Ley de Ciberresiliencia

José Almirón López
Hilario José Bandrés Sasal

Tabla de contenido

¿Qué es?

Esta propuesta busca mejorar la ciberseguridad en productos con componentes digitales, como dispositivos del Internet de las cosas y programas informáticos, con el objetivo de proteger a los consumidores y las empresas que utilizan estos productos. Para lograrlo, se plantean dos objetivos principales:

1. Garantizar que los productos con componentes digitales sean seguros a lo largo de su ciclo de vida y que los fabricantes tomen en serio la seguridad desde la etapa de diseño hasta la obsolescencia del producto. Esto implica la introducción de requisitos obligatorios de ciberseguridad para los fabricantes y minoristas, con el fin de reducir las vulnerabilidades en estos productos.

2. Facilitar a los usuarios la capacidad de evaluar y seleccionar productos con elementos digitales que sean seguros en términos de ciberseguridad. Actualmente, muchos consumidores y empresas tienen dificultades para determinar la seguridad de los productos o configurarlos adecuadamente para protegerse contra amenazas cibernéticas.

En resumen, esta propuesta busca establecer estándares más estrictos de ciberseguridad para productos con componentes digitales y empoderar a los usuarios para tomar decisiones informadas en la elección y uso de estos productos. Esto tiene como objetivo final mejorar la seguridad en el entorno digital y proteger los intereses de consumidores y empresas.

Problemas que busca solucionar

Esta propuesta tiene como objetivo resolver dos problemas relacionados con productos digitales, como dispositivos de Internet de las cosas y programas informáticos:

1. **Falta de Seguridad**: Muchos de estos productos tienen un nivel bajo de seguridad cibernética, lo que significa que son vulnerables a ataques y amenazas en línea. Esto pone en riesgo la privacidad y la integridad de los usuarios.

2. **Falta de Información**: Los consumidores y las empresas a menudo no tienen acceso a información suficiente para tomar decisiones informadas sobre la seguridad de estos productos. No saben si son seguros ni cómo configurarlos de manera segura.

Esta propuesta busca abordar estos problemas y garantizar que los productos digitales sean más seguros y que los usuarios puedan utilizarlos de manera segura sin preocupaciones.

Requisitos

La propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para productos con elementos digitales se aplicará a todos los productos con elementos digitales cuyo destino y cuyo uso razonablemente previsible incluye una conexión de datos lógica o física directa o indirecta a un dispositivo o una red.

- Normas para reequilibrar la responsabilidad de los fabricantes, que deben garantizar la conformidad de los productos con los requisitos de seguridad digitales en el mercado de la UE, incluidas la evaluación del riesgo de ciberseguridad, la declaración de conformidad y la cooperación con las autoridades competentes.
- Requisitos esenciales para los procesos de gestión de la vulnerabilidad para los fabricantes para garantizar la ciberseguridad de los productos digitales, y las obligaciones para los operadores económicos, como importadores o distribuidores, en relación con estos procesos.
- Medidas para mejorar la transparencia de la seguridad de los productos de hardware y software para los consumidores ya las empresas, y en un marco de vigilancia del mercado para hacer cumplir estas normas.
- Obligaciones de notificación de vulnerabilidades o incidentes a las autoridades nacionales competentes en lugar de a la agencia de la IE para la ciberseguridad y establecimiento de una plataforma única de presentación de informes.
- Elementos para determinar la vida útil esperada del producto.

- Permitir a las empresas y consumidores utilizar de forma segura productos que contienen elementos digitales.
- Establecer un reglamento de vigilancia y fiscalización del mercado.
- Se excluyen los dispositivos médicos o relacionados con la aviación, así como vehículos y productos militares.

Propósito

El propósito de la ley es responsabilizar más a los vendedores y proveedores, obligándolos a brindar soporte de seguridad y actualizaciones de software para solucionar las vulnerabilidades identificadas a lo largo de todo su ciclo de vida, y brindar a los consumidores más información sobre los productos en el mercado.

Se establece también que se debe dar soporte con vulnerabilidades durante todo el ciclo de vida del software o durante 5 años, todo de manera efectiva.

Diferenciación

Estos productos se dividen en dos clases.

- **Clase II** – Se consideran los productos críticos en función de la intensidad y amplitud del impacto potencial de la explotación de las vulnerabilidades presentes en ellos. Se presta especial atención a si operan en entornos sensibles o si tienen funciones esenciales en las que, por ejemplo, procesan datos confidenciales.
  Estos incluyen sistemas operativos para servidores, ordenadores de sobremesa y móviles, microprocesadores de propósito general y criptoprocesadores seguros, entre muchos otros. Los cortafuegos, los sistemas de detección o prevención de intrusiones, así como algunos routers o módems que pueden pertenecer a uso industrial.

- **Clase I** – Incluyen software de gestión de acceso privilegiado, gestores de contraseñas, navegadores autónomos e integrados, sistemas de gestión de redes y sistemas de gestión de configuración de aplicaciones, entre muchos otros.

Obligaciones

- Es imprescindible realizar evaluaciones de riesgo continuas de los productos para garantizar la ausencia de vulnerabilidades de seguridad explotables en sus fases de diseño, desarrollo y producción. Así se minimizarían los riesgos y se evitarían muchos incidentes e impactos graves.
- Una vez en el mercado, las vulnerabilidades detectadas en ellos deben corregirse lo antes posible, y los usuarios deben recibir los parches o actualizaciones correspondientes, así como descripciones e instrucciones pertinentes. En cuanto a los incidentes, también se deben informar de ellos a los usuarios para que reaccionen con rapidez y, si es posible, apliquen medidas correctoras.
- Los fabricantes deben tener y mantener políticas y procedimientos adecuados para la documentación, gestión, corrección y divulgación de las vulnerabilidades de sus productos notificadas por fuentes internas y externas.
- Las vulnerabilidades en explotación u otros incidentes de ciberseguridad deben notificarse a la Agencia de Ciberseguridad de la Unión Europea en las 24 siguientes a su identificación. Se requiere incluir detalles de la vulnerabilidad y, en su caso, cómo se ha tratado o detalles del incidente, su impacto y posibles causas.
- Como parte de la concienciación social, los usuarios deben obtener información que vaya más allá de la funcionalidad de estos productos e implique aspectos de ciberseguridad para tener en cuenta para su selección y uso.
- Como prueba explícita del cumplimiento de este reglamento, cada fabricante debe redactar y mantener una declaración UE de conformidad. Antes de que su producto entre en el mercado, también debe elaborar una documentación técnica en la que se detallen los medios utilizados para garantizar que el producto cumpla con los requisitos fundamentales de este reglamento.

Sanciones

- El incumplimiento de los requisitos esenciales puede dar lugar a multas administrativas de hasta 15 millones de euros, o en caso de una empresa de hasta el 2,5% de sus ingresos globales.
- De acuerdo con la lógica anterior, dichos valores podrían ascender hasta los 10 millones de euros o el 2% de los ingresos globales para los casos de incumplimiento de otras obligaciones reglamentarias.
- En los casos de información errónea, insuficiente o engañosa facilitada a las autoridades pertinentes, dichas multas podrían ascender hasya 5 millones de euros o el 1% de los ingresos globales.

Puesta en práctica

Podemos encontrar esta ley puesta en práctica de las siguientes maneras, por ejemplo, tenemos un catálogo de productos de Seguridad TIC donde se registran todos los productos TIC que han sido evaluados bajo esquemas de certificación de ciberseguridad por laboratorios acreditados e independientes y bajo la supervisión del CCN, para asegurar que cumplen los más altos estándares de seguridad.

Este catálogo tiene por objetivo ser una referencia para el sector público español y las empresas que les dan servicio, en las licitaciones y compras de productos TIC.

Se dividen en dos evaluaciones como ya se había recalcado anteriormente ya que las de **clase II** tienen que cumplir con los estándares de la certificación más alta y los de **clase I** pueden simplemente adaptarse a la certificación media.

Common Criteria

Common Criteria es una norma internacional y la certificación más reconocida utilizada para evaluar la seguridad de los productos de TIC. Esta certificación es exigida en algunas ocasiones por diferentes normativas. Un certificado de Common Criteria proporciona siempre una ventaja competitiva, al brindar confianza a los clientes y usuarios. El vendedor o fabricante puede especificar los requisitos funcionales de seguridad y los requisitos de garantía de la seguridad mediante el uso de perfiles de protección.

Certificación LINCE

LINCE es una metodología de evaluación y certificación para productos de seguridad TIC desarrollada por el Centro Criptológico Nacional. Se ha desarrollado para ser un medio objetivo que permita valorar y acreditar la capacidad de un producto TIC para manejar información de forma segura.

Esta metodología está pensada para productos TIC con necesidad de certificación cuya criticidad en cuanto a seguridad es media o baja. De esta forma, los costes son accesibles para todo tipo de fabricantes.

El objetivo de una evaluación LINCE es permitir a un laboratorio de evaluación verificar si un producto es conforme a su especificación, determinando la efectividad de la funcionalidad de seguridad implementada. Esta evaluación se lleva a cabo en base a la experiencia del laboratorio, la información contenida en la documentación del fabricante y en la información del producto que provenga de fuentes públicas.

Resumen

1. ¿Cuál es el objetivo principal de la ley que te ha tocado?

Esta ley nace con el objetivo de evitar la falta de seguridad y de información acerca de los productos que tengan incorporado dispositivos digitales, tanto en hardware como en software.

2. ¿A quiénes se aplica la ley que te ha tocado?

La ley protege a cualquier producto con elementos digitales lo cual 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.

Solo se excluyen los productos de carácter médico y los relacionados con la aviación civil, los vehículos y los productos militares. La propuesta tampoco cubre los servicios software como servicio, a menos que estos sirvan para la elaboración de productos con elementos digitales.

3. ¿Cuáles son los sectores críticos que la ley que te ha tocado pretende proteger?

Esta ley pretende proteger sobre todo a los usuarios ya que pueden tener más información acerca de lo que se compra además de garantizar una seguridad óptima para estos.

4. ¿Qué requisitos específicos impone la ley que te ha tocado?

- Evaluación de vulnerabilidades constantes antes y durante la salida al mercado.
- Comunicación de las vulnerabilidades encontradas en un periodo de 24 horas.
- Información del producto en términos de ciberseguridad.

5. ¿Cuáles son las obligaciones de notificación de incidentes que deben cumplir las organizaciones bajo la ley que te ha tocado?

Debe notificarse a la Agencia de Ciberseguridad de la Unión Europea en las 24 horas siguientes a su identificación

6. ¿Cuál es el papel de las autoridades nacionales de ciberseguridad con respecto a la ley que te ha tocado?

Por ejemplo, el CCN ha creado un catálogo donde están recogidos todos los productos que han pasado unas validaciones de seguridad cibernética.

7. ¿Qué sanciones se pueden aplicar en caso de incumplimiento de la ley que te ha tocado?

- 15 millones de euros o hasta el 2,5% de los ingresos por requisitos esenciales
- 10 millones de euros o hasta el 2% de los ingresos por otras obligaciones.
- 5 millones de euros o hasta el 1% de los ingresos por información errónea o engañosa.

8. ¿Cuál es el marco de cooperación establecido por la ley que te ha tocado entre los Estados miembros de la Unión Europea?

- Poner sanciones muy elevadas para garantizar la correcta implementación de esta ley.
- Protege el ciudadano o a las empresas contra posibles herramientas sin la suficiente seguridad informática.

Presentación

Enlace a la presentación

Bibliografía

- Incibe
- Delta Protect
- Ministerio de asuntos económicos y transformación digital
- Jtsec
- App+ Laboratories