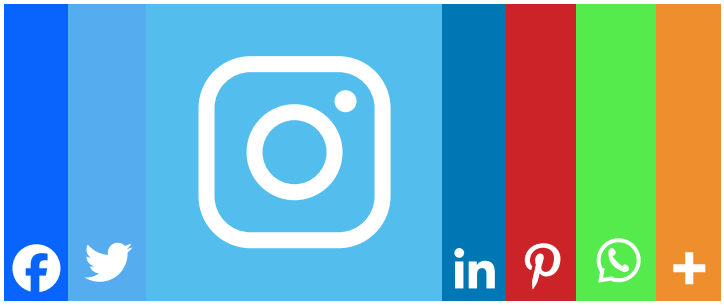
Spread the love



La Comisión Europea ha realizado una revisión de la situación de la ciberseguridad en la UE, incluyendo la ciberseguridad de las empresas (Comunicación COM(2025) 290)

Panorama general de la ciberseguridad en la Unión Europea

La ciberseguridad en la Unión Europea está cada vez más condicionada por el aumento de tensiones geopolíticas y económicas. En este contexto, los ciberataques se han convertido en herramientas estratégicas para el espionaje, el sabotaje y las campañas de desinformación. Los ataques dirigidos contra los Estados miembros y las instituciones europeas son constantes, representando una amenaza grave y sostenida. Por mencionar algún riesgo concreto, el *ransomware* sigue siendo uno de los riesgos más dañinos, cuya evolución va más allá de simplemente encriptar datos, ya que ahora se combina con la exfiltración de información sensible para ejercer una doble extorsión. Las pequeñas y medianas empresas son objetivos frecuentes, dada su menor capacidad de defensa. Por ejemplo, señala el informe, que en 2024 el sector sanitario sufrió un impacto especialmente alto: el 71 % de los incidentes que afectaron la atención al paciente estuvieron relacionados con *ransomware*. Aunque los ataques aumentaron un 11 % respecto al año anterior, la presión sobre grupos como LockBit ha fragmentado el panorama, surgiendo 46 nuevos grupos de ransomware en ese mismo año.

Los ataques a la cadena de suministro también han aumentado de forma notable, conforme a lo indicado por la Comisión Europea. Los ciberdelincuentes aprovechan las vulnerabilidades de proveedores externos, especialmente cuando estos dependen de tecnologías o proveedores considerados de riesgo o sujetos a legislaciones que obligan a reportar vulnerabilidades a sus autoridades antes que al público. Además, pueden aprovecharse de esta dependencia para atacar infraestructuras críticas, generando interrupciones en momentos clave. Por ejemplo, los ataques a dispositivos conectados al Internet de las Cosas (IoT) crecieron un 107 % en la primera mitad de 2024.

A nivel social, la percepción pública sobre la ciberseguridad está empeorando, con una disminución de la confianza en la capacidad propia para protegerse y un bajo conocimiento de los mecanismos de denuncia de incidentes. Además, la dependencia excesiva de proveedores tecnológicos únicos y no europeos plantea riesgos considerables para la

economía, como demostró la interrupción del servicio de CrowdStrike en 2024.

Un reto estructural importante es la escasez de talento especializado: la Unión Europea enfrenta un déficit de aproximadamente 299.000 profesionales en ciberseguridad. Para abordar este problema, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) impulsa iniciativas como el Marco Europeo de Competencias en Ciberseguridad (ECSF), que busca facilitar la formación, certificación y movilidad profesional en este ámbito.

Empresas y su ciberseguridad

Camelia blanca

Explica la Comisión que en 2024, la gran mayoría de las empresas europeas con más de 10 empleados (el 92,8 %) implementaron al menos una medida básica de seguridad TIC. Sin embargo, solo un tercio contaba con documentación formal o realizaba evaluaciones de riesgos periódicas. Las prácticas más habituales fueron el uso de contraseñas robustas (83,7 %) y la realización de copias de seguridad en ubicaciones separadas (79,2 %). Aun así, el 21,5 % de las empresas sufrió incidentes de seguridad con consecuencias negativas.

El presupuesto dedicado a la seguridad informática creció, llegando a representar en promedio el 9 % del total de TI, especialmente en sectores regulados por la Directiva NIS, donde la madurez en ciberseguridad es más avanzada. El sector de telecomunicaciones destaca por su nivel de preparación.

Los Estados miembros han incluido en sus Planes Nacionales unas 38 medidas para reforzar la ciberseguridad, con un presupuesto conjunto cercano a los 7.000 millones de euros,

orientados a fortalecer la formación, crear centros especializados y mejorar las capacidades tanto públicas como privadas. Pero, resulta preocupante la lenta y desigual adopción de tecnologías clave como IPv6, con una penetración superior al 40 % en países como Bélgica, Francia o Alemania, pero inferior al 10 % en otros como Croacia, Chipre o Malta.

Marco normativo y avances recientes
Entre 2024 y 2025, la UE ha dado pasos importantes en su agenda de ciberseguridad. La Directiva NIS2, con obligación de transposición en octubre de 2024, establece estándares estrictos para 18 sectores críticos. En ese mismo mes, la Comisión Europea aprobó el primer acto delegado bajo NIS2, que detalla las medidas de gestión de riesgos y los criterios para la notificación de incidentes importantes.

El Reglamento Cyber Resilience Act introduce requisitos de seguridad para productos digitales, con plena aplicación en los próximos tres años. En cuanto al Cyber Solidarity Act, estableció un sistema europeo de alerta en ciberseguridad, así como mecanismos de respuesta rápida ante incidentes, apoyados en inteligencia artificial. También se modificó el Cybersecurity Act para permitir la certificación de servicios gestionados de seguridad. Por otro lado, en enero de 2025 se adoptó un Plan de Acción para mejorar la ciberseguridad en hospitales y proveedores de salud, y en febrero se propuso un nuevo *Cybersecurity Blueprin*t que integra la cooperación civil-militar y mejora la capacidad de respuesta a crisis.

Tecnologías emergentes
El desarrollo de la Infraestructura Europea de Comunicación Cuántica (EuroQCI), dentro del programa IRIS, busca ofrecer servicios altamente seguros para el intercambio de claves criptográficas y la protección de infraestructuras críticas. En 2024, el foco estuvo en el desarrollo de redes nacionales cuánticas y la previsión de conexiones transfronterizas en 2026.

- La llegada de la computación cuántica trasformará o desplazará la criptografía actual, por lo que la Comisión Europea recomendó en 2024 que los Estados miembros

preparen hojas de ruta sincronizadas para la transición a criptografía post-cuántica, especialmente en administraciones públicas e infraestructuras críticas, con objetivos a corto y medio plazo.

En el informe comentado, la Comisión aconseja a los Estados miembros:

- Transponer la Directiva NIS2 y adoptar medidas adicionales para asegurar la implementación plena de los marcos europeos, incluyendo la caja de herramientas para seguridad 5G y restricciones a proveedores de alto riesgo.
- Fortalecer la formación y las capacidades del personal en ciberseguridad, aprovechando recursos como el Marco Europeo de Competencias.
- Elaborar, dentro del Grupo de Cooperación NIS, hojas de ruta para la transición sincronizada a criptografía post-cuántica en sectores públicos y críticos.
- Avanzar en la migración de sistemas criptográficos actuales a tecnologías post-cuánticas, con metas parciales para 2030 y finalización prevista para 2035.