NOTA INFORMATIVA

Novedades en la transposición de NIS 2

Análisis del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, por el que se lleva a cabo la transposición a nuestro Ordenamiento Jurídico de la Directiva 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea (en adelante "**NIS 2**" o la "**Directiva**").

Uso público

Lo que necesitas saber

- El pasado 14 de enero ha sido aprobado por el Consejo de Ministros el anteproyecto de **Ley de Coordinación y Gobernanza de la Ciberseguridad** que tiene como objeto transponer al Ordenamiento Jurídico español la Directiva NIS 2.

- En él se **amplían** los Sectores considerados como "críticos" a los efectos del ámbito de aplicación.

- Se configura el **marco institucional** para la gobernanza de la ciberseguridad en España.

- Las **medidas** de gestión de riesgos de ciberseguridad se "inspirarán" en el ENS, y por tanto cumplir con el ENS garantizará cumplir con NIS 2.

- Las Autoridades de Control podrán llevar a cabo **inspecciones** *in situ* y aleatorias y solicitar cualesquiera evidencias requieran para verificar el nivel de cumplimiento de las medidas de seguridad.

- Las **sanciones** por incumplimiento se impondrán con carácter solidario a entidades y directivos, pudiendo alcanzar la cuantía de hasta 10.000.000 € o el 2% de facturación

Parece que la esperada transposición de la Directiva NIS 2 a nuestro Ordenamiento Jurídico va tomando forma. El plazo para ello expiró el pasado 17 de octubre de 2024, aunque algunos de los Estados Miembros, como es el caso de nuestro país, no llegaron a tiempo. Así, aunque tarde, ya ha sido aprobado en Consejo de Ministros el borrador para la norma que se encargará de transponer las directrices de NIS 2 en España, y su tramitación parlamentaria se hará por la vía de urgencia.

El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (en adelante el "**Anteproyecto de Ley**" o el "**Anteproyecto**") trae consigo algunas novedades respecto de la Directiva, así como define algunos aspectos fundamentales que debían ser objeto de desarrollo por parte de los legisladores nacionales.

(I) Ampliación de los sectores vinculados

La norma tiene por objeto el establecimiento de medidas para alcanzar un elevado nivel común de ciberseguridad en España y en la Unión Europea. Por medio de su transposición, se amplían los ámbitos de aplicación originales de la Directiva a dos (2) nuevos sectores:

- **Sector Industria Nuclear**: Centrales nucleares y entidades relacionadas con la utilización, producción, almacenamiento y transporte de mercancías y materiales nucleares o radiológicos.

- **Sector Seguridad Privada**: Empresas de seguridad privada y despachos de detectives conforme lo recogido en la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Las obligaciones de la norma se aplican en función de la importancia de la entidad sujeto de aplicación, distinguiéndose entre "**entidades esenciales**" o "**entidades importantes**". Cabe destacar con respecto a las primeras el régimen de "autoevaluación" implementado por el Anteproyecto. Conforme al mismo las entidades deberán evaluar su inclusión en las categorías de esenciales e importantes, de conformidad con los criterios recogidos en los artículos 4.1 y 4.2, y remitir dicha información a las Autoridades de Control. Adicionalmente, la Autoridad de Control podrá por iniciativa propia identificar a entidades esenciales por su impacto en la sociedad española.

Por su parte, serán entidades importantes todas aquellas que no puedan considerarse como entidades esenciales.

(II) Marco institucional

El Anteproyecto de Ley se encarga de configurar el que será el marco institucional para la ciberseguridad en España.

Por un lado, prevé la creación de un **Centro Nacional de Ciberseguridad**, con competencia única en materia de gobernanza de la ciberseguridad a nivel nacional, y punto de contacto único para garantizar la cooperación transfronteriza y competencia para la coordinación de las autoridades de control y de los puntos de contacto sectoriales.

Serán tres (3) las **Autoridades de Control** encargadas de las funciones de supervisión y ejecución de la norma. Cada una se encuentra asociada a uno de los tres (3) Ministerios implicados:

- **Centro Criptológico Nacional**: asociado al Ministerio de Defensa.
- **Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y la Secretaría de Estado de Digitalización e Inteligencia Artificial**: asociadas al Ministerio para la Transformación Digital y de la Función Pública.
- **Oficina de la Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad:** asociada al Ministerio del Interior.

A su vez, por cada uno de los Sectores identificados, se designará un **punto de contacto sectorial**.

Por último, designa como Equipos de respuesta a incidentes de ciberseguridad o "**CSIRT**" al CCN; para entidades del sector público, al INCIBE; para el resto de las entidades y al ESPDEF-CERT; en aquellas situaciones que los primeros requieran y, necesariamente, en las relativas a incidentes de entidades con incidencia en la Defensa Nacional.

(III) Medidas para la gestión de riesgos de ciberseguridad

El paquete de medidas que configura el Anteproyecto toma como referencia los perfiles de cumplimiento del Esquema Nacional de Seguridad ("**ENS**") aplicado al contenido de NIS2. En este punto se indica que las entidades esenciales tendrán que poseer dicha certificación, mientras que las importantes podrán optar por dicha una certificación o por una autoevaluación de estado de la seguridad.

Para asegurar el establecimiento de estas medidas las entidades deberán designar la persona, entidad u órgano colegiado que asuma el rol de **Responsable de seguridad de la información**.

Mención aparte merecen las obligaciones relativas a la **gestión de incidentes** de seguridad que afecten a las redes y sistemas de información empleados en su operativa, tanto si son estas propias como si pertenecen a proveedores externos.

- **¿Cómo?**: a sus CSIRT preferentemente a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.
- **¿Qué?**: abarcarán cualquier incidente y/o ciberamenaza significativo/a, así como de forma voluntaria cualquier ciberincidente, ciberamenaza y cuasi incidente que consideren.
- **¿Cuándo?**: en el plazo de 24 horas desde que se tenga constancia de ello.
- **¿indicios delictivos?**: las entidades deberán especificar en la notificación que realicen de los ciberincidentes significativos cuando sospechen que pueda existir intencionalidad y no se traten de hechos accidentales o fortuitos, los cuales serán tratados con la finalidad de ponerlos en conocimiento del Ministerio Fiscal por parte de la Oficina de Coordinación de Ciberseguridad conforme a lo establecido por el artículo 21 y Disposición Adicional 5ª del Anteproyecto.

(IV) Régimen de supervisión y ejecución

Las Autoridades de Control, bajo la dirección del Centro Nacional de Ciberseguridad, tienen la responsabilidad de supervisar y adoptar las medidas necesarias para asegurar que las entidades sujetas al ámbito de aplicación de la norma cumplan con ella.

El régimen de supervisión y ejecución varía en función de la clasificación de la entidad. En particular, el artículo 32 establece que la supervisión de las entidades importantes se realizará **a posteriori**, es decir, siempre que se disponga de indicios, pruebas o información de que una entidad presuntamente no cumple con la ley. Por su parte, las entidades esenciales podrán ser inspeccionadas **a priori** o **a posteriori**.

La actividad de supervisión podrá consistir en inspecciones in situ y controles aleatorios, así como en el marco de las Auditorías de seguridad periódicas llevadas a cabo por una Entidad de Certificación del ENS, cuando resulte de aplicación.

(V) Sanciones

Por último, el Anteproyecto de Ley desarrolla el régimen sancionador, categorizando las infracciones en muy graves, graves y leves, y haciendo responsables, tanto a la entidad autora del hecho que dé lugar a la infracción como a los miembros del órgano de dirección de las entidades, que responderán de manera **solidaria** por las infracciones cometidas por la entidad, conforme a su artículo 35.2.

Las sanciones previstas podrán alcanzar los 10.000.000 de euros para las entidades esenciales o una cuantía equivalente al 2% del volumen de negocio anual total a nivel mundial de la empresa a la que pertenece la entidad durante el ejercicio financiero anterior, optándose por la mayor cuantía

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60