martes, 10 junio de 2025

Gestionar millor les crisis i incidents de ciberseguretat europeus

Els ministres de Telecomunicacions han adoptat el **Pla Director de la UE per a la Gestió de Crisis de Ciberseguretat**, en el qual es donen orientacions per a la resposta de la UE als incidents de ciberseguretat a gran escala o crisis de ciberseguretat.

El **Pla Director de Ciberseguretat de la UE** és una guia important amb la qual els Estats membres poden millorar la seva preparació davant incidents de ciberseguretat, així com les seves capacitats de detecció i resposta. S'han pres com a base els fonaments del Pla Director de Ciberseguretat del 2017 i s'han tingut en compte actes jurídics importants de recent adopció, com la **Directiva NIS 2** i el **Reglament de Cibersolidaritat**.

El Pla Director de Ciberseguretat de la UE es proposa fer front a un panorama de ciberamenaces cada cop més complex, reforçant les xarxes existents de la UE, fomentant la cooperació entre els Estats membres i els actors implicats, i superant els obstacles que puguin existir.

Elements essencials del Pla Director de Ciberseguretat

Aquest pla director destaca la importància de la **tecnologia digital** i de la **connectivitat mundial** com a pilars del creixement econòmic i la competitivitat de la UE. No obstant això, el fet que la societat estigui cada cop més interconnectada i digitalitzada comporta també un augment del risc d'incidents de ciberseguretat i ciberatacs. Les campanyes híbrides i els ciberatacs poden afectar directament la seguretat, l'economia i la societat de la UE.

Els Estats membres són els responsables en primera instància de gestionar els incidents i crisis de ciberseguretat, però la seva capacitat de resposta pot veure's sobrepassada quan es donen incidents a gran escala, que poden causar grans pertorbacions o fins i tot afectar diversos Estats membres.

Com que un incident d'aquest tipus podria esdevenir una crisi pròpiament dita que impedeixi el correcte funcionament del mercat interior de la UE o plantegi greus riscos per a la seguretat i la protecció públiques, la **cooperació en els nivells tècnic, operatiu i polític** és essencial per gestionar aquest tipus de crisis amb eficàcia.

Per tal de determinar concretament què constitueix un incident a gran escala o una crisi de ciberseguretat a la Unió, el Pla Director de Ciberseguretat explica amb claredat quan s'ha d'activar el marc de crisi i quines són les funcions de les xarxes, els actors i els mecanismes de la UE pertinents, com ara l'**Agència de Ciberseguretat de la UE (ENISA)** o la **Xarxa Europea d'Organitzacions d'Enllaç Nacionals per a les Crisis**

de Ciberseguretat (EU-CyCLONe). El text també assenyala la importància de coordinar la comunicació pública abans d'una crisi i també durant i després.

El Pla Director de Ciberseguretat de la UE destaca la **importància de la cooperació en matèria civil i militar** en el context de la gestió de crisis de ciberseguretat —també en col·laboració amb l'OTAN— a través de mecanismes reforçats de posada en comú d'informació quan sigui possible i es doni la necessitat.

Podeu consultar el comunicat de premsa complet **aquí** [/export/sites/Sbd/ca/.galleries/Documents/La-UE-adopta-un-plan-director-para-gestionar-mejor-las-crisis-e-incide] (Consell de la UE).