

NORMA UE · SEGURIDAD DE PRODUCTOS

Reglamento de Ciberresiliencia: seguridad para productos conectados

Quien vende en la UE hardware o software con elementos digitales es fabricante según el Reglamento de Ciberresiliencia (Cyber Resilience Act), aunque no tenga establecimiento en Europa. Las obligaciones de notificación de vulnerabilidades explotadas ya rigen desde el 11/09/2026.

FUENTE LEGAL	NOTIFICACIÓN OBLIGATORIA DESDE	TODAS LAS OBLIGACIONES DESDE	AFECTA A
Reglamento (UE) 2024/2847	11/09/2026	11/12/2027	Fabricantes de hardware y software conectados

En pocas palabras

El Reglamento de Ciberresiliencia, conocido como CRA por su nombre en inglés (Cyber Resilience Act), es un reglamento de la UE sobre requisitos de ciberseguridad para “productos con elementos digitales”. Se refiere a hardware y software que se puede conectar directa o indirectamente a un dispositivo o a una red: routers, cámaras, controladores, sensores industriales, dispositivos de hogar inteligente, pero también software comercial como aplicaciones, sistemas operativos o firmware. Quedan excluidos los ámbitos con reglas propias, como productos sanitarios, vehículos y aviación.

El CRA abarca todo el ciclo de vida. Al momento de la entrega, un producto debe cumplir los requisitos esenciales del anexo I: sin vulnerabilidades explotables conocidas, configuración segura por defecto, protección contra accesos no autorizados y posibilidad de recibir actualizaciones de seguridad. Después, el fabricante debe gestionar las vulnerabilidades y entregar actualizaciones durante un período de soporte que, por regla general, es de al menos cinco años (art. 13). Al final está el marcado CE, que en adelante también cubre la ciberseguridad.

Para la mayoría de los productos alcanza con una autoevaluación del fabricante. Para ciertos productos importantes y críticos, como firewalls, equipos de red o tarjetas inteligentes, se necesita, según la clase, una norma armonizada o un organismo notificado.

A quién afecta en Sudamérica

Un fabricante de fuera de la UE es fabricante en el sentido del CRA en cuanto su producto se comercializa en el mercado de la UE. Una empresa de Manaos que entrega electrónica de control a un fabricante de maquinaria en Italia asume, por lo tanto, las obligaciones de fabricante, siempre que

introduzca el producto en el mercado con su propio nombre. Puede designar un representante autorizado en la UE (art. 18) que se haga cargo de algunas tareas.

También quedan alcanzadas las empresas de software con productos comerciales: una aplicación contable de Santiago, un software de seguridad de Buenos Aires, un firmware para sensores agrícolas de Rosario. En el desarrollo a medida, cuando el cliente de la UE vende el producto con su propio nombre, el fabricante es el cliente. Él le trasladará entonces los requisitos por contrato.

A esto se suma la vía del importador. Según el artículo 19, un importador solo puede introducir en el mercado productos que cumplan los requisitos. Por eso verifica que existan la evaluación de la conformidad, la documentación técnica, el marcado CE y los datos de contacto del fabricante. Si faltan, no compra.

Los distribuidores tienen, según el artículo 20, obligaciones de verificación similares, algo más livianas. Si un importador o distribuidor se entera de una vulnerabilidad, debe informar al fabricante. Ante un riesgo grave, la vigilancia del mercado puede exigir que los productos se retiren o se recuperen. Para un exportador esto significa que un problema en un producto puede bloquear un envío entero en un depósito de la UE.

El software libre y de código abierto gratuito fuera de una actividad comercial no está alcanzado por el CRA. En cuanto lo incorpora a un producto que vende, usted es responsable de la seguridad de esos componentes.

Plazos

DESDE	QUÉ SE APLICA
11/06/2026	Reglas sobre los organismos de evaluación de la conformidad
11/09/2026	Obligaciones de notificación del art. 14 para vulnerabilidades explotadas activamente e incidentes graves de seguridad, también para productos que ya están en el mercado
11/12/2027	Todas las demás obligaciones, entre ellas los requisitos del anexo I, la evaluación de la conformidad y el marcado CE

Las obligaciones de notificación ya están en marcha. Si un fabricante se entera de una vulnerabilidad explotada activamente en su producto, debe enviar una alerta temprana en 24 horas, una notificación en 72 horas y un informe final a más tardar 14 días después de que haya una medida correctora disponible. Para incidentes graves de seguridad, el informe final tiene un plazo de un mes. Las notificaciones se envían a través de la plataforma única de notificación de ENISA (art. 16), que funciona desde el 11/09/2026.

La obligación de notificar se aplica también a productos que usted vendió hace años, mientras sigan en el mercado de la UE. Si no tiene un proceso para reportes de vulnerabilidades, debería armarlo ahora.

Qué piden en concreto los clientes de la UE

- Una declaración UE de conformidad, a partir del 11/12/2027 para todos los productos con elementos digitales.
- La documentación técnica con la evaluación de riesgos y la descripción de las medidas de seguridad.
- Una lista de materiales de software (SBOM) que enumere todos los componentes y bibliotecas.
- Una política de divulgación coordinada de vulnerabilidades (CVD) con una dirección de contacto para reportes.
- La indicación del período de soporte y evidencia de cómo se distribuyen las actualizaciones.
- En productos importantes o críticos, el resultado de la evaluación de la conformidad exigida y, en su caso, un certificado de un organismo notificado.
- En productos industriales, a menudo evidencia según la serie de normas IEC 62443.

Muchos importadores y distribuidores ya lo preguntan hoy, aunque la mayoría de las obligaciones recién se aplican a fines de 2027. No quieren tener en depósito mercadería que después no puedan vender.

Los grandes compradores, además, incorporan los requisitos a sus condiciones de compra: garantía de conformidad con el CRA a partir de una fecha, aviso de vulnerabilidades al cliente, entrega de actualizaciones durante un plazo mínimo acordado y responsabilidad en caso de retiros del mercado. Lea esas cláusulas con atención antes de firmar contratos de suministro que vayan más allá de 2027.

Primeros pasos

1. Haga una lista de todos los productos que entrega a la UE y que contienen software o se pueden conectar.
2. Revise para cada producto si entra en las clases de productos importantes o críticos (anexos III y IV).
3. Ponga en marcha de inmediato un proceso de notificación: ¿quién recibe los reportes de vulnerabilidades, quién los evalúa y quién notifica en 24 horas?

4. Genere una SBOM para cada versión del producto. Muchas herramientas de compilación lo hacen de forma automática.
5. Revise cuáles de sus sistemas se alcanzan desde internet, por ejemplo servidores de actualización y accesos de mantenimiento remoto. Herramientas como [veyrisk](#) lo muestran desde afuera.
6. Planifique la evaluación de la conformidad y la documentación para que estén listas antes del 11/12/2027.

Una primera orientación la ofrece el [diagnóstico UE](#) gratuito.

Relación con las certificaciones

El CRA no exige una certificación de sistema de gestión. Pero un certificado [ISO/IEC 27001](#) demuestra que su desarrollo, su entorno de compilación y su manejo de incidentes están ordenados, y ayuda con los requisitos de procesos. Ese sistema de gestión se puede armar en una plataforma GRC como [Sightadel](#). El CRA no figura ahí como marco propio, pero tareas como el proceso de notificación o la política de divulgación de vulnerabilidades se pueden llevar con sus evidencias en el mismo lugar. En productos industriales está muy difundida la IEC 62443. Los proveedores de la industria automotriz suelen necesitar [TISAX](#), aunque los vehículos en sí no están alcanzados por el CRA. Un sistema de gestión de la calidad según [ISO 9001](#) facilita la documentación. Si entrega productos a operadores de servicios críticos, se suma [NIS2](#), y las funciones de IA en productos quedan también alcanzadas por el [Reglamento de Inteligencia Artificial](#).

Para los fabricantes de [Brasil](#), donde se produce mucha electrónica y tecnología de automatización, el CRA es una de las normas nuevas más importantes de la UE. Los requisitos son los mismos, ya sea que la mercadería pase por un importador o vaya directo a un cliente industrial.

FAQ

¿El Reglamento de Ciberresiliencia se aplica al software?

Sí, al software comercial que se comercializa en la UE, incluidas aplicaciones y firmware. Quedan excluidos, entre otros, los servicios puramente en la nube sin vínculo con un producto y el software libre y de código abierto gratuito fuera de una actividad comercial.

¿Qué tengo que hacer desde el 11/09/2026?

Notificar a través de la plataforma de notificación de ENISA las vulnerabilidades explotadas activamente y los incidentes graves de seguridad en sus productos: alerta temprana en 24 horas, notificación en 72 horas.

¿Necesito un establecimiento en la UE?

No. Puede designar un representante autorizado en la UE (art. 18). Su importador en la UE debe conocer sus datos de contacto y verificar la conformidad.

¿Qué es una SBOM?

Una lista de materiales de software que enumera todos los componentes y bibliotecas de un producto. El CRA la exige como parte de la documentación técnica.

¿Cómo reviso qué sistemas vinculados a mi producto son accesibles desde internet?

Los servidores de actualización, los portales de descarga y los accesos de mantenimiento remoto se ven desde afuera como cualquier otro sistema. [veyrisk](#) revisa esa superficie de ataque externa en busca de servicios abiertos, certificados vencidos y vulnerabilidades conocidas, y entrega un informe. El producto en sí, su firmware y su SBOM se revisan con otras herramientas.

Fuentes · Actualizado: 11 de octubre de 2026

Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

Comisión Europea: Reglamento de Ciberresiliencia: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

Comisión Europea: obligaciones de notificación según el CRA: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel

Sightadel guía a su equipo por ISO 27001: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)



veyrisk

veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>