EU Cyber Resilience Act

Requisitos horizontales de ciberseguridad para los productos con elementos digitales

#WordPress

¡Hola!

Soy **Javier Casares**

- profiles.w.org/javiercasares
- robotstxt.es
- wpvulnerability.com
- 𝕏 @JavierCasares

- Hosting Team rep
- Advanced Documentation lead
- Documentation Translation lead

IMPORTANTE

No soy abogado (aunque me he leído todas las leyes que afectan a Internet).

La CRA por ahora es una propuesta, no tenemos la última versión.

Esto que voy a explicar puede cambiar en los próximos meses.

Lo que diga no podrá ser utilizado en mi contra.

Qué es la CRA

CRA = Cyber Resilience Act

- *aka* Ley de Ciber Resiliencia
- 15 de septiembre de 2022

Aplica a “productos” (hardware y software)

Disponible en línea en bit.ly/leyciberresiliencia

¿Para qué?

- Productos más seguros
- Usuarios más seguros

Excepciones: coches, dispositivos médicos o aviones.

(tienen sus propias leyes de ciberseguridad)

Objetivos

Mejorar la seguridad de los productos

Marco de seguridad estándar

Transparencia en seguridad

Uso de productos seguros

Estas medidas deben, entre otras cosas, garantizar la seguridad en la adquisición, el desarrollo y el mantenimiento de las redes y sistemas de información, incluidas la gestión y la divulgación de las vulnerabilidades.

Productos seguros ¿verdad?

Todos queremos productos seguros y que no nos *hackeen*.

¡PUES EMPIEZA POR **ACTUALIZAR**!

tu Windows / Mac / Linux

tu Móvil / portátil

tus cosas

¡Hola, soy tu nueva nevera!

Enfrío

Hago hielo

Soy “lista” *(smart)*

- *Recibes alertas en tu móvil*
- *Puedo dar “un golpe de frío” (si lo pides)*

Incluyo un software conectado a Internet…

… estoy conectada a tu Wi-Fi

… si te descuidas, me calientan

Obligaciones del fabricante

Llevarán a cabo una evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales.

Incluirá en la documentación técnica una evaluación de riesgos de ciberseguridad.

Ejercerán la diligencia debida al integrar componentes procedentes de terceros en productos con elementos digitales.

Obligaciones del fabricante

Documentará sistemáticamente los aspectos pertinentes relativos a la ciberseguridad del producto con elementos digitales, incluidas las vulnerabilidades de las que tengan conocimiento.

Desde la introducción de un producto con elementos digitales en el mercado y durante la vida útil prevista del producto o durante cinco años a partir de la introducción del producto en el mercado, los fabricantes velarán por que las vulnerabilidades de dicho producto, para tratar y subsanar las posibles vulnerabilidades.

Obligaciones de información de los fabricantes

El fabricante notificará a la ENISA, sin demora, y en cualquier caso en un plazo de veinticuatro horas cualquier vulnerabilidad activa.

El fabricante informará, sin demora, a los usuarios del producto.

Al detectar una vulnerabilidad en un componente, incluso si este es de código abierto, se notificará la vulnerabilidad a la persona o entidad a cargo del mantenimiento del componente.

Obligaciones de los distribuidores

Los distribuidores actuarán con la diligencia debida en relación con los requisitos del presente Reglamento.

Si un distribuidor tiene motivos para creer que no son conformes con los requisitos, el distribuidor no comercializará el producto.

Si tiene conocimiento de que el fabricante haya cesado sus actividades, el distribuidor informará, en la medida de lo posible, a los usuarios.

Documentación técnica

Contendrá todos los datos de los medios utilizados para garantizar el producto.

Se elaborará antes de que se introduzca en el mercado y, en su caso, se mantendrá permanentemente actualizada durante la vida útil o durante cinco años.

Se redactará en una *lengua oficial* del Estado miembro o en una *lengua aceptable*.

Requisitos esenciales de ciberseguridad

Se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad.

Se entregarán sin ninguna vulnerabilidad conocida que pueda aprovecharse:

- Configuración segura por defecto
- Protección contra el acceso no autorizado mediante mecanismos de control
- Protegerán la confidencialidad de los datos personales o de otro tipo
- Tratarán únicamente los datos que sean adecuados, pertinentes y necesarios
- Garantizarán que las vulnerabilidades se subsanen mediante actualizaciones (actualizaciones automáticas) y la notificación a los usuarios.

Requisitos esenciales de ciberseguridad

Identificarán y documentarán las vulnerabilidades, mediante la elaboración en un formato comúnmente utilizado y legible por máquina.

Llevarán a cabo exámenes y ensayos eficaces y periódicos de la seguridad

Una vez esté disponible una actualización de seguridad, divulgarán información sobre las vulnerabilidades subsanadas, incluidas una descripción de las vulnerabilidades

Requisitos esenciales de ciberseguridad

Aplicarán una política de divulgación coordinada de vulnerabilidades

Adoptarán medidas para facilitar el intercambio de información sobre posibles vulnerabilidades

Preverán mecanismos para distribuir de manera segura las actualizaciones

Cuando se disponga de parches de seguridad, se difundan sin demora y de forma gratuita

pero

Código abierto...

Para no obstaculizar la innovación o la investigación, el presente Reglamento no debe aplicarse a los programas informáticos libres y de código abierto desarrollados o suministrados al margen de una actividad comercial. Este es el caso, en particular, de los programas informáticos, incluidos su código fuente y sus versiones modificadas, que se comparten abiertamente y son accesibles, utilizables, modificables y redistribuibles libremente.

¡BIEN!

Código abierto...

En el contexto de los programas informáticos, una actividad comercial puede caracterizarse no solo por la aplicación de un precio a un producto, sino también por la aplicación de un precio a los servicios de asistencia técnica, por el suministro de una plataforma de software a través de la cual el fabricante monetiza otros servicios o por el uso de datos personales por razones distintas de las relacionadas exclusivamente con la mejora de la seguridad, la compatibilidad o la interoperabilidad del programa informático.

¡UPS!

WordPress

Todo esto ¿cómo nos afecta?

No debería afectar a los desarrolladores de código abierto (del “proyecto WordPress”, o sea, del core), voluntarios o financiados.

Sí afectará a cualquiera que desarrolle “sobre WordPress” (plugins, themes), incluidos aquellos que mantengan sitios o revendan elementos.

En principio WordPress (y su extensibilidad) estará en los “productos no-críticos”

Habrá excepciones (como firewalls o plugins de seguridad)

Todo esto ¿cómo nos afecta?

No debería afectar a las versiones *beta* o *release candidate*.

Sí o sí habrá que documentar y anunciar vulnerabilidades.

La Comunidad deberá adaptarse para facilitar la actualización forzada de plugins (aunque el usuario no las tenga automáticas).

Soy desarrollador, agencia...

Eres responsable (indirecto) de la seguridad de los servidores, WordPress, plugins y temas.

Deberás actualizar obligatoriamente cualquier vulnerabilidad.

Deberás documentar todas las pruebas e incluir una sección en tu plugin / tema sobre “Seguridad”, y dar soporte mínimo 5 años (o mientras exista el producto)

¿Cuándo?

La ley aún no está aprobada (ni es definitiva)...

...pero puedes comenzar a hacerlo, porque sí o sí te va a afectar.

Próximos pasos

Actualiza todos los WordPress, componentes y demás.

Avisa a tus clientes de forma activa de posibles vulnerabilidades

autobombo: ponles el plugin WPVulnerability

Añade una sección de “Seguridad” en el *readme* de plugin o theme, con:

- Pruebas durante el desarrollo
- Medidas de seguridad activas
- Método de contacto

¡Gracias!

Ayuda y mentorización Comunidad WordPress:
profiles.w.org/javiercasares

WordPress Hosting: make.w.org/hosting
WordPress Documentation: make.w.org/docs