REPRESENTACIÓN EN ESPAÑA
COMUNICADO DE PRENSA

Estado de la Unión: nuevas normas de la UE en materia de ciberseguridad garantizan unos equipos y programas informáticos más seguros

Bruselas, 15 de septiembre de 2022

La Comisión ha presentado hoy una propuesta de nueva Ley de Ciberresiliencia para proteger a los consumidores y las empresas frente a los productos con características de seguridad inadecuadas. Es una primera legislación de este tipo a escala de la UE e introduce requisitos obligatorios de ciberseguridad para los productos con elementos digitales, a lo largo de todo su ciclo de vida útil.

La Ley, anunciada por la presidenta Ursula **von der Leyen** en septiembre de 2021 en su discurso sobre el estado de la Unión Europea, se basa en la Estrategia de Ciberseguridad de la UE de 2020 y en la Estrategia de la UE para una Unión de la Seguridad, también de 2020, y velará por que los productos digitales, tales como los productos inalámbricos y por cable y los programas informáticos, sean más seguros para los consumidores de toda la UE. Además de ampliar la responsabilidad de los fabricantes al obligarlos a facilitar apoyo de seguridad y actualizaciones de los programas informáticos a fin de eliminar los puntos vulnerables detectados, permitirá a los consumidores tener información suficiente sobre la ciberseguridad de los productos que compren y utilicen.

Margrethe **Vestager**, vicepresidenta ejecutiva responsable de la cartera de una Europa Adaptada a la Era Digital, ha declarado: *«Merecemos sentirnos seguros con los productos que compremos en el mercado único. Del mismo modo que podemos confiar en un juguete o un frigorífico con el distintivo CE, la Ley de Ciberresiliencia garantizará que los objetos y programas informáticos conectados que compremos tengan sólidas salvaguardias en materia de ciberseguridad. La responsabilidad recaerá en quienes corresponde, esto es, en quienes comercializan los productos».*

Margaritis **Schinas**, vicepresidente responsable de la Promoción de nuestro Modo de Vida Europeo, ha hecho las siguientes observaciones: *«La Ley de Ciberresiliencia es nuestra respuesta a las amenazas modernas a la seguridad que son ahora omnipresentes en toda nuestra sociedad digital. La UE ha sido*

pionera en la creación de un ecosistema de ciberseguridad mediante normas sobre infraestructuras críticas, preparación y respuesta en materia de ciberseguridad y certificación de los productos de ciberseguridad. Hoy completamos este ecosistema mediante una ley que aporta seguridad a todos los hogares, todas nuestras empresas y todos los productos interconectados. La ciberseguridad ya no es solo una cuestión industrial sino un tema que afecta a toda la sociedad».

Por su parte, Thierry **Breton**, comisario de Mercado Interior, ha afirmado: *«En lo que respecta a la ciberseguridad, Europa solo será tan fuerte como lo sea su eslabón más débil, sea este un Estado miembro vulnerable o un producto inseguro en la cadena de suministro. Ordenadores, teléfonos, electrodomésticos, dispositivos virtuales de asistencia, automóviles, juguetes, etc., cada uno de estos cientos de millones de productos conectados es un posible punto de entrada para un ciberataque. Sin embargo, en la actualidad, la mayoría de los equipos y productos informáticos no están sujetos a ninguna obligación en materia de ciberseguridad. Al introducir la ciberseguridad desde el diseño, la Ley de Ciberresiliencia contribuirá a proteger la economía europea y nuestra seguridad colectiva»*.

Teniendo en cuenta que los ataques con programas de secuestro de archivos afectan a una organización cada once segundos en todo el mundo y que el coste anual mundial estimado de la ciberdelincuencia alcanzó los 5,5 billones de euros en 2021 [Informe del Centro Común de Investigación (2020): «Cybersecurity – Our Digital Anchor, a European perspective» (Ciberseguridad: nuestra ancla digital, una perspectica europea)], es más importante que nunca garantizar un alto nivel de ciberseguridad y limitar los puntos vulnerables de los productos digitales, que constituyen una de las principales vías de los ataques que alcanzan su objetivo. Al haber cada vez más productos inteligentes y conectados, un incidente de ciberseguridad en un producto puede incidir en toda la cadena de suministro, lo que puede dar lugar a graves perturbaciones de las actividades económicas y sociales en todo el mercado interior, reducir la seguridad o incluso poner en peligro vidas.

Las medidas propuestas hoy se basan en el nuevo marco legislativo para la legislación de la UE sobre productos y establecerán:

a) normas sobre la introducción en el mercado de productos con elementos digitales para garantizar su ciberseguridad;

b) requisitos esenciales en materia de diseño, desarrollo y fabricación de productos con elementos digitales, y obligaciones de los agentes económicos en relación con dichos productos;

c) requisitos esenciales en materia de procesos de tratamiento de puntos vulnerables establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales durante todo el ciclo de vida útil, y obligaciones de los agentes económicos en relación con estos procesos. Los fabricantes también tendrán que notificar los puntos vulnerables e incidentes activamente aprovechados;

d) normas sobre el control y la vigilancia del mercado.

Las nuevas normas harán recaer la responsabilidad en los fabricantes, que deberán garantizar la conformidad con los requisitos de seguridad de los productos con elementos digitales que se comercialicen en la UE. Como consecuencia de ello, redundarán en beneficio de los consumidores y de los ciudadanos, así como de las empresas que utilizan productos digitales, al aumentar la transparencia de las propiedades de seguridad y fomentar la confianza en los productos con elementos digitales, y también al garantizar una mejor protección de sus derechos fundamentales, tales como la privacidad y la protección de datos.

En un momento en que otros territorios de todo el planeta estudian la manera de abordar estas cuestiones, es probable que la Ley de Ciberresiliencia se convierta en un texto de referencia internacional, más allá del mercado interior de la UE. Las normas de la UE basadas en la Ley de Ciberresiliencia facilitarán su aplicación y constituirán una baza para la industria de ciberseguridad de la UE en los mercados mundiales.

La norma propuesta se aplicará a todos los productos conectados directa o indirectamente a otro dispositivo o red. Existen algunas excepciones para los productos en relación con los cuales ya existen requisitos de ciberseguridad en las normas vigentes de la UE como, por ejemplo, los dispositivos médicos, la aviación o los automóviles.

Próximas etapas

Corresponde ahora al Parlamento Europeo y al Consejo examinar el proyecto de Ley de Ciberresiliencia. Una vez adoptado, los agentes económicos y los Estados miembros tendrán dos años para adaptarse a los nuevos requisitos. Una excepción a esta norma es la obligación de notificación de los fabricantes de los puntos vulnerables y los incidentes e incidentes activamente aprovechados, que se aplicará ya un año después de la fecha de entrada en vigor, ya que requieren menos ajustes organizativos que las demás nuevas obligaciones. La Comisión revisará periódicamente la Ley de Ciberresiliencia e informará sobre su funcionamiento.

Contexto

La ciberseguridad es una de las principales prioridades de la Comisión y la piedra angular de una Europa digital y conectada. El aumento de los ciberataques producidos durante la crisis del coronavirus ha puesto de manifiesto cuán importante es proteger los hospitales, los centros de investigación y otras infraestructuras. Por tanto, es necesario adoptar medidas firmes en este ámbito, para que la economía y la sociedad de la UE estén preparadas para el futuro. Se calcula que los costes anuales de las violaciones de la seguridad de los datos ascienden como mínimo a 10 000 millones de euros y los costes anuales de los intentos malintencionados de perturbar el tráfico en internet, al menos a 65 000 millones de euros(informe de evaluación de impacto que acompaña al

Reglamento Delegado de la Comisión que complementa la Directiva sobre equipos radioeléctricos).

La Estrategia de Ciberseguridad, presentada en diciembre de 2020, propone integrar la ciberseguridad en todos los elementos de la cadena de suministro y concentrar aún más las actividades y los recursos de la UE en torno a los cuatro ámbitos relacionados con la ciberseguridad, que son el mercado interior, la policía, la diplomacia y la defensa. Se basa en la Estrategia Digital Europea de la UE y en la Estrategia de la UE para una Unión de la Seguridad, así como en una serie de actos legislativos, acciones e iniciativas aplicadas por la UE con el fin de reforzar las capacidades de ciberseguridad y conseguir que Europea sea más ciberresiliente.

La nueva Ley de Ciberresiliencia completará la normativa de la UE en materia de ciberseguridad: la Directiva sobre la seguridad de las redes y los sistemas de información (Directiva SRI), la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (Directiva SRI 2), aprobada recientemente por el Parlamento Europeo y el Consejo, y el Reglamento de ciberseguridad de la UE.

Más información

Preguntas y respuestas: Ley de Ciberresiliencia de la UE

Ficha informativa sobre la Ley de Ciberresiliencia de la UE

Propuesta de Ley de Ciberresiliencia

Ficha informativa sobre la nueva Estrategia de Ciberseguridad de la UE

Ficha informativa sobre la propuesta de Directiva sobre las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (Directiva SRI 2)

Ficha informativa sobre ciberseguridad: acción exterior de la UE

Preguntas y respuestas: Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales

Propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (SRI 2)

Propuesta de Directiva sobre la resiliencia de las entidades críticas