Spread the love

El Consejo de la UE ha aprobado un nuevo Reglamento sobre los requisitos de ciberseguridad para los productos con elementos digitales. Su objetivo es garantizar que ciertos productos como las cámaras domésticas, los frigoríficos, los televisores y los juguetes conectados sean seguros antes de que se introduzcan en el mercado . Así, cubrirá las carencias del marco legislativo vigente en materia de ciberseguridad.

Los productos del internet de las cosas, deberán ser sean seguros a lo largo de la cadena de suministro y durante su ciclo de vida.

Pisa, paseo por el centro

El texto contribuye a sistematizar las exigencias legislativas de los productos con componentes digitales. **Introduce requisitos de ciberseguridad a escala de la UE para el diseño, el desarrollo, la fabricación y la introducción en el mercado de productos de hardware y software,** a fin de evitar la superposición de requisitos establecidos en diferentes actos legislativos de los Estados miembros de la UE.

- Por ejemplo, ciertos productos de software y hardware llevarán el marcado CE para indicar que cumplen los requisitos del Reglamento.
    - Recuérdese: Las letras «CE» aparecen en muchos productos comercializados en el mercado único ampliado del Espacio Económico Europeo (EEE). Significan que los productos vendidos en el EEE han sido evaluados y cumplen unos requisitos elevados en materia de seguridad, salud y protección del medio ambiente.
- El Reglamento se aplicará a todos los productos conectados, directa o indirectamente, a otro dispositivo o a una red.
- Reconoce algunas excepciones en el caso de los productos para los que ya se establecen requisitos de ciberseguridad en otras normas vigentes de la UE, por

ejemplo, los productos sanitarios y aeronáuticos y los automóviles.

Objetivos del nuevo Reglamento UE:

1. **Refuerzo de la seguridad cibernética de productos digitales**: El reglamento establece una serie de requisitos obligatorios que los fabricantes de productos con elementos digitales deben cumplir para garantizar que dichos productos sean resistentes a amenazas y ataques cibernéticos.
2. **Protección de consumidores y empresas**: Con el fin de reducir el riesgo de ataques informáticos que puedan comprometer la seguridad de los usuarios y sistemas, el reglamento busca prevenir posibles daños y garantizar que los productos en el mercado sean lo más seguros posibles.
3. **Alineación con las normativas existentes**: Se busca una mayor armonización y coordinación con otras leyes europeas de ciberseguridad, como la Directiva NIS2 (sobre la seguridad de las redes y sistemas de información) y la Estrategia Europea de Ciberseguridad.

Contenidos clave

Garexo no verán

1. **Definición de productos con elementos digitales**:
    - El reglamento define «productos con elementos digitales» como aquellos productos que contienen software o hardware capaces de interactuar con sistemas digitales (por ejemplo, dispositivos conectados a Internet, como teléfonos inteligentes, electrodomésticos inteligentes, sistemas de control industrial, etc.).
2. **Obligaciones para los fabricantes**:La propuesta establece los requisitos que se aplicarán a los fabricantes de equipos y programas informáticos para evitar una mayor fragmentación del mercado con respecto a los requisitos de ciberseguridad para los productos en el mercado interior, y para procurar no duplicar la carga normativa para los fabricantes que tienen que manejar varios instrumentos legislativos aplicables a la

seguridad de sus productos. Parte de la asunción de que , mayoritariamene, los fabricantes que entran en el ámbito de aplicación de la propuesta ya están familiarizados con el funcionamiento del nuevo marco legislativo.

Praiña Pontevea

- **Diseño seguro**: Los fabricantes deben diseñar sus productos con medidas de seguridad robustas que minimicen las vulnerabilidades cibernéticas. Esto incluye la implementación de técnicas de cifrado, autenticación, y gestión de accesos.
- **Actualizaciones y mantenimiento**: Es obligación de los fabricantes proporcionar actualizaciones periódicas de seguridad para corregir posibles vulnerabilidades que surjan durante el ciclo de vida del producto. Esta obligación se extiende al mantenimiento de los productos después de su comercialización, garantizando que los productos sean seguros durante todo su periodo de uso.
- **Gestión de riesgos**: Los fabricantes deben llevar a cabo evaluaciones de riesgos sobre posibles amenazas a la seguridad cibernética de sus productos y tomar las medidas adecuadas para mitigarlas antes de que los productos lleguen al mercado.

2. **Requisitos para los operadores del mercado**:

   Luminaria, Pisa

   - **Vigilancia de conformidad**: Las autoridades competentes deben garantizar que los productos que se comercializan en la UE cumplan con los requisitos de ciberseguridad. Esto incluye la supervisión de las pruebas de conformidad y la toma de medidas ante productos no conformes.
   - **Documentación y trazabilidad**: Los fabricantes deben asegurarse de que se disponga de documentación adecuada que demuestre que los productos cumplen con los estándares de seguridad cibernética. Esto facilita la trazabilidad en caso de incidentes de seguridad.
   - **Gestión de incidentes**: En caso de que se identifique una vulnerabilidad o un incidente de ciberseguridad, los operadores deben informar rápidamente a las autoridades competentes y a los usuarios finales sobre los riesgos y las medidas correctivas.
3. **Responsabilidad de los distribuidores y revendedores**:

Il Giardino II

    - Los distribuidores y revendedores de productos también tienen la obligación de velar por que los productos que venden cumplan con las normativas de ciberseguridad. Esto incluye verificar que los productos estén acompañados de la información pertinente sobre su seguridad y que no presenten riesgos evidentes para los consumidores.
4. **Evaluación de conformidad y sanciones**
    - El reglamento establece un sistema de evaluación de conformidad con el que los fabricantes deberán demostrar que sus productos cumplen con los requisitos de ciberseguridad antes de su comercialización. Para ello, pueden recurrir a laboratorios de pruebas acreditados que realicen una verificación de las características de seguridad de los productos.En caso de que un producto no cumpla con las exigencias de seguridad cibernética, se prevén sanciones que pueden incluir la retirada del mercado, la imposición de multas, y la obligación de actualizar los productos defectuosos.

Complementariedad con otras disposiciones

El reglamento modifica y complementa el **Reglamento (UE) 2019/1020** sobre la vigilancia del mercado y la conformidad de los productos, integrando las normas específicas sobre ciberseguridad para los productos con componentes digitales:

- Los productos que incorporen elementos digitales estarán sujetos a los requisitos de vigilancia del mercado que aseguren su seguridad cibernética.
- Se refuerzan las medidas de cooperación entre las autoridades nacionales para garantizar que los productos que no cumplen con los requisitos de ciberseguridad sean retirados rápidamente del mercado.
- Se establecen mecanismos más ágiles para gestionar los incidentes de ciberseguridad relacionados con productos defectuosos y se facilita la retirada rápida de estos productos del mercado europeo.

Este Reglamento contiene previsiones sobre su relación con el Reglamento (UE) 2019/881 que establece un marco europeo voluntario de certificación de la ciberseguridad para productos, procesos y servicios de TIC:

- Los **esquemas europeos de certificación de la ciberseguridad del Reglamento (UE) 2019/881 pueden aplicarse a productos con elementos digitales**
- A fin de facilitar la evaluación de la conformidad con los requisitos establecidos en ambos textos, se presupondrá que los productos con elementos digitales que hayan sido certificados o para los que se haya expedido una declaración de conformidad en el marco de un esquema de ciberseguridad establecido en virtud del Reglamento (UE) 2019/881 y reconocido por la Comisión mediante acto de ejecución son conformes con los requisitos esenciales del nuevo Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de estos, cubran dichos requisitos.
- La necesidad de nuevos esquemas europeos de certificación de la ciberseguridad para productos con elementos digitales será evaluada a la luz del nuevo Reglamento.
- Para evitar el exceso de carga administrativa la Comisión debe especificar si un certificado de ciberseguridad expedido en el marco de dichos esquemas europeos de certificación de la ciberseguridad elimina la obligación para los fabricantes de llevar a cabo una evaluación de la conformidad por parte de terceros, tal como dispone el presente Reglamento para los requisitos correspondientes.

En relación con el marcado CE, es decir, con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación, el nuevo reglamento reconoce que seguirá existiendo un único marcado si bien, en lo relativo a la ciberseguridad, procede a incorporar los requisitos para su uso. Señala que para que los operadores puedan demostrar la conformidad con los requisitos esenciales establecidos en el nuevo Reglamento y para que las autoridades de vigilancia del mercado puedan garantizar el cumplimiento se deben establecer procedimientos de evaluación de la conformidad. La Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo19 establece módulos de procedimientos de evaluación de la conformidad proporcionales al nivel de riesgo existente y al nivel de seguridad requerido. Para garantizar la coherencia intersectorial y evitar variantes ad hoc, los procedimientos de evaluación de la conformidad de la ciberseguridad de productos deben incluir el exámen y verificación de los requisitos relacionados con los productos y con los procesos que abarcan todo el ciclo de vida de los productos con elementos digitales, en particular la planificación, el diseño, el desarrollo o la producción, los ensayos y el mantenimiento del producto.

- Como norma general, el fabricante debe llevar a cabo la evaluación de la conformidad de los productos con elementos digitales bajo su propia responsabilidad mediante un procedimiento basado en el módulo A de la Decisión n.º 768/2008/CE. Si el producto está considerado producto crítico de la clase I, se requieren garantías adicionales

- El fabricante que opte por la evaluación de la conformidad de terceros puede elegir el procedimiento que mejor se adapte a su proceso de diseño y producción. Y en relacion con ciertos productos (clasificados como productos críticos de la clase II), la evaluación de la conformidad de estos productos siempre debe contar con la participación de un tercero.

VER: Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia), propuesta de la Comisión, 15.9.2022