Consejo de la UE

PRESS
ES

COMUNICADO DE PRENSA
449/25
6.6.2025

La UE adopta un plan director para gestionar mejor las crisis e incidentes de ciberseguridad europeos

Los ministros de Telecomunicaciones han adoptado hoy el Plan Director de la UE para la Gestión de Crisis de Ciberseguridad, en el que se dan orientaciones para la respuesta de la UE a los incidentes de ciberseguridad a gran escala o crisis de ciberseguridad.

> Hoy damos un paso decisivo para reforzar la resiliencia de Europa en materia de ciberseguridad. El Plan Director de la UE para la Gestión de Crisis de Ciberseguridad aclara cómo los Estados miembros pueden detectar los incidentes de ciberseguridad a gran escala y las crisis de ciberseguridad que podrían afectar a toda la UE, responder ante ellos, así como recuperarse y aprender de la experiencia. Con este plan director, demostramos que estamos firmemente decididos a lograr una Europa más segura, resiliente y mejor preparada, una gran prioridad de la Presidencia polaca.
>
> *Krzysztof Gawkowski, vicepresidente del Consejo de Ministros, ministro de Digitalización*

El Plan Director de Ciberseguridad de la UE **es un recurso de orientación importante por medio del cual los Estados miembros pueden mejorar su preparación ante incidentes de ciberseguridad, así como sus capacidades de detección y respuesta**. Se han tomado como base los fundamentos del Plan Director de Ciberseguridad de 2017 y se han tenido en cuenta actos jurídicos importantes de reciente adopción como la Directiva SRI 2 y el Reglamento de Cibersolidaridad.

El Plan Director de Ciberseguridad de la UE se propone hacer frente a un panorama de ciberamenazas cada vez más complejo **reforzando las redes existentes de la UE, fomentando la cooperación entre los Estados miembros y los actores implicados** y superando los obstáculos que puedan existir.

Elementos esenciales del Plan Director de Ciberseguridad

En este plan director se destaca la importancia de la tecnología digital y de la conectividad mundial como puntales del crecimiento económico y la competitividad de la UE. Sin embargo, el **que la sociedad esté cada vez más interconectada y digitalizada conlleva también un aumento del riesgo de incidentes de ciberseguridad y ciberataques.** Las campañas híbridas y los ciberataques pueden afectar directamente a la seguridad, la economía y la sociedad de la UE.

Los Estados miembros son los responsables en primera instancia de gestionar los incidentes y crisis de ciberseguridad, pero su capacidad de respuesta puede verse sobrepasada cuando se dan incidentes a gran escala, que pueden causar grandes perturbaciones o incluso afectar a varios Estados miembros.

Dado que un incidente de este tipo podría convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior de la UE o plantee graves riesgos para la seguridad y la protección públicas, la **cooperación en los niveles técnico, operativo y político es esencial** para gestionar este tipo de crisis con eficacia.

A fin de determinar concretamente qué constituye un incidente a gran escala o una crisis de ciberseguridad en la Unión, el Plan Director de Ciberseguridad explica con claridad cuándo debe activarse el marco de crisis y cuáles son las funciones de las redes, los actores y los mecanismos de la UE pertinentes como, por ejemplo, la Agencia de Ciberseguridad de la UE (ENISA) o la Red

Europea de Organizaciones de Enlace Nacionales para las Crisis de Ciberseguridad (EU-CyCLONe). El texto también señala la importancia de coordinar la comunicación pública antes de una crisis y también durante y después.

El Plan Director de Ciberseguridad de la UE destaca la **importancia de la cooperación en materia civil y militar** en el contexto de la gestión de crisis de ciberseguridad —también en colaboración con la OTAN— a través de mecanismos reforzados de puesta en común de información cuando sea posible y se dé la necesidad.

Por último, en este nuevo plan director también se incluyen capítulos sobre recuperación y se intenta que mejore la puesta en común de lecciones extraídas entre los Estados miembros.

Contexto

Desde 2017, el panorama de las amenazas y el marco de ciberseguridad de la UE ha cambiado notablemente gracias a la creación de varios instrumentos sobre la gestión de la ciberseguridad, como la Directiva SRI 2 o el Reglamento de Cibersolidaridad. De ahí surgió la necesidad de modificar el plan director de 2017.

Los debates sobre el Plan Director de Ciberseguridad de la UE se intensificaron durante la Presidencia polaca, en particular durante la reunión informal del Consejo de Transporte, Telecomunicaciones y Energía de los días 4 y 5 de marzo en Varsovia, que se dedicó por completo a la cuestión de la ciberseguridad.

- Plan Director sobre Ciberseguridad - Proyecto de Recomendación del Consejo (publicación, Comisión Europea, 24.2.2025)
- La Comisión pone en marcha un nuevo plan de ciberseguridad para mejorar la coordinación de la UE en materia de crisis de ciberseguridad (comunicado de prensa, Comisión Europea, 24.2.2025)
- Ciberseguridad (información de referencia)
- Ciberdefensa (información de referencia)

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press