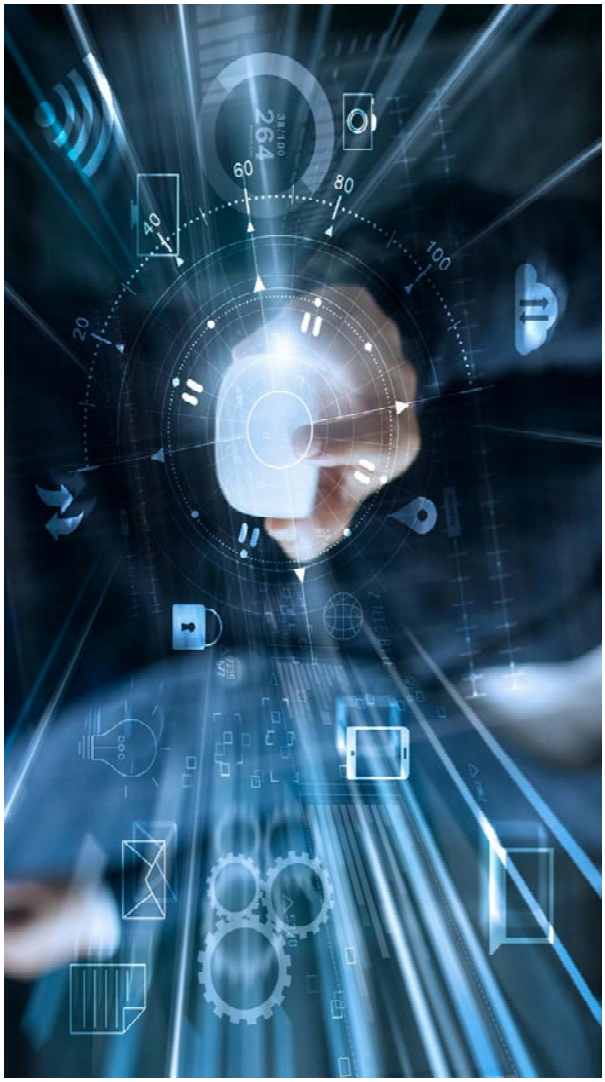
CUATRECASAS

Reglamento de Ciberresiliencia

El Reglamento de Ciberresiliencia, publicado en el Diario Oficial de la UE el 20 de noviembre de 2024, establece estándares unificados de ciberseguridad para productos con elementos digitales en el mercado de la UE.

Legal Flash

20 de noviembre de 2024



Aspectos clave

El 20 de noviembre de 2024 se ha publicado en el Diario Oficial de la UE el **Reglamento de Ciberresiliencia** (Reglamento (UE) 2024/2847, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828).

Estos son algunos de sus aspectos clave:

- Los fabricantes deben integrar **medidas de seguridad** desde la fase de diseño y asegurar el marcado CE.
- Los importadores y distribuidores son responsables de verificar los **estándares de ciberseguridad del producto.**
- Es obligatorio para los fabricantes informar oportunamente sobre **vulnerabilidades e incidentes.**
- Se imponen sanciones significativas por incumplimiento, con exenciones para pequeñas empresas.

Reglamento de Ciberresiliencia

Con su publicación en el Diario Oficial de la UE del 20 de noviembre de 2024, culmina la tramitación legislativa de este Reglamento, que ha estado en curso desde la presentación de la propuesta de la Comisión Europea a mediados de 2022.

El **Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia)**, en adelante, "RCR", establece requisitos de ciberseguridad para productos de hardware y software con elementos digitales introducidos en la Unión Europea ("UE"). Entre otros productos con elementos digitales cubiertos por el RCR, el Reglamento se aplica a la gestión de redes, sistemas operativos o de contraseñas, asistentes virtuales de propósito general para hogar inteligente, tarjetas inteligentes o dispositivos similares, junto con dispositivos de hardware con cajas de seguridad.

Antes de la aprobación del RCR, varias iniciativas nacionales y a nivel de la UE abordaban los desafíos de ciberseguridad de manera fragmentada, creando un marco regulatorio inconsistente en el mercado interior. Y si bien la legislación de la UE (por ejemplo, la Directiva (UE) 2022/2555 [Directiva NIS2] y el Reglamento (UE) 2019/881 [Reglamento de Ciberseguridad]) ya abordaba varios aspectos de la ciberseguridad desde diferentes perspectivas, no imponía requisitos de seguridad obligatorios específicamente para productos con elementos digitales.

El RCR es particularmente importante debido a la naturaleza transfronteriza de los riesgos de ciberseguridad. Los productos desarrollados en un país son frecuentemente utilizados por empresas y consumidores en toda la UE, lo que pone de relieve la necesidad de un marco regulatorio unificado.

Los operadores económicos (fabricantes, importadores, distribuidores y representantes autorizados) ostentan roles específicos para asegurar que los productos con elementos digitales sean seguros y cumplan con el RCR antes de ser introducidos en la UE. Los requisitos difieren entre fabricantes e importadores o distribuidores, y dependiendo de si los productos con elementos digitales se definen como productos importantes (Anexo III del RCR) o productos críticos (Anexo IV del RCR).

Fabricantes, importadores y distribuidores

Los fabricantes[1] están obligados a incorporar medidas de ciberseguridad desde el principio, asegurando que los productos se diseñen, desarrollen y produzcan de manera segura. Estas medidas incluyen:

[1] Definidos en el Artículo 3.13 del RCR como la "persona física o jurídica que desarrolla o fabrica productos con elementos digitales o para quien se diseñan, desarrollan o fabrican productos con elementos digitales, y que los comercializa con su nombre o marca comercial, ya sea de manera remunerada, monetizada o gratuita".

- promover evaluaciones rigurosas para cada producto para identificar y mitigar cualquier riesgo de ciberseguridad durante el diseño y desarrollo;
- mantener registros detallados que muestren cómo se abordaron los riesgos de ciberseguridad, poniendo esta información a disposición de los organismos reguladores si es necesario;
- mantener la información y las instrucciones para el usuario establecidas en el Anexo II a disposición de los usuarios y las autoridades de vigilancia del mercado durante al menos diez años desde que el producto con elementos digitales haya sido introducido en el mercado o durante el período de soporte, lo que sea más largo;[2]
- asegurar que los productos lleven el marcado CE, indicando que cumplen con los estándares necesarios y pueden ser vendidos de manera segura en toda la UE; y
- establecer procesos para manejar posibles problemas de ciberseguridad que surjan después del lanzamiento del producto, como proporcionar actualizaciones de seguridad y asesorar a los usuarios sobre cómo gestionar vulnerabilidades.

El RCR introduce el rol del representante autorizado, que será designado por el fabricante mediante un mandato escrito para realizar en su nombre las tareas especificadas en el mandato. El mandato permitirá al representante autorizado (i) mantener la declaración de conformidad de la UE y la documentación técnica a disposición de las autoridades de vigilancia del mercado durante al menos diez años desde que el producto con elementos digitales haya sido introducido en el mercado o durante el período de soporte, el tiempo que sea más largo; (ii) proporcionar a esa autoridad toda la información y documentación necesaria para demostrar la conformidad del producto con elementos digitales; y (iii) cooperar con las autoridades de vigilancia del mercado, a solicitud de estas.

En cuanto a los importadores[3] y distribuidores[4], les corresponde verificar, evaluar y garantizar que los productos que se están vendiendo sean seguros y cumplan con los estándares de ciberseguridad. Por ejemplo, los importadores deben verificar que los productos cumplan con todos los requisitos de ciberseguridad antes de ser comercializados, incluyendo la verificación del marcado CE y la documentación adecuada. Los distribuidores deben estar atentos a cualquier problema de seguridad y asegurar que los productos que manejan sigan cumpliendo a lo largo del tiempo.

El RCR identifica un conjunto de medidas de ciberseguridad que deben ser aplicadas por los

---

[2] Cuando dicha información e instrucciones se proporcionen en línea, los fabricantes deberán asegurarse de que sean accesibles, fáciles de usar y estén disponibles en línea durante al menos 10 años después de que el producto con elementos digitales haya sido introducido en el mercado o durante el período de soporte, lo que sea más largo.

[3] Definido en el Artículo 3.16 del RCR como la "persona física o jurídica establecida en la Unión que introduce en el mercado un producto con elementos digitales que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión".

[4] Definido en el Artículo 3.17 del RCR como la "persona física o jurídica que forma parte de la cadena de suministro, distinta del fabricante o el importador, que comercializa un producto con elementos digitales en el mercado de la Unión sin influir sobre sus propiedades".

fabricantes y verificadas por los importadores y distribuidores, incluyendo las siguientes:

- **Seguridad por diseño**: Los productos deben ser desarrollados teniendo presente desde el principio la seguridad. Esto incluye incorporar medidas de protección para prevenir el acceso no autorizado y asegurar la integridad y confidencialidad de cualquier dato procesado.

- **Protección de productos críticos**: Los productos que realizan funciones esenciales de ciberseguridad o que presentan un riesgo elevado en caso de resultar comprometidos, como los cortafuegos o los sistemas de prevención de intrusiones, deben cumplir requisitos de seguridad más estrictos. Estos productos deben someterse a evaluaciones más exhaustivas para asegurar su robustez.

- **Gestión de vulnerabilidades**: Todos los productos deben tener un plan para gestionar las vulnerabilidades durante todo su ciclo de vida. Se espera que los fabricantes proporcionen actualizaciones de seguridad, parches e instrucciones para mitigar los riesgos a medida que surjan. Esto es especialmente importante para los productos críticos (listados en el Anexo IV del RCR), donde las actualizaciones oportunas son esenciales para mantener la seguridad.

- **Seguridad de la cadena de suministro**: Los operadores económicos deben gestionar cuidadosamente los riesgos de ciberseguridad asociados con los componentes de terceros utilizados en sus productos, incluyendo el software de código abierto. El nivel de escrutinio depende de la naturaleza del componente y sus riesgos asociados. Los fabricantes deben asegurar que cualquier componente de terceros, incluyendo el software, sea seguro, se actualice regularmente y esté libre de vulnerabilidades conocidas.

- **Actualizaciones de seguridad y soporte**: Las modificaciones de un producto, ya sea a través de actualizaciones de software o cambios de hardware, pueden afectar a su estado de ciberseguridad. Por ejemplo, una actualización que introduce nuevas funcionalidades podría aumentar la exposición potencial del producto a amenazas cibernéticas, requiriendo una nueva evaluación de riesgos. Sin embargo, no todas las actualizaciones se consideran sustanciales. Los parches menores, como las correcciones de errores o las mejoras de la interfaz, normalmente no cambian el riesgo general de seguridad de un producto. Sin embargo, los cambios más significativos, especialmente aquellos que afectan a las funcionalidades principales, requieren un escrutinio mayor para asegurar que no introduzcan nuevas vulnerabilidades. En situaciones donde la modificación de un producto altera significativamente su propósito previsto o perfil de riesgo, puede ser preciso pasar por una nueva evaluación de conformidad. Esto asegura que el producto continúe cumpliendo con los estándares de seguridad requeridos después de actualizaciones o cambios importantes.

Cuando se trata de software de código abierto, los operadores económicos deben tener un cuidado especial al integrar este tipo de software en productos comerciales. Mientras que los proyectos de código abierto no destinados a uso comercial pueden estar exentos de ciertas obligaciones, cualquier producto que incorpore componentes de código abierto en un contexto comercial debe asegurar que esos componentes cumplan con los estándares de ciberseguridad. Para los administradores de comunidad de software de código abierto —organizaciones que

proporcionan soporte a largo plazo para tales proyectos— se aplica un enfoque más flexible. Sin embargo, los productos comerciales que incorporan estos componentes deben cumplir con todos los requisitos de seguridad.

Además de lo anterior, es oportuno mencionar que el RCR prevé algunos casos en los que las obligaciones de los fabricantes se aplican a los importadores y distribuidores; específicamente, cuando el importador o distribuidor pone un producto con elementos digitales en el mercado bajo su nombre o marca comercial o realiza una modificación sustancial de un producto con elementos digitales ya introducido en el mercado. En tales casos, bajo el RCR, el importador o el distribuidor estarán sujetos a las obligaciones de los fabricantes establecidas en el RCR.

Respuesta a incidentes y notificaciones

Los requisitos de notificación establecidos en el RCR tienen como objetivo garantizar la transparencia, la respuesta rápida y los esfuerzos colaborativos entre los fabricantes, la Agencia de la Unión Europea para la Ciberseguridad ("ENISA") y los Equipos de Respuesta a Incidentes de Seguridad Informática ("CSIRTs"). El RCR exige que los fabricantes de productos con elementos digitales notifiquen a las entidades pertinentes sobre vulnerabilidades aprovechadas activamente e incidentes de ciberseguridad graves. Los incidentes se considerarán graves si afectan negativamente a la capacidad del producto para proteger datos o funciones sensibles o si conducen a la introducción o ejecución de código malicioso en un sistema, causando riesgos de ciberseguridad para el producto con elementos digitales.

El proceso y los plazos para notificar tanto las vulnerabilidades aprovechadas como los incidentes graves siguen el *modus operandi* habitual en la legislación de ciberseguridad, a saber, a través de las siguientes notificaciones principales:

- Una notificación de advertencia temprana, que debe ser presentada dentro de las 24 horas de haber tenido conocimiento de la vulnerabilidad o incidente, especificando información relevante, como por ejemplo si el incidente resultó de actos ilícitos o maliciosos.

- Una notificación intermedia y más detallada del incidente, que debe realizarse dentro de las 72 horas, proporcionando un contexto más amplio, incluyendo la naturaleza de la vulnerabilidad o incidente, las medidas correctivas ya tomadas y los posibles pasos de mitigación que los usuarios pueden adoptar.

- Un informe final, que debe presentarse al cabo de un mes, detallando la gravedad de la vulnerabilidad, los posibles actores maliciosos involucrados y las medidas de mitigación completas.

En circunstancias excepcionales, los fabricantes pueden solicitar un aplazamiento para la difusión de la notificación, particularmente si una vulnerabilidad está sujeta a una divulgación coordinada de vulnerabilidades en curso. Sin embargo, este aplazamiento está estrictamente limitado en el tiempo y depende de motivos relacionados con la ciberseguridad.

Los fabricantes deben notificar simultáneamente al CSIRT designado como coordinador y a ENISA. Esta notificación debe presentarse a través de una plataforma única de notificación gestionada por ENISA, facilitando la comunicación fluida con todos los CSIRTs en el conjunto de la UE.

En casos de vulnerabilidades aprovechadas activamente o incidentes graves, los fabricantes están obligados a informar a los usuarios afectados, proporcionando detalles sobre los riesgos y las acciones de mitigación. Si el fabricante no informa a los usuarios, los CSIRTs notificados pueden asumir la responsabilidad de la comunicación, asegurando así que se difunde información crucial de seguridad.

Además, siguiendo otras legislaciones de ciberseguridad y marcos de referencia, se contempla en el RCR el intercambio voluntario de amenazas de ciberseguridad, vulnerabilidades e incidentes. Así, los fabricantes y otras partes interesadas pueden notificar voluntariamente vulnerabilidades o incidentes a ENISA o a la red de CSIRTs. Este enfoque voluntario fomenta un entorno de ciberseguridad colaborativo, mejorando la transparencia y la resiliencia en toda la industria.

Notificación de organismos de evaluación de la conformidad

Los Estados miembros están obligados a designar y a notificar a la Comisión Europea y a los demás Estados miembros los organismos autorizados para llevar a cabo evaluaciones de conformidad con arreglo al RCR.

Estos organismos están encargados de evaluar si los productos con elementos digitales cumplen con los criterios de ciberseguridad requeridos por el RCR. El proceso de notificación tiene como objetivo crear un enfoque estandarizado en toda la UE, asegurando que todos los organismos designados se adhieran a los mismos estándares de evaluación.

Los organismos de evaluación de la conformidad deben cumplir con ciertos criterios estrictos, entre otros, los siguientes:

- Independencia e imparcialidad: Estos organismos deben operar independientemente de los fabricantes, evitando así cualquier conflicto de intereses y asegurando evaluaciones imparciales.
- Competencia técnica: Deben poseer la experiencia y los recursos necesarios para evaluar con precisión los productos en relación con los requisitos establecidos en el RCR.
- Gestión de calidad: Se espera que los organismos designados implementen sistemas de gestión de calidad robustos que garanticen la consistencia y la fiabilidad en sus evaluaciones.

Cumplimiento y vigilancia del mercado

De manera similar, los Estados miembros están obligados a designar autoridades de vigilancia del mercado responsables de monitorizar el cumplimiento del RCR. Estas autoridades son fundamentales para garantizar que los productos introducidos en el mercado cumplan de forma consistente los estándares de ciberseguridad requeridos.

Sus responsabilidades incluyen monitorizar activamente el mercado para asegurar el cumplimiento de la normativa de ciberseguridad, lo que implica inspecciones regulares, pruebas y evaluaciones de los productos disponibles para la venta.

Estas autoridades también tienen el poder de investigar productos sospechosos de incumplimiento, realizar auditorías, revisar la documentación técnica y evaluar el marcado CE junto con la declaración de conformidad de la UE.

Si se identifica un incumplimiento, las autoridades de vigilancia del mercado tienen la autoridad para adoptar acciones correctivas, que pueden comportar que los fabricantes deban cesar en la comercialización de productos no conformes, retirarlos del mercado o recuperarlos de los consumidores.

Para identificar y abordar sistemáticamente el incumplimiento, se alienta a las autoridades de vigilancia del mercado a realizar acciones de control coordinadas, comúnmente conocidas como "barridos", que implican inspecciones simultáneas de productos o categorías específicas en múltiples Estados miembros, así como la agregación y publicación de los resultados.

Confidencialidad y sanciones

Cabe destacar que el RCR pone un énfasis significativo en la confidencialidad y en la aplicación de sanciones. Los objetivos principales de las disposiciones de confidencialidad son salvaguardar la información sensible y asegurar que el marco regulatorio opera sin comprometer los derechos de propiedad intelectual o la seguridad nacional.

En cuanto a las sanciones, el RCR requiere que los Estados miembros establezcan sanciones efectivas y proporcionadas para las infracciones. En particular, se fijan las siguientes:

- Infracciones de los requisitos esenciales de ciberseguridad: hasta 15 millones de euros o el 2,5% del volumen de negocios anual total mundial del infractor, la cifra que sea mayor.
- Infracciones de las obligaciones generales: hasta 10 millones de euros o el 2% del volumen de negocios anual total mundial del infractor, la cifra que sea mayor.
- Proporcionar información engañosa: hasta 5 millones de euros o el 1% del volumen de negocios anual total mundial del infractor, la cifra que sea mayor.

Al determinar la cuantía de la multa administrativa deben considerarse cuidadosamente las circunstancias relevantes, como la naturaleza, la gravedad y la duración de la infracción. Se establecen exenciones para ciertas entidades. Por ejemplo, los fabricantes considerados microempresas o pequeñas empresas pueden quedar exentos de multas administrativas por ciertos incumplimientos de plazos. También se exime de multas a los administradores de software de código abierto por cualquier infracción del RCR.

Próximos pasos para las empresas

Para ayudar a implementar el RCR, la Comisión Europea proporcionará orientaciones, especialmente dirigidas a las pequeñas y medianas empresas (PYMEs). Este apoyo ayudará a los operadores económicos a entender cómo implementar efectivamente las medidas de ciberseguridad necesarias. También se otorga a las empresas un período de transición para adaptar a los nuevos requisitos de ciberseguridad los productos que ya se hallan en el mercado, permitiéndoles continuar operando sin interrupciones inmediatas mientras realizan los ajustes necesarios.

Los próximos pasos para los operadores económicos, particularmente los fabricantes, serán realizar un análisis de brechas en las medidas de ciberseguridad existentes, no solo a nivel organizacional, sino también para la fabricación de sus productos con elementos digitales. Este análisis de brechas debe centrarse en un enfoque basado en el riesgo, incluyendo el riesgo de la cadena de suministro, y en las capacidades de los fabricantes para detectar y responder a las vulnerabilidades emergentes.

El Reglamento será aplicable a partir del 11 de diciembre de 2027, si bien el artículo 14, referido a las obligaciones de información de los fabricantes será aplicable a partir del 11 de septiembre de 2026; y el capítulo IV, relativo a la notificación de los organismos de evaluación de la conformidad, será aplicable a partir del 11 de junio de 2026.

Para obtener información adicional sobre el contenido de este documento puede enviar un mensaje a nuestro equipo del *Área de Conocimiento e Innovación* o dirigirse a su contacto habitual en Cuatrecasas.