*Carlos Bereciartua*
*Head of Cyber Consulting de AON España*

# Cómo prepararse para la nueva legislación en ciber

*COMO PARTE FUNDAMENTAL DE LA GESTIÓN DE RIESGOS, LAS ORGANIZACIONES DEBEN CONSIDERAR LOS RIESGOS DERIVADOS DEL INCUMPLIMIENTO NORMATIVO. EN RELACIÓN AL RIESGO CIBER, EL USO INTENSIVO (E IMPARABLE) DE LA TECNOLOGÍA DE LA INFORMACIÓN EN LOS ÚLTIMOS AÑOS ESTÁ INCREMENTANDO CONSIDERABLEMENTE LA EXPOSICIÓN A LOS CIBERDELINCUENTES, LOS ERRORES DE LOS EMPLEADOS, Y OTRAS AMENAZAS DE CIBERSEGURIDAD.*



El número, la magnitud, la sofisticación, la frecuencia y los efectos de estos ataques, van en aumento y representan una grave amenaza para el funcionamiento de los sistemas de redes y de información de cualquier organización. Por ello, se está intensificando el entorno normativo, con regulaciones como la Directiva relativa a la seguridad de las redes y sistemas de información (Directiva NIS21) o la Ley de Resiliencia Operacional Digital (Reglamento Dora2), que imponen, entre otros, rigurosos requisitos de gestión de riesgos y notificación de incidentes (para las empresas incluidas en el ámbito de aplicación).

Ambas normativas, ya en vigor y de obligado cumplimiento a partir de finales de 2024 y principios de 20253, obliga a las organizaciones a reducir las amenazas de sus sistemas de redes y de información, cumpliendo diferentes requisitos y medidas de seguridad con el objetivo fundamental de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, disponibilidad y conservación de los datos que gestionan en el ejercicio de su actividad.

Por tanto, las organizaciones deben prepararse, adaptarse a los requisitos correspondientes y evaluar su cumplimiento antes de la fecha de implantación. Dichos requisitos incluyen la adopción de medidas en torno a la gestión del ciber riesgo operativo, análisis de riesgos, la respuesta a incidentes, la notificación de incidentes y la seguridad de la cadena de suministro.

## *NIS 2*

La Directiva NIS 2 entró en vigor el 16 de enero de 2023, sin embargo, necesita transposición al ordenamiento jurídico español (antes del 17 de octubre de 2024) y será aplicable a partir del 18 de octubre de 2024.Tiene como objetivo mejorar la ciberseguridad en toda la UE y garantizar la resiliencia de las infraestructuras críticas a las ciber amenazas.

Muchas organizaciones de diversos sectores quedan bajo el alcance de esta legislación, con el requisito de fortalecer sus acuerdos de seguridad cibernética, con multas potencialmente elevadas para quienes no la cumplan.

Cada empresa debe revisar los requisitos de NIS2 y evaluar su cumplimiento para evitar posibles sanciones. Estos incluyen tomar medidas en torno a la gestión operativa del riesgo cibernético, respuesta al incidente, informe de incidentes, seguridad de la cadena de suministro, entre otros.

## *DORA*

El Reglamento DORA, publicado el 14 de diciembre de 2022 y que será aplicable a partir del 17 de enero de 2025, persigue garantizar y proteger la integridad y la eficiencia del sector financiero y facilitar su correcto funcionamiento.

Este reglamento, conlleva que las entidades financieras se preparen y planifiquen cómo mantener operaciones resilientes en caso de que un incidente digital cause una interrupción operativa grave.

Las entidades financieras deben disponer de capacidades integrales que permitan una gestión sólida y eficaz de los riesgos de las TIC, así como de mecanismos y políticas específicos para gestionar todos los incidentes relacionados con las TIC y notificar aquellos incidentes importantes.

El alcance de aplicación de la norma es universal y de obligado cumplimiento para todos los actores del sector financiero a nivel europeo. Se amplia, por tanto, el perímetro tradicional, yendo más allá de las Entidades Financieras tradicionales incluyendo a un amplio rango de los players del sector financiero.

Aon ha desarrollado servicios específicos, que ayudan a nuestros clientes a comprender su madurez en relación con los requerimientos de estas legislaciones, y recomendaciones que les permitan dar cumplimiento También, dispone de un conjunto integral de soluciones de riesgo cibernético para gestionar el ciclo de vida completo de su seguridad cibernética.