Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia · España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

M. V. Carriegos
presenta el resumen del trabajo

Cybersecurity in the EU: How the NIS2 directive stacks up against its predecessor

Niels Vandezande

Computer Law & Security Review, 52 (2024) 105890.

21 de marzo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

E**Palabras clave:** Ciberseguridad, directiva NIS, seguridad de la información, política europea en ciberseguridad, regulación operacional del sector financiero, resiliencia del sector financiero .

Introducción

La segunda directiva sobre seguridad en redes y sistemas de información, NIS 2, fue publicada en diciembre de 2022. La primera directiva, que fue adoptada en 2016, y que solicitaba un nivel alto de ciberseguridad en común para todos los estado miembros, ha sido dificil de implementar.

El trabajo documenta datos relativos a ciberseguridad de finales de la década 2010-2020 proporcionados por Eurostat y otras agencias. Cabe destacar:

- El número de incidentes de seguridad afectaron al 22 % de las empresas europeas en 2021 mientras que en 2018 fue sólo del 12 %.
- Los ataque de ransomware han aumentado un 41 % en 2022.
- Los ataques usando el e-mail como vestor de propagación han aumentado un 48 % en 2022.
- El coste económico de los eventos de ciberseguridad ha aumentado en consonancia con el número de incidentes.
- A pesar de las políticas desplegadas para proteger todo tipo de entidades frente a las ciberamenazas, el 54 % de estas entidades aún consideran que no están preparadas para afrontar los retos de ciberseguridad.
- Se estima que el 95 % de los problemas de ciberseguridad se deben a errores humanos en la implementación de medidas de ciberseguridad,

La UE adoptó una directiva en seguridad en 2016 (la Directiva NIS) que ha resultado insuficiente, por lo cual se dejará sin efecto el 18 de octubre de 2024 y que ha sido reemplazada por una nueva directiva, la NIS2, adoptada en diciembre de 2022.

El trabajo revisa los principales objetivos de las políticas de NIS2 y las compara con su predecesora NIS.

1. Metodología

El trabajo usa una metodología descriptiva basada en la comparación de las Directivas NIS y su sucesora NIS2.

2. Resultados

Se resalta que quizá la principal diferencia entre ambas disposiciones es que mientras que la Directiva NIS se centra en la *seguridad de las redes de sistemas de información*, la Directiva NIS2 trata de una noción mas amplia: la Ciberseguridad tal y como está definida en el Acta de Ciberseguridad. Por lo tanto se pasa de proteger las redes y los sistemas de informacióna aproteger también a los usuarios de tales sistemas así como a otras personas afectadas por las ciberamenazas.

Se apunta el ámbito de aplicación de la Directiva NIS2: las entidades públicas y privadas de tamaño medio y grande en sectores críticos. Estos sectores críticos están también definidos en los anexos de la Directiva.

Se comentan las obligaciones de los estados miembros con respecto a esta Directiva:

- Aclarar la gobernanza y los roles y responsabilidades de las autoridades en políticas de ciberseguridad. En particular, es obligatoria una lista de autoridades competentes y roles de las mismas así como los mecanismos de coordinación.
- Mejorar la calidad de las estrategias naciona-

les por medio de la revisión por pares. Así las estrategias nacionales pueden someterse voluntariamente a escrutinio por pares mediante la designación de grupos de expertos de al menos otros dos países utilizando una metodología objetiva, no discriminatoria y transparente.

- Proveer y reforzar las unidades CSIRT de respuesta a incidentes críticos. Esats unidades ya furon dispuestas en 2017 y se refuerzan efectivamente ampliando las nociones de ciber-amenaza y de ciber-incidente a *eventos que comprometan la disponibilidad, autenticidad, integridad o confidencialidad de datos almacenadso, transmitidos o procesados de servicios ofrecidos o accesibles via redes o sistemas de información*.
- Cooperación entre estados miembros por medio de la red de CSIRT.
- ENISA proporcionará un informe bianual sobre ciberseguridad en la UE.
- Responsabilidad de los agentes en su propia cibreseguridad, en particular la localización presia de los responsables de seguridad de las entidades.
- NIS2 cambia el criterio de imortancia de un incidente desde el número de usuarios afectados, la duración y la amplitud geográfica a criterios sobre la corrupción operativa del sistema afectado, la pérdida económica y la capacidad del incidente de causar daño a presonas físicas o jurídicas.
- NIS2 trata de encontrar un equilibrio para que el reporte de incidentes sea efectivo y riguroso pero no sea alarmista.
- NIS2 pone límites estrictos a la temporalidad de los reportes de ciberseguridad: en 24 horas debe haber empezadoel reporte y en 72 horas debe estar hecha la notificación. El reporte final debe estar hecho antes de un mes.
- NIS2 establece que la jurisdicción de las entidades en cuanto a ciberseguridad recae en el estado miembro donde están radicadas.
- Se pone énfasis especial en la compartición de información voluntaria entre los estados miembros y de forma especial a través de la red de CSIRT
- ENISA mantendrá un registro de entidades, de infraestructuras digitales y de proveedores. Otro registro se dedicará a los nombres de dominios.
- Cunado mas de un estado miembro esté involucrado, las autoridades competentes deberán proporcionar asistencia mutua, así como acciones conjuntas. La Comisión Europea adoptará competencias delegadas asistida por un comité.

3. Discusión/Conclusiones

La Directiva NIS2 fue adoptada formalmente el 14 de diciembre de 2022 y entró en vigor 20 días después. Los estados miembros tienen que trasponer la Directiva antes del 17 de octubre de 2024 y comenzar efectivamente las medidas dispuestas antes del 18 de octubre de 2024, día en que decae la Directiva NIS. La Comisión Europea eleboaraá un informe para el 17 de octubre de 2027 y, a partir de ahí, cada 36 meses.

Se enfatiza la necesidad de una definición más precisa de la importancia de un incidente, así como la armonización del concepto en los diferentes estados miembros.

Se advierte igualmente que el reporte efectivo y riguroso de incidentes podría causar sierta alarma en algún momento; no obstante se sigue prefiriendo el sobrerreporte de incidentes y la prontitud de las actuaciones a la falta del mismo.

4. Valoración del documento original

Es un documento valioso para comprnder las diferencias entre las Directivas NIS y su sucesora NIS2.

Referencias

· REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the .EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").
· DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

· DIRECTIVE (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)