APORTACIONES DE ISMS FORUM AL ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD EN EL MARCO DEL PROCEDIMIENTO TRIS DERIVADO DE LA DIRECTIVA (UE) 2015/1535

Introducción

La Directiva (UE) 2022/2555 (NIS2) establece un marco normativo robusto y común para todos los estados miembros, para mejorar la ciberseguridad en toda la Unión Europea, imponiendo obligaciones significativas a una a las entidades que sean esenciales o importantes según los criterios que establece la propia Directiva.

Un análisis detallado de las leyes nacionales que transponen esta directiva (muchas de ellas todavía pendientes de aprobación) revela una **necesidad inherente, ya sea explícita o implícita, de que los operadores designen una figura con responsabilidades equivalentes a las de un Responsable de Seguridad de la Información (RSI) o Chief Information Security Officer (CISO).** Esta figura es absolutamente necesaria, para establecer un marco de gobierno y gestión de la ciberseguridad, sirviendo de enlace entre los órganos de dirección y muy especialmente, entre quién ostente la responsabilidad última de la ciberseguridad en ese órgano y la gestión táctica y operativa (cuando no también en su partición estratégica), que la actividad de la ciberseguridad requiere para ser eficiente y eficaz en su desempeño.

Sin embargo, la imposición de requisitos nacionales adicionales, como la acreditación obligatoria por parte del Ministerio del Interior en España, y más aún en una ley ajena a la ciberseguridad como es la ley de seguridad privada, genera preocupaciones significativas en cuanto a la armonización perseguida por la NIS2 y podría constituir un agravio comparativo perjudicial entre los profesionales europeos de la ciberseguridad.

La Figura del RSI/CISO en la Transposición de la NIS2

La propia estructura y las exigencias de la Directiva NIS2 hacen **indispensable** la existencia de una figura responsable de la ciberseguridad dentro de las entidades obligadas. Las legislaciones nacionales, al transponer las disposiciones de la NIS2, reflejan esta necesidad de diversas maneras:

- **España:** La **Ley que transpone la Directiva NIS2 establece de forma explícita la figura del Responsable de la Seguridad de la Información** tanto para entidades esenciales como importantes. El **artículo 16** detalla sus funciones como punto de contacto y coordinación técnica con las autoridades de control y los CSIRT. Además, en el caso de entidades esenciales, se exige que esta persona, unidad u órgano colegiado sea acreditado por el Ministerio del Interior.
- **Luxemburgo:** De manera similar, la legislación de Luxemburgo prevé la designación de un **"correspondant pour la sécurité"** para los operadores de infraestructuras críticas. Esta figura actúa como punto de contacto con el Alto Comisionado para la Protección Nacional en temas de seguridad, desempeñando un rol análogo al del RSI.

- **Alemania:** Si bien la ley alemana no exige explícitamente la designación de un "Informationssicherheitsbeauftragter" (ISB) o CISO para todas las entidades esenciales e importantes, sí establece obligaciones significativas en materia de gestión de riesgos y medidas organizativas y técnicas. La mención de una **"zentrale Anlaufstelle CSIRT" (punto de contacto central CSIRT)** subraya la necesidad de un interlocutor dentro de la organización para interactuar con los equipos de respuesta a incidentes de seguridad. Además, para las "besonders wichtige Einrichtungen" (instalaciones particularmente importantes) y "wichtige Einrichtungen" (instalaciones importantes), la implementación de medidas de seguridad requiere inherentemente la designación de personal responsable. A nivel de la administración pública federal, se fundamenta legalmente la figura del "Informationssicherheitsbeauftragte der Ressorts" (ISB de los Departamentos), lo que demuestra el reconocimiento de la necesidad de roles específicos en ciberseguridad.
- **Otros Estados Miembros:** Aunque los extractos de las legislaciones de **Bélgica, Dinamarca, Italia, Países Bajos, República Checa, Eslovenia u otros países de la Unión** no siempre mencionan explícitamente la figura del RSI/CISO, la **imposición de obligaciones detalladas** en áreas como la implementación de medidas de seguridad (artículo 15 de la ley española), la gestión y notificación de incidentes (artículo 17 y 18), la cooperación con las autoridades (artículo 23), y la gobernanza (artículo 14) **implica la necesidad práctica de que las entidades designen personal responsable para coordinar y supervisar estas actividades.** Sin un punto de contacto claro y una responsabilidad definida, el cumplimiento efectivo de estas obligaciones se vuelve altamente improbable.

El Requisito Español de Acreditación del RSI por el Ministerio del Interior: Un Potencial Agravio Comparativo y Obstáculo a la Armonización

La exigencia establecida en el **artículo 16.3 de la ley española** de que el Responsable de la Seguridad de la Información en entidades esenciales (y todo el de ciberseguridad en el caso de entidades críticas) deba ser **personal acreditado por el Ministerio del Interior**, bajo la ley de seguridad privada, plantea serias dudas sobre la armonización que persigue la Directiva NIS2 y podría generar un **agravio comparativo significativo entre los profesionales europeos de la ciberseguridad**.

Del análisis de las legislaciones de otros Estados Miembros proporcionadas, **no se desprende la existencia de un requisito similar de acreditación gubernamental obligatoria para la figura del RSI/CISO**. Si bien algunos países pueden establecer requisitos de competencia o formación, la imposición de una acreditación específica por un ministerio nacional es una **medida singular de la legislación española y alejada de la práctica de la ciberseguridad**.

La imposición de un requisito nacional de acreditación para los Responsables de Seguridad de la Información en España (o de igual forma si se incluyera en cualquier otro país de la UE) supone un obstáculo al reconocimiento mutuo de cualificaciones, ya que contraviene el objetivo de la Directiva NIS2 de establecer un nivel común de ciberseguridad en la Unión Europea. Además, esta exigencia va en contra del espíritu de libre circulación de trabajadores y del reconocimiento de cualificaciones consagrados en la normativa europea, como establece la Directiva 2005/36/CE relativa al reconocimiento de cualificaciones profesionales, cuyo propósito es facilitar el ejercicio profesional en los distintos Estados miembros. Por otra parte, un profesional cualificado en otro Estado miembro podría verse impedido de ejercer como CISO en España si no cuenta con esta acreditación, lo que vulnera el principio de libre circulación de trabajadores (TFUE, art. 45) y el derecho a ejercer una profesión (Carta de Derechos

Fundamentales de la UE, art. 15). De igual forma si otros países establecieran requisitos de certificación conforme a esquemas propios.

Hay que señalar muy especialmente que este requisito español resulta incompatible con el Reglamento (UE) 2019/881 relativo a ENISA, el cual establece como uno de sus principales objetivos la **armonización** en el ámbito de la ciberseguridad dentro de la Unión Europea, incluyendo la creación de **esquemas de certificación armonizados**. Existen numerosos aspectos de este Reglamento que resulta incompatibles con el requisito de certificación previsto por la transposición a la legislación española, como son:

- El considerando (68) reconoce que los esfuerzos pasados para el reconocimiento mutuo de certificados dentro de la Unión solo han tenido un éxito parcial, mencionando el Acuerdo de Reconocimiento Mutuo (ARM) del SOG-IS como ejemplo limitado. Esto subraya la necesidad de un enfoque más amplio y armonizado.
- El considerando (69) afirma explícitamente la necesidad de adoptar un **"planteamiento común y establecer un marco europeo de certificación de la ciberseguridad"** que permita que los certificados sean reconocidos y usados en todos los Estados miembros. Se menciona como objetivo evitar la "multiplicación de los esquemas de certificaciones nacionales de la ciberseguridad contradictorias o redundantes" para reducir costes para las empresas en el mercado único digital.
- El artículo 1, apartado 1, letra b), del reglamento establece como uno de sus objetivos la creación de **"un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión"**. Este artículo define claramente la intención de armonizar a través de esquemas europeos y prevenir la fragmentación por esquemas nacionales.
- El artículo 46, apartado 1, declara la creación del "marco europeo de certificación de la ciberseguridad con el fin de **mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad**". Este artículo enfatiza el vínculo entre la certificación armonizada y la mejora del mercado interior.
- El artículo 49 detalla el proceso para la preparación, adopción y revisión de los esquemas europeos de certificación de la ciberseguridad, implicando la participación de ENISA, la Comisión y el Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad (GECC). Este proceso a nivel europeo busca asegurar la **coherencia y armonización** de los esquemas.
- El artículo 57, apartado 2, establece que los Estados miembros deben abstenerse de introducir nuevos esquemas nacionales de certificación de la ciberseguridad para productos, servicios y procesos de TIC cubiertos por un esquema europeo de certificación de la ciberseguridad en vigor, buscando así **reemplazar los esquemas nacionales por los europeos armonizados**.

En resumen, el Reglamento ENISA tiene un fuerte enfoque en la **armonización de la ciberseguridad en la Unión Europea** a través de la creación de **esquemas europeos de certificación de la ciberseguridad**. El objetivo es establecer un marco común que evite la fragmentación del mercado interior causada por la proliferación de esquemas nacionales divergentes, promoviendo el reconocimiento mutuo de los certificados y elevando el nivel general de ciberseguridad en toda la Unión.

Al exigir una acreditación específica para los CISOs de entidades esenciales y, en el caso de entidades críticas, también para el resto del personal de ciberseguridad, España se aparta del modelo promovido por ENISA, comprometiendo la coherencia del sistema europeo de certificación. Esta medida no solo dificulta la movilidad profesional dentro del mercado único, sino que también puede interpretarse como una barrera injustificada para el ejercicio de la profesión en otros países y para la atracción de talento de otros Estados Miembros a España.

El Requisito Español de Acreditación del RSI por el Ministerio del Interior: inadecuado, desproporcionado y generador de costes innecesarios

El requisito de certificación como medida obligatoria y generalizada en la transposición española resulta inadecuado, desproporcionado e innecesario (por ejemplo, siendo un generador de costes innecesarios). Este hecho se refleja en el propio contenido del documento:

- **Flexibilidad en las medidas de gestión de riesgos:** La Directiva NIS2 se centra en establecer un marco para la gestión de riesgos de ciberseguridad y obligaciones de notificación. Si bien fomenta el uso de normas técnicas y la certificación como medios para demostrar el cumplimiento, no impone explícitamente la certificación como un requisito obligatorio y universal para todas las entidades. El anteproyecto de ley español indica que el Centro Nacional de Ciberseguridad determinará las medidas técnicas, operativas y de organización adecuadas y proporcionadas, tomando como base el Esquema Nacional de Seguridad y normas equivalentes, y que incluso podrá aprobar perfiles específicos de cumplimiento. Esta flexibilidad sugiere que el cumplimiento puede demostrarse a través de diversos medios, no únicamente mediante una certificación obligatoria.
- **Consideraciones de coste y carga administrativa:** La imposición de una certificación obligatoria para un amplio número de entidades, incluyendo las importantes, podría generar costes significativos y una carga administrativa considerable. De hecho, en la memoria que acompaña la propuesta de ley española, se contabiliza como una fuente de ingresos para el estado una nueva acreditación, denominada “Director de Ciberseguridad”. El principio de proporcionalidad, mencionado en el contexto de la elaboración de la ley española, aboga por que las obligaciones impuestas sean mínimas y suficientes para cumplir los objetivos, lo que cuestiona la necesidad de una certificación obligatoria generalizada.
- **Mecanismos alternativos de supervisión y cumplimiento:** La Directiva NIS2 prevé mecanismos de supervisión y ejecución por parte de las autoridades competentes. Estas autoridades pueden requerir información, realizar auditorías y adoptar otras medidas para garantizar el cumplimiento. La existencia de estos mecanismos sugiere que la certificación obligatoria para todas las entidades no es el único medio para asegurar un nivel elevado de ciberseguridad. El anteproyecto de ley español detalla las funciones de supervisión y ejecución sobre entidades esenciales e importantes, lo que refuerza la idea de que el cumplimiento puede verificarse de diversas maneras.
- **La propia Directiva no exige una certificación obligatoria universal:** Al revisar el contenido de la Directiva NIS2 a través de las transposiciones nacionales, se observa que, si bien se menciona la certificación y se establecen las bases para esquemas de certificación europeos (como se relaciona con el Reglamento ENISA), **no se articula un mandato de certificación para las entidades cubiertas por la directiva**.

Adicionalmente deberíamos tener en cuenta que la acreditación se produciría bajo la Ley de seguridad privada, Ley 5/2014, en concreto en su desarrollo. Esta ley, lleva quince (15) años a la espera de un reglamento que la desarrolle. Ese reglamento, por falta de consenso no ha visto la luz en ese largo periodo; por tanto, no es realista confiar en que dicha ley se adapte con la necesaria rapidez a los desafíos que la ciberseguridad y sus profesionales requieren.

En conclusión, si bien la certificación puede ser una herramienta valiosa para demostrar el cumplimiento de las medidas de ciberseguridad, imponerla como un requisito obligatorio y generalizado para la transposición de la Directiva NIS2 podría ser desproporcionado y generar costes innecesarios para las entidades, no siendo estrictamente exigido por la propia directiva, que aboga por un enfoque basado en el riesgo y permite la existencia de mecanismos alternativos para garantizar el cumplimiento y la supervisión.

Recomendación y Conclusión

Si bien la designación de una figura responsable de la ciberseguridad es fundamental para el cumplimiento de la Directiva NIS2, la **exigencia específica de acreditación por el Ministerio del Interior en España y máxime en una ley (Ley 5/2014) la ley de seguridad privada alejada de la cultura, los conocimientos y la práctica de los profesionales de la ciberseguridad, parece a todas luces inadecuada, innecesaria, costosa y potencialmente perjudicial para la armonización y la movilidad profesional.**

Se **recomienda encarecidamente al legislador que valore la eliminación de este requisito de acreditación obligatoria** para la figura del Responsable de Seguridad de la Información. En su lugar, se podrían explorar mecanismos que fomenten la competencia y la formación continua en ciberseguridad, alineados con estándares europeos e internacionales, facilitando así la movilidad de los profesionales y promoviendo un mercado laboral de la ciberseguridad más integrado y competitivo en la Unión Europea. Mantener este requisito podría interpretarse como una **restricción desproporcionada a la libre circulación de trabajadores y al reconocimiento mutuo de cualificaciones**, principios fundamentales del mercado interior europeo.

La eliminación de esta exigencia de la transposición española contribuiría a una transposición más armónica de la Directiva NIS2, beneficiando tanto a los profesionales europeos como al objetivo general de alcanzar un elevado nivel común de ciberseguridad en toda la Unión Europea.