Nota informativa

Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (transposición NIS2): Nuevas obligaciones de ciberseguridad para determinados sectores

El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad transpone la Directiva NIS2 al ordenamiento español, estableciendo nuevas obligaciones para entidades públicas y privadas de sectores estratégicos. La normativa introduce requisitos más estrictos de seguridad digital, incluyendo la notificación de incidentes en 24 horas, la creación del Centro Nacional de Ciberseguridad, entre otras. Esta Directiva afecta a sectores considerados esenciales como la energía, el transporte, la banca, la sanidad y servicios digitales, y prevé sanciones de hasta 10 millones de euros por incumplimiento. Las organizaciones deberán implementar medidas técnicas y organizativas reforzadas para garantizar la protección de sus redes y sistemas de información.

Contexto y objetivos

El **Anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad**, en proceso de aprobación de urgencia, establece el marco para la transposición en España de la Directiva (UE) 2022/2555 ya vinculante (conocida como NIS2), **afectando a determinadas Administraciones, así como, a entidades públicas y privadas de los sectores que se indican más adelante** con residencia fiscal en España o que operen en el país desde otro Estado miembro de la UE

Este nuevo marco **legal refuerza las medidas de ciberseguridad, imponiendo nuevas obligaciones a empresas y a entidades públicas de sectores estratégicos** para garantizar la seguridad de sus redes y sistemas de información.

Su incumplimiento conlleva **sanciones más estrictas** y una mayor supervisión por parte de las autoridades competentes.

Principales novedades y puntos clave

El nuevo marco legal **introduce cambios significativos en la regulación de la ciberseguridad**, afectando a un mayor número de sectores y aumentando las exigencias de cumplimiento. Entre sus principales novedades destacan:

- Mayor protección para entidades críticas: Se identifican como "esenciales" aquellas organizaciones que operan en sectores vitales para la sociedad, como energía, transporte, banca, salud o infraestructuras digitales. Estas entidades estarán sujetas a controles más estrictos y obligaciones de seguridad reforzadas.
- Obligaciones para entidades esenciales e importantes: Se establecen requisitos específicos, como la elaboración de planes de ciberseguridad, la notificación de incidentes y la realización de auditorías de seguridad periódicas.
- Gestión de riesgos de seguridad: Se exige la implementación de medidas técnicas y organizativas adecuadas para mitigar los riesgos en redes y sistemas de información, asegurando la continuidad del negocio frente a ciberataques.
- Notificación de incidentes: Se establece un proceso de notificación obligatoria más claro y ágil. Las entidades afectadas deberán informar a la autoridad competente sobre incidentes graves en un plazo de 24 horas, incluyendo detalles sobre su impacto y las medidas adoptadas. Además, se refuerza la divulgación de vulnerabilidades y la supervisión de la seguridad en la cadena de suministro.
- Creación del Centro Nacional de Ciberseguridad (CNC): Se prevé la creación de un organismo central encargado de la ciberseguridad en España, que coordinará las acciones en este ámbito y colaborará con otras agencias de la UE para mejorar la respuesta ante amenazas cibernéticas.
- Régimen sancionador más estricto: Se establecen multas de hasta 10 millones de euros o el 2% de la facturación anual global para aquellas entidades que incumplan la normativa. Además, se podrán aplicar sanciones adicionales como la suspensión de directivos responsables o la prohibición temporal de operar en determinados mercados.

Sectores afectados

La NIS2 establece un marco de aplicación ampliado por el Anteproyecto de la Ley, afectando a **sectores considerados esenciales o importantes**, entre ellos:

Energía y agua: Empresas de suministro de electricidad, gas, petróleo, agua potable y gestión de residuos deberán reforzar sus infraestructuras críticas ante posibles ataques cibernéticos.

Transporte y logística: Aeropuertos, ferrocarriles, transporte marítimo y terrestre deberán garantizar la seguridad de sus sistemas para evitar interrupciones en el servicio.

Banca y servicios financieros: Se refuerzan los requisitos de protección de datos y continuidad operativa en bancos, aseguradoras y mercados financieros.

Sanidad y sector farmacéutico: Clínicas, hospitales y laboratorios deberán aplicar medidas específicas para proteger información sensible y garantizar la continuidad asistencial. Se incluyen como entidades afectadas las distribuidoras titulares de una autorización de distribución de medicamentos.

Infraestructura digital y telecomunicaciones: Proveedores de servicios de internet, hosting y centros de datos estarán obligados a adoptar medidas reforzadas de ciberseguridad.

Administración pública e infraestructuras críticas: Se imponen nuevas exigencias de seguridad para organismos estatales y locales, así como para sectores estratégicos como defensa e industria manufacturera.

E-commerce y servicios digitales: Plataformas de comercio electrónico, servicios en la nube y proveedores de software deberán adoptar controles de seguridad más estrictos.

Medidas a adoptar

Las entidades y empresas incluidas en el ámbito de aplicación citado deberán revisar y adaptar sus protocolos de seguridad para garantizar el cumplimiento normativo.

Entre las acciones a adoptar se incluyen las siguientes:

- Evaluación y diagnóstico del grado de madurez en ciberseguridad.
- Identificación de los riesgos detectados en ciberseguridad.
- Implementación de controles y medidas de protección adecuadas.
- Revisión de contratos con proveedores para garantizar el cumplimiento de las nuevas obligaciones.
- Diseño de planes de respuesta y de recuperación ante incidentes.
- Formación del personal en gestión de riesgos de ciberseguridad.
- Seguimiento continuo y planes de auditoría.

Asesoramiento y cumplimiento

Desde Durán-Sindreu, ofrecemos asesoramiento especializado para facilitar la adaptación a la NIS2 y al marco legal nacional que está en proceso de aprobación, ayudando a las organizaciones a implementar las medidas necesarias para garantizar el cumplimiento normativo y la seguridad de sus sistemas, así como otros servicios de análisis inicial sobre el ámbito subjetivo de aplicación y de auditoría.

Ateniendo que el Anteproyecto se está **tramitando por el procedimiento de urgencia se espera que la norma sea aprobada lo antes posible**. Sin perjuicio de lo anterior, atendiendo el ya carácter vinculante de la NIS2 resulta necesario que las entidades de los sectores afectados **inicien su proceso de diagnóstico y adecuación al marco legal indicado**.

Para más información o para solicitar una evaluación inicial, puede contactar con nuestro equipo de Ciberseguridad y LawTech de Durán-Sindreu a través de los contactos indicados en esta nota informativa.

Contacto

Carme Setó
Socia | IP&IT y protección de datos
Espacialista en Ciberseguridad y TechLaw
cseto@duransindreu.com
93 602 52 22

Cristina Miñana
Abogada | IP&IT y protección de datos
Espacialista en Ciberseguridad y TechLaw
cminyana@duransindreu.com
93 602 52 22