Coordinación y gobernanza en ciberseguridad: nuevo marco normativo y operativo

Las normativas NIS-2 y DORA refuerzan la obligación de supervisar proveedores críticos, unificando la responsabilidad de estas entidades con la gestión integral de su ecosistema digital

Año nuevo, nuevos retos y con nueva normativa: NIS-2 y DORA. Vienen cambios, y con ello, dudas. Toca generar certidumbre. Toca generar crecimiento. Abordemos ideas-fuerza, tanto legales como operativas, que potenciarán la eficacia en la gestión corporativa. Al lío.

El anteproyecto de ley tiene como principales objetivos incorporar al ordenamiento jurídico español la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, conocida como NIS-2 y establecer medidas para la gestión de riesgos y obligaciones de notificación de incidentes de ciberseguridad.

A su vez, el reglamento DORA, ya en vigor desde el pasado 17 de enero, exige a las entidades financieras europeas implementar sistemas de gestión de riesgos TIC robustos, notificar incidentes graves en 24 horas y someterse a pruebas periódicas de resiliencia operativa. Por su parte, el anteproyecto de ley amplía este marco al establecer medidas adicionales específicas para sectores críticos en España, como energía, telecomunicaciones, salud y transporte. Ambas normativas refuerzan la obligación de supervisar proveedores críticos, unificando la responsabilidad de estas entidades con la gestión integral de su ecosistema digital.

En este sentido, el anteproyecto de ley establece un criterio uniforme para clasificar entidades como esenciales o importantes. Estas entidades deben estar encuadradas en sectores considerados de alto nivel crítico para el normal funcionamiento del país.

Sin gobernanza no hay crecimiento corporativo. Para ello, el artículo 14 establece: “Los órganos de dirección de las entidades esenciales e importantes serán responsables de aplicar las medidas para la gestión de riesgos de ciberseguridad incluidas en esta ley, de supervisar su implantación efectiva y, en su caso, asumirán la responsabilidad por su incumplimiento”.

De esta manera, el Consejo de Administración asume un papel muy operativo y de absoluta responsabilidad. De ahí la importancia de la incorporación de la ISO 31022 sobre Gestión de Riesgos Legales, aportando el valor de la seguridad operacional y contractual.

Son sujetos obligados para DORA, principalmente, bancos, aseguradoras, gestoras de activos y proveedores TIC del sector financiero. El Anteproyecto amplía su repercusión y se dirige también a hospitales, centrales energéticas, universidades y proveedores de servicios de comunicaciones clave. Además, obliga a los responsables de estas entidades a garantizar un cumplimiento íntegro, tanto en la adopción de medidas preventivas como en la colaboración con las autoridades en caso de incidentes.

Por su parte, el anteproyecto establece (artículo 35) un sistema sancionador que clasifica las infracciones en leves, graves y muy graves, con multas que podrían alcanzar millones de euros, dependiendo de la magnitud del daño causado, la reincidencia y la falta de medidas preventivas.

En este contexto geopolítico y estratégico, la Empresa Nacional de Innovación (ENISA) analiza el contexto de amenazas para Europa de la siguiente forma. Primero, abarca diez áreas (las más problemáticas por sus consecuencias para personas y países). A continuación propone 16 líneas de mejora, y termina con cinco conclusiones.

Nos centraremos en las conclusiones de este informe. En primer lugar, coordinar sesiones de trabajo en las que participen todos los Estados miembros para definir una lista de mecanismos de cibercrisis a escala de la UE que permitan una evaluación común de los incidentes e identificar a los actores que deben intervenir en función de la gravedad, lo que daría lugar a un modelo de plan de respuesta a las cibercrisis. En segundo lugar, desarrollar ejercicios de simulación a escala europea que pongan a prueba, en particular, a los actores y procedimientos a nivel operativo.

En tercer lugar, apoyar a los Estados miembros en la creación de plataformas de comunicación seguras para intercambiar información con entidades esenciales, incluso para la comunicación informal, durante una crisis cibernética. En cuarto lugar, garantizar que las autoridades nacionales de gestión de cibercrisis de los Estados miembros, en coordinación con el Grupo de Cooperación NIS, actualicen periódicamente los mapas de entidades críticas de su país. Y en quinto y último lugar, apoyar la organización de sesiones de media training para los ejecutivos de las autoridades nacionales de gestión de cibercrisis de los países.

Ambas normativas convergen en un objetivo común: aumentar la seguridad digital y operativa de los sectores más críticos, creando un ecosistema más seguro para los consumidores y una red más confiable para las operaciones transfronterizas. Su implementación, aunque compleja, resulta esencial para afrontar las amenazas actuales y garantizar la seguridad de las redes y sistemas de información en España y Europa.

En definitiva, concluimos este análisis jurídico y estratégico reafirmando la necesidad de una gestión eficaz de riesgos, tanto legales como operativos, a través de un sistema integrado de gestión. El miedo activa. Los miedos paralizan. Seamos, por lo tanto, siempre proactivos. Creer para crecer.

Fuente: https://cincodias.elpais.com/

LINK DE LA NOTICIA