

La UE refuerza la ciberseguridad con la entrada en vigor de la Ley de Resiliencia Cibernética

La Unión Europea da un paso decisivo para proteger los dispositivos tecnológicos de uso cotidiano ante el incremento constante de ciberataques. Con la aplicación de las primeras obligaciones de la Ley de Resiliencia Cibernética (CRA, por sus siglas en inglés), la legislación comunitaria busca blindar desde programas informáticos y aplicaciones móviles hasta hardware como relojes inteligentes, monitores para bebés o sistemas de cierre de puertas conectados. La normativa establece un marco regulatorio exigente que responsabiliza directamente a los fabricantes en el diseño, actualización y mantenimiento de cualquier producto con componentes digitales que se comercialice dentro del mercado único.

A partir del 11 de septiembre de 2026, las empresas del sector tecnológico están obligadas a notificar con inmediatez cualquier vulnerabilidad que esté siendo explotada activamente o cualquier incidente grave que comprometa la seguridad de sus productos. La reglamentación fija un protocolo estricto que exige a las compañías enviar una alerta temprana en un tras detectar el problema, el cual deberá ser complementado con una notificación detallada en un plazo de 72 horas para dar cuenta del alcance de la brecha.

El proceso de reporte incluye la entrega de un informe final que deberá presentarse en un plazo máximo de 14 días desde que se disponga de una medida correctiva o parche de mitigación para la vulnerabilidad. En los casos de incidentes graves que no involucren una explotación activa, el margen de entrega del informe definitivo se extiende hasta un mes. La normativa aclara que estas exigencias de comunicación afectan a la totalidad de los artículos con elementos digitales comercializados en la Unión Europea, abarcando de forma explícita a aquellos dispositivos que ya se encontraban previamente a la venta en el mercado.

Para gestionar este flujo de información, la Agencia de Ciberseguridad de la Unión Europea (ENISA) ha desarrollado la Plataforma Única de Notificación de la CRA, el portal centralizado a través del cual los fabricantes deberán remitir todas sus alertas. Con el fin de facilitar la adaptación técnica de la industria, la Comisión Europea ha difundido una guía práctica dirigida a desarrolladores y empresas, mientras que las autoridades nacionales de vigilancia del mercado de cada Estado miembro serán las encargadas de supervisar el cumplimiento de los preceptos y sancionar las eventuales infracciones.

Esta iniciativa legislativa se engloba dentro de la Estrategia de Ciberseguridad de la UE y la Estrategia de la Unión Europea para la Seguridad, orientadas a elevar los estándares defensivos del entorno digital comunitario. En este esquema, la inclusión del marcado CE en los embalajes servirá como distintivo visible para que consumidores y empresas puedan identificar con garantías los aparatos que cumplen los requisitos legales de ciberprotección, asegurando avisos más ágiles ante cualquier fallo de seguridad que ponga en riesgo la privacidad del hogar.

El calendario de implantación de la Ley de Resiliencia Cibernética contempla dos fases clave para el tejido empresarial. Tras la entrada en funcionamiento del sistema obligatorio de notificación de incidentes y vulnerabilidades fijado para el 11 de septiembre de 2026, el conjunto principal de las obligaciones de diseño, soporte técnico y certificación contempladas en la directiva comunitaria pasará a ser de obligado cumplimiento a partir del 11 de diciembre de 2027.

Fuente: La UE refuerza la ciberseguridad con la entrada en vigor de la Ley de Resiliencia Cibernética - Interdiario