ANÁLISIS Y PROPUESTAS RELATIVAS A LA SEGURIDAD DE LA CADENA DE SUMINISTRO

FORO NACIONAL DE CIBERSEGURIDAD

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

NIPO (edición on-line): 143-25-028-9
Fecha de edición: Septiembre 2025

ANÁLISIS Y PROPUESTAS RELATIVAS A LA SEGURIDAD DE LA CADENA DE SUMINISTRO

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen. El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes, quienes no necesariamente comparten todas las conclusiones o propuestas

EL FORO NACIONAL DE CIBERSEGURIDAD

MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

La Estrategia Nacional de Ciberseguridad, aprobada por el Consejo de Seguridad Nacional en abril de 2019, considera la colaboración público-privada como un elemento clave para impulsar la seguridad y confiabilidad del ciberespacio.

La propia Estrategia establece específicamente que dicha colaboración se articule a través del Foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la comunidad académica, asociaciones, organismos sin ánimo de lucro, entre otros, con el fin de potenciar y crear sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

El Foro Nacional de Ciberseguridad se constituye oficialmente en julio del año 2020, siguiendo el mandato de su creación acordado en el Consejo Nacional de Ciberseguridad. La composición del Foro responde a la pretensión de contar con la mayor representatividad posible de organismos públicos y de la sociedad civil en el ámbito de la ciberseguridad. Bajo la presidencia del Departamento de Seguridad Nacional y las vicepresidencias del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro Criptológico Nacional (CCN), el Foro está constituido por 18 organizaciones representantes de la sociedad civil, además de otros organismos con competencia en ciberseguridad.

El documento "**Análisis y propuestas relativas a la seguridad de la cadena de suministro**", elaborado por el Foro Nacional de Ciberseguridad, responde a la medida 8 de la línea de acción 2 de la Estrategia Nacional de Ciberseguridad: comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.

FORO
NACIONAL DE
CIBERSEGURIDAD

Agradecimientos

Coordinador institucional:

Oficina de Coordinación de Ciberseguridad (Ministerio del Interior)

Coordinador sociedad civil:

Félix Arteaga Martín. Real Instituto Elcano.

Javier Alonso Lecuit. Real Instituto Elcano.

Autores y colaboradores:

Maite Arcos
Lorenzo Avello
Herminio del Campo
Concepción Cordón
José Ramón Ferreira
Rogelio Flórez
Natalia Galán
Vanesa Gil
Borja Larrumbide
Francisco Lázaro
Pedro Pablo López *
Elena Maestre
Elena Marloa
Ángel Martínez
Verónica de Mata
Pedro Manuel Mosquera
Ramón Ortiz
Alberto Pinedo
Francisco Prados
Antonio Ramos *
Carlos Alberto Saiz
José Antonio Sánchez
Fernando Sanz de Galdeano

**editores*

ÍNDICE

ANÁLISIS DE LA SITUACIÓN

La seguridad, tanto física como lógica, de la cadena de suministro se ha convertido en un elemento fundamental de cualquier programa de seguridad. La utilización creciente de los proveedores por los agentes malintencionados como punto de entrada para sus ataques, unido al incremento de la regulación en esta materia y al amplio alcance que supone la aplicación de esta medida, ha convertido la seguridad de la cadena de suministro en uno de los mayores retos actuales para todas las compañías, especialmente para aquellas que operan en sectores críticos o esenciales.

Los retos principales para implementar un programa eficiente de gestión de riesgos de terceros serían los siguientes:

1. **La imposibilidad de que los usuarios supervisen a todos sus proveedores de servicio**.

   El enfoque habitual de las normativas existentes en materia de gestión de riesgos de terceros es depositar en el usuario de los servicios la responsabilidad de asegurar que sus proveedores cuenten con un nivel de ciberseguridad adecuado al procesamiento de información para los que se les va a utilizar. Aunque es evidente que sólo los usuarios de los servicios basados en tecnología pueden evaluar la criticidad de estos, no es menos cierto que el volumen de servicios de terceros utilizado con acceso a sistemas o información propias hace inviable una revisión exhaustiva de todos ellos. Además, resulta impracticable que los proveedores atiendan individualmente las solicitudes de cada cliente en materia de ciberseguridad.

2. **La ausencia de un mecanismo de certificación global aplicable a todos los casos de uso.**

   Aunque existen certificaciones específicas para ciertas situaciones, resulta difícil contar con un sistema universal que valore la especificidad de los servicios. Dependiendo del aspecto a evaluar —como privacidad, resiliencia, disponibilidad o ciberseguridad— y del análisis de riesgo correspondiente, hay múltiples certificaciones que ofrecen una visión parcial de los servicios. Por ejemplo, certificaciones como HIPAA o PCI-DSS garantizan ciertos aspectos en contextos específicos, pero no son aplicables a otros escenarios, como un sistema para un operador esencial en distribución eléctrica. Además, en algunos casos, se requiere evaluar servicios específicos para un cliente particular, lo que hace que las validaciones generales sean insuficientes.

   Esta diversidad de esquemas de evaluación genera esfuerzos dispersos y, en muchos casos, confunde más que ayuda a determinar si un servicio cuenta con un nivel adecuado de ciberseguridad.

3. **La ausencia de requisitos obligatorios para los proveedores de servicios**.

   El objetivo de estos requisitos sería asegurar, de manera general, el cumplimiento de medidas de seguridad para sus clientes y contribuyan a las acciones de diligencia debida, como facilitar auditorías, mostrar o compartir acreditaciones que demuestren el cumplimiento de niveles de seguridad necesarios, o monitorizar el cumplimiento de dichas medidas.

4. **Una regulación segmentada**, que dificulta la adhesión del ecosistema a unas reglas conocidas y generales.

5. **La ausencia de mecanismos de evaluación variados**, que limita la adaptabilidad a diferentes realidades, como pequeñas empresas, *startups* o sectores emergentes.

6. **La dificultad para evaluar toda la cadena de suministro de los proveedores**, especialmente en contextos donde múltiples actores participan en la prestación de servicios o fabricación de productos, lo que incrementa los riesgos y vulnerabilidades. La inclusión de estos actores en las evaluaciones de riesgo es compleja, ya que muchas veces se desconocen o se encuentran en el quinto, sexto o séptimo eslabón de la cadena de subcontrataciones.

7. **Las dificultades existentes para que los proveedores sean auditados en términos de seguridad contractual y para implementar acciones correctivas ante las debilidades detectadas**. Todo ello sin perjuicio de que las cláusulas de auditoría durante la prestación de servicios son generalmente aceptadas. Un ejemplo de ello, puede ser la comunicación a la hora de confirmar la gestión y resolución de determinadas vulnerabilidades de seguridad que han podido identificarse en la infraestructura utilizada para la provisión del servicio, por parte del proveedor, en el caso de que, a nivel contractual, se haya incluido algún control relativo a la gestión de vulnerabilidades.

En la tabla siguiente se ofrece un análisis de las principales normativas relacionadas con la seguridad en la cadena de suministro.

Norma	Descripción
RD 311/2022	Esquema Nacional de Seguridad Artículo 2 1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma. 2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que traten información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales. 3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Artículo 13 5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, [...]

Norma	Descripción
RDL seguridad de las redes 5G	El Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, establece que la protección la cadena de suministro en el contexto de las redes 5G es fundamental para garantizar la seguridad, la fiabilidad técnica, la independencia de injerencias externas y la diversificación que minimice los riesgos e impactos de contingencias en las redes y servicios de comunicaciones electrónicas. Esto implica el cumplimiento de estándares de seguridad, la certificación de productos y servicios, la diversificación de la cadena de suministro y la evaluación de riesgos. Artículo 4. Ámbito de aplicación. Este real decreto-ley se aplica a: a) Los operadores 5G. b) Los suministradores 5G. c) Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación.
Ley de Seguridad Privada	La Ley 5/2014, de 4 de abril, de Seguridad Privada, tiene por objeto regular la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y servicios de seguridad privada que, desarrollados por éstos, son contratados, voluntaria u obligatoriamente, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Artículo 51. Adopción de medidas 8. Quedarán sometidos a lo establecido en esta ley y en sus disposiciones de desarrollo los usuarios que, sin estar obligados, adopten medidas de seguridad, así como quienes adopten medidas de seguridad adicionales a las obligatorias, respecto de éstas.
Ley 19/2003 (inversiones extranjeras)	La Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención del blanqueo de capitales, considera importante proteger o garantizar la cadena de suministro frente a una inversión extranjera para asegurar la estabilidad y el buen funcionamiento de la economía de un país. Esto puede lograrse mediante la adopción de medidas adecuadas, como la suspensión del régimen de liberalización para ciertas inversiones extranjeras directas en España que puedan afectar al orden público, la seguridad pública y la salud pública, y la exigencia de requisitos específicos a las empresas extranjeras que deseen invertir en España.

Norma	Descripción
Directiva NIS2	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. Artículo 21.2. Las medidas a que se hace referencia en el apartado 1 se fundamentarán en un enfoque basado en todos los peligros que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a incidentes, e incluirán al menos los siguientes elementos: [...] d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos [...] Adicionalmente, se realizan, entre otras, menciones a la cadena de suministro en los considerandos 44, 56, 85, 90 y 91, así como en el artículo 7.2.a).
Directiva REC	La Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas, considera la importancia de garantizar la seguridad de la cadena de suministro, reconociendo cómo la perturbación de la misma puede tener repercusiones económicas y sociales negativas en múltiples sectores y a través de las fronteras. Este enfoque destaca la interdependencia de las entidades críticas y la necesidad de proteger la continuidad de la cadena de suministro en situaciones de crisis o perturbaciones. Artículo 12. [...] La evaluación de riesgos de la entidad crítica tendrá en cuenta el grado en que otros sectores indicados en el anexo dependen del servicio esencial prestado por dicha entidad crítica y el grado en que esta depende de otros servicios esenciales prestados por otras entidades en esos otros sectores [...]

Norma	Descripción
Reglamento DORA	El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero, conforme al cual todas las empresas deben asegurarse de que pueden resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse de ellas. Este Reglamento realiza un tratamiento profuso de esta temática al incluir todo un capítulo (V. Gestión del riesgo relacionado con las TIC derivado de terceros) con 17 artículos al respecto organizados en 2 secciones: Principios fundamentales de una buena gestión del riesgo relacionado con las TIC derivado de terceros y Marco de supervisión de los proveedores terceros esenciales de servicios de TIC.
Cyber Resilience Act	El Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, tiene por objeto fijar condiciones límite que permitan el desarrollo de productos con elementos digitales seguros, garantizando que los productos consistentes en equipos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto. También aspira a crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utiliza productos con elementos digitales. (10) El establecimiento de requisitos de ciberseguridad para la introducción en el mercado de productos con elementos digitales persigue la mejora de la ciberseguridad de dichos productos tanto para los consumidores como para las empresas. Esos requisitos garantizarán asimismo que se tenga en cuenta la ciberseguridad a lo largo de todas las cadenas de suministro, mejorando así la seguridad de los productos finales con elementos digitales.
RGPD	El Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos en la UE y el Espacio Económico Europeo (EEE). Artículo 28.1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

Norma	Descripción
Reglamento eIDAS	El Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, tiene como objetivo garantizar el correcto funcionamiento del mercado interior a la vez que se aspira a un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza. Artículo 20. Supervisión de los prestadores cualificados de servicios de confianza. 1. Los prestadores cualificados de servicios de confianza serán auditados, al menos cada 24 meses [...]. La finalidad de la auditoría será confirmar que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento. [...] Las normas utilizadas para estas auditorías han sido desarrolladas por CEN y ETSI como organismos de normalización europeos.
Cybersecurity Act	El 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, comparte la aspiración de alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión, en particular, desarrollando un marco de certificación de la ciberseguridad de ámbito europeo. Artículo 46.2. El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida. El primer esquema aprobado desde que entró en vigor el Reglamento ha sido el EUCC (*European Union Common Criteria*). Además, se han propuesto los esquemas EUCS (*European Cybersecurity Certification Scheme for Cloud Services*), *Identification of European Digital Identity* (EUDI) Wallets, y 5G.

A pesar de las dificultades mencionadas anteriormente, existen iniciativas que merecen ser destacadas, ya que demuestran mecanismos potencialmente útiles para abordar esta problemática:

- **Certificación del Esquema Nacional de Seguridad**. La regulación de los requisitos necesarios para trabajar con el sector público en España junto con la implementación de un sistema de certificación que valida el cumplimiento de dichos requisitos ejemplifica cómo la Administración puede regular que los proveedores adopten medidas para dar servicio a colectivos con unas necesidades similares.

- **Certificaciones de producto (LINCE y *Common Criteria*)**. La certificación LINCE, desarrollada recientemente por el CCN, es una metodología de evaluación basada en los principios de *Common Criteria*, pero orientada al análisis de vulnerabilidades. Incluye el listado de librerías de terceros que implementan funcionalidades de seguridad declaradas (SBOM - *Software Bill of Materials*) y realiza pruebas de intrusión, lo que reduce el esfuerzo, coste y duración del proceso, aunque con reconocimiento limitado a nivel nacional. Esta certificación permite a los productos certificados acceder al catálogo CPSTIC para niveles bajo y medio.

  Por otro lado, la certificación *Common Criteria*, en sus niveles superiores (EAL4 a EAL7), establece una serie de actividades de auditoría durante el ciclo de vida del producto. Estas actividades incluyen la auditoría de la cadena de suministro, la inspección del código fuente proporcionado por terceros e incluso visitas de inspección a las fábricas para verificar la implementación de medidas de seguridad técnicas, organizativas y procedimentales adecuadas.

- **Servicio de calificación de ciberseguridad Pinakes**. Se trata de un mecanismo dirigido a un grupo relativamente homogéneo, las entidades financieras españolas, que se caracteriza por utilizar una metodología de medición de la seguridad que no establece requisitos mínimos universales. En cambio, cada usuario determina, en función de su análisis de riesgos, el nivel de seguridad que considera necesario. Además, este mecanismo no es obligatorio; los proveedores de servicios pueden adherirse de manera voluntaria. Es importante señalar que muchas de las medidas del Esquema Nacional de Seguridad están integradas en este servicio.

- **Agencia de calificación para la cadena de suministro autorizada en Austria**. En este caso, existe un mecanismo autorizado por el Ministerio del Interior austriaco que homologa a entidades de calificación, cada una con su propio método, para evaluar la seguridad de los proveedores que desean prestar servicios a las entidades sujetas a la Directiva NIS.

Otras normas ISO susceptibles de tenerse en cuenta:

Norma ISO	Descripción
ISO 27001	Estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. Este estándar está incluido dentro del servicio de calificación de ciberseguridad de Pinakes.
ISO 27002	Estándar internacional que sirve como referencia para la implementación de controles en un Sistema de Gestión de Seguridad de la Información, incluyendo el control de acceso a datos, la protección criptográfica de información confidencial y la gestión de claves.
ISO 27017	Estándar internacional que proporciona controles para clientes y proveedores de servicios en la nube. Su importancia radica en la precisión con la que establece las relaciones entre ambos determinando qué puede exigir el cliente y qué información debe proporcionarle el proveedor. El cumplimiento de esta guía permite fortalecer la ciberseguridad y la gestión del servicio abarcando aspectos como la arquitectura, las medidas de seguridad, las funcionalidades disponibles, las tecnologías de cifrado y la localización geográfica de los datos.
ISO 27018	Estándar internacional que constituye un compendio de buenas prácticas referentes a controles de protección de datos para servicios en la nube, dirigido específicamente a los proveedores. Su objetivo central es delimitar las normas, procedimientos y controles que los proveedores, en su calidad de "procesadores de datos", deben aplicar. Además, garantiza el cumplimiento de la normativa legal en la gestión de datos personales.

Norma ISO	Descripción
ISO 27032	Estándar internacional que ofrece directrices para la seguridad en Internet y explica su relación con la seguridad web, la seguridad de la red y la ciberseguridad. Ofrece orientación de alto nivel para abordar problemas comunes de seguridad en Internet. Esta norma de ciberseguridad va dirigida a cualquier organización que utilice Internet, identifica las partes interesadas y describe sus funciones dentro de la seguridad de Internet. Además, fortalece y complementa otras normas de ciberseguridad como, por ejemplo, la UNE-ISO/IEC 27001:2023 sobre sistemas de gestión de la seguridad de la información y la UNE-EN ISO/IEC 27002:2023, que trata de los controles de la seguridad de la información.
ISO 27110	Estándar internacional que ofrece directrices para desarrollar marcos de ciberseguridad con el objetivo de proteger contra ciberataques. Se dirige a todo tipo de organizaciones, independientemente de su sector o su tamaño.
ISO 27701	Estándar internacional que nace de la publicación del Reglamento General de Protección de Datos (RGPD) el año 2018, y que propone implementar un Sistema de Gestión de Privacidad de la Información (SGPI) para la aplicación de políticas y controles que protejan los datos personales de la empresa, ya sea desde el punto de vista de Controlador de Datos Personales o de Procesador de Datos Personales.
ISO 28000	Estándar internacional que establece un marco de buenas prácticas para reducir los riesgos que enfrentan las personas y las cargas en la cadena de suministro. Facilita la gestión y mitigación de amenazas potenciales en logística, incluyendo el terrorismo, el fraude y la piratería.

Además, la Agencia de la UE para la ciberseguridad, ENISA, publicó el informe "G*ood Practices for Supply Chain Cybersecurity*" [1] que ofrece una visión general de las actuales prácticas de ciberseguridad en la cadena de suministro seguidas por entidades esenciales e importantes en la UE, basándose en los resultados de un estudio de ENISA de 2022 que se centró en las inversiones de los presupuestos de ciberseguridad de las organizaciones de la Unión.

Otra publicación de ENISA, en colaboración con el *Joint Research Centre* de la Comisión Europea, realizada a raíz de los análisis previos para el Reglamento de Ciber Resiliencia, es el estudio titulado "*Cyber Resilience Act Requirements Standards Mapping*"[2] , Este análisis busca identificar los estándares de ciberseguridad más relevantes para cada requisito de la directiva, evaluar la cobertura actual en relación con el alcance.

Tras analizar este escenario, se realizó un análisis de cuatro mecanismos de evaluación considerados relevantes para este estudio: Esquema Nacional de Seguridad, Norma ISO/IEC 27001, marco de calificación Pinakes e informes de auditoría SOC2. Este análisis ha servido de base para valorar las diferentes alternativas existentes, así como para formular las propuestas y recomendaciones que se detallan en este trabajo.

[1] https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[2] https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

EVALUACIÓN DE ALTERNATIVAS

Dado el volumen de organizaciones que componen actualmente la cadena de suministro de cualquier compañía, todas las alternativas posibles pasan por la aplicación de **proporcionalidad** en las medidas adoptadas:

- Proporcionalidad en el nivel de seguridad requerido a los terceros; y
- Proporcionalidad en el mecanismo de evaluación utilizado para asegurar la implementación de dichas medidas, en línea con los tres niveles de garantías, básico, sustancial y alto, definidos en el Reglamento Europeo de Certificación de Ciberseguridad (*Cybersecurity Act)*.

De esta manera, los proveedores responsables de servicios con un impacto potencialmente elevado, ya sea en la operativa de los servicios que prestan a sus clientes o en la gestión de información de alto valor, deberían cumplir con requisitos más estrictos y demostrarlo mediante mecanismos más rigurosos.

Certificación

Según la Asociación Española de Normalización (UNE), la certificación es el proceso llevado a cabo por una entidad reconocida como independiente de las partes interesadas, mediante el que se manifiesta la conformidad de una determinada empresa, producto, proceso, servicio o persona con los requisitos definidos en normas o especificaciones técnicas. Es decir, el resultado es dual, o se cumplen o no se cumplen los requisitos correspondientes.

Por lo tanto, los procesos de certificación se apoyan en estándares y normas técnicas desarrollados por organismos de normalización que tienen que ser previamente consensuados por los expertos y organizaciones representados en dichos organismos. Para definir los requisitos contenidos en las normas, generalmente se realiza un análisis de riesgos sobre un caso de uso específico y, posteriormente, se identifican las medidas necesarias para reducir el riesgo al nivel deseado.

PRO

- **Resultados altamente objetivos.**
- **Fomento de la competitividad entre certificadoras, con la consiguiente reducción de costes.**
- **Reducción de precios a medio plazo por la competencia entre certificadoras.**
- **Reutilización de los resultados.**
- **Alineamiento de las características de seguridad de productos a los requisitos para la certificación.**

CONTRA

- **Tiempo para el desarrollo de normas técnicas.**
- **Tiempo requerido para el propio proceso de certificación.**
- **Conversión del certificado en un objetivo en sí mismo (los clientes priman la facilidad de obtención).**
- **Comoditización[3] de la función de certificación.**
- **Rigidez del resultado (criterios poco flexibles).**

[3] La comoditización se refiere al proceso por el cual un producto o servicio, que inicialmente tenía características únicas o diferenciadas, se vuelve cada vez más similar a otros productos o servicios del mercado, hasta el punto de que los consumidores lo perciben como una "mercancía" o "commodity". En esencia, la comoditización reduce la percepción de valor único, lo que puede llevar a que la competencia se base principalmente en el precio.

Calificación

Los sistemas de calificación son muy variados y no se encuentran regulados de la misma manera que las certificaciones, sino que cada sistema aplica sus propios criterios y son los usuarios los que seleccionan aquellos que mejor responden a sus necesidades.

Los sistemas de calificación proporcionan una escala de valoración y un sistema de evaluación en el que cada calificadora, denominadas habitualmente agencias de calificación, da su opinión, en este caso, sobre el nivel de seguridad de un servicio o una organización.

El mayor valor de estos esquemas es proporcionar un mecanismo de transparencia mediante una escala (más o menos objetiva) que permite a los usuarios entender cuál es el nivel de seguridad de una organización o servicio sin necesidad de realizar una evaluación propia.

Ejemplos de sistemas de calificación serían las agencias de calificación crediticias, el sistema de estrellas de los hoteles o las evaluaciones de seguridad de los vehículos (EuroCAP).

PRO

- **Flexibilidad y reutilización de los resultados.**
- **Fácil interpretación del significado de la evaluación.**
- **Viabilidad económica.**
- **Velocidad de evolución de los criterios de evaluación.**
- **Fomento de los modelos que mejor evalúen.**

CONTRA

- **Convivencia de diversos modelos de calificación.**
- **Mercado no regulado.**

Auditoría

Las auditorías constituyen la base de la mayoría de los sistemas mencionados anteriormente, entendidas como auditorías de cumplimiento en ciberseguridad, no limitándose únicamente a auditorías técnicas como las de *hacking*. Es importante recordar que, en sí mismas, estas auditorías pueden generar resultados que los destinatarios de productos y servicios utilizan para comprender la seguridad de lo que desean emplear.

En particular, en el ámbito de los sistemas de información, se emplean auditorías conforme al estándar internacional ISAE 3000, conocidas como SOC (*Service Organization Controls*). Estas auditorías se pueden realizar respecto a cinco principios fundamentales: seguridad, disponibilidad, integridad, confidencialidad y privacidad.

Este proceso de evaluación es, quizás, el más riguroso de todos los mencionados, ya que requiere verificar la efectividad de los controles implementados. En el caso de los informes de tipo II, se evalúa la efectividad durante un período de cobertura, generalmente de doce meses, en contraste con los informes de tipo I, que solo evalúan el diseño de los controles. El auditor realiza un muestreo exhaustivo para asegurar que las medidas hayan sido efectivas a lo largo de dicho período.

Los auditores en este esquema deben ser organizaciones conocidas como "firmas de auditoría", similares a las que realizan auditorías de cuentas, dado que el régimen de responsabilidad es equivalente.

PRO

- **Necesidad de evaluación de la eficiencia de los controles en los 12 meses previos a la auditoría.**
- **Adaptabilidad de los criterios.**
- **Reputación y capacidad del auditor relevante para el proceso de selección.**

CONTRA

- **Coste elevado del proceso.**
- **Dificultad para la reutilización de resultados.**
- **Resultados subjetivos (criterio del auditor).**

Supervisión de la Administración Pública

Podríamos denominar a este proceso como "**homologación**", entendido la aprobación oficial de un servicio o producto. Este proceso implica que un organismo oficial verifique el cumplimiento de reglamentos técnicos o especificaciones establecidas por alguna entidad de la administración.

En ocasiones, la homologación requiere que se realicen ensayos o pruebas para comprobar que un producto, proceso o servicio cumple con los requisitos establecidos. En estos casos suele requerirse que los ensayos se lleven a cabo por laboratorios acreditados para garantizar su validez.

Es decir, que en ocasiones es la propia Administración Pública la encargada del proceso, pero también nos encontramos con situaciones en las que las Administraciones Públicas delegan esta supervisión técnica en terceros de confianza debidamente acreditados. Ejemplos de ello son la supervisión de las autorizaciones de instalaciones que utilizan espectro radioeléctrico, delegada en instituciones como los colegios profesionales, o la inspección técnica de vehículos (ITV), que se delega en empresas privadas debidamente acreditadas.

PRO

- **Eliminación de conflictos de intereses del evaluador.**
- **Homogeneidad de criterios.**
- **Validez general del resultado de la evaluación.**

CONTRA

- **Inviabilidad económica para la Administración.**
- **Tiempo para el desarrollo de especificaciones y las propias actividades de supervisión de los resultados.**

Declaraciones de conformidad

La declaración de conformidad es un documento elaborado por el propio interesado, en el que afirma que su producto o servicio cumple con las características establecidas por una norma o especificación técnica. Este proceso no involucra la participación de un tercero independiente y está permitido en ciertos casos.

PRO

- Bajo impacto en la rentabilidad de las compañías afectadas.

CONTRA

- Tiempo para el desarrollo de especificaciones.
- Bajo nivel de garantías proporcionado.
- Necesidad de desarrollar un marco supervisor y sancionador por la Administración Pública (evaluación a posteriori).

CONCLUSIONES Y PROPUESTAS

Tras analizar diversas alternativas, la conclusión principal es que, para garantizar un nivel adecuado de seguridad en la cadena de suministro, no existe un único mecanismo capaz de resolver todos los desafíos que implica que un ecosistema empresarial mejore su nivel de seguridad, teniendo en cuenta, además, que es fundamental establecer un sistema proporcionado que no exija niveles excesivos o insuficientes de seguridad.

Por ello, se propone:

- Establecer los principios fundamentales sobre los que se sustentaría el sistema.
- Simplificar la gobernanza del sistema, redistribuyendo responsabilidades entre todos los actores involucrados.
- Combinar diferentes mecanismos, como la opción más adecuada para mejorar la seguridad y la eficiencia del sistema.

Además, para conseguir una adecuada gestión del riesgo en la cadena de suministro se propone:

- Establecer un ámbito objetivo de aplicación.
- Definir un esquema combinado de medidas de seguridad mínimas y obligación de transparencia.
- Identificar las medidas mínimas exigibles a todos los actores.

Principios fundamentales

Sobre los principios fundamentales en los que se sustentaría el sistema, se destacan los siguientes:

1. **Responsabilidad**. Todos los agentes que participan en el mercado deben compartir la responsabilidad, cada uno, en función de su rol en el ecosistema.
2. **Transparencia**. Dado que unos agentes deben tomar decisiones en función de las medidas de seguridad de otros, es esencial mantener una adecuada transparencia sobre las capacidades de seguridad para garantizar un correcto funcionamiento del mercado.
3. **Armonización y seguridad jurídica**. Considerando la multiplicidad de normativas y estándares existentes en ciberseguridad, es necesario crear un entorno que facilite la integración de los esfuerzos realizados por diferentes organizaciones, independientemente del tipo de normativa (gobierno, gestión, eficiencia operativa, guías, etc.). Esto puede incluir la creación de marcos de supervisión sectoriales o comunes, ajustados a la criticidad de los servicios y con distintos niveles de exigencia.
4. **Proporcionalidad**. Reconociendo que existen múltiples casos de uso con impacto potencial diferente y que la cadena de suministro está compuesta por organizaciones de diferente índole (desde *start-ups*, a empresas multinacionales, pasando por pequeñas organizaciones o empresas de nicho), los requerimientos y mecanismos de conformidad deben ser proporcionales a las consecuencias de un incidente de ciberseguridad.
5. **Eficiencia, reducción de cargas administrativas y agilidad**. Cabe señalar que las obligaciones legales en materia de seguridad establecidas para los agentes que forman parte de una cadena de suministro deben alinearse con los principios de buena regulación establecidos en el artículo 129 de la *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*, y, en particular, incluyendo procesos ágiles y mecanismos de colaboración público-privada.

Gobernanza del sistema

En cuanto a la **distribución de responsabilidades** se propone:

- **La Administración**: definiría claramente la responsabilidad de cada agente en materia de seguridad dentro de la cadena de suministro. Es esencial que la Administración sea el último garante del cumplimiento de la normativa vigente, aunque no necesariamente realice toda la supervisión de forma exclusiva. Se puede establecer un mecanismo de colaboración público-privada para reducir la carga administrativa, reservando los recursos públicos para funciones imprescindibles como inspección y sanción, similar a otros ámbitos como las telecomunicaciones.

- **Los proveedores de servicios y productos**, especialmente aquellos que ofrecen soluciones tecnológicas: asumirían responsabilidades en la implementación de medidas de seguridad y en la transparencia hacia sus clientes.

- **Los usuarios de productos y servicios**: realizarían análisis de seguridad para asegurarse de que utilizan componentes alineados con su perfil de riesgo y el uso final de las tecnologías, mediante un proceso de debida diligencia (*due diligence*).

En relación con la **combinación de mecanismos** para aprovechar sus ventajas y reducir sus posibles debilidades se propone:

- Una **certificación** de medidas mínimas de seguridad para todos los productos y servicios.

- Una evaluación de las medidas de seguridad basada en sistemas de **calificación y auditoría**.

- Un sistema de **supervisión y control** por parte de la Administración, apoyado en la colaboración público-privada, para agilizar procedimientos, similar a los mecanismos de autorización de instalaciones radioeléctricas o las inspecciones técnicas de vehículos (ITV) con empresas certificadoras.

Establecimiento de un ámbito objetivo de aplicación

La regulación actual pone el foco en los destinatarios de los servicios y productos, requiriéndoles que ejerzan una debida diligencia en la contratación y que sólo homologuen o adquieran aquellos que reúnan las características adecuadas de protección para afrontar el escenario de riesgo existente. Este modelo no resultaría viable en una sociedad basada en la especialización y en la interconexión de actividades empresariales, ya que las dependencias existentes podrían considerarse "casi infinitas", imposibilitando que cualquier entidad, de manera aislada e independiente, asegure el correcto funcionamiento de toda la cadena de suministro necesaria para su actividad empresarial.

Por ello, se propone **definir un ámbito objetivo de aplicación y transparencia en las medidas de seguridad para todos los actores expuestos a riesgos de ciberseguridad en la prestación de sus servicios o en la fabricación de sus productos**.

Alternativamente, se podría identificar un conjunto de actividades empresariales que conllevasen estas mismas responsabilidades, tanto en la de implementación de medidas como en la transparencia respecto a ellas. El listado final de actividades debería incluir todas aquellas que potencialmente pudieran tener un impacto significativo en la actividad de sus clientes.

La evaluación del impacto que puede originarse en PYMES proveedoras de servicios es importante ya que son parte fundamental del tejido empresarial español. Existe la necesidad de considerar que existen proveedores pequeños o incluso *start-ups* que participan en las cadenas de suministro y que las medidas que se plateen deben reconocer esta pluralidad.

En este sentido, se es consciente de que el establecimiento de obligaciones adicionales en la legislación española podría afectar la competitividad del tejido productivo nacional. Por un lado, establecer requisitos en materia de ciberseguridad prepararía mejor a las empresas españolas para afrontar futuros incidentes cibernéticos en el medio y largo plazo. No obstante, en el corto plazo, estas empresas podrían experimentar una menor rentabilidad debido a los mayores costes operativos necesarios para cumplir con los niveles de seguridad exigidos. En consecuencia, en caso de superar ese posible empeoramiento competitivo en el corto plazo, las empresas españolas estarían mejor preparadas para abordar el futuro. Por tanto, sería necesario asegurar que todas aquellas empresas que quisieran ofrecer sus servicios o productos en España compitieran en igualdad de condiciones.

En resumen, **el ámbito de aplicación debería regirse por el mercado en el que la empresa ofrezca sus productos y servicios y no por la ubicación de su sede operativa o jurídica**. Esto implicaría aplicar un criterio similar al del Reglamento General de Protección de Datos, que obliga a quienes traten datos de ciudadanos europeos, independientemente de la ubicación de su sede social.

Esquema combinado de medidas mínimas de seguridad y obligación de transparencia

La definición de un esquema de medidas mínimas de seguridad que deben implementar todos los proveedores de servicios y productos supone un reto por varios motivos:

- Impacto en la competitividad del tejido empresarial español.
- Abundancia de pequeñas empresas, nuevas empresas y empresas de nicho con dificultades de acceso al conocimiento y recursos para implementar las medidas.
- Imposibilidad de estandarizar las medidas de seguridad necesarias para la amplísima variedad de escenarios de riesgo posibles.

Por ello, se propone adoptar una estrategia similar a la utilizada en otras actividades empresariales, como la restauración, la hostelería o la seguridad vial: establecer un conjunto de medidas mínimas de seguridad exigibles a todos los actores, junto con la obligación de transparencia respecto a las medidas de seguridad implementadas en los servicios y productos comercializados.

Esta propuesta facilitaría la creación de un mecanismo para asegurar que todos los servicios y productos comercializados cuentan con un nivel mínimo de seguridad, y, para cubrir el hecho cierto de que dichas medidas serán insuficientes para ciertos servicios (porque requerirán medidas mayores por su criticidad), la transparencia sobre las medidas de seguridad finalmente implementadas facilitarán que el destinatario de los mismos puedan entender el nivel de protección para poder hacer una adecuada evaluación del riesgo (debida diligencia requerida).

Este mecanismo también implicaría la aplicación combinada de mecanismos de conformidad, puesto que las medidas mínimas deberían ser objeto de certificación o de un mecanismo equivalente. Además, para garantizar la transparencia, se ofrecería libertad de elección en el mecanismo de conformidad, dejando a criterio del cliente decidir si el mecanismo presentado cumple con los niveles de garantías necesarios según sus requisitos de diligencia debida.

Para la aplicación del principio de transparencia, se podría proponer la existencia de un registro público que facilitase la compartición de información sobre las empresas proveedoras de servicios. En este registro figuraría la siguiente información:

- Datos de contacto en materia de ciberseguridad.
- Nivel de seguridad alcanzado y mecanismo de evaluación utilizado.

Esta información detallaría los diferentes servicios ofrecidos, que podrían tener diferentes niveles de seguridad, y la fecha de la última evaluación.

Considerando que esta medida sería aplicable a la industria en general, la entidad más adecuada para gestionar dicho registro podría ser el Instituto Nacional de Ciberseguridad de España (INCIBE).

Medidas mínimas exigibles a todos los actores

En aras de mantener los principios de proporcionalidad y responsabilidad que son el hilo conductor de las propuestas, se considera fundamental establecer las medidas mínimas que todos los actores deberían cumplir, según el ámbito de aplicación mencionado anteriormente.

Estas medidas mínimas, que deben ser aplicables a todo tipo de empresas, sectores y casos específicos, deben ser aspectos fundacionales de cualquier programa de seguridad. Al menos, estas medidas mínimas deberían incluir:

- Responsable o punto de contacto de ciberseguridad del proveedor.
- Existencia de una organización de seguridad y un marco normativo interno, que incluya normas internas y procedimientos establecidos.
- Existencia y aplicación sistemática de análisis de riesgos, para fundamentar las decisiones en materia de ciberseguridad.
- Clasificación de la Información y manejo conforme a la misma, incluyendo la devolución y el borrado seguro de la información.
- Medidas de seguridad en los equipos de usuario, especialmente cuando trabajan en instalaciones del cliente, particularmente en operadores esenciales o importantes.
- Realización periódica de escaneos de vulnerabilidades, incluyendo entornos simulados en caso de que la operación en producción no permita impactos potenciales.
- Capacidad de trazabilidad de acciones (logs), asegurando que en sistemas de control industrial estas capacidades no afecten la disponibilidad ni los tiempos de respuesta.
- Para actividades de desarrollo, implementación de procesos de desarrollo seguro.
- Procedimientos para gestionar incidentes de ciberseguridad, incluyendo la comunicación y la colaboración con los afectados hasta su resolución, a través de un punto de contacto definido, así como la compartición de Indicadores de Compromiso (IOC: *Indicators of Compromise*).
- Comunicación a las autoridades competentes, en función de la estructura organizacional, en caso de incidentes: autoridad competente de la que el proveedor dependa y en su ausencia, a la autoridad de control de coordinación y en ausencia de este, a las autoridades de control que sus clientes le hayan notificado.
- Formación mínima continua en ciberseguridad para los roles implicados en la gestión e implementación de las medidas, así como formación en aspectos legales y estratégicos para el personal directivo y órganos de administración.
- Acciones de concienciación para todo el personal, adaptadas a los riesgos y amenazas más habituales en materia de ciberseguridad.

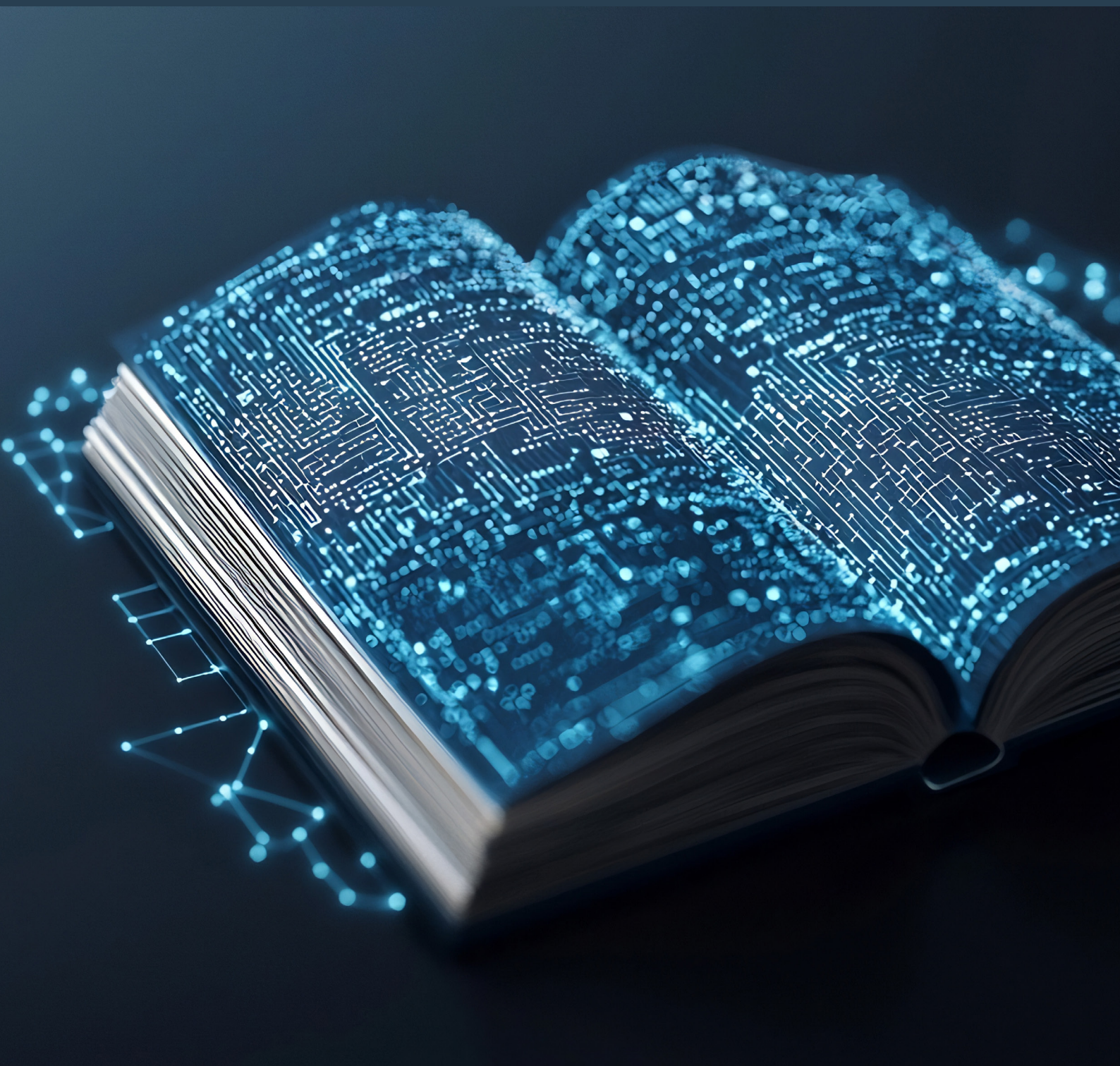
- Definición, implantación y monitorización de un programa de ciberseguridad.
- Responsabilidad de los órganos de dirección y administración en aprobar, supervisar y dotar de recursos adecuados al programa.
- Transparencia con los clientes respecto a las medidas de seguridad implementadas y los resultados de su supervisión, pudiendo optar por autoevaluaciones u otros métodos.
- Incluir en los contratos con clientes el compromiso de cumplimiento con estas medidas mínimas y, en particular, con la transparencia en materia de incidentes y medidas de seguridad implementadas.
- En contratos con proveedores que puedan afectar la ciberseguridad de sus servicios, incluir cláusulas de ciberseguridad similares.

Además, se recomienda establecer mecanismos de control para verificar el cumplimiento de estas medidas, proponiendo un sistema de certificación delegado a entidades acreditadas por la autoridad competente como, por ejemplo, la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior, para mejorar la eficiencia y facilitar el cumplimiento.

Este esquema de conformidad debería complementarse con mecanismos de calificación o similares que aseguren transparencia sobre el nivel de seguridad de los servicios ofrecidos, como la homologación por organismos competentes, similar al sistema utilizado en Austria.

Por último, se debería definir un régimen sancionador en caso de incumplimiento de estas medidas. Considerando que la mencionada Directiva NIS2 incluye esta provisión, se facilitaría la introducción de este régimen como parte del régimen general.

ANEXO I



DECÁLOGO DE RECOMENDACIONES

Este decálogo, presentado como buenas prácticas y recomendaciones, aborda la contratación de proveedores y sus servicios o productos en aspectos relacionados con la seguridad de la información, la ciberseguridad y la ciberresiliencia. Está estructurado en siete etapas vinculadas al ciclo de vida del proveedor en relación con el operador principal que lo contrata. Estas etapas se alinean con las buenas prácticas del NIST, la Metodología de Resiliencia ROSS 3.0 de Continuam y los Estándares UNE de externalización de procesos y servicios. Además, se complementan con dos acciones relacionadas con el posible cambio de proveedor y la finalización de sus servicios.

En total, son siete momentos en el ciclo de la cadena de suministro que el operador, junto con su personal como CISO, DPO, CIO y los departamentos de compras, soporte legal y auditoría, deben tener en cuenta y participar, con el apoyo necesario de recursos internos o externos.

Las etapas son:

1. Prevención - riesgos - evaluación y selección.
2. Detección/monitorización - seguridad integral - contratación e implementación y puesta en marcha.
3. Respuesta - incidentes/emergencias - gestión crisis y comunicación.
4. Recuperación - planes de contingencia y continuidad - protocolos y cooperación, colaboración y coordinación.
5. Superar - planes de resiliencia y ciber resiliencia -reevaluación lecciones aprendidas y mejora (mantenimiento).
6. Rescisión y finalización del servicio - riesgos - posibles impactos y consecuencia.
7. Post-finalización del servicio - acuerdos contractuales de salida - posibles compensaciones y cautelas.

Además, las recomendaciones se presentan agrupadas en dos categorías:

- **Básicas** - Aquellas recomendaciones que consideramos que pueden ser aplicadas por cualquier empresa, con independencia de su tamaño y sector.
- **Avanzadas** - Recomendaciones que requieren de una madurez más elevada en materia de ciberseguridad para poder ser aplicadas. Normalmente, esta madurez está asociada a un tamaño de compañía mayor, una dedicación a una actividad en la que la ciberseguridad sea esencial, o finalmente, un entorno productivo altamente tecnológico.

Prevención

Básicas

- Establecer un proceso de compras que permita seleccionar a los proveedores con la debida diligencia en materia de ciberseguridad, garantizando que ofrezcan servicios con un nivel de protección acorde a las necesidades.
- Comprobar experiencia en servicios y proyectos, tipos de clientes y *feedback* del sector.
- Solicitar las homologaciones, calificaciones y certificaciones que acrediten su postura de ciberseguridad para los servicios y productos ofrecidos, asegurando transparencia, resiliencia y cumplimiento legal.

Avanzadas

- Involucrar a todas las partes interesadas como Compras, Legal, Compliance, DPO, CISO, etc., para evaluar al proveedor y proponer a la Dirección la contratación del más adecuado, considerando más que solo costes.

Detección / monitorización

Básicas

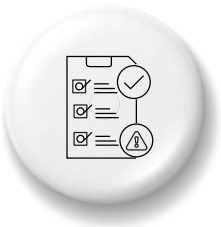
- Incluir una matriz RACI de responsabilidades[4], prestando especial atención a la distribución de actividades entre proveedor y cliente.
- Definir y mantener actualizados los contactos a niveles técnicos y soporte, gestión responsable servicio y comercial y gobierno a nivel directivo.
- Establecer cláusulas de privacidad, protección de datos y procesos de devolución.

Avanzadas

- Establecimiento de períodos mínimos para la rescisión unilateral de los servicios.
- Prever los sistemas de cambios y monitorización y mejora.
- Establecer los requisitos de formación y capacitación del personal del servicio así como los mecanismos para evitar los riesgos de *insiders*.
- Definir los clausulados de salida o cambio o vuelta del servicio al propio cliente.

[4] https://es.wikipedia.org/wiki/Matriz_de_asignaci%C3%B3n_de_responsabilidades

Respuesta



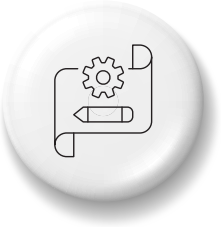
Básicas

- Implementar protocolos basados en escenarios para la respuesta a incidentes, identificando al personal técnico, de gestión y de gobierno involucrado previsto y actualizado.
- Crear mensajes predefinidos para comunicación en caso de incidentes.
- Establecer plazos máximos para la notificación de incidentes, en particular, aquellos que involucren datos de carácter personal.

Avanzadas

- Definir Acuerdos de Niveles de Servicio (ANS), indicadores y métricas.
- Acordar y formalizar los niveles de respuesta ante incidentes, incluyendo gestión de crisis, comunicación y recuperación.
- Entrenar protocolos de forma conjunta basados en escenarios para la respuesta a incidentes.
- Disponer de soluciones de localización, canales de comunicación y acceso a documentación e información.

Recuperación



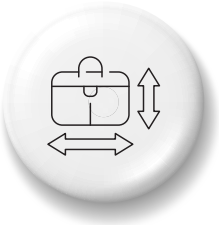
Básicas

- Definición de planes de contingencia y continuidad en caso de indisponibilidad del proveedor.
- Identificar los equipos y recursos necesarios para operar en caso de contingencia.

Avanzadas

- Realizar pruebas conjuntas de los planes de contingencia y continuidad basadas en escenarios, impactos y consecuencias potenciales.
- Analizar la interrelación y secuencias entre los planes de continuidad y contingencia de cliente y del proveedor.
- Colaborar con agentes externos, como instituciones y CSIRTs.

Superación (planes de resiliencia)



Básicas

- Realizar análisis y evaluación posterior sobre lo sucedido, la respuesta y la recuperación. Identificación de errores y oportunidades de mejora.
- Revisar protocolos, personal y herramientas.
- Reentrenamiento e identificación de habilidades adicionales necesarias.

Avanzadas

- Reentrenar al personal e identificar habilidades adicionales necesarias.

Rescisión y finalización del servicio

Básicas

- Ejecutar los procesos acordados para la devolución o destrucción de la información gestionada terceros.
- Eliminar los accesos y privilegios concedidos durante el ciclo de vida del servicio.

Avanzadas

- Asegurar la ejecución de los períodos de traspaso del proveedor saliente a un nuevo proveedor o al propio cliente.

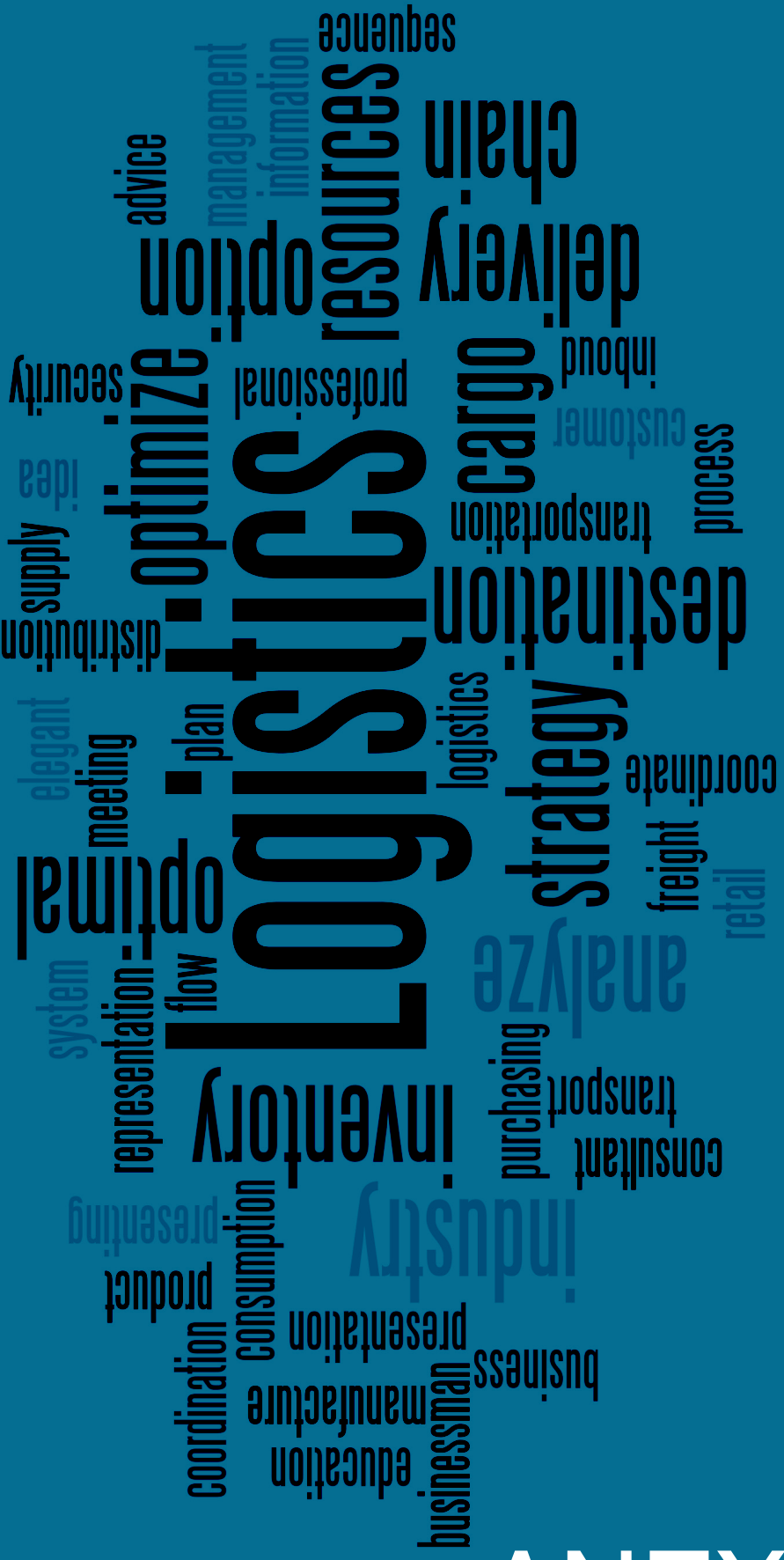
Post-finalización del servicio

Básicas

- Realizar análisis y evaluación posterior a la finalización de los servicios, identificando oportunidades de mejora.

Avanzadas

- Actualizar las condiciones de salida pre-establecidas en función de los problemas detectados en finalizaciones previas.
- Iniciar las acciones que fueran necesarias ante el potencial incumplimiento de las condiciones de salida.


sequence
resources
chain
delivery
option
advice
management
information
optimize
security
professional
cargo
inbound
customer
process
transportation
idea
supply
distribution
destination
Logistics
plan
logistics
strategy
coordinate
meeting
elegant
optimal
freight
retail
analyze
system
flow
representation
purchasing
consultant
transport
inventory
industry
presenting
product
consumption
coordination
presentation
business
manufacture
education
businessman

ANEXO II

INVERSIÓN EXTRANJERA Y CADENA DE SUMINISTRO

La *Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior*, considera importante proteger y garantizar la cadena de suministro para asegurar la estabilidad y el buen funcionamiento de la economía de un país.

Se considera que la protección o garantía de la cadena de suministro, según lo previsto en la *Ley 19/2003*, puede lograrse mediante la implementación de medidas adecuadas, como la suspensión del régimen de liberalización para ciertas inversiones extranjeras directas en España que puedan afectar el orden público, la seguridad pública y la salud pública, así como la exigencia de requisitos específicos a las empresas extranjeras interesadas en invertir en España.

Régimen jurídico actual sobre los movimientos de capitales y de las transacciones económicas con el exterior

- Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención del blanqueo de capitales.
- Real Decreto-ley 34/2020, de 17 de noviembre, de medidas urgentes de apoyo a la solvencia empresarial y al sector energético, y en materia tributaria, publicado en el BOE número 303, de 18 de noviembre de 2020, modificado por Real Decreto-ley 20/2022, de 27 de diciembre, de medidas de respuesta a las consecuencias económicas y sociales de la Guerra de Ucrania y de apoyo a la reconstrucción de la isla de La Palma y a otras situaciones de vulnerabilidad.

Importancia de la inversión extranjera en la cadena de suministro

La regulación de las inversiones extranjeras en la cadena de suministro de proveedores de infraestructuras críticas es de vital importancia para garantizar la seguridad y soberanía nacionales. Las infraestructuras críticas, tanto físicas como virtuales, son esenciales para el funcionamiento de la sociedad y la economía, abarcando sectores como energía, transporte, comunicaciones, etc.

Al regular las inversiones extranjeras en estos sectores, se busca prevenir posibles riesgos de seguridad, proteger la información sensible y asegurar el correcto funcionamiento de estas infraestructuras. La legislación establece criterios para determinar qué inversiones extranjeras pueden representar una amenaza para la seguridad pública, el orden público y la salud pública, y en base a ello suspender o requerir autorización previa para dichas inversiones.

Controlar las inversiones extranjeras en la cadena de suministro de proveedores de infraestructuras críticas, ayuda a evitar la dependencia excesiva de actores extranjeros, a proteger la información estratégica y a mantener la integridad de las operaciones en sectores vitales para el país, contribuyendo así, a la seguridad nacional y a la protección de los intereses fundamentales del Estado.

Amenaza de la inversión extranjera en la cadena de suministro

Se considera necesario valorar la inclusión de la inversión extranjera como una amenaza en la cadena de suministro, ya que podría derivar en una dependencia excesiva y en la transferencia de tecnología sensible o estratégica.

Existen diversas circunstancias que justifican esta evaluación, ya que una inversión de este tipo podría poner en riesgo la prestación de servicios críticos debido a fallas en la cadena de suministro. Dos de ellas podrían ser las siguientes:

- **Caso 1**.- La compra de capital o adquisición de derechos de una sociedad extranjera sobre una sociedad española que forme parte de la cadena de suministro esencial de un operador crítico, podría ser una amenaza en la medida en la que no exista ningún mecanismo normativo que obligue a la sociedad extranjera matriz a someterse al derecho español en lo que respecta a ese suministro.

- **Caso 2**.- La dependencia en la cadena de suministro de la sociedad española con la extranjera para la prestación del servicio esencial. Este caso es muy parecido al anterior, y podría, nuevamente, considerarse una amenaza en la medida en la que no exista ningún mecanismo normativo que obligue a la sociedad extranjera a someterse al derecho español.

Medidas contempladas en la actualidad

Artículo 7 bis de la Ley 19/2003, "Suspensión del régimen de liberalización de determinadas inversiones extranjeras directas en España", en su punto 2 "Queda suspendido el régimen de liberalización de las inversiones extranjeras directas en España, que se realicen en los sectores que se citan a continuación y que afectan al orden público, la seguridad pública y a la salud pública:

a) Infraestructuras críticas [5], ya sean físicas o virtuales [...]

b) Tecnologías críticas y de doble uso, tecnologías clave para el liderazgo y la capacitación industrial [...]

c) Suministro de insumos fundamentales, en particular energía [...]

d) Sectores con acceso a información sensible, en particular a datos personales [...]

[5] Lo que incluye, específicamente, a las infraestructuras de cables submarinos.

En el contexto de las amenazas previamente identificadas, sería necesario definir con precisión las medidas que podrían incorporarse, de modo que las entidades extranjeras quedasen sujetas a obligaciones equivalentes a las de las entidades nacionales.

Como medidas generales, se podrían incluir las siguientes obligaciones:

- Designación de sucursales en España.
- Designación de representaciones legales en España.
- Establecimiento de Acuerdos de Nivel de Servicio (ANS) en los contratos correspondientes u otras obligaciones contractuales.
- Resolución de conflictos en las relaciones contractuales, sometidos a la jurisdicción española y, en su defecto, a la de la Unión Europea.

Estas medidas deberían ser lo más amplias posibles e incluir tanto el reporte de incidentes y vulnerabilidades, como la obligación de establecer contramedidas para mitigar los riesgos asociados.

FORO
NACIONAL DE
CIBERSEGURIDAD