FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2022 / 2023

TRABAJO DE FIN DE MÁSTER

DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

CIBERSEGURIDAD DE LA CADENA DE SUMINISTRO DE LAS TIC: ANÁLISIS DEL MARCO JURÍDICO DE LA UNIÓN EUROPEA

CYBERSECURITY OF ICT SUPPLY CHAIN: ANALYSIS OF THE LEGAL FRAMEWORK OF THE EUROPEAN UNION

AUTOR: ARMANDO JOSUE VEGA ESPINOZA

TUTORA: DRA. Dª ELENA FÁTIMA PÉREZ CARRILLO

AGRADECIMIENTOS:

En primer lugar, agradezco a la Fundación Carolina y a la Universidad de León por haberme permitido cursar el Máster en Derecho la Ciberseguridad y Entorno Digital.

Le agradezco profundamente a mi tutora, por su guía, palabras de ánimo y dedicación brindada para la elaboración de este Trabajo de Fin de Máster.

Por último, quiero agradecer a mis padres, quienes a pesar de la distancia no han dejado de estar presentes, y a mis amigas, Agostina y Wendy por todo su apoyo.

INDICE

ABREVIATURAS:

AENOR: Asociación Española de Normalización y Certificación

CCN: Centro Criptológico Nacional

CESE: Comité Económico y Social Europeo

DNIS 1: Directiva (UE) 2016/1148

DNIS 2: Directiva (UE) 2022/2555

EE. UU: Estados Unidos de Norteamérica

ENISA: Agencia de la Unión Europea para la Ciberseguridad

ENS: Esquema Nacional de Seguridad

IAAS: Infraestructura como servicio

ISO: Organización internacional de estandarización

NAAS: Red como servicio

NIST: National Institute of Standards and Technology

PAAS: Plataforma como servicio

PYME: Microempresa, pequeña y medianas empresa

RGPD: Reglamento general de protección de datos

SAAS: Software como servicio

SGSI: Sistema de Gestión de Seguridad de la Información

TIC: Tecnologías de la información y comunicación

UE: Unión Europea

UNE: Unidad de Normalización Española

RESUMEN

El presente trabajo académico consiste en brindar un acercamiento a la regulación de la ciberseguridad en la cadena de suministro de las tecnologías de la información y comunicación en el marco jurídico de la Unión Europea. Así mismo, se presenta su efecto en las empresas del sector privado y principales obligaciones de gobernanza y gestión de riesgo que estas deben de cumplir.

Adicionalmente, se exploran los roles y responsabilidades de la ciberseguridad, que se deben de considerar en una organización, para afrontar los retos de dicha cadena de suministro, así como las acciones y procesos que se deben de tomar en cuenta en la elaboración de una política interna que contribuya a su supervisión.

Palabras clase: Cadena de suministro, Gobernanza, Gestión de Riesgos, Ciberseguridad, Seguridad de las redes y sistemas de información, Política, Transformación digital, Entidades reguladas; Empresas, Sector privado, Estándares.

ABSTRACT

This academic dissertation aims to provide an approach to the regulation of cybersecurity of the ICT supply chain in the legal framework of the European Union. It also presents its effect on private sector companies and the main governance and risk management obligations they must fulfill.

Additionally, it explores the roles and responsibilities of cybersecurity, that an organization must consider facing the challenges of ICT supply chain, along with the actions and processes that must be taken into account in the development of an internal policy that contributes to its supervision.

Keywords: Supply Chain, Governance, Risk Management, Cybersecurity, Security of Network and Information Systems, Policy, Digital Transformation, Regulated Entities, Companies, Private Sector, Standards.

OBJETO DEL TRABAJO.

El presente trabajo académico tiene por objeto principal analizar el marco jurídico de la Unión Europea (en delante, UE) relacionado con la ciberseguridad de la cadena de suministro de las tecnologías de la información y comunicación (en delante, TIC), así como las obligaciones que impone a las empresas del sector privado la nueva Directiva (UE) 2022/2555 de seguridad de las redes y sistemas de información (en delante, DNIS 2) en esta área específica, incluyendo algunas consideraciones de Derecho comparado y normas internacionales de estandarización.

Para este propósito, la primera parte estará dedicada a introducir una noción a la transformación digital empresarial impulsada por la UE, los riesgos intrínsecos que representa, el origen de una nueva cadena de suministro junto con la importancia de brindarle una especial atención. En este panorama la ciberseguridad se erige como principal aliada para una transformación digital segura.

La segunda parte se enfoca en realizar un análisis de la DNIS 2, incluyendo una breve comparación con su antecesora, y sus efectos regulatorios sobre la cadena de suministro de las TIC. También se presta atención a la Propuesta del Reglamento de Ciberresiliencia. Además, se brinda una aproximación a la gobernanza de la ciberseguridad con un alcance a la cadena de suministro de las TIC, sin dejar de lado ciertas previsiones para incorporar en una política de proveedores que permita reforzar la ciberseguridad en dicha área.

METODOLOGÍA

En el desarrollo de las materias cursadas a lo largo del Máster, llamó mi atención como el Derecho y la Ciberseguridad se encuentran en el área mercantil, así como su efecto en el sector privado, dando génesis a un nuevo cumplimiento regulatorio en materia de ciberseguridad que debe de ser considerado por los órganos de administración de las sociedades mercantiles.

Posteriormente, en seguimiento de las actualizaciones legislativas del marco jurídico de ciberseguridad de la UE, se destacó la aprobación de la DNIS 2 y su regulación sobre la cadena de suministro de las TIC. Así como las nuevas obligaciones y responsabilidades derivadas de esta a las empresas que desarrollen actividades económicas en el mercado europeo.

Para la elaboración del presente trabajo académico, se empleó un método de investigación cualitativo deductivo. Por ello, su estructura consta de dos capítulos centrales que abordan diferentes aspectos de la ciberseguridad en la cadena de suministro de las TIC.

El primer capítulo se enfoca en proporcionar una descripción de la génesis de la cadena de suministro de las TIC, incluyendo sus riesgos intrínsecos y la importancia de brindarle una especial atención. En el segundo capítulo, se proporciona un análisis al marco jurídico de la UE que regula la ciberseguridad en dicha cadena de suministro. Asi mismo, incluye una aproximación a la gobernanza, y elaboración de una política de ciberseguridad de la relación con proveedores con un alcance a la cadena de suministro de las TIC.

En este sentido, el resultado de esta investigación académica se ha desarrollado en base al análisis y consulta de una variedad de fuentes. En primera instancia, se consultaron una variedad de libros, informes institucionales, artículos de una variedad de autores y documentos de buenas prácticas relacionadas al ámbito de investigación. En segunda instancia, se utilizaron fuentes legislativas, estrategias supranacionales, normas internacionales de estandarización y marcos de trabajo. Conjuntamente a todo lo anterior, para el desarrollo de este trabajo académico, ha sido de gran importancia el apoyo, guía y espacio de intercambio de ideas brindado por la tutora.

CAPÍTULO PRIMERO: INTRODUCCIÓN A LA CIBERSEGURIDAD, LA ALIADA DE LA TRANSFORMACIÓN DIGITAL DEL SECTOR PRIVADO.

1) La transformación digital como riesgo empresarial:

En los últimos años, se ha evidenciado como la tecnología tiene la capacidad de optimizar las actividades empresariales, haciéndolas más competentes, organizadas y globalizadas. Esto se debe a la implementación de las TIC[1] en sus operaciones, lo cual han contribuido a la «automatización, interconexión computacional y a los procesos en línea»[2].

La transformación digital de las empresas ha adquirido gran importancia en el desarrollo económico y comercial de un país o región. De modo que, en la actualidad es fundamental para la elaboración de políticas públicas y estratégicas, en todos los países y zonas supranacionales, verbigracia las establecidas por la Unión Europea.

La UE mediante la Decisión (UE) 2022/2481 del 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030, establece como una de las metas digitales, que el 75% de las empresas europeas como mínimo, hayan adoptado dentro de sus operaciones, herramientas tecnológicas que provean un acercamiento a la transformación digital, tales como: i) servicios de computación en nube; ii) macrodatos e iii) inteligencia artificial. [3]

[1] La Unión Europea define a las TIC como "un término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones" COMISION DE LAS COMUNIDADES EUROPEAS. *Comunicación de la comisión al consejo y al parlamento europeo relativa a las tecnologías de la información y de la comunicación en el ámbito del desarrollo. El papel de las TIC en la política comunitaria de desarrollo*. 2021. [En línea] [Fecha de consulta: 16/05/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52001DC0770&qid=1684593170662]

[2] SANTIAGO, Enrique y ALLENDE, Jesús. Riesgos de ciberseguridad en las Empresas. *Revista Tecnologí@ y desarrollo*. [En línea]. 2017, vol. 15, P. 1-33. [En línea]. [Fecha de consulta: 14/06/2023]. [Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174/964]

[3] Véase el artículo 4 apartado 3 inciso "a". Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030 (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 323 de 19.12.2022, p. 4-26. [Fecha de consulta:14/06/2023. [Disponible en: https://eur-lex.europa.eu/eli/dec/2022/2481/oj]

La transformación digital[4], no se puede realizar en el seno de una sola empresa, por el contrario, apunta a dependencias entre proveedores de productos y servicios TIC, sus clientes e incluso con sus competidores, por lo tanto, esta dependencia no está exenta de riesgos.

Debido al contexto de hiperconectividad en el que las empresas ejercen su actividad económica, es posible afirmar que, si bien la nueva era de la digitalización brinda grandes oportunidades, también cambia la naturaleza y la dimensión de los ciberriesgos. El software, hardware o los servicios TIC propiamente dichos están sometidos a riesgos, estando entre ellos los ciberataques[5].

Por lo tanto, se debe prestar especial atención a las compañías del sector privado que brinden servicios fundamentales a la sociedad, en razón de la implementación de medidas tecnológicas que optimicen el suministro de servicios, tales como agua o de energía, la distribución de alimentos o medicamentos, entre otros. Debido a los ciberriesgos inherentes a la transformación digital que han de ser atendidos para evitar el desabastecimiento o interrupción de servicios[6].

En el contexto de ciberseguridad, se entiende por ciberriesgo[7] como la probabilidad de que se materialice un incidente que perjudique los activos digitales de una organización y pueda producir un impacto. Con el objetivo de no abusar de la palabra ciberriesgo, en el desarrollo del presente trabajo también se podrá referir a este término como riesgo.

---

[4]Véase el considerando "A", el cual especifica la prioridad de la transformación digital para el espacio europeo, asi como las ciberamenazas que representa. PARLAMENTO EUROPEO. *Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital*. [En línea]. [Fecha de consulta: 18/06/2023] [Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_ES.html]

[5]THE HAGUE CENTRE FOR STRATEGIC STUDIES. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.* [En Linea]. 1ª. Belgica. The European Economic and Social Committee. 2018. P.7. [Fecha de consulta: 18/06/2023]. [Disponible en: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf]

[6]FUERTES. Mercedes. Soberanía Digital Europea. *El Cronista del Estado Social y Democrático de Derecho.* [En línea]. 2020. N° 90-91. Editorial Iustel. PP. 56-71. [Fecha de consulta: 13/07/2023]. [Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7666272]

[7]SEVILLANO, Fernando y BELTRAN, Marta. *Dirección de seguridad y gestión del ciberriesgo*. [En línea]. 1ª, Madrid, RA-MA Editorial. 2020. P. 34. [Fecha de consulta: 18/06/2023] [Disponible en: https://elibronet.unileon.idm.oclc.org/es/ereader/unileon/222733?page=34]

2) Hacia una ciberseguridad empresarial:

En virtud de los riesgos emanados de la transformación digital, se plantea la necesidad de brindar nuevas respuestas que logren mitigarlos. En este contexto surge la ciberseguridad, término que resulta complejo de definir debido a su amplia variedad de fuentes. A los efectos de este trabajo académico, se utiliza la definición brindada por la UE.

La UE define "ciberseguridad" en el artículo 2, del Reglamento (UE) 2019/881 de 17 de abril de 2019 relativo a ENISA, (en delante, Reglamento (UE) 2019/881), el cual expone la siguiente definición: *«Ciberseguridad: todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas»*[8].

En esta definición, las redes y sistemas de información ocupan un lugar preeminente, en razón de ser el objetivo de los ciberataques, pues son el medio de acceso para alcanzar los activos de las empresas, tales como información confidencial, información financiera, datos personales de clientes o trabajadores y propiedad intelectual.

En suma, la ciberseguridad tiene como principal finalidad, la protección de los activos y los sistemas más importantes para una organización. Para la ejecución de este cometido, se basa en tres principios fundamentales[9]:

- Confidencialidad: Que la información solo sea accesible para los usuarios autorizados.
- Disponibilidad: Que la información almacenada se encuentre disponible en cualquier momento para el usuario autorizado.
- Integridad: Que la información preserve su exactitud, de modo que no pueda ser editada, manipulada ni alterada por usuarios no autorizados.

[8] 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») (Texto pertinente a efectos del EEE). L 151 de 7.6.2019, p. 15/69. [En línea]. [Fecha de consulta: 20/06/2023]. [Disponible en: http://data.europa.eu/eli/reg/2019/881/oj]

[9] ORTEGA CANDEL, José. *Ciberseguridad. Manual práctico*. 1ª. Santiago de Compostela. Ediciones Parainfo, SA. 2021. P. 4

Si algo tienen en común los principios previamente expuestos, es que la persona que acceda a la información debe de estar autorizada, lo cual debe de ser verificado tomando en consideración los siguientes criterios adicionales[10]:

- Autenticidad: Que la identidad del usuario que acceda a la información almacenada pueda ser confirmada.
- Trazabilidad: Consiste en conocer, quien, donde y como accedió a la información y si se ha modificado la información almacenada.

Cabe destacar que una correcta implementación de la ciberseguridad en una organización debe de combinar de modo equilibrado, factores de seguridad, privacidad y de usabilidad[11].

Como herramientas para la ejecución de los principios y criterios previamente mencionados, surgen los marcos de estandarización internacional, las cuales se desarrollan en el siguiente apartado.

2.1) Marcos de estandarización internacional:

Conocer las medidas de ciberseguridad adecuadas e implementarlas en las operaciones empresariales puede ser una tarea compleja, tomando en consideración que el nivel de dificultad está relacionado con el tamaño de la empresa y actividad económica que desempeña.

Como una solución a la problemática anterior, son de gran utilidad las normas internacionales de estandarización (en delante, estándares) debido a que proporcionan acciones y procesos a seguir para superar la adversidad de la implementación de medidas encaminadas a la necesaria seguridad informática.

Dichos estándares son elaborados por la organización internacional de estandarización y la comisión electrónica internacional, denominadas como ISO/IEC por sus

[10] Idem.
[11]ARROYO GUARDEÑO. David, GAYOSO MARTÍNEZ. Víctor y HERNÁNDEZ ENCINAS. Luis. ¿Qué sabemos de? *Ciberseguridad.* [En línea]. 1ª. Madrid. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. P. 13. [Fecha de consulta: 07/06/2023] [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/172144]

siglas en inglés, quienes en conjunto conforman un sistema especializado para la publicación de estándares internacionales[12] relacionados a las tecnologías de la información.

Estos estándares son de carácter privado, técnico y de adhesión voluntaria para las empresas u organizaciones que las deseen implementar, no obstante, para poder demostrar la adhesión a las orientaciones y medidas establecidas, se deben de someter a una auditoria, la cual, en caso de ser satisfactoria, certifica el debido cumplimiento.

La certificación del cumplimiento mencionado en el párrafo anterior se encuentra sujeto al tipo de estándar implementado. En este orden de ideas, aquellos que pueden ser certificables son las de rango principal, caso contrario de los que emerjan de estas como extensiones y guías de implementación.

En el ámbito de la ciberseguridad, los estándares que destacan por proporcionar directrices que brindan protección a las redes y sistemas de información, son las siguientes:

- ISO/IEC 27000: 2018: Marca el inicio del compendio de estándares dirigidos a la implementación de un sistema de gestión de seguridad de la información (en delante, SGSI) y proporciona una visión general, los términos y definiciones más comunes que se utilizaran en los demás estándares que tengan una relación con la seguridad de la información[13].
- ISO/IEC 27001: 2022: Es un estándar diseñado para la implementación de un SGSI, el cual tiene como principal objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información por medio de la gestión de riesgos pertenecientes a la organización que pretende adherirse. Un SGSI es un conjunto de procedimientos que posibilitan el establecimiento, implementación, mantenimiento y mejora constante de la protección de la información. Estas acciones se basan en la evaluación de los riesgos a los que una organización está expuesta[14]. Este estándar

[12]GOMEZ HERVAS. Nuria del Carmen. *Normativa de ciberseguridad.* [En línea]. 1ª. Madrid. Ra-Ma editorial. 2021. P. 155. [Fecha de consulta: 16/06/2023]. [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/222663?page=4]

[13]ASOCIACION ESPAÑOLA DE NORMALIZACION. T*ecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). visión de conjunto y vocabulario.* UNE-EN ISO/IEC 27000. Madrid: UNE. 2021.

[14]GÓMEZ FERNÁNDEZ, Luis y FERNÁNDEZ RIVERO, Pedro. *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad*. [En línea]. 1. Madrid. AENOR -

consta de 93 controles que deben de ser aplicados en función de brindar seguridad a la información de las organizaciones. [15]

- ISO/IEC 27002:2022: Este estándar se encuentra relacionado con el anterior, y consiste en una guía de implementación de controles de seguridad que se pueden aplicar para fortalecer la implementación del SGSI.[16]
- ISO/IEC 27005:2022: La funcionalidad de este estándar consiste es proporcionar directrices para la implementación de los requisitos de la ISO/IEC 27001 sobre la gestión de riesgo del SGSI.[17]
- ISO 31000:2018: Este estándar brinda un conjunto acciones y procesos para efectuar una adecuada gestión del riesgo de las organizaciones. Cabe destacar que su aplicabilidad no se encuentra restringido al ámbito de seguridad de la información, sino que es de aplicabilidad amplia para otros sectores[18]. Es importante mencionar que su implementación no es certificable.

2.2) Efectos jurídicos de los estándares internacionales:

En el ámbito jurídico, estos estándares son denominadas como *"SOFT LAW[19]"*. La Real Academia Española las define como «*Conjunto de normas o reglamentaciones no vigentes que pueden ser consideradas por los operadores jurídicos en materias de carácter preferentemente dispositivo y que incluye recomendaciones (...)*».

En el contexto de la ciberseguridad, dichos estándares han tenido gran relevancia en los últimos años, debido a la poca efectividad que tiene que una ley regule bajo un método

Asociación Española de Normalización y Certificación. 2018. P. 13 [Fecha de consulta: 08/07/2023]. [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/53624?page=14]

[15]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.* UNE-ISO/IEC 27001. Madrid: UNE. 2023

[16]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Seguridad de la información, ciberseguridad y protección de la* privacidad. Control de la seguridad de la información UNE-EN ISO/IEC 27002. Madrid. UNE:2023.

[17]INTERNATIONAL STANDARD. *Information security, cybersecurity, and privacy protection – Guidance on managing information security risk*. ISO/IEC 27005. Switzerland. ISO/IEC 2022.

[18]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Gestión del riesgo. Directrices.* UNE ISO 31000. Madrid. UNE: 2018.

[19]REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*. [En línea]. [Fecha de la consulta: 19/06/2023]. [Disponible en: https://dpej.rae.es/lema/soft-law]

de números clausus las medidas detalladas de seguridad informática y de las redes que debe implementar una organización[20]. Debido a la versatilidad y constante cambio de las TIC.

Por su parte, la UE, las incorpora al Derecho Europeo por medio del REGLAMENTO (UE) No 1025/2012 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de octubre de 2012 sobre la normalización europea, el cual en su artículo 2 establece las siguientes definiciones:

- Norma*: «especificación técnica adoptada por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria (…)»*[21]
- Norma internacional*: «norma adoptada por un organismo internacional de normalización».* [22]

Así mismo, dichos estándares han sido consideradas en los textos legislativos como medios u herramientas para realizar un cumplimiento de las obligaciones impuestas en el ámbito de la seguridad de la información[23].

Por ejemplo, el REGLAMENTO (UE) 2016/679 de 27 de abril de 2016 también conocido como Reglamento General de Protección de Datos (en delante, RGPD), las toma en consideración el establecer que las empresas que realicen tratamiento de datos podrán a

[20]PEREZ CARRILLO. Elena. Gobierno corporativo y ciberseguridad: algunos retos para el órgano administración. *Revista de Derecho de Sociedades*. [En línea]. 2023. Núm. 67. Editorial Aranzadi, S.A.U. PP. 2.1–2.19. [Fecha de consulta: 02/07/2023]. [Disponible en: https://proview-thomsonreuters-com.unileon.idm.oclc.org/title.html?redirect=true&titleKey=aranz%2Fperiodical%2F108262200%2Fv20230067.2&titleStage=F&titleAcct=i0adc41900000014d7b8f901e2b449b4f#sl=0&eid=90bdffaf151fb41e4a6082df3c775bd3&eat=%5Bereid%3D%2290bdffaf151fb41e4a6082df3c775bd3%22%5D&pg=I&psl=p&nvgS=fals]

[21]Reglamento (UE) n o 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n o 1673/2006/CE del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 316 de 14.11.2012, p. 12. [Fecha de consulta: 19/06/2023]. [Disponible en: https://eur-lex.europa.eu/eli/reg/2012/1025/2015-10-07]

[22]Idem.

[23]VIGURI CORDERO. Jorge. Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. *Revista de los Estudios de Derecho y Ciencia Política.* 2021. N°33. PP. 1-12. [Fecha de consulta: 07/07/2023]. [Disponible en: https://doi.org/10.7238/idp.v0i33.376366]

adherirse a mecanismos de certificación con el objetivo de demostrar la existencia de garantías adecuadas[24].

2.3) Estándares ISO y sus ventajas de aplicación:

La implementación de los estándares en una organización, además de brindar un acercamiento a la ciberseguridad, y, por consiguiente, tener una mejor protección de los activos empresariales, representa un estándar de calidad y de fiabilidad hacia los terceros, tanto para consumidores y empresas relacionadas. Además, permiten cumplir con las obligaciones impuestas por las regulaciones jurídicas de los Estados. [25]

2.4) Marco de trabajo de ciberseguridad (NIST Framework).

Así mismo, como herramienta para implementar medidas de ciberseguridad en las empresas, son de gran utilidad los marcos de trabajo desarrollados por el Instituto Nacional de Estándares y Tecnología de Estados Unidos, también conocido como National Institute of Standards and Technology (en delante, NIST)[26].

Entre la variedad de marcos de trabajo elaborados por NIST, en el ámbito de ciberseguridad, destacan dos, el marco de trabajo de ciberseguridad y el marco de gestión del riesgo de la cadena de suministro de ciberseguridad para sistemas y organizaciones, también conocido como NIST SP 800-161r1.

El primero, nace a partir de un constante incremento en el número de incidentes de seguridad cibernética en los Estados Unido. Por lo que el presidente Barack Obama en el año 2013 emitió la orden ejecutiva 13636 orientando al NIST el desarrollo de un marco de

[24]Véase el artículo 42 apartado 2 del RGPD.
[25]ISO. *Benefits of standards*. [En línea]. [Fecha de consulta: 19/06/2023]. [Disponible en: https://www.iso.org/benefits-of-standards.html]
[26]ORTEGA CANDEL, José. *Ciberseguridad. Manual práctico*. Ibidem. P. 21.

ciberseguridad[27]. Este marco se caracteriza por brindar buenas prácticas para la gestión de riesgo que se debe realizar en el ámbito de ciberseguridad.[28]

El segundo, se origina a partir de la Iniciativa Nacional para Mejorar la Ciberseguridad en las Cadenas de Suministro. Se caracteriza por proporcionar pautas y prácticas para la gestión del riesgo de la cadena de suministro de ciberseguridad. Su principal objetivo es ayudar a las organizaciones a evaluar, mitigar y gestionar los riesgos relacionados con la cadena de suministro de las TIC[29].

3) Una nueva percepción de la cadena de suministro - la cadena de suministro de las TIC:

Comúnmente, la cadena de suministro es concebida como la integración de procesos logísticos y de distribución entre fabricantes, importadores y distribuidores, con la finalidad de ingresar bienes o servicios en el mercado[30]. No obstante, la innovación tecnológica ha creado una nueva categoría, la cadena de suministro de las TIC.

A esta nueva categoría, alude el consejo de la UE en su informe de *conclusiones del consejo sobre la seguridad de las cadenas de suministro de las TIC*[31]. Cabe destacar que dicha categoría no cuenta con una definición oficial, pero si se cuenta con elementos que facilitan su comprensión.

De acuerdo con el artículo 2 del Reglamento (UE) 2019/881, se debe de entender por: 1) Producto TIC: *«un elemento o un grupo de elementos de las redes y los sistemas de*

[27]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *cybersecurity framework.* [En línea]. [Fecha de consulta: 28/06/2023]. [Disponible en: https://www.nist.gov/cyberframework/framework]

[28] ORGANIZACIÓN DE ESTADOS AMERICANOS. *Ciberseguridad Marco NIST. Un abordaje integral de la ciberseguridad. 2019*. [En línea]. [Fecha de consulta: 07/08/2023]. [Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf]

[29]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management C-SCRM.* [En línea]. [Fecha de consulta: 11/07/2023]. [Disponible en: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management]

[30]Véase la sección: 3.9 de la UNE - ISO 28000. ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Especificación para los sistemas de gestión de la seguridad para la cadena de suministro.* UNE-ISO 28000. Madrid. UNE. 2008.

[31]Conclusión número 3. CONSEJO DE LA UNIÓN EUROPEA. *El Consejo acuerda reforzar la seguridad de las cadenas de suministro de las TIC.* [En línea]. [Fecha de consulta: 17/06/2023]. [Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/]

información»[32] y 2) Servicio TIC: *«un servicio que consista, en su totalidad o principalmente, en la transmisión, almacenamiento, extracción o tratamiento de información mediante redes y sistemas de información»*[33].

Congruentemente la cadena de suministro está conformada por una gran variedad de recursos, tales como y sin ser limitativos a: equipos y programas informáticos, almacenamiento en nube y local, aplicaciones web, tiendas virtuales de comercio electrónico y programas informáticos de gestión. [34]

3.1) Entendiendo las amenazas y riesgos de la cadena de suministro de las TIC:

De acuerdo con el informe de panorama de amenazas de ciberseguridad publicado en el año 2022[35] y el informe de panorama de ciberseguridad del sector transporte publicado en el año en curso, ambos elaborados por la agencia ENISA. Se identificó que globalmente una de las principales y emergentes amenaza en el ámbito de ciberseguridad son los ataques a la cadena de suministro.

A su vez, de manera específica en el sector transporte de la UE, dentro del periodo de enero 2021 a octubre 2022 los ataques tipo de cadena de suministro representaron un 10% de incidentes acontecidos. [36]

Por dicha razón, es que las empresas deben prepararse para mitigar los riesgos provenientes de la cadena de suministro de las TIC, pero primero deben de comprender su alcance.

[32]Véase el artículo 12 apartado 12 del Reglamento (UE) 2019/881.
[33]Véase el artículo 12 apartado 13 del Reglamento (UE) 2019/881.
[34]ENISA. *Informe panorama de amenazas de las enisa relacionadas con ataques a la cadena de suministro. 2021*. p.10.[En línea]. Oficina de publicaciones de la Unión Europea. 2021. [Fecha de consulta 12/06/2023]. [Disponible en: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-supply-chain-attacks_es.pdf]*
[35]ENISA. *Threat Landscape 2022*. p. 88. [En línea]. Publications Office of the European Union. 2022. [Fecha de consulta: 12/06/2023]. [Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022]
[36]ENISA. *ENISA Transport Threat Landscape Sector.* [En línea]. Publications Office of the European Union. 2023. [Fecha de consulta: 12/06/2023]. [Enlace de acceso: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape]

La cadena de suministro de las TIC comienza con el diseño de cada componente, tanto en hardware como software y se extiende a través de las etapas de desarrollo, tales como abastecimiento, fabricación, manipulación y, entrega productos y servicios al adquirente. Lo que significa que cada etapa antes de que llegue a las manos del adquiriente es una oportunidad para los ciberatacantes para introducir, ya sea un componente infeccioso en hardware o encontrar una vulnerabilidad en el desarrollo de software que logre comprometer la disponibilidad, confidencialidad e integridad de la información[37].

Ahora bien, para fortalecer lo previamente expuesto, es necesario distinguir entre un ciberataque común y un ciberataque a la cadena de suministro de las TIC. El primero es el que se realiza de manera directa hacia una organización o persona natural, mientras que el segundo es indirecto, se ataca al proveedor como un medio y no como un fin. [38]

De acuerdo con el informe panorama de amenazas de ENISA, los ataques a la cadena de suministro se caracterizan por ser ataques complejos debido a que son una combinación de varios factores y técnicas, tales como: dirigidos a un proveedor para llegar a un objetivo final, realizan acceso no autorizado a los sistemas de la víctima mediante la ejecución de código, y continua en el tiempo[39].

3.2) Principales ciberataques a la cadena de suministro:

De acuerdo con el informe panorama de amenazas relacionadas con ataques a la cadena de suministro publicado por ENISA en el año 2021, entre los meses de enero 2020 hasta principios de julio del año 2021, entre los ciberataques conocidos y más relevantes por los menoscabos causados, destacan[40:]

[37]FEDERAL VIRTUAL TRAINING ENVIRONMENT. *Cyber Supply Chain Risk Management for the Public*. [En línea]. [Fecha de consulta: 12/07/2023]. [Disponible en: https://fedvte.usalearning.gov/publiccourses/cscrm/index.htm?track=trackingon]

[38]ENISA define un ataque a la cadena de suministro como una combinación de dos ataques. El primer ataque es contra un proveedor que luego se utiliza para atacar al objetivo y obtener acceso a sus activos. El objetivo puede ser el cliente final u otro proveedor. Por lo tanto, para que un ataque se clasifique como de cadena de suministro, tanto el proveedor como el cliente deben ser objetivos. ENISA. *Informe panorama de amenazas de las enisa relacionadas con ataques a la cadena de suministro.* P.10 [En línea]. Oficina de publicaciones de la Unión Europea. 2021. [Fecha de consulta 10/05/2023]. [Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-supply-chain-attacks_es.pdf].

[39]Ibidem. P. 17

[40]Ibidem. P. 19

- Ciberataque a la empresa SolarWinds: Descubierto a finales del año 2020. Los atacantes modificaron el código de una aplicación de gestión de red de la empresa para crear un acceso inidentificado, lo que afectó a casi 18000 entidades del sector público y privado, entre ellas entidades públicas del gobierno de Estados Unidos. El incidente tuvo múltiples derivadas, siendo una de las más importantes el acceso de los atacantes aparte del código fuente de la nube de Microsoft.[41]
- Ciberataque a la empresa Kaseya: Fue un ataque de ransomware que fue realizado en julio de 2021 al software administrador virtual de sistemas de kaseya, el cual era utilizado por otros proveedores de tecnología para proveer servicios. Este incidente afecto alrededor de 1500 empresas que no tenían una relación con kaseya sino con sus clientes. [42]

3.3) Derecho comparado sobre la cadena de suministro de las TIC:

Para lograr la transformación digital del sector privado de una manera segura y confiable, sobre todo de aquellas empresas que, en razón de su actividad económica, brinden servicios fundamentales a la sociedad, es de gran relevancia que las cadenas de suministro de las TIC estén protegidas ante incidentes de ciberseguridad. Ya que a como se expuso en el apartado anterior, los ataques a las cadenas de suministro no solo perjudican a una empresa de forma aislada, sino que tienen efectos en cascada contra aquellas que han contratado los servicios[43].

En esta misma línea, los países miembros de la Organización para la Cooperación y Desarrollo Económico, conocida como OCDE, se comprometen a trabajar de manera

[41]CENTRO CRIPTOLOGICO NACIONAL. *Ciber_Amenazas y* tendencias. [En línea]. Gobierno de España. Ministerio de Defensa. 2021. [Fecha de consulta: 21/05/2023] [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html*]*.

[42]MARQUARDAT ALEX. *Kaseya dice que menos de 1.500 empresas fueron afectadas por un ataque de ransomware.* [En línea] [Fecha de consulta: 21/05/2023] [Disponible en: https://cnnespanol.cnn.com/2021/07/06/kaseya-empresas-ciberataque-ransomware-trax/*]*

[43]Considerando 56, Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 333 de 27.12.2022. [Fecha de consulta: 19/06/2023]. [Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2555/oj]

conjunta para desarrollar un entorno digital seguro, y proteger las cadenas de suministro de tecnología digital, contra cualquier interrupción que cause un menoscabo contra la transformación digital de las economías y sociedades.[44]

3.3.1) Estados Unidos de Norteamérica - Orden Ejecutiva 14028 del año 2021:

El presidente Biden de Estados Unidos de Norteamérica, (en delante, EE. UU.) con la finalidad de implementar medidas de ciberseguridad en las entidades gubernamentales que, por naturaleza de sus funciones, almacenan datos de carácter personal y confidencial de la sociedad, y que en consecuencia requieren que los programas informáticos que utilicen dichas entidades en el desarrollo de sus funciones sean seguros y resistentes contra ciberataques. Dicta la orden ejecutiva 14028 denominada "mejorando la ciberseguridad de la nación" en donde se establecen orientaciones dirigidas a mejorar la ciberseguridad de la cadena de suministro de los servicios de software utilizados por tales administraciones.

La orden ejecutiva previamente mencionada es de mucha relevancia para la ciberseguridad de cadena de suministro de EE. UU, debido a que introduce la obligación de desarrollo seguro[45] de los programas informáticos.

Dicha orden orienta al NIST a la creación de estándares y requerimientos para mejorar la seguridad de la cadena de suministro de software, de modo que los nuevos y existentes proveedores de software de las instituciones gubernamentales federales, están obligados a cumplirlas para poder ofrecer sus servicios tecnológicos de programas informáticos.

Los tipos de software que deberán de cumplir las orientaciones de seguridad indicados por el NIST son los proveedores de firmware[46], sistemas operativos, aplicaciones y

[44]OECD LEGAL INSTRUMENTS. *Declaration on a Trusted, Sustainable and Inclusive Digital Future.* [En línea]. 2022. [Fecha de consulta: 19/06/2023]. [Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488]

[45]El desarrollo seguro de software es una metodología cuyo objetivo es considerar la seguridad de las aplicaciones durante todo su ciclo de vida, empezando desde la propia definición de requisitos de estas. LOPEZ ANGEL. *Desarrollo seguro de software*. [En línea] [Fecha de consulta: 27/05/2023] [Disponible en: https://itcl.es/blog/desarrollo-seguro-de-software/].

[46]Firmware es un tipo de software que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes. INCIBE. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*.

aplicaciones de servicio como por ejemplo los softwares basados en nube asi como los productos que contengan software.

Adicional, la orden ejecutiva introduce el término "software crítico" y orienta al NIST que brinde una definición sobre el termino, lo que genera una distinción en la clasificación de tipos de software que sean parte de una cadena de suministro.

De acuerdo con NIST, un software adquiere el nivel crítico, cuando administre y posea accesos privilegiados a información, redes, recursos informáticos, seguridad informática y tenga controle los accesos a datos o tecnología operacional, es decir que opere fuera de los límites normales de confianza con acceso privilegiado. [47]

En conclusión, en este capítulo se destaca como la transformación digital brinda ventajas económicas y operativas al sector privado. Adicionalmente, debido a los nuevos servicios y productos de índole TIC, se origina una cadena de suministro de las TIC. Por lo tanto, es menester que la transformación digital sea acompañado con la disciplina de la ciberseguridad, de manera que los riesgos provenientes de la cadena de suministro de las TIC puedan ser mitigados.

[En línea]. [Fecha de consulta: 19/06/2023]. [Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf].

[47]NATIONAL CYBER SECURITY CENTRE. *Definition of Critical Software Under Executive Order (EO) 14028*. P.3 [En línea]. U.S. Department of Commerce. 2021. [Fecha de consulta: 25/05/2023] [Disponible en: https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf]

CAPÍTULO SEGUNDO: ANÁLISIS DE LA DIRECTIVA (UE) 2022/ 2555 Y SU REGULACIÓN SOBRE LA CIBERSEGURIDAD DE LA CADENA DE SUMINISTRO.

1) Marco jurídico de la Seguridad de las Redes y Sistemas de Información en la Unión Europea:

A como se indicó en el capítulo anterior, la definición de ciberseguridad estipulada por la UE se enfoca hacia la protección de las redes y sistemas de información. Esta perspectiva fue desarrollada en primera instancia por el legislador europeo por medio de la Directiva (UE) 2016/1148 del 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la unión (en delante, DNIS 1). En segunda instancia y en la misma orientación se localiza su sucesora, la vigente Directiva (UE) 2022/2555 del 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (DNIS2). Con el propósito de entender su impacto sobre la ciberseguridad en las empresas y cadena de suministro de las TIC, conviene tener en cuenta lo que DNIS1 había previsto algunos años antes.

1.1) Antecedentes - La Directiva (UE) 2016/1148:

La DNIS1 fue adoptada con el objetivo de fortalecer la ciberseguridad del mercado interior y la seguridad de las redes y sistemas de información de las empresas europeas que brinden servicios esenciales en sectores fundamentales y que su interrupción pudiese ocasionar estragos a la sociedad, y a las instituciones públicas que provean servicios.

Por medio de dicha Directiva, la UE definió seguridad de las redes y de sistemas informáticos[48] como: *«la capacidad de (…) resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad*

[48]Véase el artículo 4 apartado 2 de la Directiva (UE) 2016/1148.

de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos».[49] En esta definición se aprecia que la UE incorpora los principios de la ciberseguridad en torno a un objeto concreto de tutela: las redes y sistemas de información. Con DNIS1 se dibuja una sinergia entre ambos conceptos: ciberseguridad y redes/sistemas de información.

El *modus operandi* con el que la DNIS 1 pretendió llevar a cabo dicha protección fue por medio del establecimiento de obligaciones a aquellas empresas y entidades públicas catalogadas como operadores de servicios esenciales y proveedores de servicios digitales [50]. Las principales obligaciones, estipuladas en los artículos 14 y 16, consistieron en:

- Implementar medidas para la gestión de riesgos.
- Aplicar medidas de seguridad para reducir los efectos de incidentes que afecten la seguridad de las redes y sistemas de información.
- Notificar a los equipos de respuesta a incidentes de seguridad informática (en delante, CSIRT por sus siglas en inglés) los incidentes de seguridad que afecten la continuidad de los servicios que prestan.

Cabe destacar que estuvieron exentas de las obligaciones anteriores las microempresas y pequeñas empresas que fuesen concebidas dentro de la definición establecida por la *Recomendación 2003/361/CE*.[51] Según consta en su artículo 2 apartado 1, la cual identifica como pymes, a las empresas que tengan menos de 250 empleados, cuyas ventas brutas no superen los 50 millones o cuyo balance general anual no exceda de 43 millones de euros.

[49]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 sistemas de información en la Unión. Diario oficial de la Unión Europea: L 194 de 19.7.2016, p. 1-30. [Fecha de consulta: 09/06/2023] [Disponible en: https://eur-lex.europa.eu/eli/dir/2016/1148/oj]

[50]De acuerdo con el Anexo II de la DNIS 1, operadores esenciales corresponde a los sectores: energía, transporte, banca, infraestructura de mercados financieros, sector sanitario, suministro y distribución de agua potable e infraestructura digital. Proveedores de servicios digitales, corresponde a los sectores: mercado en línea, motor de búsqueda y servicios de computación en nube.

[51]Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (Texto pertinente a efectos del EEE) [notificada con el número C (2003) 1422]. Diario oficial de la Unión Europea: L 124, 20.5.2003, p. 36–41. [Fecha de consulta: 10/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32003H0361]

1.2) La vigente regulación Europea de las Redes y Sistemas de Información - Directiva (UE) 2022/2555:

La DNIS 2 entró en vigor el 27 de diciembre del año 2022 y debe de ser transpuesta por los Estados miembros a más tardar el 17 de octubre del 2024[52]. Esta Directiva introduce una nueva calificación hacia las empresas que debido a la actividad que ejerzan en cierto sector crítico o de alta criticidad y tamaño, sean considerades como entidades esenciales o importantes (en delante, denominadas de manera conjunta como, entidades reguladas).

Cabe destacar que DNIS 2 no establece una definición de que lo considera sector crítico o de alta criticidad. Por consiguiente, con el objetivo de brindar una aproximación a dicho término, en el desarrollo del presente trabajo académico, se entenderá por sector crítico o de alta criticidad, como el conjunto de ámbitos fundamentales para el mantenimiento de funciones sociales vitales, actividades económicas, salud pública, seguridad, o el medio ambiente[53], por lo que su interrupción, significaría un gran menoscabo hacia la sociedad.

1.3) Entidades sometidas a la Directiva (UE) 2022/2555:

En contraste con su antecesora, la DNIS 2, amplía los sectores de aplicabilidad. Además, establece servicios en los cuales tendrá aplicación directa independientemente del tamaño de la empresa que los proporcione[54], siendo estos los siguientes: a) proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas; b) prestadores servicios de confianza; c) proveedores registros de nombres de dominio de primer nivel y de servicios de sistema de nombres de dominio.

En este mismo orden de ideas, establece que tendrá aplicación directa cuando el proveedor sea: 1) el único proveedor de un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas; 2) una interrupción del servicio

[52]Véase el artículo 41 de la Directiva (UE) 2022/2555.
[53]La Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas, en su artículo 2 apartado 5, define servicio esencial como: un servicio que es crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad, o el medio ambiente.
[54]Véase el articulo 2 apartado 2 de la Directiva (UE) 2022/2555.

brindado pudiera producir daños significativos sobre la seguridad pública, orden público, la salud pública, y que estos daños puedan tener efectos transfronterizos; y 3) entidades críticas.

De acuerdo con el artículo 3[55] de la Directiva en análisis, serán entidades esenciales aquellas que superan el techo establecido para las medianas empresas y que desarrollen sus actividades económicas dentro de los sectores de alta criticidad establecidas en su anexo I, siendo estos: 1) energía; 2) transporte; 3) banca; 4) infraestructura de los mercados financieros; 5) sanidad; 6) agua potable; 7) aguas residuales; 8) infraestructura digital; 9) gestión de servicios tic y 10) espacio.

Adicionalmente, son consideradas entidades esenciales: a) las entidades críticas y b) cualquier entidad que el estado miembro identifique como esencial en virtud de su participación en los sectores mencionados en el párrafo anterior. Atendiendo a criterios de: unicidad, criticidad, repercusiones y riesgos en la interrupción de los servicios[56].

En relación con la identificación de las entidades importantes, serán aquellas que no puedan considerarse entidades esenciales por su tamaño, es decir que no sobrepasen el límite de las medianas empresas, pero que desarrollan sus actividades dentro de los sectores de alta criticidad al igual que estas. Adicionalmente, serán aquellas que brinden sus servicios dentro de otros sectores establecidos en el anexo II, siendo estos: 1) servicios postales y de mensajería; 2) gestión de residuos; 3) fabricación, producción y distribución de sustancias y mezclas químicas; 4) producción, transformación y distribución de alimentos; 5) fabricación de productos sanitarios, informáticos, electrónicos y ópticos, material eléctrico, maquinaria, vehículos de motor y de otro material de transporte y 6) proveedores de servicios digitales [57]

[55]Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 333 de 27.12.2022, p. 80-152. [Fecha de consulta:21/06/2023]. [Disponible en: http://data.europa.eu/eli/dir/2022/2555/oj]

[56]Véase el artículo 3, apartado 1, letra F de la Directiva (UE) 2022/2555.

[57]ROBLES CARRILLO. Margarita. *Análisis de la Directiva (UE) 2022/2055 sobre las medidas para garantizar un elevado nivel común de ciberseguridad en la Unión Europea (NIS 2).* 2023. Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad. Universidad de Vigo-INCIBE, pp. 367-374.

1.4) Especial tratamiento a los servicios de computación en nube:

De acuerdo con las estadísticas de Eurostat[58], en el año 2021 el 41% de las empresas de la UE ya utilizaban los servicios de computación en nube, por lo tanto, es muy probable que ese porcentaje en la actualidad sea mayor debido al auge de la transformación digital del sector privado.

La computación en nube es un modelo de computación que permite al proveedor ofrecer servicios informáticos a través de internet. De modo que los recursos tales como hardware, software y datos pueden ser ofrecidos a las empresas bajo demanda.[59]

Los principales servicios en nube se pueden clasificar en cuatro tipos[60]:

- **Software como servicio (SAAS)**: El proveedor del servicio aloja las aplicaciones del de la empresa en sus servidores de almacenamiento. Como por ejemplo de servicio, destacan **Google Drive** o **Dropbox**.
- **Plataforma como servicio (PAAS)**: El proveedor pone a disposición un entorno digital con características pactadas de hardware y software, en donde el cliente accede de manera remota al servicio. Por ejemplo, los servicios ofrecidos por **Google App Engine**, el cual es mayormente utilizado para crear aplicaciones.
- **Infraestructura como servicio (IAAS)**: Consiste en brindar a las empresas recursos informáticos, tales como servidores, redes, almacenamiento. Un ejemplo de este servicio es el brindado por **Amazon Web Services** (AWS).
- **Red como servicio (NAAS):** Este servicio se basa en brindar acceso a una infraestructura de red en la nube a los clientes[61].

[58]COMISIÓN EUROPEA. *Computación en la nube*. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://digital-strategy.ec.europa.eu/es/policies/cloud-computing]
[59]INCIBE. *Cloud computing: una guía de aproximación para el empresario.* [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.incibe.es/empresas/guias/cloud-computing-guia-aproximacion-el-empresario]
[60]TELEFÓNICA. *Qué es el Cloud Computing: tipos y ventajas.* [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/que-es-el-cloud-computing-tipos-y-ventajas/]
[61]CLOUDFLARE. *¿Qué es NaaS (red como servicio)?. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/network-as-a-service-naas/]*

Habiendo comprendido la definición y los tipos de servicios basados en nube, es necesario resaltar el especial tratamiento que establece la DNIS 2 a este tipo de proveedores.

Los proveedores de este tipo de servicios ingresan dentro del sector de infraestructura digital, identificado como de alta criticidad según el anexo 1 de la Directiva. Por lo tanto, forman parte de las entidades reguladas y deben de someterse a las obligaciones impuestas por la DNIS 2. No obstante, la Comisión Europea por medio de un acto de ejecución que debe publicarse antes del 17 de octubre del 2024, establecerá las medidas de gestión de riesgo específicas que estos proveedores deben de cumplir a nivel de la UE[62]. De modo que los Estados Miembros no podrán establecer medidas adicionales en la transposición de la DNIS 2 a su marco jurídico.

1.5) Exegesis de la cadena de suministro en la Directiva (UE) 2022/2555:

La DNIS 2 en su artículo 21 apartado 2 inciso "d", incorpora que se tome en consideración los riesgos derivados de la cadena de suministro, lo cual es alineado con la *Estrategia de Ciberseguridad para la Década Digital de la UE.* Debido a que en este documento se expresa la intención de liderar el desarrollo de tecnologías seguras en toda la cadena de suministro en la década del 2020 – 2030[63].

Es importante resaltar que dicha Directiva no brinda una definición sobre cadena de suministro, sin embargo, en su análisis, resalta un enfoque hacia la cadena de suministro de las TIC, asi lo demuestra en su considerando 85 al hacer referencia a los *«(…) riesgos de ciberseguridad provenientes de la cadena de suministro (…)»*. La cual a como se indicó en el capítulo anterior, se encuentra compuesta por productos y servicios TIC.

Cabe destacar que en el abanico de regulaciones sobre diferentes sectores que involucran la cadena de suministro de cualquier producto, su definición goza de cierta versatilidad y facilidad de adaptación al contexto sobre el que el verse el documento legal.

[62]Véase el artículo 21 apartado 5 de la Directiva (UE) 2022/2555.
[63]COMISIÓN EUROPEA. *Estrategia de Ciberseguridad de la UE para la Década Digital*. 2020. [En línea]. [Fecha de consulta: 21/06/2023]. [Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_20_2391]

No obstante, la cadena de suministro de las TIC se diferencia del concepto general por incluir servicios TIC, el cual se desarrolla en un espacio desmaterializado. En donde no son necesarios la ejecución de procesos logísticos, sino que este es reemplazado por el internet para llegar al consumidor final.

Conviene señalar que esta categoría ya es utilizada en documentos regulatorios de la UE. Asi la reconoce en el considerando 105 del Reglamento (UE) 2019/881, el cual reza en su parte conducente de la siguiente manera: *«(…) Con el fin de seguir facilitando el comercio y reconociendo que las cadenas de suministro de TIC son mundiales (…)».*

Adicionalmente, debido al riesgo que puedan representar las cadenas de suministro de las TIC para la ejecución de los servicios esenciales brindados por las entidades reguladas. El legislador europeo introduce las cadenas de suministro críticas, las cuales serán identificadas y evaluadas por el Grupo de Cooperación, establecido en el artículo 14 de la DNIS 2.

La identificación deberá obedecer a los criterios establecidos en el considerando 91 de la DNIS 2, siendo estos: a) frecuencia de uso y dependencia; b) relevancia para brindar los servicios esenciales; c) posibilidad de encontrar sustitutos en el mercado; d) resiliencia de la cadena de suministro e importancia a largo plazo.

Una vez identificadas, se realizará el proceso de evaluación que tomará en consideración factores de riesgos técnicos y de otra índole cuando sea necesario[64], tales como el marco jurídico y político de los proveedores de productos y servicios TIC en terceros países[65].

Por último, destaca la inclusión de la resiliencia en la cadena de suministro como criterio para identificar a aquellas consideradas como críticas.

De acuerdo con el artículo 2 apartado 2 de la Directiva (UE) 2022/2557[66] relativa a la resiliencia de las entidades críticas, se entiende por resiliencia como: *«la capacidad (…)*

[64]Véase el artículo 22 apartado 1 de la Directiva (UE) 2022/2555.
[65]Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G C/2019/2335. L 88 de 29.3.2019, p. 42-47. [Fecha de consulta: 08/07/2023]. [Disponible en: http://data.europa.eu/eli/reco/2019/534/oj]
[66]Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (Texto

para prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación en caso de un incidente (…)».

Por consiguiente, es evidente que el propósito del legislador europeo al incluir la resiliencia en la cadena de suministro es que los productos y servicios TIC que la conforman, incluyan dichas características para lograr el fortalecimiento de la ciberseguridad del mercado interior[67].

1.6) Sinergia entre la Directiva (UE) 2022/2555 y la propuesta de Reglamento de Ciberresiliencia en el tratamiento a la cadena de suministro:

En palabras de Thierry Breton[68], comisario del Mercado Interior de la UE, *«En lo que respecta a la ciberseguridad, Europa solo será tan fuerte como lo sea su eslabón más débil, sea este un Estado miembro vulnerable o un producto inseguro en la cadena de suministro (…)». En este orden de ideas,* la UE elaboró la propuesta de Reglamento de Ciberresiliencia[69] el cual tiene como principal objetivo, reducir los riesgos de ciberseguridad que provengan de las vulnerabilidades de los productos o servicios TIC, sobre todo de aquellos que utilicen las entidades reguladas de la DNIS 2 para el desarrollo de sus servicios.

Por dicho motivo, esta propuesta introduce un conjunto de requisitos y obligaciones encaminadas a la ciberseguridad que deben de ser cumplidos por los sujetos que son parte de la cadena de suministro (fabricante, distribuidor e importador) previo y post ingreso en el mercado interior, de cualquier producto con elementos digitales que para su funcionamiento incluya una conexión directa o indirecta a un dispositivo o a una red.

pertinente a efectos del EEE). L 333, 27.12.2022, p. 164–198. [Fecha de consulta: 03/07/2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2557]

[67]Véase el artículo 6, apartado 5, letra b, de la propuesta del Reglamento de Ciberresiliencia.

[68]COMISION EUROPEA. *Estado de la Unión: nuevas normas de la UE en materia de ciberseguridad garantizan unos equipos y programas informáticos más seguros. [En línea]. [Fecha de consulta: 23/06/2023]. [Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5374]*

[69]Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020. [Fecha de consulta: 30/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52022PC0454]

Adicionalmente, el artículo 6 de la propuesta, introduce dos categorías de productos con elementos digitales: 1) productos con elementos digitales críticos y 2) los altamente críticos.

Los primeros, corresponden a los establecidos en el anexo III de la propuesta. Adicionalmente, podrán ser aquellos identificados en razón del nivel de riesgo de ciberseguridad que representen, el cual será evaluado atendiendo a criterios de funcionalidad, uso por entidades reguladas bajo la DNIS 2, utilización en realización de funciones críticas, y posibles y conocidas repercusiones.

Los segundos, serán aquellos que sean identificados por la Comisión Europea, teniendo en cuenta el nivel de riesgo y los criterios previamente indicados. Adicionalmente, si son utilizados por entidades esenciales de los sectores del anexo I de la DNIS 2, asi como su importancia en un futuro y resiliencia de la cadena de suministro global.

En relación con la identificación de las cadenas de suministro críticas que debe realizar el grupo de cooperación, se deberán tomar en cuenta los productos o servicios críticos que conformen la cadena de suministro bajo evaluación[70].

Así mismo, ambos cuerpos normativos se apoyan en las certificaciones en el marco de un esquema europeo de certificación de ciberseguridad. En este sentido el artículo 24 de la DNIS 2, plantea que los Estados miembros o que la Comisión Europea por medio de actos delegados, podrán obligar a las entidades reguladas a utilizar productos o servicios que cuenten con una certificación de ciberseguridad. Los cuales son desarrolladas por ENISA.

En este mismo orden de ideas lo establece la actual propuesta de Reglamento de Ciberresiliencia. Debido a que establece que los fabricantes de los productos altamente críticos con elementos digitales deberán contar con una certificación de ciberseguridad dentro del marco de un esquema europeo de certificación de ENISA.

Por último, en lo que concierne a los productos con elementos digitales, con el objetivo de fomentar la utilización de la certificación de ciberseguridad dentro del marco de un esquema europeo de certificación, a los fabricantes que se les haya expedido una

[70]Véase el considerando 91 y artículo 22 de la Directiva (UE) 2022/2555.

declaración de conformidad de la UE, o una certificación del marco de esquema europeo, gozaran de un reconocimiento de presunción de conformidad de requisitos establecidos para la fabricación de sus productos que pretendan ingresar al mercado interior de la UE[71].

En razón de lo previamente expuesto, estas dos iniciativas jurídicas se encuentran estrechamente relacionadas en el ámbito de la ciberseguridad de la cadena de suministro de las TIC y representen los medios por el cual la UE pretende fortalecer la ciberseguridad del mercado interior.

2) Gobernanza de la ciberseguridad de las entidades reguladas por la Directiva (UE) 2022/2555:

La DNIS 2 marca un antes y después[72] en el sector privado, al incorporar al Marco Jurídico Europeo la figura de gobernanza en materia de ciberseguridad que deben desarrollar los órganos de administración de las entidades reguladas.

Así consta en su artículo 20 apartado 1, al imponer a los órganos de administración de las entidades reguladas, la obligación de aprobar y supervisar medidas de gestión de riesgo de ciberseguridad, so pena de incurrir en incumplimiento cuando estas adopten la forma de sociedad mercantil[73].

2.1) Definición de gobernanza de la ciberseguridad:

Para definir la gobernanza de la ciberseguridad, se deben tomar en cuenta las definiciones relacionadas a gobierno corporativo, gobernanza de la seguridad de la información y gobernanza de las TIC. Puesto que en el desarrollo del presente trabajo no se encontró una definición oficial.

[71]Véase el articulo 18 apartado 3 de la Propuesta de Reglamento de Ciberresiliencia.
[72]Si bien esta figura ya es adoptada por las empresas con un mayor nivel de madurez en el ámbito de la ciberseguridad por haber implementado las normas de estandarización internacional en sus procesos operativos, no obstante, esto era de carácter voluntario, sin embargo, a partir de la DNIS 2, es de carácter obligatorio.
[73]PEREZ CARRILLO. Elena. Gobierno corporativo y ciberseguridad: algunos retos para el órgano administración. *Revista de Derecho de Sociedades*. Ibidem. P. 2.4.

Se entiende por gobierno corporativo como el *«conjunto de responsabilidades y practicas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable».*[74]

Así mismo, con una noción evolutiva, el gobierno corporativo es el resultado de la distribución de facultades dentro de una sociedad mercantil y de las influencias, recomendaciones o imposiciones a las que sean sometidas[75].

Por otro lado, según AENOR, el gobierno de las TIC consiste en la unión de las TIC con la estrategia de la organización, de modo que se realice un control, responsabilidad, y gestión de riesgo de las TIC[76]. Por último, la ISO 27000:2018 define gobernanza de la seguridad de la información, como *«Sistema mediante el cual una organización dirige y supervisa las actividades de seguridad* de la información»[77]

Tomando en consideración los conceptos previamente indicados y con el objetivo de brindar una definición aproximada, se puede definir gobernanza de la ciberseguridad en un contexto empresarial, como la dirección estratégica definida por el órgano de administración para el cumplimiento de objetivos encaminados a la supervisión, seguridad de las redes e información y gestión de riesgos de las TIC como prioridad en todos los procesos de la empresa, tanto a nivel interno como externo, tomando en cuenta el aseguramiento de recursos para su ejecución. Dentro de esta definición, cabe destacar que, con órgano de administración, se hace referencia al consejo de administración o persona natural que tenga

[74]ORTEGA CANDEL, José. *Ciberseguridad. Manual práctico*. Ibidem. P.12
[75]PÉREZ CARRILLO. Elena, ALBOR BALTAR. Ángel. *GOBIERNO CORPORATIVO Y RESPONSABILIDAD SOCIAL DE LAS EMPRESAS.* 1ª. Madrid. Ediciones jurídicas y sociales, S.A. 2009. P. 54.
[76]AENOR. *Modelo para el gobierno de las TIC basado en las normas ISO. [En línea].* 1ª. MADRID. AENOR INTERNACIONAL, S.A.U. 2012. P.20. [Fecha de consulta: 24/06/2023]. [Disponible en: https://tienda.aenor.com/libro-modelo-para-el-gobierno-de-las-tic-basado-en-las-normas-iso-10179]
[77]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. T*ecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). visión de conjunto y vocabulario.* UNE-EN ISO/IEC 27000. Ibidem. Control 3.23.

la facultad de dirección más alta, que pueda definir la gobernanza de la ciberseguridad de la empresa[78]

Una efectiva gobernanza de la ciberseguridad permitirá a las entidades reguladas operar en una economía digital, y realizar una transformación digital sostenible[79]. Por lo tanto, se torna necesario garantizar que los miembros de los órganos cuenten con conocimientos relacionados con la disciplina de la ciberseguridad para poder cumplir con dicha tarea de manera eficiente y fortalecer la toma de decisiones.

2.2) Fortaleciendo la formación en ciberseguridad en las entidades reguladas por la Directiva (UE) 2022/2555:

El contar con un órgano de administración con conocimiento de ciberseguridad fortalece la gobernanza de una organización, por lo tanto, la DNIS 2, por medio de su artículo 20 apartado 2, introduce la obligación de los órganos de administración de las entidades reguladas de asistir a formaciones de ciberseguridad e igualmente de brindarlas de manera periódica a los empleados con el fin de que tengan las capacidades necesarias para identificar y gestionar los riesgos de manera adecuada en toda la organización.

No obstante, si bien dicha obligación representa un paso adelante para el fortalecimiento de conocimientos de ciberseguridad, el Comité Económico y Social Europeo (en delante, CESE) recomendó en su dictamen sobre la propuesta de la DNIS 2, que la Directiva debería de hacer referencia al contenido y capacidades mínimas que se esperan que los miembros de los órganos de administración de las entidades reguladas posean, con el objetivo de que los cursos de formación no varíen entre los estados miembros[80].

[78]NATIONAL CYBER SECURITY CENTRE. *Charting Your Course: Cyber Security Governance. P.4.* [En línea]. New Zealand Government. 2022. [Fecha de consulta: 24/06/2023]. [Disponible en: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Governance.pdf]
[79]Ibidem. P. 3.
[80]Dictamen del Comité Económico y Social Europeo sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 y sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la resiliencia de las entidades críticas [COM (2020) 823 final — 2020/0359 (COD) — COM (2020) 829 final — 2020/0365 (COD)]. Diario oficial de la Unión Europea: DO C 286 de 16.7.2021, p. 170-175. [Fecha de consulta: 28/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52020AE5749]

Siguiendo la línea de la recomendación del CESE, también se debe tomar en cuenta que las formaciones sean enfocadas en los sectores en que cada entidad regulada ejerce su actividad económica. Adicionalmente estos deben de incluir la gestión de riesgos de ciberseguridad en la cadena de suministro TIC.

Es importante resaltar que la gestión de riesgos en materia de ciberseguridad nunca va a ser la misma gestión de riesgos para una empresa que se desarrolle en el sector energético, que una que se desarrolle en el sector de servicios postales de mensajería, por lo tanto, la formación no debe de ser estándar.

2.3) El liderazgo de la gobernanza en la gestión de riesgos:

La figura de la gobernanza tiene un gran protagonismo en la gestión de riesgos que deben de realizar las entidades reguladas, a tal modo, que no es posible realizar una correcta gestión de riesgo, sin el apoyo del órgano de administración. Por dicha razón la gobernanza es primordial[81].

En este mismo sentido lo establece el estándar ISO 37000:2022, relacionada a la gobernanza de las organizaciones, la cual se enfoca en brindar principios y prácticas que los órganos de administración deben seguir para realizar una oportuna gobernanza.

Al respecto, el estándar indica que la gobernanza y la gestión son actividades codependientes, debido a que la gobernanza conlleva al establecimiento de responsabilidades y objetivos a cumplir por la organización mientras que la gestión es el medio que se encarga de cumplir los objetivos establecidos[82].

Por lo tanto, la gobernanza de la ciberseguridad incluye la gestión de riesgos que deben de realizar las organizaciones desde la gobernanza para proteger la redes y sistemas de información.

[81]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Gestión del riesgo. Directrices.* UNE-ISO 31000. Ibidem. Control 5.1

[82]ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Gobernanza de las organizaciones. Orientación.* UNE-ISO 37000. Madrid. UNE. 2022. Control. 4.2.3.

Para su implementación, es de gran utilidad el estándar ISO 31000:2018, debido a que establece una serie de acciones y responsabilidades que deben de ser asumidas por los órganos de administración de las organizaciones con la finalidad de poder gobernar con un enfoque basado en riesgos.

2.3.1) La política de ciberseguridad como principal herramienta para la gestión de riesgos:

Para una eficaz gobernanza, y cumplimiento del artículo 20, apartado 1 de la DNIS 2, los órganos de administración de las entidades reguladas deben de aprobar una política de ciberseguridad enfocada en la gestión de riesgos[83]. Esta acción determina el compromiso que tiene el órgano de administración para garantizar la seguridad de las redes y sistemas de información en la organización. Para su efectividad, debe de ser comunicada a todos los miembros que formen parte de la organización.

Por consiguiente, la aprobación de dicha política permitiría que todos los miembros de la organización se sientan compelidos a proteger la confidencialidad, integridad y disponibilidad de la información y seguridad de las redes.[84]

De acuerdo con el estándar ISO 31000:2018, cualquier política enfocada en la gestión de riesgos deberá contener los siguientes puntos[85]: 1) el propósito de la gestión de riesgos, así como las conexiones que pueda tener con otro objetivo y política ya establecida; 2) la imprescindibilidad de que la gestión de riesgos forme parte integral de la organización; 3) la consideración de la gestión de riesgos en las actividades económicas de la organización así como la toma de decisiones; 4) la implementación de roles y responsabilidades dentro de la organización, así como su rendición de cuentas; 5) la asignación de recursos para su ejecución; 6) el proceso para afrontar los objetivos ante un conflicto; 6) la evaluación y reportes para conocer la efectividad de la política y 7) la revisión y mejora constante de la política.

[83]UNE - ISO 31000:2018. Control 5.2.
[84]NATIONAL CYBER SECURITY CENTRE. *Charting Your Course: Cyber Security Governance*. Ibidem.P.7.
[85]UNE - ISO 31000:2018. Control 5.4.2

2.3.2) Los roles y responsabilidades de la ciberseguridad incorporando los relacionados con la cadena de suministro:

La ciberseguridad es una disciplina compleja y generalizada que compromete todas las áreas de una organización. Por lo que es necesario que, en el desarrollo de su implementación, las organizaciones cuenten con un liderazgo y estructura, integrado por profesionales con la debida formación y experiencia. [86]

En este mismo orden de ideas lo estipula la ISO 31000:2018. Establece que el órgano de administración debe determinar los roles y responsabilidades de los miembros en que delegara la supervisión y cumplimiento de la política de ciberseguridad indicada previamente, denominados como órganos de supervisión[87]

Asi mismo, es importante destacar de que a pesar de que el órgano de administración delegue funciones sobre la gestión de riesgo en los órganos de supervisión, mantendrá la responsabilidad y rendición de cuentas sobre dicha gestión, y los órganos de supervisión, rendirán cuentas por la supervisión ejecutada[88]

No debe confundirse que el órgano de administración puede delegar todas las responsabilidades, debido a que existen algunas que son indelegables[89], siendo estas las siguientes: 1) aprobación de la política de ciberseguridad de la organización; 2) identificación activos de alta importancia; 3) identificación de principales ciberriesgos de la organización y 4) evaluación de la eficacia de la política de ciberseguridad.

[86]FORO NACIONAL DE CIBERSEGURIDAD. *Código de buen gobierno de la ciberseguridad.* [En línea]. 1ª. Gobierno de España. Ministerio de la presidencia, relaciones con las cortes y memoria democrática. 2023. P. 13. [Fecha de consulta: 13/07/2023]. [Disponible en: https://foronacionalciberseguridad.es/index.php/documentacion/publico/123-codigo-buen-gobierno-de-la-ciberseguridad/file]
[87]UNE - ISO 31000:2018. Control 5.2.
[88]UNE - ISO 31000:2018. Control 5.2.
[89]NATIONAL CYBER SECURITY CENTRE. *Charting Your Course: Cyber Security Governance*. Ibidem. P.11.

Por consiguiente, los principales roles de ciberseguridad que se incorporan en una organización son los expuestos a continuación:

- Director de la seguridad de la información (en inglés denominado, *chief information security officer*) y sus principales funciones son: 1) desarrollar e implementar la estrategia de seguridad de la información y políticas de ciberseguridad y 2) identificar y gestionar los riesgos de seguridad de la información y 3) coordinar el equipo de ciberseguridad de la empresa. [90]
- Director de seguridad (en inglés denominado, chief security officer) y se encarga de velar por la seguridad física y digital de la empresa[91], asi mismo es responsable por implementar los planes de continuidad del negocio como respuesta ante cualquier incidente y supervisar el cumplimiento los objetivos empresariales establecidos[92].

Es importante señalar el informe de buenas prácticas para la ciberseguridad de la cadena de suministro recientemente publicado por ENISA. De acuerdo con este documento, apenas el 24% de las operadores esenciales y proveedores de servicios digitales regulados por la DNIS 1, han establecido roles y responsabilidades para la ciberseguridad de la cadena de suministro de las TIC[93].

Por lo tanto, es de gran relevancia para los lectores del presente trabajo académico, conocer que el principal rol encargado de la ciberseguridad en la cadena de suministro de las TIC corresponda a el:

- Director de la cadena de suministro (en inglés denominado, chief supply chain officer) y sus principales actividades son: 1) integración de nuevas tecnologías/servicios; 2) operaciones empresariales (por ejemplo, fabricación, prestación de servicios, etc.); 3) continuidad del negocio y recuperación ante desastres; 4) integración y gestión de

[90]INCIBE. *Roles en ciberseguridad: desde el CEO a los usuarios finales* [En línea]. [Fecha de consulta: 26/06/2023]. [Disponible en: https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales]
[91]Idem
[92]ORTEGA CANDEL, José. *Ciberseguridad. Manual práctico*. Ibidem. P. 9
[93]ENISA. *Good Practices for Supply Chain Cybersecurity.* P.10. [En línea]. Publications Office of the European Union. 2023. [Fecha de consulta: 30/06/2023]. [Disponible en: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity]

relaciones con terceros (por ejemplo, proveedores, prestadores de servicios, contratistas, etc.). Y 5) retirada de tecnologías, servicios y relaciones con terceros[94].

Adicionalmente, merece la pena revisar los roles establecidos en el artículo 13 del vigente Esquema Nacional de Seguridad[95] de España (en delante, ENS), debido a que estos se caracterizan por su delimitación de funciones.

- Responsable de la información: Su función consiste en *determinar «los requisitos de la información tratada»*
- Responsable del servicio: Se encarga de determinar *«los requisitos de los servicios prestados»*
- Responsable de la seguridad: Su función gira en torno a determinar los requisitos de seguridad de la información y de los servicios, incluyendo la supervisión y reporte de que estas se cumplan.
- Responsable del sistema: Se encarga de desarrollar, implantar y supervisar la seguridad de los sistemas.

Así mismo, destaca el esquema de modelo básico de referencia para la gobernanza de la ciberseguridad[96] que propone el Centro Criptológico Nacional de España (en delante, CCN) en su guía de aproximación al marco de gobernanza de la ciberseguridad debido a que toma en consideración la cadena de suministro de las TIC y especifica las actividades de supervisión que se deben de realizar en estas.

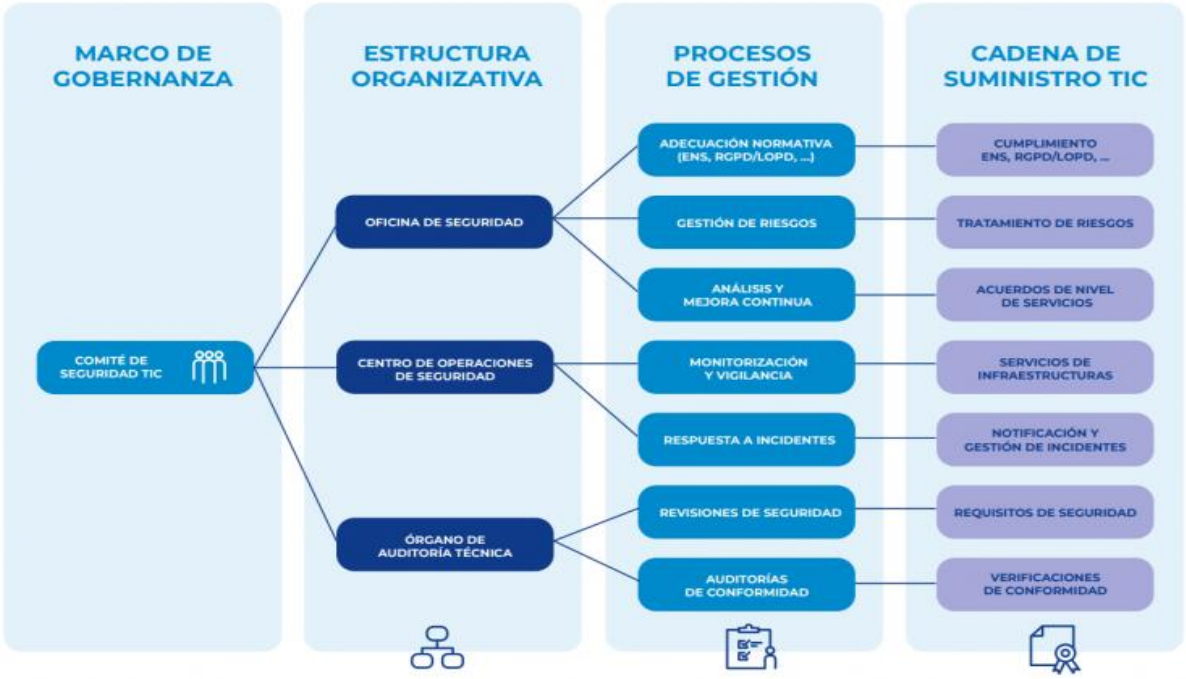
Cabe aclarar que este modelo es basado en los requerimientos del ENS, por lo tanto, su principal aplicación es para entidades públicas y sus proveedores, no obstante, puede ser

[94]COMPLIANCE FORGE. *Cybersecurity Supply Chain Risk Management (C-SCRM) Fundamentals*. [En línea]. [Disponible en: https://www.complianceforge.com/free-guides/cybersecurity-supply-chain-risk-management-scrm]

[95]El Esquema Nacional de Seguridad de España es una norma de obligatorio cumplimiento, que detalla los principios básicos y requisitos mínimos que deben de implementar las entidades públicas y sus proveedores para asegurar la información, redes y sistemas de información que estos utilicen en el ejercicio de sus competencias. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (BOE núm. 106 de 4 de mayo de 2002)

[96]CENTRO CRIPTOLOGICO NACIONAL. *Aproximación a un marco de gobernanza.* [En línea]. Gobierno de España. Ministerio de Defensa. 2022. [Fecha de consulta: 27/06//2023]. [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6431-aproximacio-n-al-marco-de-gobernanza-de-la-ciberseguridad/file.html]

adaptado a una empresa en base a la proporcionalidad del tamaño y dependencia en sistemas informáticos.



Del modelo previamente señalado, destaca la creación de un comité de seguridad TIC, del cual nacen tres unidades adicionales, 1) la oficina de gobernanza y cumplimiento normativo TIC, 2) órgano de auditorías técnica y 3) centro de operaciones de ciberseguridad.

En relación con el tema en análisis del presente trabajo académico, sobresale la asignación de supervisiones en la cadena de suministro TIC, que deben de realizar las unidades de la estructura organizativa.

En este sentido, la oficina de gobernanza y cumplimiento, supervisa que los proveedores que sean parte de la cadena de suministro TIC, cumplan con: 1) las obligaciones impuestas por otras normales legales, como, por ejemplo, la establecida por el RGPD sobre la contratación del encargado de tratamiento de datos[97], en donde la empresa contratante no se desprende de la responsabilidad del tratamiento de datos sino de la gestión; 2) tratamiento del riesgo de los productos o servicios TIC que sean brindados por terceros y 3) la implementación de acuerdos de nivel de servicios también conocido como service level

[97]Véase el artículo 28 apartado 1 del Reglamento General de Protección de Datos.

agreement, los cuales consisten en ser contratos que especifican las condiciones y calidad de los servicios que serán brindados[98].

El centro de operaciones de ciberseguridad se encarga de: 1) supervisar los servicios de infraestructuras TIC, siendo estos por lo general los servicios IAAS y 2) Notificar a las demás áreas de ciberseguridad de la organización los incidentes que se acontezcan desde la cadena de suministro de las TIC.

En último lugar, el órgano de auditoría técnica determina los requisitos de seguridad de los servicios o productos TIC que obtenga la organización y verifica que estos se cumplan.

Por otro parte, el marco de trabajo NIST SP 800-161r1, indica la creación de un equipo de gestión específico para la cadena de suministro de las TIC.

El equipo de gestión de riesgo de la cadena de suministro debe de estar integrado con un enfoque multidisciplinario y de miembros relacionados a las áreas críticas de la empresa, tales como: seguridad de la información, adquisiciones, gestión de riesgos empresariales, ingeniera, desarrollo de software, tecnología de la información, legal y recursos humanos. Es imprescindible que las personas designadas comprendan los aspectos técnicos y de interdependencia de los sistemas o de información. [99]

Lo que permitirá a las empresas llevar a cabo de manera efectiva un análisis integral y multidisciplinario de su cadena de suministro, responder a los riesgos de manera efectiva, comunicarse con socios externos y partes interesadas y alcanzar un amplio consenso respecto a los recursos adecuados para la gestión de riesgos en la cadena de suministro. [100]

Con relación a la ubicación del equipo dentro de un mapa organizacional, este puede ser una extensión del departamento existente de gestión de riesgos de ciberseguridad u operar desde un departamento diferente.[101]

---

[98]INCIBE. *Historias reales: la importancia de los acuerdos de nivel de servicio.* [En línea]. [Fecha de consulta: 27/06/2023]. [Disponible en: https://www.incibe.es/empresas/blog/historias-reales-importancia-los-acuerdos-nivel-servicio]

[99]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management Practices for System and Organizations*. P. 23 [En línea]. 1ª. Gaithersburg. NIST. 2022. [Fecha de consulta: 30/06/2023]. [Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf].

[100]Idem.

[101]Idem.

2.3.3) Comunicación y consulta[102]:

La política aprobada por el órgano de administración debe de contener un enfoque que permita la comunicación y consulta. Con comunicación, se refiere a compartir información relevante con las partes interesadas (internas y externas) con el objetivo de facilitar la concientización y compresión de los riesgos.

Lo que a su vez permite el proceso de consulta, el cual consiste en que estas partes a las quienes se les compartió información, brinden una retroalimentación que ayude a fortalecer la toma de decisiones informadas.

Las organizaciones pueden implementar las siguientes acciones para optimizar el proceso de comunicación y consulta[103]:

- Establecer metas y objetivos en el intercambio de información.
- Especificar el alcance de la información a compartir.
- Establecer reglas en el proceso de distribución de información, incluyendo la firma de acuerdos de confidencialidad.
- Utilizar flujos de trabajo seguros y automatizados para publicar, consumir, analizar y actuar sobre los resultados del proceso.

2.3.4) Aseguramiento de los recursos[104]:

Para ejecutar las medidas establecidas en la política de ciberseguridad, el órgano de administración debe de asegurar una serie de recursos que posibiliten que las actividades relacionadas a la gestión de riesgo se realicen.

Es fundamental para el buen desempeño en la gestión de riesgo, que el personal cuente con habilidades, experiencia y competencias necesarias para el efectivo desarrollo de sus

[102]UNE - ISO 31000:2018. Control 5.4.5.
[103]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management Practices for System and Organizations.* Ibidem. P.43
[104]UNE - ISO 31000:2018. Control 5.4.4.

funciones. Así mismo, es imprescindible que la organización cuente con los procesos, métodos y herramientas adecuadas que faciliten la ejecución de las actividades del personal.

Adicionalmente para garantizar la ejecución de cada actividad de manera ordenada, es necesario documentar todos los procesos y procedimientos, describiendo cada etapa de forma clara.

Así mismo, se debe disponer de un sistema de gestión de la información y del conocimiento. La gestión de información abarca su adquisición, organización, almacenamiento, custodia y distribución, mientras que la gestión del conocimiento implica utilizar la información para tomar acciones y decisiones estratégicas[105].

Por último, es importante que la organización promueva el desarrollo profesional y fomente la necesidad de formación de sus empleados. Vale la pena destacar la relación que tiene con lo establecido en el artículo 20 de la DNIS 2, ya que a como se indicó previamente, el órgano de administración de las entidades reguladas deberá capacitar a los empleados con el fin de que estos puedan identificar y gestionar los riesgos de ciberseguridad.

3) Política de ciberseguridad en la relación con proveedores y la cadena de suministro de las TIC:

La integración de gestión de riesgos en los procesos de adquisición de productos y servicios TIC, son esenciales para fortalecer la ciberseguridad de la cadena de suministro[106]. A tales efectos, sirve como principal herramienta la implementación de una política que incluya la relación con proveedores y que tenga un alcance a la cadena de suministro.

Retomando el informe previamente mencionado sobre buenas prácticas de ciberseguridad en la cadena de suministro. Este documento destaca que uno de los principales hallazgos de la investigación realizada por ENISA, fue encontrar que las operadores esenciales y proveedores de servicios digitales regulados por la DNIS 1, no contaban con la

[105]NACIONES UNIDAS. CEPAL. *Biblioguias – Biblioteca de la Cepal* [En línea]. [Fecha de consulta: 28/06/2023]. [Disponible en: https://biblioguias.cepal.org/c.php?g=738015&p=5275988]
[106]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management Practices for System and Organizations.* Ibidem. P.37.

implementación de una política de relación con proveedores y no realizaban una gestión efectiva de verificación de la calidad de los productos adquiridos[107].

Ahora bien, a partir de la DNIS 2, dicha política es de gran importancia para dar cumplimiento a la obligación establecida en el artículo 21 inciso "d" de la DNIS 2, relativa a la gestión de riesgo de la cadena de suministro.

Cabe destacar que al igual que la política de ciberseguridad, la política de relación con proveedores y cadena de suministro debe de ser aprobada por los órganos de administración de las organizaciones, quienes deben de orientar su cumplimiento, definir los roles y responsabilidades que estarán a cargo de su supervisión, y los recursos para su ejecución.

Resulta de gran utilidad para una correcta elaboración de la política previamente mencionada, el estándar ISO/IEC 27002:2022, ya que por medio del control 5.19 relativo a la seguridad de la información en las relaciones con los proveedores, y del control 5.21 relacionado a la gestión de la seguridad de la información en la cadena de suministro, detalla una serie de acciones preventivas que las entidades reguladas pueden realizar para mitigar los riesgos derivados de los proveedores y de su cadena de suministro.

Con el objetivo de facilitar la comprensión de dichos procedimientos, se expondrán los controles previamente indicados de manera conjunta, vinculados a las acciones y procesos que las entidades reguladas deben de realizar en los segmentos de proveedores, productos y servicios TIC y sus gestiones derivadas.

[107]ENISA. *Good Practices for Supply Chain Cybersecurity* Ibidem. P.19.

3.1) Acciones vinculadas a los proveedores:

Relación con proveedores	Cadena de suministro
Identificar a los proveedores que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.	En caso de que los proveedores subcontraten parte del servicio TIC suministrado, deberán de difundir los requisitos de seguridad establecidos por la entidad.
Establecer: a) criterios de evaluación para la selección de proveedores, y b) requisitos necesarios para garantizar una desvinculación segura con un proveedor. [108]	Obligar a los proveedores que propaguen prácticas de seguridad adecuadas, cuando los productos suministrados dependan de componentes proporcionados por terceros.
Establecer la información, servicios TIC e infraestructura física, las cuales podrán ser accedidas, supervisadas y utilizadas por proveedores.	Los proveedores deberán brindar información relacionada con: a) los componentes y elementos de software que utilizan los productos suministrados y b) las funciones de seguridad incorporadas en los productos, asi como la configuración para su funcionamiento seguro.
Establecer requisitos de seguridad de la información para cada tipo de proveedor y supervisar su cumplimiento por medio de revisión de terceros y verificación de los productos.	Regularizar procedimientos para el intercambio de información sobre la cadena de suministro, la gestión de problemas y compromisos entre la organización y los proveedores.

Haciendo énfasis en la identificación de los proveedores, para la ejecución de esta actividad, las empresas pueden realizar una clasificación en base a los riesgos inherentes que representen, dicha clasificación puede ser elaborada en base a métodos cualitativos o cuantitativos.

En el presente trabajo académico se expondrá el método cualitativo, el cual se caracteriza por ser subjetivo, sin embargo, en la práctica ha demostrado ser más ágil en su aplicación, sin sacrificar su eficacia en la gestión de riesgos[109].

[108] Se debe de realizar tomando en consideración los siguientes puntos: 1) la retirada de los derechos de acceso; 2) el tratamiento de la información; 3) la determinación de la titularidad de la propiedad intelectual desarrollada durante el contrato; 4) la portabilidad de la información en caso de cambio de proveedor o de contratación interna; 5) la gestión de registros; 6) la devolución de activos; 7) la eliminación segura de la información y otros activos asociados; 8) los requisitos de confidencialidad en curso. ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Seguridad de la información, ciberseguridad y protección de la* privacidad. Control de la seguridad de la información UNE-EN ISO/IEC 27002. Ibidem. Control 5.19.

[109] ESCUELA EUROPEA DE EXCELENCIA. *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger?* [En línea]. [Fecha de consulta: 29/06/2023]. [Disponible en:

Conforme esta clasificación[110], la consideración "Muy alto" corresponde a proveedores que pueden afectar el desarrollo y operatividad de un servicio crítico, incluyendo aquellos que pueden afectar la confidencialidad de la información sensible que se encuentre regulada en base a normativas legales.

La consideración "Alto" corresponde a proveedores que brinden servicios necesarios para la operatividad de la empresa, en consecuencia, una interrupción en sus servicios tendría un gran impacto, incluyendo aquellos proveedores que, por tener una alta conectividad con los sistemas informáticos de la empresa, en caso de sufrir un ciberataque, este podría expandirse a los sistemas propios.

La consideración "Medio" corresponde a proveedores que tengan acceso a información interna de la empresa y a los dispositivos tecnológicos de la empresa.

Por último, la consideración "Bajo" corresponde a proveedores que no brinden servicios ni productos tecnológicos que no pongan en riesgo la ciberseguridad de la empresa.

Como beneficio de haber implementado una clasificación en base riesgos, esto permite que, al momento de realizar una terminación con un proveedor, las organizaciones pueden ejecutarlas implementando un conjunto de buenas prácticas vinculadas a la clasificación asignada[111]. Cabe destacar que estas medidas son graduales y sucesivas, de modo que los proveedores clasificados[112] en la consideración de riesgo muy alto deberán cumplir con las acciones estipuladas en las consideraciones de riesgo, alto, medio y bajo.

Por lo tanto, a los proveedores clasificados en la consideración de riesgo "Muy Alto", la organización deberá de establecer un margen de tiempo que permita llevar a cabo la terminación sin que esta interrumpa el desarrollo de las actividades.

---

https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cual-escoger/#:~:text=La%20evaluaci%C3%B3n%20cualitativa%20es%20%C3%A1gil,para%20la%20toma%20de%20decisiones.]

[110] PEREZ. Ángel. et al. *Guía para la Gestión de Crisis por Ciberincidente en la cadena de suministro.* [En línea]. 1ª. Madrid. ISMS fórum. 2020. PP. 17-18. [Fecha de consulta: 30/06/2023]. [Disponible en: https://www.ismsforum.es/noticias/1581/consulta-la-gu-a-para-la-gesti-n-de-crisis-por-ciberincidente-en-la-cadena-de-suministro/]

[111] Idem.

[112] Se recomienda que previo al comienzo de todo servicio, el proveedor firme un contrato de confidencialidad, el cual indique que esta obligación tiene efectos post contractuales. Ibidem. P. 22.

A aquellos que se encuentran en la consideración de riesgo "Alto" y "Bajo", la organización debe de requerir que estos emitan un documento en donde conste que ha eliminado toda la información que obtuvo de la organización en el periodo de prestación de servicios.

Sucesivamente, a los ubicados en la consideración de riesgo "Medio", la organización debe de ejecutar las siguientes acciones: a) eliminar todos los permisos de acceso del proveedor; b) solicitar que el proveedor devuelva o borre la información sensible de la organización de sus sistemas de información y c) certificar que el proveedor ha devuelto todos los activos que obtuvo en el periodo en que brindo servicios.

3.2) Acciones vinculadas a los productos y servicios TIC:

Relación con proveedores	Cadena de suministro
Seleccionar y evaluar los productos o servicios que demuestren la implementación de medidas de ciberseguridad en el desarrollo o fabricación de estos, de modo que dichas medidas garanticen la seguridad de la información de la organización.	Definir los requisitos de seguridad que los productos o servicios TIC deben de poseer para poder ser adquiridos y posterior, supervisar y validar que estos sean cumplidos por los proveedores.
Definir la gestión de incidentes y contingencias derivadas de los productos o servicios tercerizados, tomando en consideración la responsabilidad de la organización o del proveedor.	Obtener garantía de que: 1) los componentes críticos sean rastreables a lo largo de la cadena de suministro; 2) los productos TIC suministrados funcionaran según lo esperado, sin contener alguna característica inesperada y no deseada y 3) los productos TIC cumplen con los niveles de seguridad requeridos.

Haciendo hincapié en la gestión de incidentes, vale la pena mencionar que esta es ejecutada por medio de un plan de respuesta[113], el cual es un documento interno de la organización que debe de establecer las responsabilidades, mecanismos metodológicos y organizativos para hacer frente a un incidente[114].

[113]Ibidem. PP. 29 -30.
[114]MORENO GARCIA. Maite. *Gestión de incidentes de ciberseguridad*. [En línea]. 1ª. Madrid. RA-MA Editorial. 2020. [Fecha de consulta: 07/07/2023]. [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/222669?page=72]

Consecutivamente, para garantizar una respuesta eficiente, es importante definir acciones tácticas que fomenten la coordinación y agilidad en el proceso de toma de decisiones. Así mismo, en este documento se deben clasificar y categorizar de manera proactiva los posibles tipos de ciberincidentes ante los cuales la organización puede estar expuesta, incluyendo acciones para minimizar sus efectos y valoración para determinar el nivel de criticidad y su impacto.

Debido a lo anterior, es fundamental identificar y establecer canales de comunicación con las partes interesadas. A su vez, para garantizar una gestión adecuada, el documento debe de establecer un proceso de escalamiento interno y externo de los ciberincidentes, incluyendo la notificación a las autoridades competentes cuando sea necesario.

Es esencial identificar los roles y responsabilidades de los participantes involucrados en la gestión del incidente. Además, se deben tomar medidas para mitigar los riesgos a los que la organización pueda estar expuesta. Por último, se requiere preparar la documentación necesaria para finalizar el incidente y restablecer las operaciones habituales.

De manera complementaria a los controles previamente mencionados de la ISO 27002:2022, se pueden añadir las siguientes acciones propuestas por la NIST SP 800-161r1[115]: 1) Establecer y referenciar una lista de proveedores prohibidos en base a regulaciones legales; 2) Establecer que los servicios de software suministrados por proveedores sean desarrollados en base a la obtención de software de código abierto de librerías examinadas y aprobadas.

[115]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management Practices for System and Organizations.* Ibidem. P. 38

3.3) Acciones vinculadas a gestión:

Relación con proveedores	Cadena de suministro
Gestionar y evaluar los tipos de riesgos asociados: a) por el uso que le puedan dar los proveedores y sus activos, tomando en consideración los riesgos asociados al mal uso intencional de sus empleados y b) por el mal desempeño y vulnerabilidades contenidas en los productos y programas informáticos adquiridos, así como los servicios brindados por los proveedores.	Implementar un proceso que permita la identificación de componentes críticos de los productos o servicios para el mantenimiento de su funcionalidad que sean subcontratados por los proveedores y que, por lo tanto, requieren especial atención y seguimiento.
Aplicar medidas de monitorización para poder detectar y mitigar los posibles riesgos derivados del incumplimiento de un proveedor.	Establecer procesos enfocados en: a) gestión de la información; b) el ciclo de vida, disponibilidad y los riesgos de seguridad de los componentes TIC; c) acciones o alternativas por aquellos componentes que dejen de estar disponibles o que se vuelvan obsoletos y d) identificación de proveedores alternativos de servicios TIC y el proceso de transferencia de software.
Gestionar las transferencias de información necesaria, incluyendo activos asociados y de cualquier otro elemento que deba de ser modificado, así como garantizar que la transferencia de información se mantenga segura durante todo el proceso.	La organización debe de implementar controles de evaluación y revisión de los componentes de los productos y servicios TIC para confirmar que son auténticos y han sido inalterados.

Por último, es importante mencionar que no existe un límite del alcance de supervisión de la cadena de suministro, sino que este responde a factores de criticidad, en donde se debe de tomar en cuenta la sensibilidad de la información que se intenta proteger, asi como la continuidad de los servicios esenciales que se intenta asegurar[116].

Por lo tanto, la implementación de las acciones y procesos previamente expuestos, debidamente establecidos en la política de ciberseguridad de relación de proveedores y la cadena de suministro de las TIC, deben de responder a criterios de proporcionalidad y ser contemplados en los contratos suscritos con los proveedores para obligar a su cumplimiento.

[116]ISACA. *Supply Chain Risk Management: Where Do We Start?*. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/supply-chain-risk-where-do-we-start]

CONCLUSIONES:

Estas conclusiones se redactan una vez desarrollados los objetivos planteados para este trabajo académico, y realizados los análisis e investigaciones pertinentes. El estudio se ha centrado especialmente dentro del marco legislativo de la Unión Europea vinculado a regulación de la cadena de suministro de las TIC, marcos de estandarización internacional y marcos de trabajo de ciberseguridad para hacer frente a los ciberriesgos inherentes a la cadena de suministro de las TIC. La Directiva Europea de Redes y Sistemas de Información (DNIS2) resulta muy relevante en estas páginas.

1. La ciberseguridad de la cadena de suministro de las TIC implica y obliga a una reformulación sobre los roles y responsabilidades de la ciberseguridad en la empresa. En este trabajo académico se identifican diferentes perspectivas relativas a cómo abordar los riesgos de la cadena de suministro desde la gobernanza, incluyendo su estructura, dirección estratégica y supervisión.

2. En la disciplina de la ciberseguridad, los estándares internacionales elaborados por la organización internacional de estandarización y la comisión electrónica internacional (ISO/IEC) junto con los marcos de trabajo (frameworks) desarrollados por el Instituto Nacional de estándares y Tecnología de los Estados Unidos de Norteamérica. Se presentan como herramientas de alta utilidad de aplicación voluntaria para las empresas. Incorporan medidas, controles, procesos y procedimientos que pueden ser implementados para la adecuada gobernanza de ciberseguridad, y para la gestión orientada a garantizar la seguridad de las redes y de sistemas de información. En este trabajo se analizaron los estándares ISO 31000:2018; 27002:2022 y 37000:2022, en conjunto con el marco de trabajo NIST SP 800-161r1 debido a que brindan una aproximación a la gobernanza enfocada en riesgo, así como las acciones y procesos que se deben considerar en la elaboración de la política de ciberseguridad en la relación con proveedores con un alcance a la cadena de suministro de las TIC. En términos de las exigencias regulatorias, pueden utilizarse para cumplir con los artículos 20 y 21 inciso “d” de la DNIS 2.

3. En la Unión Europea, la DNIS2 representa un paso de fortalecimiento de la ciberseguridad del mercado interior, de tal modo que las entidades reguladas por esta Directiva tienen la obligación de gestionar sus riesgos de cadena de suministro de las TIC. Con todo, el legislador europeo no brinda una definición sobre esta categoría de cadena de suministro. Sí que establece en cambio, que no todas las cadenas de suministro recibirán la misma atención, pues las cadenas de suministro críticas están sometidas a más regulación. Es importante que, en un futuro, la UE defina lo que considera cadena de suministro de las TIC y cadena de suministro críticas. Una delimitación centralizada a nivel europeo resulta mucho más oportuna que dejar que se lleve a cabo en los distintos Estados Miembro.

4. La investigación realizada sobre los roles y responsabilidades de la ciberseguridad, denota las diferentes perspectivas existentes en cómo abordar los riesgos de la cadena de suministro de las TIC, desde la estructura que se encarga de la supervisión, no obstante, considero acertado, que en razón de criterios tamaño y de dependencia de servicios o productos TIC suministrados por terceros, las compañías deberían de incorporar en su estructura de ciberseguridad, el rol de Director de la cadena de suministro (en inglés denominado, chief supply chain officer), asi como vincular distantes áreas, (como por ejemplo, adquisiciones, T.I y legal) en la gobernanza y control de ciberriesgo de la cadena de suministro.

5. La gobernanza del ciberriesgo conforme a DNIS2 y a los estándares internacionales analizados, se basa en situar al órgano de administración de las organizaciones frente a la aprobación de políticas y de su supervisión. Para ello, DNIS2 exige su formación periódica y actualizada. Sin embargo, la Directiva no especifica los conocimientos y capacidades mínimas que se espera que tengan los miembros de los órganos de administración de las entidades reguladas. Así mismo, se debe de considerar atendiendo a criterios de criticidad y proporcionalidad, que, para ser miembro del órgano de administración de una entidad regulada, el deber de ya constar con formación en ciberseguridad. Es importante que tales precisiones se desarrollen en legislación europea de desarrollo, y solo en menor medida, en los Estados miembros para garantizar la coherencia y homogeneidad en el plano europeo.

BIBLIOGRAFÍA:

AENOR. *Modelo para el gobierno de las TIC basado en las normas ISO*. [En línea]. 1ª. MADRID. AENOR INTERNACIONAL, S.A.U. 2012. [Fecha de consulta: 24/06/2023]. [Disponible en: https://tienda.aenor.com/libro-modelo-para-el-gobierno-de-las-tic-basado-en-las-normas-iso-10179]

ARROYO GUARDEÑO. David, GAYOSO MARTÍNEZ. Víctor y HERNÁNDEZ ENCINAS. Luis. *¿Qué sabemos de? Ciberseguridad*. [En línea]. 1ª. Madrid. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. [Fecha de consulta: 07/06/2023] [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/172144]

CENTRO CRIPTOLOGICO NACIONAL. *Aproximación a un marco de gobernanza*. [En línea]. Gobierno de España. Ministerio de Defensa. 2022 [Fecha de consulta: 27/06//2023]. [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6431-aproximacio-n-al-marco-de-gobernanza-de-la-ciberseguridad/file.html]

CENTRO CRIPTOLOGICO NACIONAL. *Ciber_Amenazas y tendencias*. Gobierno de España. [En línea]. Gobierno de España. Ministerio de Defensa. 2021. [Fecha de consulta: 21/05/2023] [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html]

ENISA. *Transport Threat Landscape Sector*. [En línea]. Publications Office of the European Union. 2023. [Fecha de consulta: 12/06/2023]. [Enlace de acceso: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape]

ENISA. *Good Practices for Supply Chain Cybersecurity*. [En línea]. Publications Office of the European Union. 2023. [Fecha de consulta: 30/06/2023]. [Disponible en: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity]

ENISA. *Informe panorama de amenazas de las enisa relacionadas con ataques a la cadena de suministro.* [En línea]. Oficina de publicaciones de la Unión Europea. 2021. [Fecha de consulta 10/05/2023]. [Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-supply-chain-attacks_es.pdf].

ENISA. *Threat Landscape 2022*. [En línea]. Publications Office of the European Union. 2022. [Fecha de consulta: 12/06/2023]. [Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022]

FORO NACIONAL DE CIBERSEGURIDAD. *Código de buen gobierno de la ciberseguridad.* [En línea]. Gobierno de España. Ministerio de la presidencia, relaciones con las cortes y memoria democrática. 2023. [Fecha de consulta: 13/07/2023]. [Disponible en: https://foronacionalciberseguridad.es/index.php/documentacion/publico/123-codigo-buen-gobierno-de-la-ciberseguridad/file]

GÓMEZ FERNÁNDEZ, Luis y FERNÁNDEZ RIVERO, Pedro. *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad*. [En línea]. 1. Madrid. AENOR - Asociación Española de Normalización y Certificación. 2018. [Fecha de consulta: 08/07/2023]. [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/53624?page=14]

GOMEZ HERVAS. Nuria del Carmen. *Normativa de ciberseguridad*. [En línea]. Edición: 1ªMadrid. Ra-Ma editorial. 2021. [Fecha de consulta: 16/06/2023]. [Disponible en: https://elibro-net.unileon.i dm.oclc.org/es/ereader/unileon/222663?page=4]

MORENO GARCIA. Maite. *Gestión de incidentes de ciberseguridad*. [En línea]. 1ª. Madrid. RA-MA Editorial. 2020. [Fecha de consulta: 07/07/2023]. [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/222669?page=72]

FUERTES. Mercedes. Soberanía Digital Europea. *El Cronista del Estado Social y Democrático de Derecho.* [En línea]. 2020. N° 90-91. Editorial Iustel. PP. 56-71. [Fecha de consulta: 13/07/2023]. [Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7666272]

NATIONAL CYBER SECURITY CENTRE. *Charting Your Course: Cyber Security Governance.* [En Linea]. New Zealand Government. 2022. [Fecha de consulta: 24/06/2023]. [Disponible en: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Governance.pdf]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Definition of Critical Software Under Executive Order (EO) 14028*. [En línea]. U.S. Department of Commerce. 2021. [Fecha de consulta: 25/05/2023] [Disponible en: https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf]

ORGANIZACIÓN DE ESTADOS AMERICANOS. *Ciberseguridad Marco NIST. Un abordaje integral de la ciberseguridad*. [En línea] 2019. [Fecha de consulta: 07/08/2023]. [Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf]

OECD LEGAL INSTRUMENTS. *Declaration on a Trusted, Sustainable and Inclusive Digital Future.* [En línea]. 2022. [Fecha de consulta: 19/06/2023]. [Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488]

ORTEGA CANDEL, José. *Ciberseguridad. Manual práctico*. 1ª. Santiago de Compostela. Ediciones Parainfo, SA. 2021.

PÉREZ CARRILLO. Elena, ALBOR BALTAR. Ángel. *GOBIERNO CORPORATIVO Y RESPONSABILIDAD SOCIAL DE LAS EMPRESAS.* 1ª. Madrid. Ediciones jurídicas y sociales, S.A. 2009.

PEREZ CARRILLO. Elena. Gobierno corporativo y ciberseguridad: algunos retos para el órgano administración. *Revista de Derecho de Sociedades*. [En línea]. 2023. Núm. 67. Editorial Aranzadi, S.A.U. PP. 2.1–2.19. [Fecha de consulta: 02/07/2023]. [Disponible en: https://proview-thomsonreuters-com.unileon.idm.oclc.org/title.html?redirect=true&titleKey=aranz%2Fperiodical%2F108262200%2Fv20230067.2&titleStage=F&titleAcct=i0adc41900000014d7b8f901e2b449b4f#sl=0&eid=90bdffaf151fb41e4a6082df3c775bd3&eat=%5Bereid%3D%2290bdffaf151fb41e4a6082df3c775bd3%22%5D&pg=I&psl=p&nvgS=fals]

PEREZ. Ángel. et al. 2020. *Guía para la Gestión de Crisis por Ciberincidente en la cadena de suministro*. [En línea]. 1ª. Madrid. ISMS fórum. 2020. [Fecha de consulta: 30/06/2023]. [Disponible en: https://www.ismsforum.es/noticias/1581/consulta-la-gu-a-para-la-gesti-n-de-crisis-por-ciberincidente-en-la-cadena-de-suministro/]

ROBLES CARRILLO. Margarita. *Análisis de la Directiva (UE) 2022/2055 sobre las medidas para garantizar un elevado nivel común de ciberseguridad en la Unión Europea (NIS 2).* 2023. Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad. Universidad de Vigo-INCIBE, pp. 367-374.

SANTIAGO, Enrique y ALLENDE, Jesús. Riesgos de ciberseguridad en las Empresas. *Revista Tecnologí@ y desarrollo.* [En línea]. 2017*, vol. 15, p. 1-33. [En línea]. [Fecha de consulta: 14/06/2023]. [Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174/964]*

SEVILLANO, Fernando y BELTRAN, Marta. *Dirección de seguridad y gestión del ciberriesgo*. [En línea]. 1ª, Madrid, RA-MA Editorial. 2020. [Fecha de consulta: 18/06/2023] [Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/222733?page=34]

THE HAGUE CENTRE FOR STRATEGIC STUDIES. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*. [En Linea]. 1ª. Bélgica. The European Economic and Social Committee. 2018. [Fecha de consulta: 18/06/2023]. [Disponible en: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf]

VIGURI CORDERO. Jorge. Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. *Revista de los Estudios de Derecho y Ciencia Política.* 2021. N°33. Pp. 1-12. [Fecha de consulta: 07/07/2023]. [Disponible en: https://doi.org/10.7238/idp.v0i33.376366]

LEGISLACIÓN, ESTANDARES Y MARCO DE TRABAJO:

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. T*ecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). visión de conjunto y vocabulario.* UNE-EN ISO/IEC 27000. Madrid: UNE. 2021.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.* UNE-ISO/IEC 27001. Madrid: UNE. 2023

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Seguridad de la información, ciberseguridad y protección de la* privacidad. Control de la seguridad de la información UNE-EN ISO/IEC 27002. Madrid. UNE: 2023.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN. *Especificación para los sistemas de gestión de la seguridad para la cadena de suministro.* UNE-ISO 28000. Madrid. UNE. 2008.

COMISIÓN EUROPEA. *Estrategia de Ciberseguridad de la UE para la Década Digital*. 2020. [En línea]. [Fecha de consulta: 21/06/2023]. [Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/IP_20_2391]

CONSEJO DE LA UNION EUROPEA. *El Consejo acuerda reforzar la seguridad de las cadenas de suministro de las TIC.* [En línea]. [Fecha de consulta: 17/06/2023]. [Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/]

COMISIÓN DE LAS COMUNIDADES EUROPEAS. *Comunicación de la comisión al consejo y al parlamento europeo relativa a las tecnologías de la información y de la comunicación en el ámbito del desarrollo. El papel de las TIC en la política comunitaria de desarrollo*. 2021. [En línea] [Fecha de consulta: 16/05/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52001DC0770&qid=1684593170662]

Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030 (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 323 de 19.12.2022, p. 4-26. [Fecha de consulta:14/06/2023. [Disponible en: https://eur-lex.europa.eu/eli/dec/2022/2481/oj]

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 333 de 27.12.2022. [Fecha de consulta: 19/06/2023]. [Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2555/oj]

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 sistemas de información en la Unión. Diario oficial de la Unión Europea: L 194 de 19.7.2016, p. 1-30. [Fecha de consulta: 09/06/2023] [Disponible en: https://eur-lex.europa.eu/eli/dir/2016/1148/oj]

Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (Texto pertinente a efectos del EEE). L 333, 27.12.2022, p. 164–198. [Fecha de consulta: 03/07/2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2557]

Dictamen del Comité Económico y Social Europeo sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 y sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la resiliencia de las entidades críticas [COM (2020) 823 final — 2020/0359 (COD) — COM (2020) 829 final — 2020/0365 (COD)]. Diario oficial de la Unión Europea: DO C 286 de 16.7.2021, p. 170-175. [Fecha de consulta: 28/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52020AE5749]

INTERNATIONAL STANDARD. *Information security, cybersecurity, and privacy protection – Guidance on managing information security risk*. ISO/IEC 27005. Switzerland. ISO/IEC 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *cybersecurity framework.* [En línea]. [Fecha de consulta: 28/06/2023]. [Disponible en: https://www.nist.gov/cyberframework/framework]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management Practices for System and Organizations*. [En linea]. 1ª. Gaithersburg. NIST. 2022. [Fecha de consulta: 30/06/2023]. [Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf].

PARLAMENTO EUROPEO. *Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital*. [En línea]. [Fecha de consulta: 18/06/2023] [Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_ES.html]

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020. [Fecha de consulta: 30/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52022PC0454]

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») (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 151, 7.6.2019, p. 15–69. [Fecha de consulta: 08/06/2023]. [Disponible en: https://eur-lex.europa.eu/eli/reg/2019/881/oj]

Reglamento (UE) n o 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE,

2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n o 1673/2006/CE del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE). Diario oficial de la Unión Europea: L 316 de 14.11.2012, p. 12. [Fecha de consulta: 19/06/2023]. [Disponible en: https://eur-lex.europa.eu/eli/reg/2012/1025/2015-10-07]

Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (Texto pertinente a efectos del EEE) [notificada con el número C (2003) 1422]. Diario oficial de la Unión Europea: L 124, 20.5.2003, p. 36–41. [Fecha de consulta: 10/06/2023]. [Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32003H0361]

Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G C/2019/2335. L 88 de 29.3.2019, p. 42/47. [Fecha de consulta: 08/07/2023]. [Disponible en: http://data.europa.eu/eli/reco/2019/534/oj]

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (BOE núm. 106 de 4 de mayo de 2002)

SITIOS WEB:

COMISIÓN EUROPEA. *Computación en la nube.* [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://digital-strategy.ec.europa.eu/es/policies/cloud-computing]

COMISIÓN EUROPEA. *Estado de la Unión: nuevas normas de la UE en materia de ciberseguridad garantizan unos equipos y programas informáticos más seguros.* [En línea]. [Fecha de consulta: 23/06/2023]. [Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5374]

CLOUDFLARE. *¿Qué es NaaS (red como servicio)?.* [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/network-as-a-service-naas/]

COMPLIANCE FORGE. Cybersecurity Supply Chain Risk Management (C-SCRM) Fundamentals. [En línea]. [Disponible en: https://www.complianceforge.com/free-guides/cybersecurity-supply-chain-risk-management-scrm]

ESCUELA EUROPEA DE EXCELENCIA. *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger.* [En línea]. [Fecha de consulta: 29/06/2023]. [Disponible en:https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cualescoger/#:~:text=La%20evaluaci%C3%B3n%20cualitativa%20es%20%C3%A1gil,para%20la%20toma%20de%20decisiones.]

FEDERAL VIRTUAL TRAINING ENVIRONMENT. *Cyber Supply Chain Risk Management for the Public.* [En línea]. [Fecha de consulta: 12/07/2023]. [Disponible en: https://fedvte.usalearning.gov/publiccourses/cscrm/index.htm?track=trackingon]

GOOGLE CLOULD. *¿Qué es IaaS?.* [En línea]. [Fecha de consulta: 27/06/2023]. [Disponible en: https://cloud.google.com/learn/what-is-iaas?hl=es#:~:text=La%20infraestructura%20como%20servicio%20(IaaS,a%20trav%C3%A9s%20de%20la%20nube .]

INCIBE. *Historias reales: la importancia de los acuerdos de nivel de servicio*. [En línea]. [Fecha de consulta: 27/06/2023]. [Disponible en: https://www.incibe.es/empresas/blog/historias-reales-importancia-los-acuerdos-nivel-servicio]

INCIBE. *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.* [En línea]. [Fecha de consulta: 19/06/2023]. [Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf]

INCIBE. *Cloud computing: una guía de aproximación para el empresario*. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.incibe.es/empresas/guias/cloud-computing-guia-aproximacion-el-empresario]

INCIBE. *Roles en ciberseguridad: desde el CEO a los usuarios finales* [En línea]. [Fecha de consulta: 26/06/2023]. [Disponible en: https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales]

ISO. *Benefits of standards.* [En línea]. [Fecha de consulta: 19/06/2023]. [Disponible en: https://www.iso.org/benefits-of-standards.html]

ISACA. Supply Chain Risk Management: *Where Do We Start?*. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/supply-chain-risk-where-do-we-start]

LOPEZ ANGEL. *Desarrollo seguro de software*. [En línea] [Fecha de consulta: 27/05/2023] [Disponible en: https://itcl.es/blog/desarrollo-seguro-de-software/]

MARQUARDAT ALEX. *Kaseya dice que menos de 1.500 empresas fueron afectadas por un ataque de ransomware*. [En línea] [Fecha de consulta: 21/05/2023] [Disponible en: https://cnnespanol.cnn.com/2021/07/06/kaseya-empresas-ciberataque-ransomware-trax/]

NACIONES UNIDAS. CEPAL. *Biblioguias – Biblioteca de la Cepal* [En línea]. [Fecha de consulta: 28/06/2023]. [Disponible en: https://biblioguias.cepal.org/c.php?g=738015&p=5275988]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Supply Chain Risk Management C-SCRM.* [En línea]. [Fecha de consulta: 11/07/2023]. [Disponible en: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management]

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*. [En línea]. [Fecha de la consulta: 19/06/2023]. [Disponible en: https://dpej.rae.es/lema/soft-law]

TELEFÓNICA. *Qué es el Cloud Computing: tipos y ventajas*. [En línea]. [Fecha de consulta: 03/07/2023]. [Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/que-es-el-cloud-computing-tipos-y-ventajas/]