ASEPEC

ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD QUE TRANSPONE LA DIRECTIVA NIS2: NOVEDADES PARA LOS PRESTADORES DE SERVICIOS DE CONFIANZA CUALIFICADOS (QTSP)

Avanza la esperada transposición al ordenamiento jurídico español de la 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 (en adelante, "Directiva NIS2" o "NIS2").

El pasado 14 de enero, el Consejo de Ministros aprobó el anteproyecto de "Ley de Coordinación y Gobernanza de la Ciberseguridad", cuyo objetivo es incorporar al ordenamiento jurídico nacional las directrices de la Directiva NIS2 y su tramitación parlamentaria se realizará por la vía de urgencia, teniendo en cuenta que el plazo concedido a los Estados Miembros para la transposición venció el pasado 17 de octubre de 2024.

Para los Prestadores Cualificados de Servicios de Confianza nacionales la carrera para la adaptación de sus servicios a NIS2 ya se inició en la práctica, motivados fundamentalmente por los cambios relevantes que se han sucedido en 2024 a nivel europeo. En un primer momento por la modificación del estándar técnico ETSI EN 319 401 en su versión 3.1.1. (2024-06) para incorporar los requisitos de ciberseguridad de NIS2, cuya aplicación obligatoria debía comenzar el 28 de febrero de 2025. Este calendario quedó sin efecto por la entrada en vigor en fecha 7 de noviembre de 2024 del Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17.10.2024, por el que se establecen disposiciones de aplicación de la Directiva NIS2 en lo que respecta a los requisitos técnicos y metodológicos de las medidas de gestión de riesgos en materia de ciberseguridad. De esta manera los controles de NIS2 pueden ser evaluados en auditorías de evaluación de la conformidad para el mantenimiento y recertificación de los servicios, aún sin normativa nacional de transposición de la citada Directiva.

No obstante, teniendo en cuenta la relevancia del Anteproyecto para desarrollar algunas de las principales obligaciones estipuladas por NIS2 para los QTSP como entidades esenciales en materia de ciberseguridad, se detallan a continuación algunos de los principales aspectos que regula.

I.- MARCO INSTITUCIONAL

El Anteproyecto de Ley se encarga de configurar el que será el marco institucional para la ciberseguridad en España, que se estructurará como se detalla a continuación:

• **Centro Nacional de Ciberseguridad**, de nueva creación y se erigirá como la **Autoridad Nacional competente en materia de ciberseguridad,** con competencia en materia de gobernanza de la ciberseguridad a nivel nacional. Asimismo, ejercerá como Autoridad Nacional de gestión de crisis de ciberseguridad y punto de contacto único para garantizar la cooperación transfronteriza. Adicionalmente tendrá competencias para la coordinación de las Autoridades de Control y de los puntos de contacto sectoriales y CSIRT nacionales de referencia.

• **Autoridades de Control encargadas de supervisión y ejecución de la norma:** El Anteproyecto define que serán tres las autoridades de control. Cada una se encuentra asociada a uno de los tres 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 (SEDIA):** asociadas al Ministerio para la Transformación Digital y de la Función Pública. La SEDIA es en la actualidad el Órgano de Supervisión de los QTSP en el marco de los servicios electrónicos de confianza conforme al Reglamento eIDAS.

- **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, el Anteproyecto designa como equipos de respuesta a incidentes de ciberseguridad o **"CSIRT"** a los siguientes:

- al CCN-CERT para entidades del sector público.
- al INCIBE-CERT para el resto de las entidades, **entre ellas los QTSP**.
- al ESPDEF-CERT en aquellas situaciones que los primeros requieran y, necesariamente, en las relativas a incidentes de entidades con impacto en la Defensa Nacional.

II.- MEDIDAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

II.1. Medidas de ciberseguridad a aplicar

El paquete de medidas que configura el Anteproyecto toma como referencia los perfiles de cumplimiento del Esquema Nacional de Seguridad ("**ENS**") aplicados 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 certificación o por una autoevaluación de estado de la seguridad.

Además de las medidas del ENS, el Anteproyecto estipula que también pueden **desplegarse medidas de ciberseguridad definidas en normas técnicas europeas e internacionales equivalentes**, que garanticen un nivel adecuado de seguridad de las redes y sistemas de información, así como de su entorno físico, adecuado en relación con los riesgos planteados (artículo 15 apartado 2 del Anteproyecto). En este caso, podrían considerarse los requisitos del citado estándar técnico ETSI EN 319 401 v3.1.1 que ya contempla los requisitos de la Directiva NIS2.

En cualquier caso, de requerirse en la práctica una certificación conforme a un perfil de cumplimiento específico de ENS como por ejemplo el recogido en la **guía CCN-STIC 892**, que establece el **"Perfil de Cumplimiento Específico para organizaciones esenciales o importantes en el ámbito de aplicación de la Directiva NIS2 (PCE-NIS2)"**, entendemos que para el QTSP requerirá menos esfuerzos en tiempo, recursos humanos, recursos organizativos y costes económicos asociados, dado que la mayoría de las medidas ya estarán incorporadas en sus sistemas por exigencias de la citada norma técnica ETSI EN 319 401.

II.2. Responsable de Seguridad de Redes y de la Información

Otro de los aspectos que desarrolla el Anteproyecto es la figura del **Responsable de seguridad de redes y de la información**. Para garantizar el establecimiento de estas medidas, las entidades deberán designar la persona, entidad u órgano colegiado que asuma este rol. Al respecto estipula que debe existir una designación formal de la persona física que actúe en el rol o como representante del órgano colegiado y también de su sustituto en caso de ausencia, vacante o enfermedad.

Se establece además la **obligación de comunicar el nombramiento del responsable de seguridad a la Autoridad de Control** (en el caso de los QTSP a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de la Transformación Digital y de la Función Pública) **dentro del plazo de tres meses desde su designación**. Asimismo, **comunicarán los sucesivos nombramientos y ceses en el plazo de un mes desde que aquellos se produzcan.**

II.3. Gestión y notificación de incidentes

Respecto a los incidentes, el Anteproyecto desarrolla la operativa práctica para gestionar la notificación a las Autoridades de Control. En el ámbito de los QTSP se prevé lo siguiente:

¿A quién?

El QTSP notificará al Ministerio para la Transformación Digital y de la Función Pública a través de su CSIRT de referencia (INCIBE-CERT) el incidente de seguridad significativo.

¿Cómo?

Preferentemente a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

¿Cuándo?

Sin demora indebida, en el plazo máximo de 24 horas desde que se tenga constancia del incidente significativo.

¿Qué?

Cualquier incidente categorizado como significativo que afecte a las redes y sistemas de información empleados en su operativa o en la prestación de sus servicios, **tanto si son redes y servicios propios, como si pertenecen a proveedores externos.** Igualmente hay que comunicar si el incidente puede estar motivado por una acción intencional o delictiva y si tiene o puede tener un impacto transfronterizo.

¿Quién gestiona internamente la notificación?

El responsable de la seguridad de la información.

¿Indicios delictivos?

El QTSP deberá 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.

¿Otras notificaciones voluntarias a las autoridades?

El QTSP podrá notificar de forma voluntaria al Supervisor eIDAS a través de CCN-CERT, los incidentes, ciberincidentes y cuasiincidentes que consideren pertinentes. En este caso no se define plazo y la comunicación puede realizarse por el mismo canal que la notificación obligatoria de incidentes significativos; siempre se dará prioridad a estos últimos.

III.- RÉGIMEN DE SUPERVISIÓN Y EJECUCIÓN

Bajo la dirección del Centro Nacional de Ciberseguridad, el Supervisor eIDAS como Autoridad de Control, tiene la responsabilidad de supervisar y adoptar las medidas necesarias para asegurar que los QTSP, como entidades esenciales, cumplan la normativa.

De manera general, 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 como es el caso de los QTSP 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.

IV.-OBLIGACIÓN DE INFORMACIÓN PARA REGISTRO EN LA LISTA DE ENTIDADES ESENCIALES

El Centro Nacional de Ciberseguridad elaborará una lista de entidades esenciales e importantes. Esta lista será revisada con regularidad y se actualizará con **periodicidad bienal**.

A efectos de registrarse en la citada lista, los QTSP en su calidad de entidades esenciales están obligados a remitir a las Autoridades de Control (el Supervisor eIDAS), **en el plazo máximo de tres meses** desde la adquisición de su condición como entidad esencial, al menos, la información siguiente:

1. El nombre de la entidad.

2. La dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono, incluyendo en su caso los datos de contacto del responsable de la seguridad de la información de la entidad.

3. El sector y el subsector al que pertenecen, de acuerdo con el Anexos I y II del Anteproyecto.En este caso los QTSP están categorizados en el sector de infraestructura digital dentro de los sectores de alta criticidad contemplados en el Anexo I.

4. En su caso, una lista de los Estados Miembros de la Unión Europea en los que prestan servicios comprendidos en el ámbito de aplicación de la Directiva NIS 2.

Reglamentariamente se podrán establecer los mecanismos para que las entidades den cumplimiento a las obligaciones de este apartado registrándose ellas mismas.

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.

ASEPEC

C/Serrano 69, Madrid. ECIJA HQ
info@asepec.es