Aspectos de seguridad digital incluidos en el *strategic compass* de la Unión Europea

Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE para 2030

El *Strategic Compass* aprobado el pasado **21 de marzo** es un documento de gran importancia por lo que se refiere al ámbito de la **ciberseguridad y la ciberdefensa**. Establece un detallado **marco de actuaciones** concretas a emprender por la UE en los próximos años. Además, fija con claridad la posición de la UE ante el **nuevo contexto geopolítico** creado por la guerra en Ucrania. **Va a tener importantes repercusiones para las empresas, especialmente en lo relativo a las líneas generales de inversión e investigación a implementar por la UE.**

1. El pasado 21 de marzo de 2022 el Consejo Europeo aprobó formalmente el *Strategic Compass* en un momento de **cambio radical del paradigma geopolítico** mundial.
2. Se trata de un ambicioso plan de acción para reforzar la política de seguridad y defensa de la UE hasta **2030** en una clara muestra de que la situación exige aproximarse a enfoques de hard power que hasta ahora no habían sido una prioridad para la UE.
3. El objetivo de la Brújula Estratégica es **reforzar las capacidades de la UE** de proteger a sus ciudadanos y contribuir a la paz y la seguridad internacionales.
4. Todo ello deberá hacerse de forma **complementaria a la OTAN**, que sigue siendo la base de la defensa colectiva de sus miembros.
5. El documento presenta propuestas concretas y ejecutables, con un calendario muy preciso.
6. Se articula en torno a **cuatro pilares: actuar, invertir, trabajar de manera asociativa y garantizar la seguridad.**

EL CONTEXTO ESTRATÉGICO EN RELACIÓN CON EL CIBERESPACIO

Responde a estas características según el documento:

- El espectro de amenazas se ha diversificado y se ha vuelto más impredecible.
- Aumenta la dependencia de las tecnologías digitales.
- El ciberespacio se ha convertido en un ámbito de competencia estratégica. Los datos y los estándares tecnológicos son instrumentos de competencia política.
- Los ciberataques son cada vez más sofisticados. Resulta indispensable preservar la apertura, libertad, estabilidad y seguridad del ciberespacio
- La competencia entre sistemas de gobernanza que va acompañada de una verdadera guerra de relatos.

ACTUACIONES CONCRETAS QUE SE SEÑALAN EN EL ÁMBITO DEL CIBERESPACIO

- Establecimiento de una política de ciberdefensa de la UE que impulsará la investigación y la innovación, y supondrá un estímulo para la base industrial de la UE. Además, promoverá la educación y la formación.
- Sentar la determinación de combatir, con respuestas inmediatas y a largo plazo, a los agentes de riesgo que intenten impedir un acceso seguro y abierto al ciberespacio a la UE y a sus socios.
- Mejorar la ciberseguridad, lo cual permitirá aumentar la eficacia y seguridad de los esfuerzos en tierra, en el aire, en el mar y en el espacio ultraterrestre.
- Utilización intensiva de las nuevas tecnologías, en particular la informática cuántica, la inteligencia artificial y la inteligencia de datos, para lograr ventajas comparativas.
- Impulsar las capacidades de análisis de inteligencia.
- Creación de una Unidad Informática Conjunta de la UE para reforzar la conciencia situacional común de las instituciones de la UE, los Estados miembros y la cooperación entre ellos.
- Desarrollar un conjunto de instrumentos y equipos de respuesta contra las amenazas híbridas capaces de responder con rapidez y contundencia a ciberataques con respaldo estatal contra infraestructuras críticas.
- Seguir desarrollando el conjunto de instrumentos de ciberdiplomacia, en particular las medidas preventivas y las sanciones a agentes externos por actividades informáticas malintencionadas contra la Unión y sus Estados miembros.
- Crear instrumentos contra la manipulación de información y la injerencia por parte de agentes extranjeros.
- Ofrecer incentivos para fomentar la participación de los Estados miembros en proyectos colaborativos de desarrollo de capacidades.
- Invertir conjuntamente en elementos de apoyo estratégicos y capacidades de nueva generación, en especial: el transporte estratégico, la protección de las fuerzas, los recursos médicos, de ciberdefensa y de comunicación por satélite y las capacidades de inteligencia, vigilancia y reconocimiento.
- Adopción de criterios y normas adicionales sobre la protección de la información clasificada y la información sensible no clasificada de la UE para facilitar los intercambios seguros con los Estados miembros.
- Aumentar la interoperatividad y el intercambio de información a través de la cooperación entre los equipos militares de respuesta a emergencias informáticas.
- Entender la ciberdefensa como garantía fundamental en el ámbito prioritario de la mejora de la movilidad militar como elemento de apoyo esencial.
- Poner en funcionamiento el Centro Europeo de Competencia en Ciberseguridad al objeto de desarrollar en Europa un sólido ecosistema industrial y tecnológico de ciberseguridad y apoyar a las empresas especializadas en ciberseguridad.

Vicente Moret
Of Counsel del área de Derecho Procesal
vicente.moret@es.Andersen.com

ANDERSEN®