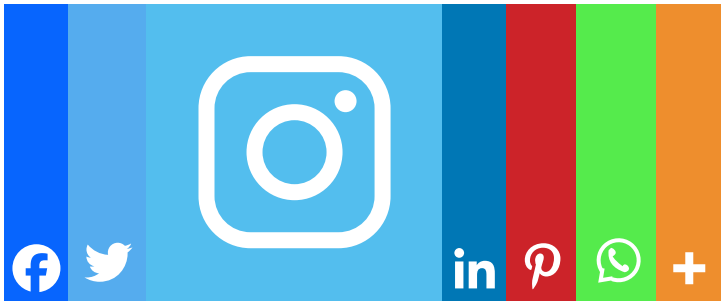
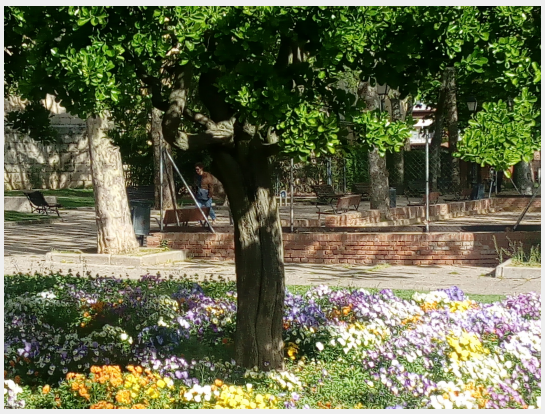
Spread the love



Los productos de hardware y software son a menudo objeto de ciberataques que causan daños. Si el coste anual directo a nivel mundial es muy elevado, hay que unirle además los costes para los usuarios y la sociedad. Un bajo nivel de ciberseguridad implica que las vulnerabilidades estén generalizadas, que las actualizaciones de seguridad sean dispuestas en modo incoherente e insuficiente, que los usuarios tengan dificultades graves para comprender y para diferenciar los productos con propiedades de ciberseguridad adecuadas, así como para utilizarlos de forma segura.

Sobre este trasfondo, la propuesta de la Comisión Europea de un Reglamento sobre Ciberresiliencia (CRA) tiene por objeto proteger a los consumidores y las empresas que compran o utilizan productos o programas informáticos con un componente digital. El Reglamento de Resiliencia de Productos con elementos digitales (CRA) o **Propuesta de Reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020** propuesto en septiembre de 2022 había sido anunciado en la Estrategia de Ciberseguridad de la UE 2020, y es un complemento de NIS2 **. Se aplicará a todos los productos conectados directa o indirectamente a otro dispositivo o red, salvo exclusiones específicas** como el software de código abierto o los servicios que ya están cubiertos por normas existentes, como es el caso de los dispositivos médicos, la aviación, los automóviles y servicios SaaS (en la nube), a menos que estos sirvan para la elaboración de productos con elementos digitales.



Primaveras en primavera

ANTECEDENTES

Los abundantes ciberataques y ciber-incidentes que se van conociendo ponen en evidencia el inadecuado nivel de ciberseguridad inherente a muchos productos, o las insuficientes actualizaciones de seguridad de tales productos y programas informáticos. También denotan la dificultad de los consumidores y las empresas para determinar qué productos son ciberseguros, o para configurarlos de forma que se garantice su ciberseguridad.

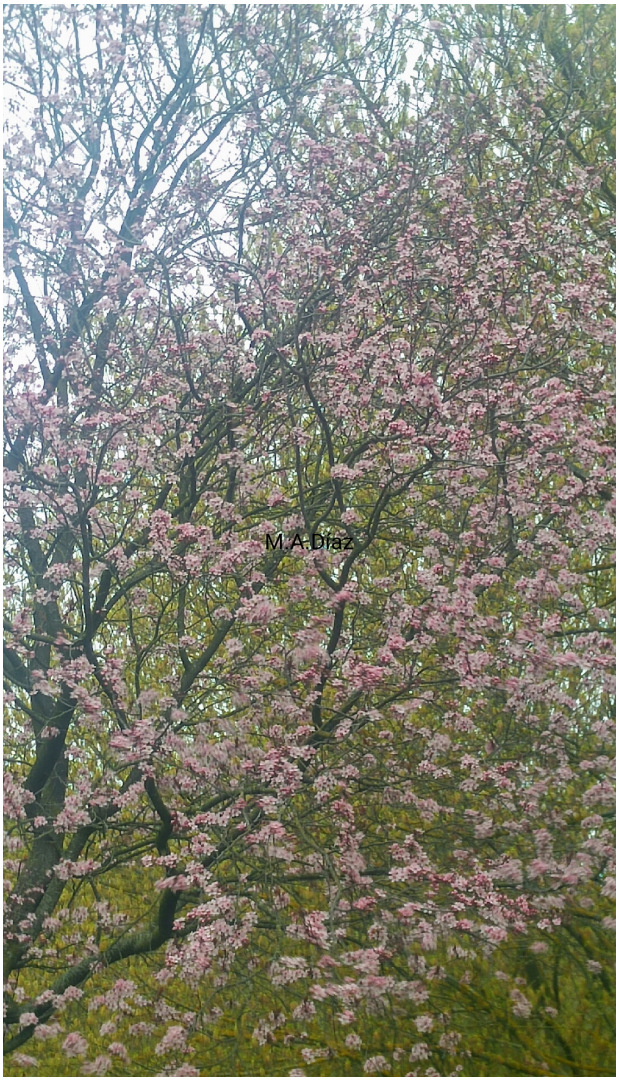
Aunque el ordenamiento de la UE ya se aplica a determinados productos con elementos digitales, la mayoría del hardware y software no están cubiertos actualmente por legislación de la UE que aborde su ciberseguridad. En particular, el actual marco jurídico de la UE no aborda la ciberseguridad de los programas informáticos no integrados, aun cuando muchos ataques se dirigen cada a sus vulnerabilidades y dan lugar a importantes costes sociales y económicos.El Reglamento de Resiliencia de Productos con elementos digitales (CRA) propuesto en septiembre de 2022 había sido anunciado en la Estrategia de Ciberseguridad de la UE 2020, y es un complemento de NIS2 .

PROPUESTA DE REGLAMENTO DE RESILIENCIA (DE PRODUCTOS)

La propuesta introduce un marcado CE sobre ciberseguridad que ha de colocarse en todos los productos cubiertos y establece requisitos obligatorios de ciberseguridad para los fabricantes de productos: Amplía la protección a lo largo de todo el ciclo de vida del producto. Incorpora normas armonizadas para comercializar productos o programas informáticos con un componente digital con requisitos de ciberseguridad para la planificación, el diseño, el desarrollo y el mantenimiento de tales productos. Impone obligaciones que deberán cumplirse en cada etapa de la cadena de valor y una obligación de diligencia durante todo el ciclo de vida de tales productos. La CRA persigue cuatro objetivos:

1. **garantizar que los fabricantes mejoren la seguridad de los productos que tienen elementos digitales en la fase de diseño y desarrollo y a lo largo de todo su ciclo de vida.** Así, el fabricante es apto para comercializar sus productos si pone a disposición la lista de los diversos componentes de software de sus productos, emite rápidamente soluciones gratuitas en caso de nuevas vulnerabilidades, publica y detalla las vulnerabilidades que detecta y resuelve y verifica periódicamente la «solidez» de los productos que comercializa. Estas y otras actividades deben llevarse a cabo durante toda la vida de un producto, o al menos durante cinco años a partir de su introducción en el mercado.;
2. **garantizar un marco coherente de normas de ciberseguridad**, facilitando su cumplimiento por parte de los fabricantes de hardware y software;
3. **mejorar la transparencia de las características de seguridad** de los productos con elementos digitales;
4. permitir que las **empresa y los consumidores utilicen estos productos de manera segura**.

Se destacan aquí algunas definiciones extraídas de la Propuesta (artículo 3), y otros conceptos importantes:



- Producto con elementos digitales. «*cualquier producto consistente en programas informáticos o equipos informáticos y sus soluciones de tratamiento de datos a distancia, incluidos los componentes de programas informáticos o equipos informáticos que se introduzcan en el mercado por separado*». Nótese la que definición de «productos con elementos digitales» es muy amplia e incluye cualquier producto de software o hardware, así como cualquier software o hardware no incorporado al producto pero introducido en el mercado por separado.
- Operador económico: *el fabricante, el representante autorizado, el importador, el*

distribuidor o cualquier otra persona física o jurídica sujeta a las obligaciones establecidas en el presente Reglamento»

- Marcado CE. *Un marcado con el que un fabricante indica que un producto con elementos digitales y los procesos establecidos por el fabricante son conformes con los requisitos esenciales establecidos en el anexo I (del Reglamento) y otras normas de la Unión aplicables que armonicen las condiciones para la comercialización de productos y prevean su colocación*
- Norma armonizada, conforme a la definición del artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012;
- Organismo de evaluación de la conformidad, según se define en el artículo 2, punto 13, del Reglamento (UE) n.º 765/2008;

- La definición de «productos con elementos digitales» es muy amplia e incluye cualquier producto de software o hardware, así como
  cualquier software o hardware no incorporado al producto pero introducido en el mercado por separado.
- Se considera que un producto es «seguro» si está diseñado y fabricado de manera que tenga un nivel de seguridad adecuado a los riesgos cibernéticos que conlleva su uso, no presenta vulnerabilidades conocidas en el momento de su venta, tiene una configuración segura por defecto, está protegido de conexiones ilícitas, protege los datos que recopila y si esta recopilación se limita a aquellos datos que sean necesarios para su funcionamiento

Conforme al CRA, la seguridad de los productos y *software* «normales» – sobre el 90% de los que circulan en el mercado- se puede confiar en una autoevaluación del fabricante, como ya ocurre con otros tipos de certificación del marcado CE. En relación con éstos productos, el fabricante podrá comercializarlos si realiza una autoevaluación, que también será preceptiva cuando se modifica el producto. El 10 % restante de los productos se divide los de la clase I, menos peligrosos; y los de la clase II, más peligrosos («productos críticos con elementos digitales»). Para los productos de la clase 1 las autocertificaciones básicas solo son admisibles si el fabricante ha seguido normas específicas de mercado y especificaciones

de seguridad o certificaciones de ciberseguridad ya previstas por la UE. En caso contrario, necesita obtener la certificación del producto por parte de un organismo de certificación acreditado. La certificación externa es obligatoria para los productos de la clase II

Algunos productos afectados por el CRA están también sometidos al futuro Reglamento IA, que también clasifica a los productos conforme a su riesgo. Para evitar solapamientos y dudas, la CRA establece que -por regla general- los productos con elementos digitales clasificados también como «sistemas de IA de alto riesgo» con arreglo al Reglamento IA lo serán también para CRA, tendrán que cumplir el procedimiento de evaluación de conformidad establecido en el Reglamento IA, y en el caso de los «productos digitales críticos» se les aplicarán también las normas de evaluación de la conformidad de CRA.Las sanciones por incumplimiento de CRA —en función de la gravedad de la infracción— pueden llegar a ascender a 15 millones EUR o al 2,5 % del volumen de negocios del ejercicio fiscal anterior.

Miño- Perbes. A Coruña

Más:

- Ver comentario INCIBE
- Dictamen CES (EU)
- Resumen del Dictamen SEPD (EU)
- Entrada reciente relacionada (RC por IA)
- Propuesta relacionada. Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos (28.09.2022)
- Reglamento relacionado: Reglamento (UE) 2023/988 de 10 de mayo de 2023 relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.o 1025/2012 y la Directiva (UE) 2020/1828 y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo