclusión de cláusulas de ciberseguridad en los pliegos de contratación pública.

## 4.2 España

### 4.2.1 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

El Real Decreto-ley 12/2018 corresponde a la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión a la legislación española, habiéndose considerado la referida Directiva (UE) 2016/1148 como el punto origen en la UE de la regulación en cuanto a las necesidades de ciberseguridad en las redes y en los sistemas de información.

Por tanto, a equivalencia, se podría considera este Real Decreto-ley como el origen de la regulación en cuanto a ciberseguridad en la legislación española. Pero esta suposición sería errónea, dado que a fecha de su entrada en vigor ya existía normativa de rango legislativo en cuanto a medidas de seguridad en redes y sistemas de información, como era el caso del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[16].

El Real Decreto-ley en cuestión identifica los principales actores destinatarios (operadores de servicios esenciales y proveedores de servicios digitales, de acuerdo con los criterios nacionales, ampliando por tanto los sectores indicados en la Directiva (UE) 2016/1148, salvo que no sean considerados operadores críticos o que sean microempresas o pequeñas empresa, según lo estipulado

[16] España. 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*, 29 de enero de 2010, núm. 25. Texto consolidado, última modificación 04 de noviembre de 2015 [en línea]. [Consulta: 26 de abril de 2022]. Derogado. Disponible en: https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf

para ambos casos en la normativa vigente), debiendo los mismos proceder a responder de la protección de las redes y sistemas de información de los servicios considerados esenciales. Para ello adoptarán las medidas (tanto técnicas como organizativas) mitigadoras oportunas y de acuerdo con el nivel de seguridad a implementar que se requiera ante los potenciales riesgos y amenazas que les afectasen, estando obligados a la notificación de los incidentes sufridos.

Asimismo, el Real Decreto-ley identifica los CSIRT nacionales de referencia a día de entrada en vigor de este, siendo los puntos de entrada de las notificaciones de incidentes. Estos CSIRT de referencia en la actualidad son:

- CCN-CERT del Centro Criptológico Nacional.
- INCIBE-CERT del Instituto Nacional de Ciberseguridad de España.
- ESPDEF-CERT del Ministerio de Defensa, orgánico del Mando Conjunto del Ciberespacio.

En cuanto al punto de contacto único nacional en las relaciones transfronterizas, corresponderá el mismo al Consejo de Seguridad Nacional.

En relación con el procedimiento de notificación de incidentes, el Real Decreto-ley estipula la necesidad de establecer un procedimiento regulado, entrando a marcar la obligatoriedad en cuanto a la notificación de ciberincidentes y detallando los factores a considerar a la hora de valorar la relevancia de un incidente.

Finalmente, hay que indicar que el Real Decreto-ley recoge un procedimiento sancionador ante la falta de cumplimiento de las medidas o procedimientos establecidos para la protección de seguridad de las redes y sistemas de información.

#### 4.2.2 Real Decreto-ley 7/2022, de 29 de marzo, sobre los requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

El Real Decreto-ley considera la siguiente normativa de la UE:

- Recomendación (UE) 2019/534 de la Comisión de 26 de marzo de 2019, Ciberseguridad de las redes 5G.
- Comunicación de 29 de enero de 2020, (COM 2020) 50 final, de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de la Regiones Despliegue seguro de la 5G en la UE – Aplicación de la caja de herramientas de la UE.

Este Real Decreto-ley es considerado por el autor del presente TFM como el documento normativo de mayor alcance y concreción elaborado por el legislador español en cuanto a seguridad en redes y sistemas de información. Y no por el hecho de contemplar la evolución hacia la tecnología bajo el paraguas de 5G, sino por el hecho de que detalla y agrupa con precisión los requisitos a cumplir en cuanto a seguridad de las redes y de los sistemas por los distintos actores identificados en el Real Decreto-ley. A su vez, legisla la posibilidad de limitar el acceso al mercado nacional de potenciales proveedores de tecnología 5G.

Y dado que es así considerada, es oportuno reproducir literalmente el siguiente párrafo de este Real Decreto-ley: *«Las redes y servicios 5G poseen ventajas comparativas en seguridad respecto a las de generaciones precedentes. Pero presentan también riesgos específicos derivados por ejemplo de su arquitectura de red más compleja, abierta y desagregada, y de su capacidad de transportar ingentes volúmenes de información y permitir la interacción simultánea de múltiples personas y cosas. Su interconexión con otras redes y el carácter trasnacional de muchas de las amenazas inciden en su seguridad, y en el previsible empleo generalizado de estas redes para funciones esenciales para la economía y la sociedad, incrementará el impacto potencial de los incidentes de seguridad que sufran.»*[17]

Es decir, el Real Decreto-ley reconoce la complejidad de los sistemas, sus ventajas, su empleo como base de las funciones esenciales tanto económicas como sociales en las que se sustenta la sociedad española y se anticipa a

[17] España. 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, *Boletín Oficial del Estado*, 30 de marzo de 2022, núm. 76, p. 41546.

considerar la necesaria seguridad sobre las redes y servicios 5G ante potenciales incidentes como posibles causas de desestabilización de las funciones esenciales y de la sociedad española.

Para ello, con el objeto de proteger y garantizar (bajo la premisa de que la seguridad total no existe) la disponibilidad, confidencialidad e integridad de los sistemas frente a ataques exteriores, el primer paso que da es considerar dicha regulación con el rango de ley, con el objeto imponer a posibles proveedores limitaciones de acceso al mercado nacional de proveedores (o suministradores) de tecnología 5G. Y lo hace imponiéndoles obligaciones en cuanto a estrictos controles de seguridad, con el fin de garantizar tanto la fiabilidad técnica como la independencia ante potenciales injerencias externas, de acuerdo con los análisis de riesgos y medidas mitigadoras en vigor[18].

Por otro lado, se considera relevante del presente Real Decreto-ley (inicialmente propuesto en su anteproyecto como ley) el procedimiento de aprobación por urgencia realizado (de ahí que sea un Decreto-ley) sobre la base de la situación en el momento de su aprobación de la crisis Rusia-Ucrania, al haberse detectado un incremento elevado de ciberataques de motivación geoestratégica.

A su vez, hay que destacar del presente Real Decreto-Ley el acierto del legislador en cuanto a la exigencia sobre la necesidad de establecer un Esquema Nacional de Seguridad de redes y servicios 5G, estableciendo el marco para el desarrollo de este sobre la base del análisis de riesgos y gestión de estos (incluyendo posibles medidas mitigadoras) referidos a la gestión integral y global de seguridad en la redes y servicios 5G, detallando los actores con deber de colaboración y ejecución.

Asimismo, el Real Decreto-ley no sólo recoge, como no podría ser de otra forma, la debida necesidad de colaboración internacional en la elaboración del Esquema Nacional de Seguridad de redes y servicios 5G (principalmente en el

[18] Sirva como ejemplo el artículo de MANSO CHICOTE, Carlos, 2022. Huawei pide una regulación «objetiva y proporcional» para la seguridad del 5G en España. *ABC.* 20 de mayo de 2022 [en línea]. [Consulta: 20 de mayo de 2022]. Disponible en: https://www.abc.es/economia/abci-huawei-pide-regulacion-objetiva-y-proporcional-para-ciberseguridad-espana-202205200808_noticia.html

seno de la UE), sino que también destaca la necesidad de potenciar la investigación, desarrollo, innovación y formación de personal sobre la base de dicho Esquema.

Finalmente, se considera oportuno resaltar que el primer Esquema Nacional de Seguridad de redes y servicios 5G deberá estar aprobado en un plazo de seis meses desde la entrada en vigor del Real Decreto-ley.

#### 4.2.3 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

El presente Real Decreto concreta y establece «*el marco estratégico e institucional de seguridad de las redes y sistemas de información, las obligaciones de seguridad y la gestión de incidentes*»[19], completando la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión ya iniciada con el Real Decreto-ley 12/2018, de 7 de septiembre.

Este Real Decreto marca los aspectos que deben de contener las políticas de seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales, siendo los mínimos los que a continuación se detallan[20]:

- Análisis y gestión de riesgos.
- Gestión de riesgos de terceros o proveedores.
- Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
- Gestión de personal y profesionalidad.
- Adquisición de productos o servicios de seguridad.
- Detección y gestión de incidentes.
- Planes de recuperación y aseguramiento de la continuidad de las operaciones.

[19] España. 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*, 28 de enero de 2021, núm. 24, p. 8188.
[20] Ibidem, p. 8193.

- Mejora continua.
- Interconexión de sistemas.
- Registro de la actividad de los usuarios.

La relación de las medidas de seguridad adoptadas por la organización serán recogidas en un documento denominado Declaración de Aplicabilidad de las medidas de seguridad. La responsabilidad de este recae en el designado como responsable de seguridad de la información de la organización, debiendo recoger tanto las medidas mínimas anteriormente relacionadas, como aquellas otras que la organización haya considerado oportunas para la seguridad de sus redes y sistemas de información. Las mismas deberán ser sobre la base de las reflejadas en el Real Decreto en vigor que regule sobre el Esquema Nacional de Seguridad, pudiéndose elaborar el documento de Declaración de Aplicabilidad de las medidas de seguridad sobre otros estándares reconocidos, pero sin perjuicio de los exigido por la legislación española.

Hay que destacar del presente Real Decreto, el procedimiento de notificación de incidentes, siendo obligatoria la notificación de todos aquellos incidentes considerados como de nivel crítico, muy alto o alto, por los actores estipulados en la normativa en vigor. Para ello, se constituye la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, responsabilidad del CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT, como la herramienta fundamental para dicha notificación, empleándose además para el intercambio de información entre las autoridades competentes y los CSIRT de referencia[21].

Finalmente, el Real Decreto recoge la clasificación/taxonomía de ciberincidentes aprobada por la ENISA, lo que facilita su identificación.

[21] Además de los CSIRT de referencia, se pueden consultar la relación actualizada de Equipos de Seguridad y Gestión de Incidentes existentes en España mediante consulta en el enlace https://www.csirt.es/index.php/es/miembros

#### 4.2.4 Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021

Uno de los objetos del presente Real Decreto es la concreción de los riesgos y amenazas que pudiesen ser potencialmente hostiles contra España.

En cuanto a dichos riesgos y amenazas potenciales, los mismos se relacionan en el documento, pudiendo ser agrupados en riesgos y amenazas explicitas (directamente recogidos y catalogados como tales) y en riesgos y amenazas implícitas (no directamente recogidos como riesgos y amenazas, pero si relacionados como factores que amenazan a la seguridad de España).

En cuanto al campo de la ciberseguridad, se indican los siguientes riesgos y amenazas explícitas en el ciberespacio, como nuevo dominio estratégico:

- Ciberataques.
- Uso del ciberespacio para realizar actividades ilícitas.

No obstante, a lo largo del documento se relacionan las siguientes vulnerabilidades que, en su caso, afectarían a las redes y sistemas de información, pudiendo ser considerados como riesgos o amenazas implícitos:

- Estrategias híbridas por parte de actores estatales o no estatales (por ejemplo, injerencias de terceros en el uso del ciberespacio, ciberespionaje, cibercrimen, etc.).
- Dependencia de recursos críticos de proveedores/suministradores exteriores (principalmente de China en cuanto a tecnología 5G[22]).
- Irrupción de tecnologías de nueva generación, complejas y de protección dificultosa.
- Irrupción de tecnologías potencialmente disruptivas.
- Prevalencia de criterios comerciales y económicos frente a los de seguridad en el diseño de productos y servicios.

[22] Vid nota 18.

### 4.2.5 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

El objeto del Esquema Nacional de Seguridad (ENS) es el establecimiento de la política de seguridad en la utilización de los medios electrónicos requeridos para la implementación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[23].

Siendo la base de su objeto la protección de la información tratada, almacenada y la resiliencia de los medios electrónicos que compongan sus sistemas, el ENS se sustentará sobre los principios básicos y requisitos mínimos que se detallarán a continuación.

Los principios básicos que contempla son[24]:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

De los mismos, en relación con la diferenciación de responsabilidades, introduce la figura de distintos responsables en relación con los sistemas de información, siendo estos de la información, del servicio, de la seguridad y del sistema. Diferencia la responsabilidad de la seguridad de los sistemas de información de la responsabilidad sobre la explotación de estos, clarificando a su vez que *«la política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.»*[25]

[23] España. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. *Boletín Oficial del Estado*, 2 de octubre de 2015, núm. 236. Texto consolidado, última modificación 30 de marzo de 2022 p. 83 [en línea]. [Consulta: 22 de junio de 2022]. Disponible en: https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf
[24] España. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 4 de mayo de 2022, núm. 106, p. 61725.
[25] Ibidem p. 61727.

Hay que destacar que el Real Decreto define como política de seguridad de la información «*el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta*»[26], detallando los mínimos que debe incluir dicha política de seguridad de la información de la organización:

- Objetivos o misión de la organización.
- Marco regulatorio en el que se desarrollarán las actividades.
- Roles o funciones de seguridad, definiendo deberes y responsabilidades, así como procedimiento de designación y renovación.
- Estructura y composición del comité o comités para la gestión y coordinación de la seguridad, con detalle del ámbito de responsabilidad y relaciones con el resto de los órganos de la entidad.
- Directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- Riesgos que se deriven del tratamiento de los datos personales.

Siendo los requisitos mínimos de seguridad de la organización, que deberán también incluirse en la política de seguridad de esta[27]:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.

[26] Ídem.
[27] Ibidem p. 61728.

- Registro de actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

El conjunto de los principios básicos junto con los requisitos mínimos detallados serán los indicadores que establezcan las medidas de seguridad a aplicar, las cuales podrán ser aplicadas en el marco organizativo, viendo la organización en su globalidad; en el marco operacional, en cuanto a proteger la operatividad del sistema de información empleado; o como medidas de protección, enfocadas a activos concretos del sistema o que usan el mismo.

En cuanto a la categorización de los sistemas de información, el Real Decreto los categoriza de acuerdo a la seguridad a proporcionar a la información que manejan y los servicios que prestan. Las medidas de ciberseguridad deberán ser implementadas en función de los riesgos a los que se encuentren expuestos y su impacto en el caso de sufrir un incidente de seguridad, con perjuicio de la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad del sistema, siendo las categorías definidas como de nivel bajo, medio o alto.

Finalmente, el Real Decreto indica que **el Esquema Nacional de Seguridad requiere de la aplicación de** una serie de **Instrucciones Técnicas de Seguridad,** en algunos casos designadas de manera concreta (explícitamente nombradas en el Real Decreto) y en otros casos indicadas como «*Instrucción Técnica de Seguridad correspondiente*» en el Real Decreto, siendo las mismas las que a continuación se detallan:

- **Esquema de certificación de responsables de la seguridad.**
- **Interconexión de sistemas de información.**
- **Notificación de incidentes de seguridad.**
- **Auditoría de la seguridad de los sistemas de información.**
- **Adquisición de productos de seguridad.**
- **Criptología de empleo en el ENS.**

El Real Decreto recoge, por tanto, las medidas de seguridad a implementar en los sistemas sobre la base de la información a proteger, el análisis de riesgos, la amenaza a la puede estar sometido el sistema y el impacto ante el éxito de la amenaza, estableciendo también los procedimientos y periodicidad de auditorías del sistema y de la seguridad de la organización, considerando su conjunto como seguridad global del sistema.


*Ilustración 1. Legislación UE y España en relación con la ciberseguridad y transposición de la primera en la segunda*

# 5. Otras amenazas de ciberseguridad para España a nivel estratégico. Comunicado de la Cumbre de la OTAN 2021 (Bruselas)

En relación con la OTAN, a la que España se adhirió en 1982, es relevante que sus decisiones o comunicaciones se realizan por consenso, no por votación, siendo en la actualidad 30 estados los miembros de esta Alianza.

En cuanto a las amenazas que consensuaron en la Cumbre de Bruselas de 2021, los jefes de estado o gobierno de los países miembros recogen la preocupación por la creciente amenazada en el ciberespacio como nuevo entorno estratégico, constituyéndose como un dominio propio de operaciones de entidades estatales y no estatales, acordando apoyar a empresas de nueva creación que desarrollen y trabajen tecnologías emergentes y disruptivas de doble uso en áreas clave para la seguridad de los aliados.

Para ello, la OTAN y los aliados se comprometieron a incrementar la resiliencia, enfocando la misma, dentro de sus regulaciones, a mantener y mejorar la seguridad de infraestructuras críticas, industrias clave, cadenas de suministro y redes de información, incluyendo la tecnología 5G[28].

De dichas amenazas se detectan los siguientes actores:

- Rusia: Como responsable de acciones maliciosas en el ciberespacio, así como por su permisibilidad ante ciberdelicuentes que atacan a las infraestructuras críticas de los miembros de la Alianza operando desde su territorio y por el empleo del medio cibernético para diferentes acciones híbridas de desestabilización.
- Grupos Terroristas: Empleando en su beneficio las nuevas tecnologías emergentes.

[28] NATO, "Brussels Summit Communiqué", 14 de junio de 2021 (actualizada el 8 de abril de 2022) [en línea]. Punto 30. [Consulta: 28 de abril de 2022]. Disponible en: https://www.nato.int/cps/en/natohq/news_185000.htm

- China: Como potencial actor de acciones no acordes a los compromisos internacionales adoptados en cuanto al uso del ciberespacio, entre otros espacios.

# 6. Normativas técnicas aplicables a las redes 5G

## 6.1 Unión Europea. Ciberseguridad en redes 5G. Caja de Herramientas de la UE para medidas de mitigación de riesgos

La misma no es más que un compendio de medidas de mitigación para reducir el posible impacto de los riesgos en las redes 5G, sobre la base de la evaluación efectuada por la UE de los riesgos y las amenazas a la seguridad en las redes de dicha tecnología.

A su vez, detalla planes de reducción de riesgo mediante la aplicación de una serie de medidas acordes para cada uno de los riesgos, a implementar tanto por estados miembros de la UE y por los propios órganos de la UE.

Dichas medidas se pueden agrupar en:

- Medidas estratégicas: referenciadas a competencias legislativas/normativas para la regulación de la contratación y despliegue de redes de tecnologías 5G, así como todas aquellas medidas relativas a vulnerabilidades no técnicas.
- Medidas técnicas: focalizadas a mitigar los riesgos del proceso de intercambio de datos propiamente dicho, es decir, los derivados de las tecnologías y procesos implementados junto a las capacitaciones que deben cumplir el personal técnico y las infraestructuras físicas donde se alojan los componentes de las redes y sistemas de información.
- Medidas de apoyo: orientaciones que se emitan sobre la base de las buenas prácticas que hayan sido efectivas en la mitigación de riesgos y amenazas y fomenten el intercambio de y cooperación de dichas buenas prácticas.

Principalmente dichas medidas se centran en evaluar el perfil de riesgo de los proveedores/administradores de tecnologías 5G, debiéndose introducir en la legislación y normativa de la UE y de los estados miembros las oportunas restricciones a aquellos proveedores/administradores considerados de alto

riesgo, complementadas con medidas cuyo objeto sean evitar de dependencia de estos proveedores/administradores de riesgo.

Finalmente, hay que destacar que la Caja de Herramientas de UE para medidas de mitigación de riegos en redes 5G define tres tipos principales de vulnerabilidades:

- Las relacionas con el hardware, software, procesos y políticas implementadas en las redes y sistemas de información.
- Las específicas del proveedor.
- Las derivadas de la dependencia de proveedores únicos.

## 6.2 España

### 6.2.1 Instrucciones Técnicas de Seguridad

Para el presente TFM se analizarán las Instrucciones Técnicas de Seguridad (ITS) en vigor relacionadas tanto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, como las ITS no relacionadas en este Real Decreto, pero si en los Reales Decretos derogados 3/2010, de 8 de enero, y 951/2015, de 23 de octubre, los cuales regulaban el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, al dar el Real Decreto 311/2022 un plazo de 24 meses de adaptación desde su entrada en vigor.

#### 6.2.1.1 Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad

Esta ITS no se recoge dentro del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, pero si en los Reales Decretos derogados 3/2010 y 951/2022.

La misma establece *«…las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la*

*seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, …»*[29].

Dicho informe, en el caso de las redes y sistemas de información de las administraciones públicas, será reflejado de acuerdo con la herramienta existente a tal fin, Informe Nacional del Estado de Seguridad (INES), el cual requerirá ser complementado de acuerdo con lo contemplado en la guía de seguridad **CCN-STIC 824 Informe del Estado de Seguridad**, sobre la base de los datos contemplados en la guía de seguridad **CCN-STIC 815 sobre Métricas e Indicadores para el Esquema Nacional de Seguridad**.[30]

6.2.1.2 Resolución de 13 de octubre de 2016, de la Secretaría de Estado de las Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad

Esta ITS no se recoge dentro del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, pero si en los Reales Decretos derogados 3/2010 y 951/2022.

La misma establece *«…los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.»*[31]

En relación con los procedimientos, la presente ITS diferencia entre sistemas de categoría baja de los de media o alta, permitiendo que para la Declaración de Conformidad en los sistemas de categoría baja sea suficiente una autoevaluación por parte del propietario del sistema (mediante el personal que

[29] España. Disposición 10108. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. *Boletín Oficial del Estado*, 2 de noviembre de 2016, núm. 265, p. 76364.

[30] No confundir la aplicación de las guías de seguridad CCN-STIC indicadas para la implementación y mejora de las medidas de seguridad de las redes y sistemas de información con la guía de seguridad CCN-STIC 844 Manual de Usuario de la herramienta INES, que únicamente es de manejo de la herramienta INES.

[31] España. Disposición 10109. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. Boletín Oficial del Estado, 2 de noviembre de 2016, núm. 265, p. 76366.

lo administra u otros en los que se delegue dicha autoevaluación), mientras que para los sistemas de categoría media o alta es necesario realizar un proceso formal de certificación de conformidad.

La Declaración de Conformidad con el ENS se complementa con un distintivo paralelo a la misma, regulado por normativa en vigor (en este caso, la presente ITS).

En cuanto a las entidades certificadoras, las mismas deberán de estar acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas a los que se les sea de aplicación el ENS, sobre la base de la norma ISO/IEC 17065:2012. La relación de estas (junto a las que se encuentran en vías de certificación) se pueden consultar en el siguiente enlace del Centro Criptológico Nacional (CCN)[32]:

https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion

Finalmente, la Instrucción recoge el contenido que debe tener la Declaración de Conformidad con el ENS, el Distintivo de Declaración de Conformidad con el ENS y la Certificación de Conformidad con el ENS, si bien los mismos deben respetar lo indicado en la guía de seguridad **CCN-STIC 809 sobre Declaración y Certificación de Conformidad con el Esquema Nacional de Seguridad**.

6.2.1.3 Resolución de 27 de marzo de 2018, de la Secretaría de Estado de la Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información

La misma establece *«…las condiciones para la realización de las auditorías, ordinarias o extraordinarias, …»*[33], siendo las mismas un proceso metódico, independiente y documentado cuyo objeto es la obtención de evidencias y

[32] A fecha 9 de mayo de 2022 en el enlace se recogen 20 entidades de certificación acreditadas o en vías de acreditación para expedir certificaciones de conformidad con el ENS y sistemas clasificados hasta nivel Difusión Limitada.
[33] España. Disposición 4573. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. *Boletín Oficial del Estado*, 3 de abril de 2018, núm. 81, p. 35269.

evaluación de estas con el fin de obtención del grado de conformidad del sistema auditado sobre lo estipulado por el ENS.

Una auditoría satisfactoria implicará la obtención del Certificado de Conformidad con el ENS, que en el caso de sistemas de grado medio y alto tendrá una validez de dos años.

El método para aplicar en el proceso de auditoría será mediante la aplicación de las guías **CCN-STIC 802 Guía de auditoría, CCN-STIC 804 Guía de implantación y CCN-STCI 808 Verificación del cumplimiento de las medidas del Esquema Nacional de Seguridad**, debiendo llegar a las siguientes calificaciones de la auditoría:

- Favorable.
- Favorable con no conformidades, lo que implica la posibilidad de corregir las disconformidades con el Esquema Nacional de Seguridad detectadas en el plazo de un mes sobre la base de un Plan de Acciones Correctivas.
- Desfavorable, cuando se valore que un Plan de Acciones Correctivas fuese insuficiente para subsanar las deficiencias detectadas de conformidad con el Esquema Nacional de Seguridad, requiriendo en tal caso una auditoría extraordinaria para verificar las acciones correctivas aplicadas y sus efectos en el sistema en cuanto a su implementación en cumplimiento del Esquema Nacional de Seguridad en un plazo no superior a seis meses.

Para las calificaciones de auditoría se empleará la Guía de Seguridad **CCN-STIC 824 Informe del Estado de Seguridad**, debiendo el informe de auditoría reflejar los aspectos estipulados en la normativa al respecto en vigor.

6.2.1.4 Resolución de 13 de abril de 2018, de la Secretaría de Estdo de la Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad

La misma establece *«…la notificación y gestión de incidentes de seguridad de las entidades del Sector Público…cuando tales incidentes tengan un impacto*

*significativo en la seguridad de la información que manejan o los servicios que prestan, en relación con la categoría del sistema …»*[34].

Para la consideración de un incidente como de «impacto significativo», se valorará el mismo de acuerdo con lo estipulado en la guía de seguridad **CCN-STIC 817 Gestión de Ciberincidentes**, pudiendo los mismos ser calificados como irrelevante, bajo, medio, alto, muy alto o crítico.

El proceso de notificación y recopilación de evidencias se efectuará de acuerdo con la mencionada guía CCN-STIC 817, debiendo proceder a su documentación y custodia efectiva. El proceso de notificación se encuentra automatizado mediante la herramienta de Listado Unificado de Coordinación de Incidentes y Amenazas (LUCIA).

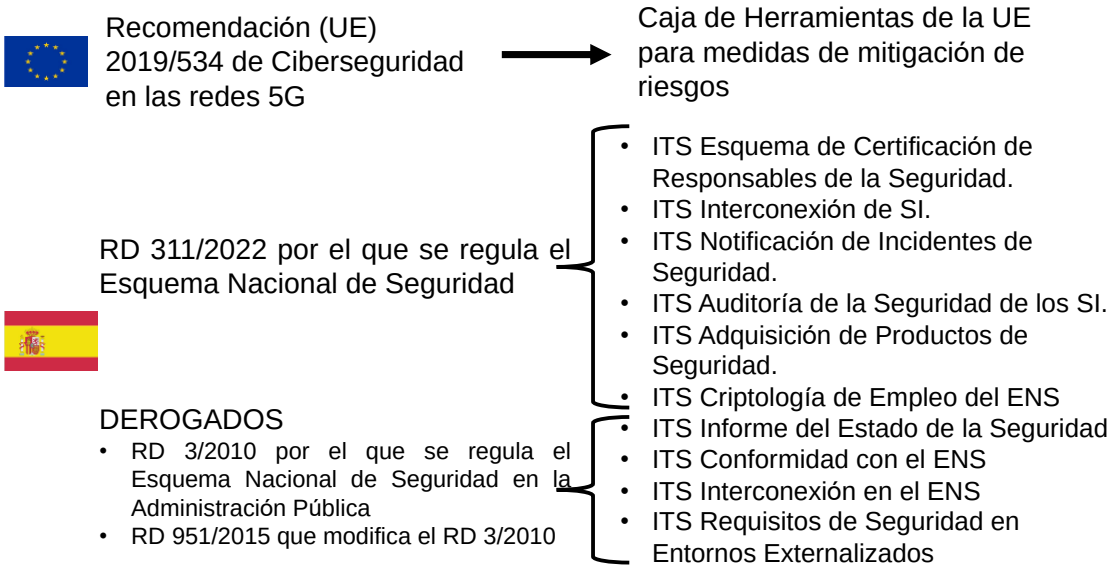


*Ilustración 2. Normativas Técnicas de Seguridad Aplicables (UE y España).*

[34] España. Disposición 5370. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. *Boletín Oficial del Estado*, 19 de abril de 2018, núm. 95, p. 40557.

### 6.2.2 Guías CCN-STIC[35]

Las mismas son un compendio normativo que comprende instrucciones y recomendaciones con el fin de ser implementadas con el objeto de aumentar la ciberseguridad en las organizaciones.

Principalmente orientadas para su implementación en las administraciones públicas y empresas consideradas de servicios esenciales según regulación española, no son en su totalidad accesibles por el público, salvo registro pertinente del usuario interesado a través la página web del CCN https://www.ccn-cert.cni.es/registro.html

Estas se agrupan por series sobre la base de su temática, siendo la serie 800[36] las guías de seguridad relativas con el ENS, de las que algunas ya han sido mencionadas en el apartado anterior relativo a las Instrucciones Técnicas de Seguridad.

Dado que en el presente TFM se han analizado en el apartado anterior las ITS en vigor de las exigidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y las recogidas y en vigor en los Reales Decretos derogados 3/2010, de 8 de enero y 951/2015, de 23 de octubre, que regulaban el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, como consecuencia del plazo de 24 meses para la adaptación al Real Decreto 311/2022, e indicado con cada ITS analizada las guías de seguridad del CCN-STIC de aplicación, a continuación se enumerarán las guías relacionadas con las ITS pendientes de desarrollo o publicación y de las que sí existe equivalente o similar como guías de seguridad del CCN-STIC.

[35] CCN-CERT. *Guías CCN-STIC.* [En línea]. [Consulta 11 de mayo de 2022]. Disponible en: https://www.ccn-cert.cni.es/guias.html
[36] CCN-CERT. *Guías CCN-STIC.* [En línea]. [Consulta 11 de mayo de 2022]. Disponible en: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

6.2.2.1 Instrucción Técnica de Seguridad de Adquisición de Productos de Seguridad

No publicada de manera oficial a día la fecha, el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, indica que «*se utilizará para ello el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN*»[37], que coincide con la actualización de la guía de seguridad **CCN-STIC 105** Catálogo de Productos Recomendados[38], denominándose esta **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación** desde su actualización de mayo de 2022.

6.2.2.2 Instrucción Técnica de Seguridad de Criptología de Empleo en el Esquema Nacional de Seguridad

La misma no se encuentra publicada oficialmente a día de la fecha, existiendo en su lugar la guía de seguridad **CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad**.

6.2.2.3 Instrucción Técnica de Seguridad de Interconexión en el Esquema Nacional de Seguridad

Esta ITS no se recoge dentro del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, pero si en los Reales Decretos derogados 3/2010 y 951/2022.

No se encuentra publicada de manera oficial a día de la fecha, existiendo en su lugar la guía de seguridad **CCN-STIC 811 Interconexión en el ENS**.

[37] España. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 4 de mayo de 2022, núm. 106, p. 61751

[38] Otra fuente de consulta para equipos que cumplan especificaciones de seguridad sobre la base de Common Criteria pueden ser consultados en el enlace: https://www.commoncriteriaportal.org

6.2.3 Instrucciones Técnicas de Seguridad no publicadas de acuerdo con el Real Decreto 311/2022, de 3 de mayo y los Reales Decretos derogados 3/2010, de 8 de enero y 951/2015, de 23 de octubre y sin equivalencias o similares en guías de seguridad CCN-STIC

En este grupo estaría encuadradas la ITS de esquema de certificación de responsables de seguridad, la ITS de interconexión de sistemas de información y la ITS de requisitos de seguridad en entornos externalizados.

Esta última ITS no se recoge dentro del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, pero si en los Reales Decretos derogados 3/2010 y 951/2022.

| |
|---|
| ITS Informe del Estado de la Seguridad<br>824 Informe Estado de Seguridad y 815 Métricas e Indicadores para el ENS |
| ITS Conformidad con el Esquema Nacional de Seguridad<br>809 Declaración y Certificación de Conformidad con el ENS |
| ITS Auditoría de la Seguridad de los SI<br>802 Guía de Auditoría, 804 Guía de implantación y 808 Verificación del cumplimiento de las medidas del ENS |
| ITS Notificación de Incidentes de Seguridad<br>817 Gestión de Ciberincidentes |
| ITS Adquisición de Productos de Seguridad (No publicada)<br>105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación |
| ITS Criptología de Empleo en el ENS (No publicada)<br>807 Criptología de Empleo en el ENS |
| ITS Interconexión en el ENS (No publicada)<br>811 Interconexión en el ENS |
| ITS Esquema de Certificación de Responsables de Seguridad (No publicada) |
| ITS Interconexión de Sistemas de Información (No publicada) |
| ITS Requisitos de Seguridad en Entornos Externalizados (No publicada) |

*Ilustración 3. Instrucciones Técnicas de Seguridad y Guías de Seguridad CCN-STIC relacionadas.*

# 7. Otros. Sentencias (España)

## 7.1 Sentencia del Tribunal Supremo 453/2022 de 15 de febrero de 2022

La misma es como consecuencia de una violación en cuanto al cumplimiento de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Debido a una incompleta implementación de medidas de seguridad por diseño en una de las aplicaciones empleadas por una empresa, en concreto usada para solicitar el alta de servicios para nuevos usuarios, esta requería, para proseguir con el proceso de alta, facilitar un correo electrónico de contacto. Dado que algunos de los mismos (al menos 14 nuevos clientes) carecían del mismo, durante el proceso de alta y con el objeto de cumplimentar el formulario requerido, por parte de quién asistía a los nuevos clientes, introducía un correo electrónico supuestamente inexistente, que resultó pertenecer a una persona física, la cual denunció dicho hecho al recibir datos de carácter personal de terceros.

Es decir, la carencia de un sistema de verificación de correo electrónico, posibilidad técnica ya existente en el momento que se producen los hechos indicados, genera una incorrecta custodia de los datos personales responsabilidad de la empresa, procediendo a su difusión automática a través del correo facilitado (aunque fuese falso o incorrecto) sin haber implementado un sistema o procedimiento de verificación de correo electrónico previo a la remisión de documentación con datos de carácter privado.

El hecho de que trabajadores de la empresa, introdujesen a sabiendas un supuesto correo falso y autorizado mediante firma física del formulario por el nuevo cliente, con el fin de completar el procedimiento de alta, no exime a la empresa de la debida responsabilidad de adoptar las medidas de seguridad oportunas para evitar la brecha de seguridad en el tratamiento de los datos personales. Los datos acabaron en conocimiento de un tercero, por no contar con las soluciones técnicas ya existentes, responsabilidad corporativa que recae en el estamento directivo y de los administradores del sistema de información de

la empresa. Estos no requirieron para el diseño de la aplicación de la introducción de las medidas de seguridad factibles con las posibilidades tecnológicas ya existentes.

La falta de una política de seguridad claramente definida y la carencia de implementación de los medios oportunos en cuanto a ciberseguridad supuso para la empresa, tanto la correspondiente sanción económica como, la merma de su prestigio dentro de su sector (lo que, con la debida publicidad, beneficia a la potencial competencia).

### 7.2 Sentencia de la Audiencia Nacional 900/2022 de 14 de marzo de 2022

La Sentencia de la Audiencia Nacional (SAN) impugna un acto administrativo en materia laboral y de seguridad social, debido a que, por inoperatividad de los sistemas de información, considerado por la empresa afectada como un motivo de fuerza mayor, no pudo tramitar telemáticamente diferentes solicitudes a la administración pública en plazo.

De la sentencia se considera relevante el hecho de valorar las condiciones de ciberseguridad implementadas por la empresa para poder estimar si el incidente pudiese ser considerado como de fuerza mayor ante la imposibilidad del manejo de los sistemas de información. Esta consideración implica poder extender plazos administrativos reglados, frente una posible negligencia por causa de falta de concienciación ante los potenciales riesgos cibernéticos o por no haber adoptado las medidas oportunas para la mitigación ante las posibles amenazas o ataques a los sistemas de información empleados.

La empresa afectada demostró la existencia de una incidencia técnica como consecuencia de la detección de un virus en el sistema de información de la empresa. Pero este hecho per se, no hubiese sido considerado como causa de fuerza mayor para poder haber ampliado el plazo administrativo legalmente estipulado.

El hecho relevante en esta sentencia es que la misma relaciona y reconoce la adopción de las siguientes medidas de ciberseguridad por parte de la empresa:

- Existencia de unas políticas de seguridad de la información basadas en un modelo, en este caso denominado PDCA (planificar, hacer, revisar, actuar por sus siglas en inglés), con una revisión anual.
- Certificación de AENOR de **cumplimiento de las técnicas de seguridad de la información según normativa ISO/IEC 27001**, renovada anualmente de acuerdo con auditorías superadas.
- Certificación de **desarrollo de controles específicos, cumplimentando los indicados en la norma de estandarización la ISO/IEC 27002**.
- Existencia de una Política de Seguridad propia de la empresa, desarrollada sobre la base de la norma de estandarización ISO/IEC 27002.
- Activos inventariados y controlados.
- Control de accesos al sistema y a las infraestructuras.
- Protocolo de renovación de sistemas y adquisición.
- Apoyo por empresa de soporte especializadas.
- Auditoría forense realizada por empresa externa.
- Póliza de responsabilidad civil ante riesgos cibernéticos suscrita y en vigor.

El completo y detallado implemento de la política de seguridad de la información, junto a las medidas técnicas y de responsabilidad adoptadas, se completaron con un acertado procedimiento, como fue la comunicación de la brecha de seguridad en plazo y forma a la Agencia Española de Protección de Datos, conforme a lo regulado en la normativa en vigor (en este caso, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016).

Todo ello permitió concluir de la existencia de causa de fuerza mayor para el no cumplimiento de los plazos establecidos en las relaciones con la administración pública, basándose sobre la conducta prudente y diligente adoptada por la empresa, demostrada por la diversidad de las medidas de seguridad adoptadas y, por la revisión periódica de las mismas.

Debiéndose considerar un ataque cibernético como previsible, el mismo resulta inevitable ante la complejidad de conocer de manera objetiva las potenciales

capacidades exteriores hacia el sistema de información o telecomunicaciones objetivo, pudiéndose en todo caso mitigar sus efectos en función de las medidas procedimentales y técnicas adoptadas.

- ISO/IEC 27001: Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información. Requisitos.
- ISO/IEC 27002: Tecnología de la Información. Técnicas de Seguridad. Código de Prácticas para los Controles de Seguridad de la Información.
- ISO/IEC 27701: Técnicas de Seguridad. Extensión de las normas ISO/IEC 27001 y 27002 para la Gestión de la Privacidad de la Información. Requisitos y Directrices.

*Ilustración 4. Normas ISO/IEC aplicables en ciberseguridad.*

# 8. Propuesta de implementación de medidas básicas de ciberseguridad

Siendo objetivos secundarios del presente TFM el conocer el qué y el cómo implementar las medidas de ciberseguridad en las redes y sistemas de información de los que se tenga responsabilidad como integrante de un CSEGTIC, o su equivalente en el entorno civil, o como responsable en la administración de un sistema de información o telecomunicaciones, en cuanto a la faceta puramente técnica, se procede a continuación a detallar las medidas básicas necesarias.

## 8.1 Qué implementar

En cuanto al qué implementar, la SAN 900/2022, de 14 de febrero de 2022 detalla que se requiere para considerar que se ha implementado las medidas oportunas en un sistema de información para, al menos, hacer frente a las amenazas de manera diligente. Aun siendo un documento del ámbito de la jurisprudencia, y con el objeto de cumplir el objetivo de conocer que responsabilidades implica la legislación vigente, incluyendo las tecnologías de nueva generación, se empleará como referente en cuanto a qué hay que implementar, sin olvidar los requisitos mínimos de seguridad contemplados en el Real Decreto-ley 7/2022, de 29 de marzo, el Real Decreto 43/2021, de 26 de enero, y el Real Decreto 311/2022, de 3 de mayo, siendo las medidas a adoptar las que a continuación se detallan:

- Constituir un CSEGTIC o equivalente[39].
- Implementar una meticulosa política de seguridad de la información, que contenga al menos:
    - Análisis y gestión de riesgos, debiendo incluir posibles agentes externos a la organización.

[39] En el caso de la SAN 900/2022, de 14 de febrero de 2022, se denomina Grupo de Respuesta ante Incidentes (GRI) p. 4.

  - Gestión de riesgos de terceros o proveedores, destacando la posible dependencia de un único proveedor o procedencia de este en el caso de componentes 5G.
  - Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas, describiendo el modelo y método a emplear.
  - Gestión de personal y profesionalidad, recogidas en normas y procedimientos que indiquen pautas de actuación seguras en el entorno de la información, incluyendo dispositivos móviles, así como los requisitos de contraseña de acceso a los sistemas de información o dispositivos móviles, o de acceso a determinados servicios (como pudiese ser a correo electrónico corporativo, otros servidores de correos o navegación web en entorno exterior a la corporación).
  - Adquisición de productos o servicios de seguridad.
  - Detección y gestión de incidentes.
  - Planes de recuperación y aseguramiento de la continuidad de las operaciones, incluyendo copias de seguridad y periodicidad.
  - Mejora conjunta.
  - Interconexión de sistemas.
  - Registro de la actividad de los usuarios, incluida la navegación web en entornos externos a la organización, siendo el acceso al sistema nominal y con el menor privilegio posible.
- Inventariar los equipos responsabilidad de la organización, debidamente identificados para el nivel de seguridad que se les permite.
- Implementar medidas de seguridad y control de accesos a las instalaciones y las dependencias en las que se encuentren equipos físicos que constituyan la red y el sistema de información de la organización.
- Apoyarse en empresas de soporte especializadas e independientes.
- Actualizar hardware y software de acuerdo con las pautas de seguridad recomendadas por los fabricantes de estos.

- Usar software antivirus de acuerdo con la gestión de riegos, potenciales amenazas y grado de seguridad deseado, preferentemente acreditado y de desarrolladores de prestigio.
- Certificar las medidas de seguridad adoptada, sobre la base de unos estándares preestablecidos y reconocidos (guías de seguridad CCN-STIC o estándares ISO/IEC).
- Suscribir una póliza de responsabilidad civil por riesgos cibernéticos.
- Revisar periódicamente las medidas anteriormente detalladas, adaptando las mejoras y actualizaciones oportunas y en ningún caso, con posterioridad al periodo de validez marcado para cada una de las medidas.

## 8.2 Cómo implementarlo

Se entenderán en este aspecto, el cómo implementarlo, al conjunto de acciones técnicas, principalmente de diseño o programación en los sistemas de información y telecomunicaciones, o de requerimientos de registro de acceso a la infraestructura que aloja los sistemas de gestión de los sistemas de información y telecomunicaciones, que se consideran necesarias para reducir los riesgos en las redes y sistemas de información. La SAN 900/2022, de 14 de febrero se considera de nuevo de utilidad, procediendo de acuerdo con las categorizaciones que a continuación se relacionan, no debiendo olvidar las medidas de protección física que se requiriesen para proteger y registrar el acceso a los componentes de las redes y de los sistemas de información.

### 8.2.1 Común a todos las redes y sistemas de información

El procedimiento de cómo implementarlo debe ser en todo momento metódico y procedimental, preferentemente mediante el seguimiento de unas guías o normas reconocidas y válidas.

Asimismo, se considera de gran validez proceder a documentar meticulosa y detalladamente las acciones y soluciones técnicas que se vayan adoptando a medida que se avanza en la implementación las medidas de ciberseguridad en las redes y en los sistemas de información de la organización.

8.2.2 Redes y sistemas de información de las administraciones públicas y de servicios considerados esenciales por el estado

En este caso no cabe otra posibilidad que ejecutar el mandato legislativo recogido en el Real Decreto-ley 7/2022, de 29 de marzo y en el Real Decreto 311/2022, de 3 de mayo.

Es decir, el cómo implementarlo se basa sobre las ITS, y en las que se identifican guías de seguridad CCN-STIC concretas.

No obstante, además de las recogidas en las ITS indicadas, se pueden completar con el resto de las guías de seguridad CCN-STIC para cumplir es Esquema Nacional de Seguridad (serie 800), recomendado a su vez el seguimiento de las guías de seguridad relativas a la organización y gestión para la seguridad y catalogación de productos.

8.2.3 Redes y sistemas de entidades privadas

Para dicho entorno existen dos posibilidades en cuanto a cómo implementar las medidas de seguridad en las redes y sistemas de información de corporaciones privadas.

Por un lado, aplicar las guías de seguridad CCN-STIC según lo recogido en el subapartado 8.2.1 del presente TFM[40].

Por otro, aplicar normas de estandarización reconocidas, como son las normas ISO/IEC, y recogidas en la SAN 900/2022, de 14 de febrero de 2022, analizada en este TFM y considerada por el autor de este como referente judicial para la implementación de posibles medidas de ciberseguridad en entornos civiles.

[40] Las guías de seguridad CCN-STIC no son en su totalidad accesibles por el público, salvo registro pertinente del usuario interesado en la de acuerdo con los requisitos en vigor que indicase la página web del CCN, como se indicó en el subapartado 6.2.2 del presente TFM.

# 9. Conclusiones

## 9.1 Profesionales

El Máster Universitario en Ciberseguridad y Ciberinteligencia (MUCC) ha cumplimentado la formación de los alumnos, incrementando su concienciación y capacitación en cuanto a la necesidad del implemento de diferentes medidas de seguridad en las redes y en los sistemas de información de los que potencialmente se pudiese ser responsable.

Pero desde el punto de vista legal, se considera que no se ha podido profundizar en su totalidad en el por qué, en el qué y en el cómo se debe de implementar las medidas de seguridad para que sean acordes a la legislación vigente, hecho que puede ser responsabilidad, a su nivel y rol asignado, de cada uno de los actores integrantes de un CSEGTIC o equivalente, de los que en el presente o en un futuro forman/formarán parte alumnos del MUCC.

Habiendo sido formados en cuanto a ser procedimentales y meticulosos en las acciones a adoptar, se considera que el presente TFM completa a qué se enfrentan cuando se les asigna un rol del CSEGTIC, y el qué y el cómo se puede implementar, con el reto que supone en la actualidad la introducción de una nueva generación tecnológica, 5G, en los sistemas de información y telecomunicaciones ya existentes.

Si bien principalmente la legislación de la UE y del Reino de España para la implementación de medidas de ciberseguridad se orientan a redes de las administraciones públicas y aquellas consideradas esenciales para el estado, se considera que su estudio y procedimientos pueden ser referencia en cuanto a un método de cómo realizarlo, a la vez que indican las responsabilidades jurídicas en las que se incurrirían por una inexistente, incorrecta o deliberada mala praxis.

Concretando en el qué implementar y en el cómo proceder en las redes y sistemas de información para reducir sus brechas de seguridad, las guías de seguridad CCN-STIC, principalmente de la serie 800, son documentos esenciales de referencia para cualquier componente del CSEGTIC de una organización (en relación con las administraciones públicas).

Pero dichas guías no son las únicas. La SAN 900/2022, de 14 de febrero de 2022 resulta de gran validez para el entorno civil. La misma se puede tomar como referencia para el caso de una corporación privada, sin obligación de cumplimiento del Esquema Nacional de Seguridad. Siguiendo un procedimiento, apoyado en una concienciación de la necesidad de proteger los activos de la organización, la emisión de una política de seguridad, el seguimiento de una normativa de estandarización reconocida (como son las normas ISO/IEC), la realización de auditorías de seguridad con carácter periódico y participando en la comunidad de conocimiento de ciberseguridad (comunicando cualquier ciberincidente sufrido a una autoridad competente, aún sin obligación de ello), da como resultado el reconocimiento de los esfuerzos realizados y la exoneración de responsabilidad, por imprudencia o por inactividad, ante un ciberataque recibido.

Se puede concluir por tanto, que en la faceta profesional, se ha conseguido saber no sólo por qué se deben implementar medidas de seguridad y la responsabilidad legal asociada a dicha necesidad, sino también el qué y el cómo, mediante el seguimiento de unas guías de seguridad o normativa reconocida al respecto. No obstante, se deberá ser conscientes de los futuros desarrollos de la normativa técnica en cuanto a los procedimientos de seguridad en sistemas 5G que se materialicen, bien por el CCN, bien por entidades de normalización reconocidas.

### 9.2 Propias

El presente TFM ha mejorado el conocimiento propio en cuanto a las responsabilidades legales en que se pueden incurrir cuando se asume un rol dentro de un CSEGTIC.

Con anterioridad, en alguna ocasión se ha sido designado responsable del área de seguridad de la información, aplicando la normativa en vigor del estamento en el que se realizaba la faceta profesional, pero sin haber profundizado en la legislación existente y en la responsabilidad que la misma asigna. Esta normativa de la organización se consideraba como una adaptación de las guías de

seguridad CCN-STIC vigentes al entorno asignado. Es decir, se era conocedor del quién, el qué, y el cómo, pero se carecería de la visión del por qué, salvo por la responsabilidad dentro de la organización, quedando la misma incompleta en cuanto a responsabilidades legales si las hubiese habido (incluido el desconocimiento de la existencia de un Esquema Nacional de Seguridad como referencia y objetivo a cumplir).

Pero no sólo eso. En conversaciones a título particular o en foros con profesionales del campo de las TIC, siempre se han elogiado el punto de referencia que supone las guías de seguridad CCN-STIC para este campo.

Sin embargo, la realización del presente TFM, y gracias a las investigaciones y a la documentación analizada, ha resultado revelador, sobre todo, en relación con la aplicación de procedimientos en el entorno civil no basados en las guías de seguridad CCN-STIC, y basados en otras normativas de estandarización, como son las normas ISO/EIC, válidas en causas judiciales.

La SAN 900/2022, de 14 de febrero, se considera un referente válido (y no sólo en el aspecto jurisprudencial) para la implementación de las medidas de ciberseguridad en el ámbito privado. Esta SAN transmite la motivación en cuanto a que la diligencia y la proactividad en la implementación de medidas de ciberdefensa, junto con un seguimiento meticuloso de unas guías o normas reguladas y reconocidas y, siendo conscientes de que la seguridad total no existe (sobre la base de contractar un seguro de responsabilidad civil ante riesgos cibernéticos) conduce a la conclusión de que la misma, debería ser incluida como referente en las políticas de seguridad de las TIC de las empresas.

### 9.3 Del TFM

El objeto del TFM se considera parcialmente alcanzado, pudiendo ser el mismo la base de un futuro estudio que lo complete.

Se han dado los primeros pasos para la transposición de la legislación europea en la legislación de España en cuanto a la implementación de medidas de seguridad en las redes y sistemas de información de quinta generación,

quedando pendiente a fecha de conclusión del presente estudio la publicación del Esquema Nacional de Seguridad de redes y servicios 5G.

El mencionado esquema constituirá la base necesaria para el desarrollo o actualización de las guías de seguridad o normativa que desarrollen las técnicas y procedimientos a aplicar para el cumplimiento de este. Por ello, una vez aprobado, se deberá hacer un seguimiento de las ITS que se adopten, actualicen o deroguen, así como las guías de seguridad del CCN-STIC afectadas, y todo ello con la suficiente habilidad para poder integrar simultáneamente sistemas 5G con sistemas con tecnologías de generaciones anteriores, sin que suponga esta integración posibles brechas de seguridad en las redes y sistemas de las administraciones públicas y sectores esenciales para el estado.

A su vez, y en cuanto a redes y sistemas de información del entorno privado, se deberá analizar la validez de normas de estandarización en vigor en la actualidad, pudiendo ser acotadas en un principio a las normas ISO/IEC referenciadas en la SAN 900/2022 de 14 de marzo de 2022, analizada en este TFM, y considerando el reto anteriormente mencionado, la convivencia de sistemas y redes 5G con sistemas y redes de anteriores generaciones.

Y no sólo por ello se considera que el objeto del TFM ha sido parcialmente conseguido, sino también, porque no es posible en el dominio cibernético alcanzar la seguridad total, sólo es posible mitigar los efectos ante potenciales riesgos y amenazas, mitigación en la que se espera haber podido colaborar con el presente TFM.

# Bibliografía

Unión Europea. Versión Consolidada del Tratado de Funcionamiento de la Unión Europea. *Diario Oficial de la Unión Europea*, 30 de marzo de 2010, núm. C 83, p. 49.

Unión Europea, 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 de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 ("Reglamento sobre la Ciberseguridad"), *Diario Oficial de la Unión Europea,* 7 de junio de 2019, núm. L 151, p.15.

Unión Europea, Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información en la Unión, *Diario Oficial de la Unión Europea*, 10 de junio de 2016, núm. L 194, p. 1.

España. Real Decreto-ley 12/2018, de 7 de septiembre de seguridad en redes y sistemas de información. *Boletín Oficial del Estado*, 8 de septiembre de 2018, núm. 218, p. 87675.

España. 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. *Boletín Oficial del Estado*, 30 de marzo de 2022, núm. 76, p. 41546.

España. 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*, 29 de enero de 2010, núm. 25. Texto consolidado, última modificación 4 de noviembre de 2015 [en línea]. Derogado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. [Consulta: 26 de abril de 2022]. Disponible en: https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf

España. Real Decreto 951/2015, de 23 de octubre, de modificación del 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*, 4 de noviembre de 2015, núm. 264, p. 104226. Derogado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

España. 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*, 28 de enero de 2021, núm. 24, p. 8187.

España. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado*, 31 de diciembre de 2021, núm. 314, p. 167795.

España. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 4 de mayo de 2022, núm. 106, p. 61715.

Unión Europea. Recomendación (UE) 2019/534 de la Comisión de 26 de marzo de 2019, Ciberseguridad de las redes 5G, *Diario Oficial de la Unión Europea*, 29 de marzo de 2019, núm. L 88, p. 42.

España. Disposición 10108. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. *Boletín Oficial del Estado*, 2 de noviembre de 2016, núm. 265, p. 76363.

España. Disposición 10109. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, 2 de noviembre de 2016, núm. 265, p. 76365.

España. Disposición 4573. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica

de Seguridad de Auditoría de la Seguridad de los Sistemas de Información. *Boletín Oficial del Estado*, 3 de abril de 2018, núm. 81, p. 35268.

España. Disposición 5370. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. *Boletín Oficial del Estado*, 19 de abril de 2018, núm. 95, p. 40556.

Sentencia del Tribunal Supremo 543/2022 – ECLI:ES:TS:2022:543 [en línea]. 15 de febrero de 2022. [Consulta 14 de mayo de 2022]. Disponible en: https://www.poderjudicial.es/search/AN/openDocument/bbb5f3256ed28cb7/20220225

Sentencia de la Audiencia Nacional 900/2022 – ECLI:ES:AN:2022:900 [en línea]. 14 de marzo de 2022. [Consulta 14 de mayo de 2022]. Disponible en: https://www.poderjudicial.es/search/AN/openDocument/effb3d7c20da99f4/20220324

Unión Europea. "Aplicar la legislación de la UE". En: *ec.europa.eu Legislación Proceso legislativo* [en línea]. [Consulta: 6 de marzo de 2022]. Disponible en: https://ec.europa.eu/info/law/law-making-process/applying-eu-law_es

Unión Europea. Comunicación Conjunta (JOIN 2013) de 7 de febrero de 2013 al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *"Estrategia de ciberseguridad de la Unión Europea: Un Ciberespacio abierto, protegido y seguro".* [Consulta 6 de marzo de 2022]. Disponible en: https://data.consilium.europa.eu/doc/document/ST%206225%202013%20INIT/es/pdf

Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *"Despliegue seguro de la 5G en la UE – Aplicación de la caja de herramientas de la UE"*. COM (2020) 50 final. 29 de enero de 2020 [consulta: 5 de mayo de 2022]. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0050&from=ES

Comisión Europea, *"Propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad de las redes y por la que se deroga la Directiva (UE) 2016/1148"* [en línea]. COM (2020) 823 final 2020/0359 (COD). 16 de diciembre de 2022 [consulta: 19 de abril de 2022]. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0012.02/DOC_1&format=PDF

NATO, "Brussels Summit Communiqué", 14 de junio de 2021 (actualizada el 8 de abril de 2022) [en línea]. [Consulta: 28 de abril de 2022]. Disponible en: https://www.nato.int/cps/en/natohq/news_185000.htm

NIS COOPERATION GROUP, *"Cybersecurity of 5G networks EU Toolbox of risk mitigating measures"* [en línea]. CG Publication. Enero de 2020 [consulta: 5 de mayo de 2022]. Disponible en: https://www.enisa.europa.eu/news/enisa-news/5g

CCN-CERT. *Guías CCN-STIC.* [En línea]. [Consulta 11 de mayo de 2022]. Disponible en: https://www.ccn-cert.cni.es/guias.html

AENOR. *Buscador de normas*. [En línea]. [Consulta 25 de mayo de 2002]. Disponible en: https://tienda.aenor.com/normas/buscador-de-normas

ALONSO LECUIT, Javier. "Directiva NIS 2: valoraciones y posiciones desde el sector privado". En *Documentos de Trabajo del Real Instituto Elcano* [en línea]. Núm. 6/2021. 20 de abril de 2021 [consulta: 12 de abril de 2022]. Disponible en:

https://media.realinstitutoelcano.org/wp-content/uploads/2021/04/dt6-2021-alonsolecuit-directiva-nis2-valoraciones-y-posiciones-desde-sector-privado.pdf

ARTEAGA, Félix. "La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0". En *Análisis del Real Instituto Elcano (ARI)* [en línea]. Núm. 19/2021. 9 de febrero de 2021 [consulta: 12 de abril de 2022]. Disponible en: https://www.realinstitutoelcano.org/analisis/la-evaluacion-y-la-revision-de-la-directiva-nis-la-directiva-nis-2-0/

GARRÓS FONT, Inma. "Avances y retos de la Agencia Europea para la Ciberseguridad. El nuevo marco de la certificación". En *Encuentros Multidisciplinares Universidad Autónoma de Madrid* [en línea]. Núm. 62, mayo-agosto 2019 [consulta: 19 de abril de 2022]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688480/EM_62_9.pdf?sequence=1&isAllowed=y

MANSILLA MORALES, José Manuel. "Caminando hacia el futuro. El ciberespacio y el educador social". En: *Educación, sociedad y tecnología.* [en línea]. Madrid: Editorial Universitaria Ramón Areces, p 169 [consulta 18 de mayo de 2022]. Disponible en: https://books.google.be/books?id=m3SUDAAAQBAJ&pg=PA169&dq=fecha+neuromante+william+gibson&hl=es&sa=X&ved=2ahUKEwjh-Oz4yen3AhVDQRoKHRbLCEYQ6AF6BAgLEAI#v=onepage&q=fecha%20neuromante%20william%20gibson&f=false

MANSO CHICOTE, Carlos, 2022. Huawei pide una regulación «objetiva y proporcional» para la seguridad del 5G en España. *ABC.* 20 de mayo de 2022 [en línea]. [Consulta: 20 de mayo de 2022]. Disponible en: https://www.abc.es/economia/abci-huawei-pide-regulacion-objetiva-y-proporcional-para-ciberseguridad-espana-202205200808_noticia.html

MARCO CLEMENT, Isabel. "La protección de las infraestructuras críticas en la UE: ¿Ciberseguridad al rescate? Tutora: Susana de Tomás Morales. Trabajo Fin de Grado Derecho Internacional Público. Universidad Pontificia Comillas Madrid. Abril 2017 [consulta 6 de marzo de 2022]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/17923/TFG

%20DERECHO%20-%20Isabel%20Marco%20Clement.pdf?sequence=1&isAllowed=y

MORET MILLÁS, Vicente. URIBE OTALORA, Ainhoa. "La Unión Europea ante el reto de la ciberseguridad: la futura Directiva NIS". En: *ieee.es Documentos de Opinión* [en línea]. Núm. 122/2014. 28 de octubre de 2014 [consulta: 6 de marzo de 2022]. Disponible en:

https://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO122-2014_Directiva_NIS_MoretxUribe.pdf

MORET MILLÁS, Vicente. "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español". En *ieee.es Documentos de Opinión* [en línea]. Núm. 21/2017. 3 de marzo de 2017 [consulta: 6 de marzo de 2022]. Disponible en:

https://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO21-2017_DirectivaNIS_VicenteMoret.pdf

ROLDÁN BENHAYÓN, Patricia. "Análisis de los aspectos legales del ciber-espacio, las principales amenazas y el marco jurídico de la ciberseguridad en la Unión Europea". En: Cuadernos de la Escuela Diplomática número 59 "Selección de memorias del Máster de Diplomacia y Relaciones Internacionales 2015-2016". Ministerio de Asuntos Exteriores y de Cooperación, pp. 313-398 [consulta: 12 de abril de 2022]. ISSN: 0464-3755. Disponible en:

https://www.exteriores.gob.es/es/Ministerio/EscuelaDiplomatica/Documents/documentosBiblioteca/CUADERNOS/59.pdf

RODRÍGUEZ CONDE, Luis. "Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013". Director: Antonio José Segovia Henares. Trabajo Fin de Máster Interuniversitario en Seguridad de las Tecnologías de la Información y Comunicaciones (MISTIC). Universitat Rovira i Virgili. Universitat Oberta de Catalunya. Universitat Autónoma de Barcelona. Junio de 2017 [consulta 6 de marzo de 2022]. Disponible en:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64545/1/liziyoTFM0617-Resumen%20Ejecutivo-Memoria.pdf

*"La Transposición de la Normativa NIS al Ordenamiento Jurídico Español: Una Perspectiva empresarial".* Fundación ESYS. Septiembre de 2017 [consulta 6 de marzo de 2022]. Disponible en:

https://fundacionesys.com/en/system/files/documentos/ESTUDIO%20NIS%2BANEXOS.pdf

*"¿En qué consiste la Directiva NIS?"*. Centro Universitario de Tecnología y Arte Digital (U-TAD). 1 de octubre de 2018 [consulta 11 de abril de 2022]. Disponible en: https://u-tad.com/en-que-consiste-la-directiva-nis

PÁGINA INTENCIONADAMENTE EN BLANCO

# Anexo: Objetivos de Desarrollo Sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

| Objetivos de Desarrollo Sostenibles | Alto | Medio | Bajo | No Procede |
|---|---|---|---|---|
| ODS 1. **Fin de la pobreza.** | | | X | |
| ODS 2. **Hambre cero.** | | | X | |
| ODS 3. **Salud y bienestar.** | X | | | |
| ODS 4. **Educación de calidad.** | X | | | |
| ODS 5. **Igualdad de género.** | | | X | |
| ODS 6. **Agua limpia y saneamiento.** | | X | | |
| ODS 7. **Energía asequible y no contaminante.** | | | X | |
| ODS 8. **Trabajo decente y crecimiento económico.** | X | | | |
| ODS 9. **Industria, innovación e infraestructuras.** | X | | | |
| ODS 10. **Reducción de las desigualdades**. | | | X | |
| ODS 11. **Ciudades y comunidades sostenibles**. | | X | | |
| ODS 12. **Producción y consumo responsables.** | | X | | |
| ODS 13. **Acción por el clima.** | | | X | |
| ODS 14. **Vida submarina.** | | | X | |
| ODS 15. **Vida de ecosistemas terrestres.** | | | X | |
| ODS 16. **Paz, justicia e instituciones sólidas.** | X | | | |
| ODS 17. **Alianzas para lograr objetivos.** | X | | | |

Reflexión sobre la relación del TFM con los ODS y con el/los ODS más relacionados.

El presente TFM tiene una relación con los ODS relacionados de acuerdo con lo que sobre los mismos recojan la legislación de la UE y del Reino de España en la implantación de las medidas de ciberseguridad en redes 5G en sus respectivos ámbitos legislativos.

Lógicamente, tendrá mayor relación en aquellos campos que posibiliten un mayor uso de las Tecnologías de la Información y de las Comunicaciones (TIC),

como son, y recientemente demostrado como consecuencia de la pandemia del COVID-19 de 2020, el de la enseñanza, la telemedicina, etc., facilitando las medidas de teletrabajo, sobre la base del grado de seguridad a implementar que se considere para proteger la información y mitigar los efectos derivados que pudiese suponer la degradación de las redes y sistemas de información que los sustentan.

En cuanto al sector económico, se considera que el mismo se encuentra sustentado en la seguridad y fiabilidad que proporcionen las medidas de ciberseguridad en las TIC, redundando en instituciones más sólidas sobre la base de un principio de la ciberseguridad: dado que la seguridad total no existe, la necesidad de compartir las buenas prácticas enriquecerá el ambiente colaborativo en beneficio del objetivo; siendo por tanto de elevada importancia el saber compaginar estos objetivos de desarrollo sostenible con las capacidades y necesidades existentes para lograr la estabilidad y protección general que requiere el normal funcionamiento de un estado de derecho, sus instituciones, sus sistemas sociales y el entorno natural y humano que encuadra.

Asimismo, repercutirá en el implemento de mejores sistemas de gestión de suministro y recursos, principalmente en aquellas áreas geográficas con elevada conectividad, no sólo referida a las TIC, sino también de mayor conectividad gracias a las infraestructuras, generalmente coincidentes con las de mayor densidad de población asentada o en tránsito.

En cuanto a otras áreas, puede facilitar y mejorar la gestión en cuanto a conservación del medio ambiente, producción y gestión de recursos propiamente dichos, e igualdad de género, siempre y cuando el implemento y desarrollo de las medidas de ciberseguridad en el campo de las TIC pudiesen ser considerados específicos para los fines indicados, no únicamente por y para el empleo de acceso a los sistemas de información, ya universalizado mediante el acceso a Internet, o por las necesidades de conectividad que proporcionan las actuales redes de telecomunicaciones de manera más segura.


**ETS Enginyeria Informàtica**
Camí de Vera, s/n. 46022. València
**T** +34 963 877 210
**F** +34 963 877 219
etsinf@upvnet.upv.es - www.inf.upv.es

No obstante, se considera que se potenciarían estos ODS, sobre la base del presente TFM, en la misma medida en que se potenciasen los accesos y servicios de las infraestructuras TIC del sector económico primario.

Los avances de las TIC y el incremento y mejoras de sus medidas de seguridad han solido ser como consecuencia del incremento de necesidades de capacidades por los otros sectores económicos, no habiendo tenido gran penetración o repercusión en el sector primario, generalmente por los costes económicos que supone el acceso a las TIC frente a la rentabilidad de este sector por entidades mediadas o pequeñas, e incluso, generalmente de carácter familiar, sin olvidar aquellos casos en que este sector primario fuese la única capacidad de subsistencia del individuo, familia, comunidad o sociedad, por lo que potenciar estas medidas en el sector primario, como base del obligado mantenimiento de los recursos de la naturales para sustentar su productividad, influenciarían en la mejora del resto de ODS no directamente relacionados con la naturaleza.

PÁGINA INTENCIONADAMENTE EN BLANCO