Directiva SRI 2: asegurar las redes y los sistemas de información

La Directiva SRI 2 establece un marco jurídico unificado para defender la ciberseguridad en dieciocho sectores críticos en toda la UE. También pide a los Estados miembros que definan estrategias nacionales de ciberseguridad y colaboren con la UE para la reacción y el cumplimiento transfronterizos.

La ciberseguridad implica proteger las **redes y los sistemas de información** (NIS), sus usuarios y otras personas afectadas de incidentes y amenazas cibernéticas. Para responder al aumento de la exposición de Europa a las ciberamenazas, la Directiva 2022/2555, también conocida como NIS2, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555) sustituyó a su predecesora, la Directiva 2016/1148 o NIS1. La SRI 2 eleva el nivel común de ambición de la UE en materia de ciberseguridad, a través de un ámbito de aplicación más amplio, normas más claras y herramientas de supervisión más sólidas. Exige a los Estados miembros que **mejoren sus capacidades de ciberseguridad,** al tiempo que introducen medidas de gestión de riesgos y requisitos de notificación a entidades de más sectores y establecen normas para la cooperación, el intercambio de información, la supervisión y el cumplimiento de las medidas de ciberseguridad.

La Directiva exige que cada Estado miembro adopte una estrategia nacional de ciberseguridad, que incluya políticas para la seguridad de la cadena de suministro, la gestión de vulnerabilidades y la educación y sensibilización en materia de ciberseguridad. Los Estados miembros también deben establecer y actualizar periódicamente una lista de operadores de servicios esenciales, garantizando que estas entidades cumplan los requisitos de la Directiva.

Además de los sectores ya cubiertos por la SRI 1 (energía, transporte, asistencia sanitaria, finanzas, gestión del agua e infraestructura digital), las nuevas normas también se aplican a los proveedores de comunicaciones electrónicas públicas, más servicios digitales (como plataformas sociales), gestión de residuos y aguas residuales, fabricación de productos críticos, servicios postales y de mensajería, y administración pública tanto a nivel central como regional, así como al sector espacial. Por regla general, las entidades medianas y grandes de estos sectores críticos tendrán que adoptar medidas adecuadas de gestión de riesgos de ciberseguridad y notificar a las autoridades nacionales pertinentes los incidentes significativos. Estos son incidentes que podrían causar interrupciones o daños significativos.

La Directiva también incluye disposiciones para la supervisión, el cumplimiento y las revisiones inter pares voluntarias para mejorar la confianza mutua y las capacidades de ciberseguridad en toda la UE. También introduce la rendición de cuentas de la alta dirección por el incumplimiento de las medidas de gestión de riesgos de ciberseguridad, señalando así la ciberseguridad a la atención de la sala de juntas.

La Directiva establece una red de equipos de respuesta a incidentes de seguridad informática (CSIRT) (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network) para intercambiar información sobre ciberamenazas y responder a incidentes. Estos equipos son cruciales para mantener el conocimiento de la situación y ofrecer asistencia. Para gestionar incidentes o crisis de ciberseguridad a gran escala, la Directiva crea la red europea de organizaciones de enlace para crisis cibernéticas (EU-CyCLONe). (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone) Esta red apoya la gestión coordinada y garantiza el intercambio periódico de información entre los Estados miembros y las instituciones de la UE en caso de incidentes y crisis a gran escala.

Paralelamente, el Grupo de Cooperación SRI (https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group) es una plataforma establecida por la Directiva SRI para facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros de la UE, la Comisión Europea y la Agencia de la UE para la Ciberseguridad (ENISA). El grupo publica directrices y recomendaciones no vinculantes para apoyar la aplicación de la Directiva SRI.

El **20 de enero de 2026,** como parte de un nuevo paquete de ciberseguridad, (https://digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities) la Comisión propuso modificaciones específicas (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act) de la Directiva SRI 2 para aumentar la claridad jurídica. Las modificaciones simplificarán el cumplimiento de las normas de ciberseguridad de la UE y los requisitos de gestión de riesgos para las empresas que operan en la UE. Facilitarán el cumplimiento para 28.700 empresas, incluidas 6.200 microempresas y pequeñas empresas.

Antecedentes

La NIS 1 (Directiva 2016/1148) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148) fue la primera legislación global de la UE destinada a impulsar la ciberseguridad de las redes y los sistemas de información para salvaguardar servicios vitales para la economía y la sociedad de la UE. En diciembre de 2020, la Comisión propuso revisar la NIS 1, lo que dio lugar a la adopción de la NIS 2, que entró en vigor en enero de 2023. Los Estados miembros tenían hasta el 17 de octubre de 2024 para transponer la Directiva SRI 2 al Derecho nacional. NIS 2 derogó NIS1 a partir del 18 de octubre de 2024.
