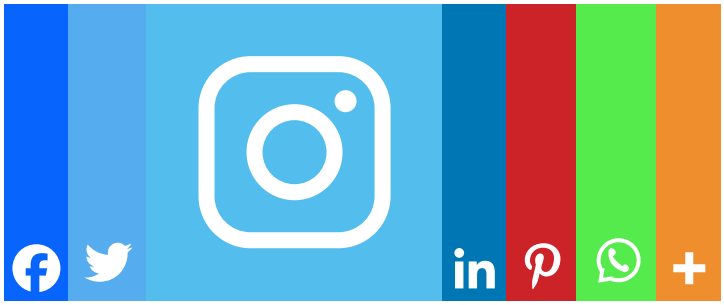
Spread the love



La Comisión presentó una propuesta de nueva Ley de Ciberresiliencia o Reglamento **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 (**COM(2022) 454 final). **Introduce requisitos obligatorios de ciberseguridad para los productos con elementos digitales, a lo largo de todo su ciclo de vida**. Sobre aquella propuesta habíamos comentado aquí.

La propuesta se basa en el nuevo marco legislativo de la UE en materia de productos y establece por un lado, **normas para la comercialización de productos con elementos digitales** para garantizar su ciberseguridad; por otro **requisitos esenciales para el diseño, el desarrollo y la producción** de productos con elementos digitales, y **obligaciones para los operadores económicos** en relación con estos productos; también requisitos esenciales para los **procesos de gestión de la vulnerabilidad** establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales durante todo el ciclo de vida, y obligaciones para los operadores económicos en relación con estos procesos, incluyendo **obligaciones de los fabricantes de informar de las vulnerabilidades e incidentes** explotados activamente. Además, establece **normas sobre vigilancia del mercado y aplicación de la legislación.** En conjunto, esta propuesta llamada «Ley de Ciber resiiencia» refuerza las normas de ciberseguridad para garantizar productos de hardware y software más seguros.

Gladiolo

Debe recordarse que los productos de hardware y software son cada vez más objeto de ciberataques con éxito. Ello implica un coste anual mundial estimado de 5,5 billones de euros para 2021. Estos productos adolecen de dos grandes problemas, un bajo nivel de ciberseguridad con vulnerabilidades generalizadas y suministro insuficiente e incoherente de actualizaciones de seguridad para abordarlas; y una comprensión y un acceso a la información insuficientes por parte de los usuarios (les impide elegir productos con propiedades de ciberseguridad adecuadas o utilizarlos de forma segura).

Hoy, la mayoría de los productos de hardware y software no están cubiertos la legislación de la UE sobre ciberseguridad. En particular, el actual marco jurídico de la UE no aborda la ciberseguridad de los programas informáticos no integrados, aun cuando son objeto de ciberataques a menudo.

La propuesta tiene dos objetivos principales, en relación con los productos.

- crear las condiciones para el **desarrollo de productos seguros con elementos digitales,** garantizando que los productos de hardware y software se comercialicen con menos vulnerabilidades y velando por que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida del producto; y
- crear **condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de seleccionar y utilizar** productos con elementos digitales.

Y cuatro objetivos específicos:

1. que los **fabricantes mejoren la seguridad de los productos con elementos**

digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida;

2. garantizar un **marco coherente de ciberseguridad que facilite el cumplimiento** de la normativa a los fabricantes de hardware y software
3. aumentar la **transparencia de las propiedades de seguridad de los productos** con elementos digitales, y
4. **fomentar que las empresas y los consumidores utilicen los productos con elementos digitales de forma segura.**

Documentación técnica (art 23 de la propuesta)
La documentación técnica debe elaborarse antes de que el producto con elementos digitales se introduzca en el mercado y, en su caso, se mantendrá permanentemente actualizada durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto con elementos digitales en el mercado, si este período fuese más breve

Marcado CE «Conformité Européenne (preámbulo 32 y art 21 de la propuesta)
El marcado CE indica la conformidad de un producto, es el resultado visible de todo un proceso que comprende la evaluación de la conformidad en sentido amplio. Los principios generales por los que se rige el marcado CE se establecen en el Reglamento (CE) n.º 765/2008 Ahora, con esta propuesta de ciber resiliencia se establecen disposiciones relativas a la colocación del marcado CE en productos con elementos digitales, siendo el marcado CE el único marcado que garantice que los productos con elementos digitales cumplen con los requisitos Téngase en cuenta que cuando existe reserva de Marcado CE, esta mención es obligatoria. Conforme a la propuesta, los productos con elementos digitales deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno.

- El marcado CE, tal como se define en el artículo 3, punto 32, estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.: ««*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 y otras normas de la Unión aplicables que armonicen las condiciones para la comercialización de productos (las «normas de armonización de la Unión») y prevean su colocación»

- Se siguen las reglas de colocación, tamaño etc del art 22

En relación con este marcado la Comisión estará facultada para adoptar actos de ejecución con el fin de especificar el formato o los elementos de los informes obligatorios y la nomenclatura de materiales de los programas informáticos, especificar los esquemas europeos de certificación de la ciberseguridad que puedan utilizarse para demostrar la conformidad con los requisitos esenciales o partes de estos establecidos en el presente Reglamento, adoptar especificaciones comunes, establecer especificaciones técnicas para la colocación del marcado CE y adoptar medidas correctoras o restrictivas a escala de la Unión en circunstancias excepcionales que justifiquen una intervención inmediata destinada a preservar el buen funcionamiento del mercado interior.

Tareas encomendadas a ENISA

- Recibir notificaciones de los fabricantes relativas a las vulnerabilidades presentes en los productos con elementos digitales y sobre los incidentes que repercutan en la seguridad de dichos productos.
- Transmitir estas notificaciones a los equipos de respuesta a incidentes de seguridad informática (CSIRT) pertinentes o, según corresponda, a los puntos de contacto únicos de los Estados miembros designados de conformidad con DNIS2, así como informar a las autoridades de vigilancia del mercado pertinentes sobre la vulnerabilidad notificada.
- Elaborar un informe técnico bienal sobre las tendencias emergentes en relación con los riesgos de ciberseguridad en productos con elementos digitales y presentarlo al Grupo de Cooperación
- Apoyar el proceso de ejecución del Reglamento. En particular, proponer actividades conjuntas que las autoridades de vigilancia del mercado deberán llevar a cabo sobre la base de determinadas indicaciones o información sobre el posible incumplimiento en productos con elementos digitales en varios Estados miembros, o de identificar

categorías de productos para las que deban organizarse acciones de control simultáneas coordinadas.
- En circunstancias excepcionales que requieran una intervención inmediata, la ENISA, a petición de la Comisión, realizará evaluaciones relativas a productos específicos con elementos digitales que presenten un riesgo de ciberseguridad significativo.

Evaluación de conformidad (arts. 25 ss. de la Propuesta)

- Recuérdese que la conformidad de un producto se efectúa antes de su comercialización. Consiste en demostrar que se cumplen todos los requisitos legislativos. Incluye pruebas, inspección y certificación.
- En general, la legislación de productos describe los procedimientos de evaluación de la conformidad para cada producto. En concreto, para cada producto se especifica en la legislación de producto aplicable, y , el fabricante puede elegir entre diferentes procedimientos de evaluación de la conformidad disponibles para sus productos, en su caso.
- En alunos casos, la evaluación la realizaría el fabricante salvo cuando a legislación requiere la intervención de un organismo de evaluación de conformidad.
- Dentro de la evaluación de la conformidad, el fabricante o el representante autorizado debe redactar una declaración de conformidad (DoC). La declaración debe contener toda la información para identificar:
    - Producto
    - Legislación aplicable a ese producto
    - Fabricante o el representante autorizado
    - Organismo notificado si procede
    - Una referencia a normas armonizadas u otros documentos normativos, cuando proceda
- **En relación con esta Propuesta, los Estados miembros notificarán a la Comisión y a los demás Estados miembros los organismos de evaluación de la conformidad autorizados a realizar evaluaciones de la conformidad con arreglo al presente Reglamento.**

Azaleas

A propósito de los organismos notificados los organismos de evaluación de conformidad (art 29 ss de la Propuesta). Y repaso al sistema de acreditación

- Con carácter general, el organismo notificado es una organización **designada por un país de la UE para evaluar la conformidad de determinados productos antes de su comercialización.** Estos organismos llevan a cabo tareas relacionadas con los procedimientos de evaluación de la conformidad establecidos en la legislación aplicable a petición de terceros como los fabricantes. La Comisión Europea publica una lista de dichos organismos notificados. En España, los Organismos Notificados deben contar con la aprobación previa de ENAC (Entidad Nacional de Acreditación). Conforme al Reglamento (CE) n.o 765/2008 la ENAC es ,en España, el organismo de acreditación: el único organismo de un Estado miembro con potestad pública para llevar a cabo acreditaciones. Estas acreditaciones son también definidas en el mismo Reglamento: *declaración por un organismo nacional de acreditación de que un organismo de evaluación de la conformidad cumple los requisitos fijados con arreglo a normas armonizadas y, cuando proceda, otros requisitos adicionales, incluidos los*

establecidos en los esquemas sectoriales pertinentes, para ejercer actividades específicas de evaluación de la conformidad

Rasgos generales de estos ONEC:

- **Imparcialidad:** su personal tiene competencia técnica libre de incentivos económicos que tienten su criterio
- **Confidencialidad:** garantizan el secreto profesional y tienen seguro de responsabilidad civil
- **Independencia:** tienen personalidad jurídica propia e independiente de la organización evaluada. En este sentido, ni los directivos ni el personal podrán diseñar, instalar, proveer, fabricar, mantener…nada que pueda entrar en conflicto con su independencia, en especial los servicios de consultoría. Los organismos notificados de certificación, son conforme al R (CE) 765/2008 organizaciones que desempeñan actividades de evaluación de la conformidad, que incluyen calibración, ensayo, certificación e inspección.

Rasgos específicos de los ONEC en la Propuesta:

- Están sometidos a las reglas específicas de notificación (art 29, apartados 2 a 12).
- Los organismos de evaluación de la conformidad se establecerán con arreglo al Derecho nacional y tendrán personalidad jurídica. Pueden pertenecer a una asociación comercial o una federación profesional que represente a las empresas que participan en el diseño, el desarrollo, la producción, el suministro, el montaje, el uso o el mantenimiento de los productos con elementos digitales que evalúen, *a condición de que se demuestre su independencia y la ausencia de conflictos de interés.*
    - Es establecen incompatibilidades: Ni el ONEC, ni sus directivos de más alto rango, ni el personal responsable de la realización de las tareas de evaluación de la conformidad pueden realizar funciones de diseño, desarrollo, fabricación, provisión de servicios de instalación. Ni serán el comprador, el dueño, el usuario o el encargado del mantenimiento de los productos con elementos digitales que

deben evaluarse. Ni el representante autorizado de ninguno de ellos. Tampoco intervendrán directamente en el diseño, el desarrollo, la producción, la comercialización, la instalación, el uso ni el mantenimiento de estos productos, ni representarán a las partes que participen en estas actividades. No realizarán ninguna actividad que pueda entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que hayan sido notificados (en particular, esta incompatibilidad afecta a los servicios de consultoría). No obstante, estas incompatibilidades no serán óbice para que usen los productos evaluados que sean necesarios para el funcionamiento del propio ONEC o con fines personales.

- Los ONEC se asegurarán de que las actividades de sus filiales o subcontratistas no afecten a la confidencialidad, objetividad o imparcialidad de sus actividades de evaluación de la conformidad.
- Los ONEC y su personal actuarán con el máximo nivel de integridad profesional y con la competencia técnica exigida para el campo específico. Estarán libres de cualquier presión o incentivo, especialmente de índole financiero, que pudieran influir en su apreciación o en el resultado de sus actividades de evaluación de la conformidad, en particular por parte de personas o grupos de personas que tengan algún interés en los resultados de estas actividades.
- El ONEC capaz de realizar todas las tareas de evaluación de la conformidad especificadas en el anexo VI de la Propuesta y para las que haya sido notificado, independientemente de si realiza las tareas el propio organismo o si se realizan en su nombre y bajo su responsabilidad.

En todo momento, para cada procedimiento de evaluación de la conformidad y para cada tipo o categoría de productos con elementos digitales para los que ha sido notificado, el organismo de evaluación de la conformidad dispondrá:

a. de personal con conocimientos técnicos y experiencia suficiente y adecuada para realizar las tareas de evaluación de la conformidad;
b. de las descripciones de los procedimientos con arreglo a los

cuales se efectúa la evaluación de la conformidad, garantizando la transparencia y la posibilidad de reproducción de estos procedimientos; dispondrá también de las políticas y procedimientos adecuados que permitan distinguir entre las tareas efectuadas como organismo notificado y cualquier otra actividad;

c. de procedimientos para desempeñar sus actividades teniendo debidamente en cuenta el tamaño de las empresas, el sector en que operan, su estructura, el grado de complejidad de la tecnología del producto y el carácter masivo o en serie del proceso de producción.
d. dispondrá de los medios necesarios para realizar adecuadamente las tareas técnicas y administrativas relacionadas con las actividades de evaluación de la conformidad y tendrá acceso a todo el equipo o las instalaciones que necesite. El personal encargado de llevar a cabo las tareas de evaluación de la conformidad dispondrá de:
    a. una buena formación técnica y profesional para realizar todas las actividades de evaluación de la conformidad para las que el organismo de evaluación de la conformidad haya sido notificado;
    b. un conocimiento satisfactorio de los requisitos de las evaluaciones que efectúe y la autoridad necesaria para efectuarlas
    c. un conocimiento y una comprensión adecuados de los requisitos esenciales, de las normas armonizadas aplicables y de las disposiciones pertinentes de las normas de armonización de la Unión aplicables, así

como de las normas de aplicación correspondientes;

d. capacidad necesaria para elaborar certificados, documentos e informes que demuestren que se han efectuado las evaluaciones.

Se garantizará la imparcialidad de los organismos de evaluación de la conformidad, de sus directivos de alto rango y del personal de evaluación.

- La remuneración de los directivos de alto rango y del personal de evaluación de los organismos de evaluación de la conformidad no dependerá del número de evaluaciones realizadas ni de los resultados de dichas evaluaciones.

Garantías frente a responsabilidad

- El organismo de evaluación de la conformidad *suscribirá un seguro de responsabilidad,* salvo que el Estado asuma la responsabilidad con arreglo al Derecho interno, o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

Secreto

- El personal del organismo de evaluación de la conformidad deberá observar el secreto profesional acerca de toda la información recabada en el ejercicio de sus tareas, con arreglo al anexo VI o a cualquier disposición de Derecho interno por la que se aplique, salvo con respecto a las autoridades de vigilancia del mercado del Estado miembro en que realice sus actividades. Se protegerán los derechos de propiedad. El organismo de evaluación de la conformidad contará con procedimientos documentados que garanticen el cumplimiento del presente apartado.

Zarzas y lila

Otras cuestiones

- Los ONEC participarán en las actividades pertinentes de normalización y las actividades del grupo de coordinación de los organismos notificados establecido con arreglo al artículo 40, o se asegurarán de que su personal de evaluación esté informado al respecto, y aplicarán a modo de directrices generales las decisiones y los documentos administrativos que resulten de las labores del grupo.
- Los ONEC funcionarán con arreglo a un conjunto de condiciones coherentes, justas y razonables que tengan particularmente en cuenta los intereses de las pymes en relación con las tasas.

Presunción de conformidad/ subcontrataciones y filiales de los organismos notificados

- **Artículo 30.- Presunción de conformidad .** Si un ONEC declara la conformidad de productos con los criterios establecidos en las normas armonizadas (o parte de ellas) cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea, se presumirá que tales productos cumples los requisitos establecidos en el artículo 29 de la propuesta, en la medida en que las normas armonizadas aplicables cubran estos requisitos.
- **Artículo 31. Subcontrataciones y filiales de los ONEC:** 1.Cuando un ONEC subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplen los requisitos establecidos en el artículo 29 e informará a la autoridad notificante en consecuencia. 2.El ONEC asumirá la plena responsabilidad de las tareas realizadas por los subcontratistas o las filiales, con independencia de dónde estén establecidos. 3.Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del fabricante. 4.Los ONEC mantendrán a disposición de la autoridad notificante los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial, así como sobre el trabajo que estos realicen con arreglo al presente Reglamento (esta Propuesta).