Cumplimiento del Reglamento de Ciberresiliencia (CRA)

La guía definitiva para cumplir con los requisitos del CRA

Índice

Introducción

El **Reglamento de Ciberresiliencia (CRA)** remodela significativamente el panorama mundial de la conformidad de los productos mediante la inclusión de obligaciones estrictas de ciberseguridad en el marco de la marca de Conformidad Europea (CE). Estos requisitos afectan potencialmente a cualquier producto OEM, independientemente de su origen, que se pretenda vender en la UE. Formalmente conocido como Reglamento (UE) 2024/2847, el CRA se aplica a cualquier producto que contenga elementos digitales cuya finalidad prevista o uso previsible incluya una conexión de datos directa o indirecta, ya sea lógica o física, a una red o dispositivo. Esta guía práctica de Digi y NXP ofrece un recorrido por los requisitos y cómo cumplirlos.

Según este reglamento, todos los productos capaces de conectarse a un dispositivo o a una red deben cumplir unos requisitos de ciberseguridad definidos para recibir el marcado CE, que es un requisito legal previo para su venta en la UE. Los productos que no cumplan la normativa no podrán comercializarse en el mercado de la UE.

El núcleo del CRA es una respuesta a las persistentes deficiencias en materia de ciberseguridad. Aunque muchos productos afirman ser seguros, a menudo no existe una forma fiable para que los consumidores o las empresas verifiquen tales afirmaciones o se garantice una protección continua. El CRA proporciona un marco unificado y obligatorio para el cumplimiento de la ciberseguridad que abarca todo el ciclo de vida del producto.

Para ello, el reglamento establece:

- Requisitos comunes para el lanzamiento de productos o software con elementos digitales, que garanticen un punto de partida coherente para todos los fabricantes
- Un único marco de ciberseguridad para la planificación, el diseño, el desarrollo y el mantenimiento de productos conectables
- Un deber de diligencia que se aplica durante todo el ciclo de vida del producto y no solo en el punto de venta

Este marco pretende facilitar el cumplimiento no solo a los fabricantes de productos acabados, sino también a los que suministran componentes de hardware y software.

Al igual que con la legislación anterior de la UE, otros países ya están siguiendo los pasos del CRA. Por ejemplo, Estados Unidos **presentó la marca de confianza cibernética US Cyber Trust Mark en septiembre de 2024**. Supervisado por la Comisión Federal de Comunicaciones (FCC), este programa voluntario de etiquetado pretende incentivar una mayor seguridad en el desarrollo de productos conectados.

La buena noticia es que ajustarse a los requisitos del CRA le ayudará a garantizar que sus productos también se ajusten a las medidas de seguridad que se están implantando en otros lugares. Y lo que es más importante, comprender el CRA ayudará a su empresa a evitar reprocesamientos potencialmente caros o que los productos sean retirados del mercado.

¿Cuáles son los riesgos del incumplimiento del CRA?

El cumplimiento del CRA es obligatorio. Si un producto cubierto por la ley no cumple los requisitos para obtener el marcado CE, no puede venderse legalmente en la UE. Los organismos reguladores tienen autoridad para retirar del mercado los productos que no cumplan la normativa y exigir retiradas, lo que podría paralizar la presencia de una organización en el mercado.

Los reguladores también pueden optar por emitir sanciones por incumplimiento, y cada violación del CRA conlleva una multa potencial de 15 millones de euros o el 2,5 % de la facturación global anual de una empresa, lo que sea más elevado.

A pesar de las duras consecuencias, sigue habiendo falsos mitos muy extendidos sobre el CRA. Una idea equivocada frecuente hace referencia al calendario. Aunque muchos fabricantes creen que el reglamento no entrará en vigor hasta 2027, el CRA ya ha entrado en vigor. Los plazos clave de cumplimiento se aproximan rápidamente.

> Aunque muchos fabricantes creen que el reglamento no entrará en vigor hasta 2027, el CRA ya ha entrado en vigor.
>
> Vea la sección **“Cuenta atrás para el cumplimiento del CRA” en la página 5** para más detalles.

También existe una confusión permanente sobre el ámbito de aplicación del reglamento, específicamente, a qué productos aplica, quién es el responsable y qué pasos son necesarios para mantener el cumplimiento. Algunas de las preguntas más acuciantes se abordan en **“Conceptos erróneos sobre la Ley de Ciberresiliencia” en la página 4**. Comprender estos detalles es crucial para los fabricantes, los responsables de los departamentos de compras y los equipos de desarrollo.

En términos más generales, una revisión exhaustiva de los fundamentos del CRA es esencial para mantener su empresa, cadena de suministro y desarrollo de productos en conformidad con esta importante normativa.

Falsos mitos sobre el Reglamento de Ciberresiliencia

Falso mito	Realidad
El CRA solo aplica a las empresas con sede en Europa.	**Todos los fabricantes, importadores y distribuidores que comercializan productos en el mercado europeo deben adherirse al CRA, independientemente de dónde tengan su sede.**
Los productos que ya estén en el mercado cuando entre en vigor el CRA estarán exentos.	**Cualquier producto comercial, ya existente o nuevo, que se modifique sustancialmente después del 11 de diciembre de 2027 tendrá que cumplir los requisitos del CRA.** **Asimismo, los fabricantes deben tener en cuenta una excepción en el Artículo 69, "Disposiciones transitorias". Las obligaciones establecidas en el Artículo 14, "Obligaciones de información de los fabricantes", se aplicarán a todos los productos incluidos en el ámbito de aplicación de este reglamento y comercializados antes del 11 de diciembre de 2027.**
Solo los fabricantes de equipos originales, OEMs (Original Equipment Manufacturers), son responsables del cumplimiento del CRA.	**El CRA se aplica a toda la cadena de suministro, desde los fabricantes hasta los importadores, distribuidores y proveedores, y todas las partes son responsables de su cumplimiento. Es aplicable a productos de hardware y software, tanto dispositivos finales como componentes. En adelante nos referiremos a estos grupos e individuos como "las partes responsables". Tenga en cuenta que este documento solo aborda las responsabilidades de los fabricantes.**
Solo los dispositivos informáticos o de comunicación están cubiertos por el CRA.	**El CRA cubre la mayoría de los productos comerciales con elementos digitales, desde dispositivos IoT hasta sistemas de control industrial.** **Sin embargo, algunos productos están excluidos de los requisitos de cumplimiento del CRA, ya que están cubiertos por otras normativas ya en vigor. Por ejemplo, se incluyen:** • **Dispositivos médicos** • **Sistemas y componentes de automoción** • **Equipos relacionados con la aviación** • **Equipamiento marino** • **Piezas de recambio para sustituir componentes idénticos en productos con elementos digitales** • **Productos relacionados con la defensa, la seguridad nacional o diseñados para procesar información clasificada**
Los productos de código abierto están exentos del CRA.	**El hecho de que un producto contenga o no componentes de código abierto es irrelevante si, por lo demás, el producto debe cumplir con el CRA.**
El CRA solo aplica a los productos que incorporan software.	**Si un producto comercial requiere una plataforma en la nube o una solución de procesamiento remoto de datos como parte de su funcionalidad principal, entonces entra en el ámbito del CRA.**
Los productos que están desconectados la mayor parte del tiempo no necesitan cumplir con el CRA.	**Cualquier producto con elementos digitales capaz de establecer, aunque sea potencialmente, una conexión de datos con un dispositivo o una red debe cumplir con el CRA.**
Los productos solo deben someterse a pruebas o certificarse una vez.	**El CRA exige mantenimiento, cumplimiento y adhesión continuos durante todo el ciclo de vida del producto, no solo en el punto de entrada en el mercado.**

Fundamentos del CRA

A diferencia de los reglamentos anteriores, el CRA introduce requisitos técnicos concretos, obligaciones claras y plazos definidos, estableciendo la responsabilidad en toda la cadena de suministro. Estas nuevas normas se basan en seis pilares fundamentales:

- ✓ **Ciberseguridad estricta:** El CRA establece rigurosos requisitos de seguridad para el diseño, el desarrollo, el mantenimiento y el soporte postventa. Los fabricantes deben vigilar las vulnerabilidades de sus productos, abordarlas de forma proactiva y proporcionar actualizaciones periódicas.
- ✓ **Evaluaciones de conformidad:** Los productos deben someterse a evaluaciones detalladas para verificar el cumplimiento de los requisitos esenciales de ciberseguridad antes de entrar en el mercado de la UE.
- ✓ **Notificaciones tempranas de vulnerabilidades e incidentes:** Cualquier vulnerabilidad aprovechada activamente e incidente grave debe notificarse a las autoridades designadas en las veinticuatro horas siguientes a su detección para permitir una respuesta rápida.
- ✓ **Clasificación de productos:** Los productos se clasifican por riesgo de ciberseguridad, por defecto, importante o crítico, con procedimientos específicos de evaluación de la conformidad para garantizar evaluaciones de seguridad proporcionadas.
- ✓ **Supervisión y auditorías:** La conformidad debe mantenerse durante todo el ciclo de vida del producto mediante una supervisión y auditoría activas, no solo en el momento de la entrada en el mercado.
- ✓ **Transparencia y comunicación:** Los OEMs deben proporcionar información clara y actualizada sobre las funcionalidades de seguridad de los productos, las vulnerabilidades y las medidas correctoras, a los usuarios y las autoridades.

Artículo 13, apartado 19: "Los fabricantes se asegurarán de que la fecha final del período de soporte a que se refiere el apartado 8, incluidos al menos el mes y el año, se especifique de manera clara y comprensible en el momento de la compra, de manera fácilmente accesible y, en su caso, en el producto con elementos digitales, en su embalaje o por medios digitales.

Cuando sea técnicamente viable habida cuenta de la naturaleza del producto con elementos digitales, los fabricantes mostrarán una notificación a los usuarios que les informe de que su producto con elementos digitales ha alcanzado el final de su período de soporte."

Juntos, estos pilares crean un enfoque estandarizado de la ciberseguridad, ayudando a garantizar que los productos conectables cumplen los requisitos esenciales de ciberseguridad antes de llegar a los usuarios finales y a lo largo de todo su ciclo de vida.

Los fabricantes deben empezar a trabajar inmediatamente para garantizar el cumplimiento dentro del plazo establecido.

Cuenta atrás para el cumplimiento del CRA

Formando parte de la Estrategia de Ciberseguridad de la UE en 2020, el CRA pretendía complementar el **Marco NIS2**. El acta fue firmada oficialmente por el Parlamento Europeo y el Consejo de la Unión Europea el 23 de octubre de 2024 y **publicada el 20 de noviembre de 2024**.

10 de diciembre de 2024

El CRA se adopta oficialmente en la legislación de la UE con un período de gracia antes de que su adopción total sea obligatoria.

11 de junio de 2026

Los organismos de evaluación de la conformidad responsables de verificar el cumplimiento del CRA entran en funcionamiento, como se indica en el Capítulo IV, Artículos 35-51.

Las organizaciones deben empezar a familiarizarse con los procedimientos de evaluación de la conformidad y determinar si su categoría de producto requiere un compromiso formal con un organismo de evaluación de la conformidad o si es adecuada una colaboración voluntaria para apoyar los esfuerzos de cumplimiento antes de la fecha límite de 2027.

11 de septiembre de 2026

Los fabricantes están ahora obligados a informar simultáneamente de las vulnerabilidades aprovechadas activamente y de los incidentes graves en los productos aplicables tanto a su Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) "designado como coordinador" como a la Agencia de Ciberseguridad de la Unión Europea (ENISA) en las 24 horas siguientes a su descubrimiento, tal y como se indica en el Artículo 14.

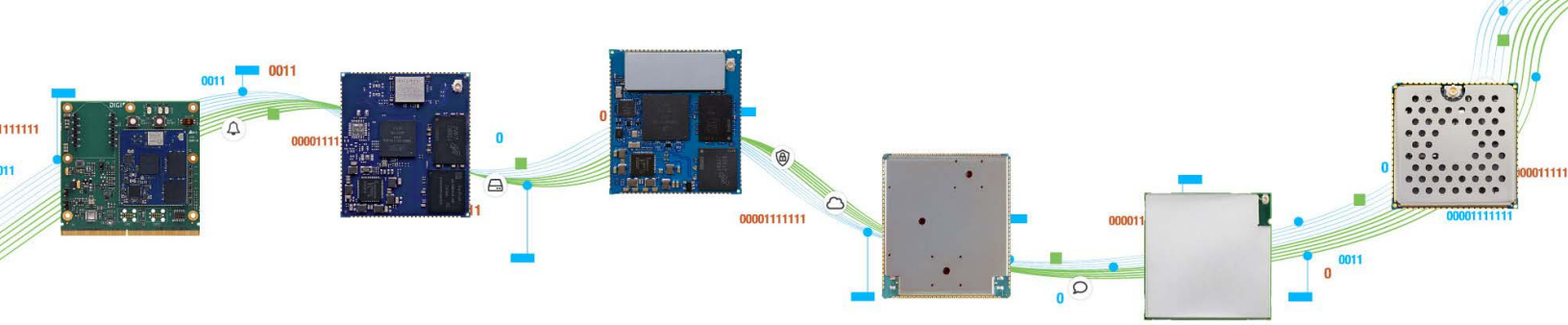
11 de diciembre de 2027

El Reglamento de Ciberresiliencia entra oficialmente en vigor. A partir de esta fecha, todos los productos aplicables requieren el marcado CE paraser autorizados para su venta en la UE.

Requisitos clave para el cumplimiento (Anexo I)

El CRA ordena el cumplimiento de la ciberseguridad "de principio a fin", exigiendo tanto el diseño seguro del producto como la continua protección durante todo el ciclo de vida del producto. Esto significa que la ciberseguridad debe abordarse en las primeras fases de desarrollo y mantenerse mucho después del lanzamiento del producto. Vea **la sección "Período de soporte" en la página 7 para más información**.

Para apoyar este objetivo, el Anexo I del CRA esboza dos categorías de requisitos de ciberseguridad: la Parte I, que se centra en las propiedades de los productos con elementos digitales, y la Parte II, que establece normas para el tratamiento de las vulnerabilidades y la gestión del ciclo de vida.



Parte I: Requisitos de ciberseguridad relacionados con el producto

Durante la fase de diseño, se espera que las organizaciones lleven a cabo una evaluación exhaustiva de los riesgos de ciberseguridad y establezcan un nivel adecuado de ciberseguridad basado en los riesgos potenciales (Anexo I, Parte I.1).

A partir de aquí sus productos con elementos digitales deben:

- Estar libres de vulnerabilidades aprovechables conocidas en el momento de su lanzamiento (Anexo I, Parte I.2(a))
- Ser suministrados con una configuración “segura por defecto” (Anexo I, Parte I.2(b))
- Garantizar que las vulnerabilidades puedan abordarse mediante actualizaciones de seguridad, que deben ser automáticas y estar activadas por defecto (Anexo I, Parte I.2(c))
- Proteger contra el acceso no autorizado mediante sistemas adecuados de autenticación, identidad o gestión de accesos (Anexo I, Parte I.2(d))
- Blindar la confidencialidad de los datos, por ejemplo, encriptando los datos almacenados o transmitidos mediante mecanismos de última generación (Anexo I, Parte I.2(e))
- Salvaguardar la integridad de los datos almacenados, transmitidos o procesados, los comandos, los programas y la configuración contra cualquier manipulación no autorizada, e informar de los casos de corrupción de datos (Anexo I, Parte I.2(f))
- Solo procesar datos estrictamente relevantes para su uso previsto (Anexo I, Parte I.2(g))
- Proteger las funciones esenciales de los ataques de denegación de servicio (DoS) (Anexo I, Parte I.2(h))
- Minimizar los impactos potenciales de los propios productos o de los dispositivos conectados sobre los servicios prestados por otros dispositivos o redes (Anexo I, Parte I.2(i))
- Limitar las superficies de ataque, incluidas las interfaces externas (Anexo I, Parte I.2(j))
- Incorporar mecanismos de mitigación de las vulnerabilidades para reducir el impacto de los incidentes de seguridad (Anexo I, Parte I.2(k))
- Proporcionar información relevante sobre la seguridad mediante la supervisión y el registro de actividades internas como el acceso o la modificación de datos, servicios o funciones, aunque también deben ofrecer a los usuarios la posibilidad de no participar (Anexo I, Parte I.2(l))
- Garantizar que todos los datos y configuraciones puedan eliminarse de forma segura o transferirse a otros productos a petición de los usuarios (Anexo I, Parte I.2(m))

Parte II: Requisitos para la gestión de vulnerabilidades

Un diseño seguro por sí solo no es suficiente. El CRA también establece varios requisitos para gestionar y corregir las vulnerabilidades. Los fabricantes deben identificar y documentar todas las vulnerabilidades y componentes contenidos en cada producto. Esto incluye el mantenimiento de una lista de materiales de software (SBOM) actualizada y legible por máquina que catalogue, como mínimo, las dependencias de primer nivel de un producto (Anexo I, Parte II.1). Además, los fabricantes deben:

- Abordar y corregir las vulnerabilidades sin demora proporcionando actualizaciones de seguridad (Anexo I, Parte II.2)
- Llevar a cabo pruebas y revisiones eficaces y periódicas de la seguridad del producto (Anexo I, Parte II.3)
- Compartir y divulgar públicamente la información sobre vulnerabilidades corregidas (Anexo I, Parte II.4)
- Establecer y aplicar una política de divulgación coordinada de vulnerabilidades (Anexo I, Parte II.5)
- Facilitar una dirección de contacto para informar de las vulnerabilidades descubiertas (Anexo I, Parte II.6)
- Implantar mecanismos para distribuir actualizaciones de forma segura con el fin de garantizar que las vulnerabilidades se corrijan o mitiguen a tiempo (Anexo I, Parte II.7)
- Garantizar que las actualizaciones de seguridad se difundan sin demora, de forma gratuita y con mensajes de aviso que proporcionen información relevante a los usuarios (Anexo I, Parte II.8)

Estas prácticas de gestión de vulnerabilidades pretenden garantizar que los productos sigan estando protegidos y cumpliendo las normas mucho después de su lanzamiento inicial, mediante esfuerzos coordinados a lo largo del período de soporte del producto y más allá.

Obligaciones fundamentales (Artículos 13 y 14)

Además de los requisitos de ciberseguridad para el diseño, el desarrollo, la producción y el mantenimiento de los productos, el CRA esboza varias obligaciones clave para los fabricantes. (Tenga en cuenta que algunas de las obligaciones se aplican a las partes responsables en toda la cadena de suministro. Sin embargo, este documento se centra únicamente en las responsabilidades del fabricante). Estas se definen en los Artículos 13 y 14 del CRA, "Obligaciones de los fabricantes" y "Obligaciones de información de los fabricantes", respectivamente, que especifican los procedimientos que deben seguirse para garantizar que los productos cumplen los requisitos esenciales de ciberseguridad establecidos en las Partes I y II del Anexo I.

Artículo 13 del CRA: Obligaciones de los fabricantes

El Artículo 13 establece las obligaciones de los fabricantes. Desglosemos las obligaciones de los fabricantes en tres fases: diseño y desarrollo, período de soporte y disponibilidad de actualizaciones de seguridad.

Diseño y desarrollo

Durante la primera fase, diseño y desarrollo, este reglamento establece una serie de obligaciones:

- Garantizar que el producto ha sido diseñado, desarrollado y producido de conformidad con los requisitos esenciales de ciberseguridad establecidos en la Parte I del Anexo I.
- Realizar una evaluación de los riesgos de ciberseguridad asociados al producto que se documentará y actualizará durante el período de soporte.
- La evaluación de los riesgos de ciberseguridad debe tener en cuenta la finalidad prevista del producto, sus usos potenciales, las condiciones de uso, como el entorno operativo, o los activos que deben protegerse, y su período de soporte. La evaluación de los riesgos de ciberseguridad indicará si los requisitos esenciales de ciberseguridad establecidos en el Anexo I, Partes I y II, son aplicables al producto en cuestión, y cómo se aplican esos requisitos en la práctica.
- Los resultados de la evaluación de los riesgos de ciberseguridad deben incluirse en la documentación técnica del producto (Artículo 31 y Anexo VII), junto con una justificación clara de la exclusión de cualquier requisito esencial de ciberseguridad. Estos resultados deben guiar las decisiones y acciones a lo largo de las fases de planificación, diseño, desarrollo, producción, entrega y mantenimiento del producto.
- También cabe destacar que los fabricantes deben actuar con la debida diligencia a la hora de integrar componentes de terceros para que dichos componentes no comprometan la seguridad del producto, incluidos los componentes de software libre y de código abierto no disponibles comercialmente en el mercado.
- También aplicarán o harán aplicar los procedimientos de evaluación de la conformidad de su elección a que se refiere el Artículo 32.
- Una vez que se haya demostrado la conformidad del producto con los requisitos esenciales de ciberseguridad del Anexo I, Partes I y II, los fabricantes elaborarán la declaración de conformidad de la UE acorde al Artículo 28 y colocarán el marcado CE acorde al Artículo 30.

> Los apartados 5, 6 y 8 del Artículo 13 establecen que los fabricantes deben actuar con la diligencia debida al integrar componentes de terceros para que dichos componentes no comprometan la seguridad del producto, incluidos los componentes de software libre y de código abierto no disponibles comercialmente en el mercado.

Período de soporte

Pasemos a la siguiente fase, el período de soporte.

- El producto ya se ha comercializado y comienza el período de soporte, durante el cual el fabricante está obligado a garantizar que las vulnerabilidades del producto se gestionan de forma eficaz y conforme a los requisitos esenciales de ciberseguridad formulados en el Anexo I, Parte II.
- Los fabricantes deberán especificar el período de soporte para reflejar el tiempo durante el cual se espera que el producto esté en uso, siendo de al menos cinco años como norma general. Deben determinar el período de soporte teniendo en cuenta las expectativas del usuario, la naturaleza del producto, su finalidad prevista, los períodos de soporte de productos con funcionalidades similares introducidos en el mercado por otros fabricantes, la disponibilidad del entorno operativo y los períodos de soporte de los componentes integrados que proporcionan las funcionalidades principales y se obtienen de terceros, entre otras consideraciones.
- Los fabricantes incluirán en la documentación técnica establecida en el Anexo VII la información que se ha tenido en cuenta para determinar el período de soporte del producto.

- Tenga en cuenta que el período de soporte comienza cuando se comercializa un producto. La fecha final del período de soporte es la última vez que el producto se vende en el mercado, más cinco años. Por lo tanto, el período de soporte sigue siendo de cinco años, pero su fin es un plazo renovable mientras el producto se comercialice. De hecho, la cuenta atrás del período de soporte comienza cuando se vende el último lote del producto. Pero en realidad, el período de soporte llega hasta el final de la vida útil del producto o hasta la última entrega a los clientes en el mercado de la UE, más cinco años.
- Es importante destacar que los fabricantes son plenamente responsables de la identificación, el tratamiento y la divulgación de las vulnerabilidades en todos los componentes, incluidos los procedentes de terceros. Cuando se solucionan las vulnerabilidades de los componentes de terceros, los fabricantes deben compartir la documentación o el código pertinentes con el responsable del mantenimiento del componente.
- El Artículo 13 también exige a los fabricantes que documenten los aspectos significativos relacionados con la ciberseguridad del producto, incluyendo cualquier vulnerabilidad de la que tengan conocimiento y cualquier información relevante proporcionada por terceros. Los fabricantes deben mantener registros exhaustivos de los elementos de ciberseguridad de sus productos, con documentación adaptada específicamente al perfil de riesgo de cada producto.
- Además, los fabricantes deben implementar políticas y procedimientos adecuados para recibir, procesar y responder a los informes de vulnerabilidad enviados por terceros. Esto crea un bucle de retroalimentación eficaz que respalda las continuas mejoras de la seguridad.
- Los fabricantes deben mantener la documentación técnica y la declaración de conformidad de la UE a disposición de las autoridades de vigilancia del mercado durante al menos diez años a partir del lanzamiento del producto, o durante la duración del período de soporte, lo que sea más largo.
- También deben mantener la información y las instrucciones para el usuario (Anexo II) a disposición de los usuarios y de las autoridades de vigilancia del mercado durante al menos diez años después de que el producto se haya comercializado, o durante la duración del período de soporte, lo que sea más largo.
- Durante el período de soporte, los fabricantes que tengan conocimiento de que su producto o sus procesos no cumplen los requisitos esenciales de ciberseguridad establecidos en el Anexo I deberán aplicar inmediatamente medidas correctoras, o retirar o recuperar el producto del mercado.
- Los fabricantes deben facilitar las SBOMs a las autoridades de vigilancia del mercado que lo soliciten para realizar evaluaciones de la dependencia del software en toda la UE, especialmente en componentes de software libre y de código abierto, en categorías de productos específicas.

El período de soporte para un producto comienza cuando el producto se **introduce en el mercado.**

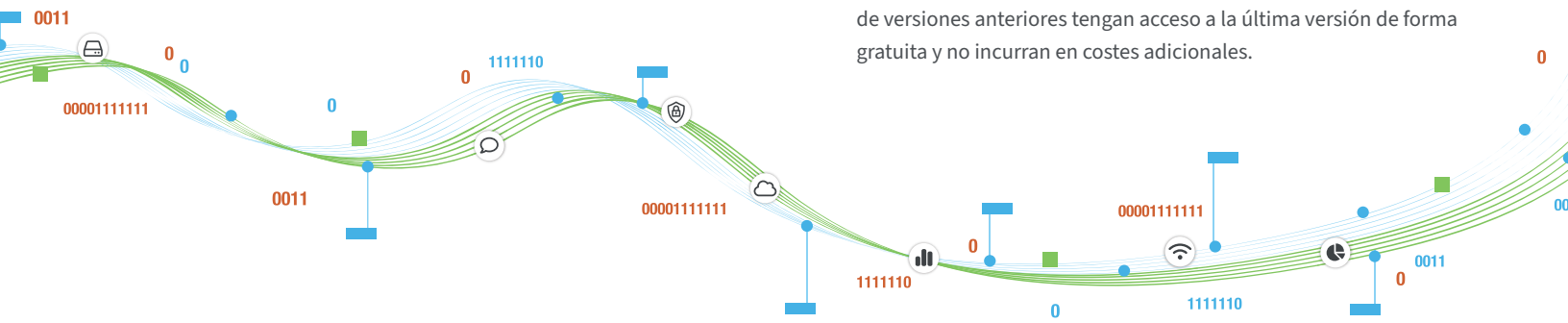
Su finalización viene determinada por la última vez que el producto se vende o se suministra en la UE, más cinco años adicionales.

La cuenta atrás de cinco años comienza solo después de que el producto deje de comercializarse, lo que significa que el período de soporte se prolonga mientras continúen las ventas o las entregas, por lo que se trata de un plazo renovable.

Disponibilidad de actualizaciones de seguridad

Por último, la disponibilidad de actualizaciones de seguridad:

- Los fabricantes se asegurarán de que cada actualización de seguridad mencionada en el Anexo I, Parte II, punto 8, que se haya puesto a disposición de los usuarios durante el período de soporte siga estando disponible después de su publicación durante un período mínimo de diez años o durante el resto del período de soporte, si este fuera más largo.
- Los fabricantes podrán garantizar el cumplimiento del requisito esencial de ciberseguridad establecido en el Anexo I, Parte II, punto 2, solo para la última versión publicada, siempre que los usuarios de versiones anteriores tengan acceso a la última versión de forma gratuita y no incurran en costes adicionales.



Obligaciones de información de los fabricantes (Artículo 14)

Un fabricante debe informar de las vulnerabilidades aprovechadas activamente y de los incidentes graves **en un plazo de 24 horas desde su descubrimiento**. Una vulnerabilidad aprovechada activamente es una debilidad conocida que, basada en pruebas fiables, está siendo utilizada por agentes malintencionados para comprometer los sistemas. Un incidente grave es un suceso que puede tener consecuencias serias para el producto, sus usuarios o los sistemas conectados, como interrupciones, violaciones o fugas de datos.

En ambos casos, una notificación de alerta temprana debe ser compartida simultáneamente con ENISA y el CSIRT designado como coordinador en cada estado miembro. La notificación debe indicar los estados miembros de la UE en los que se ha puesto a disposición el producto.

En el caso de incidentes graves, también se incluirá al menos si se sospecha que se debe a actos ilegales o malintencionados. Dicha notificación se presentará a través de una plataforma establecida por ENISA (Artículo 16).

El fabricante también está obligado a emitir una notificación en un plazo de 72 horas que contenga:

- Información general sobre la vulnerabilidad o el incidente
- Qué se ha hecho para remediar o corregir el problema
- Qué pueden hacer los usuarios para mitigar los daños
- Una evaluación inicial del incidente
- La evaluación del fabricante sobre el carácter sensible o confidencial de la información notificada

Por último, el fabricante debe presentar un informe final tanto para las vulnerabilidades aprovechadas activamente como para los incidentes graves.

En el caso de vulnerabilidades aprovechadas activamente, deberá presentarse un informe final a más tardar catorce días después de que se disponga de una medida correctiva o paliativa, que deberá incluir, como mínimo:

- Descripción de la vulnerabilidad, incluida su gravedad y consecuencias
- Información sobre cualquier agente malintencionado que haya aprovechado o esté aprovechando la vulnerabilidad
- Detalles sobre la actualización de seguridad u otras medidas correctoras disponibles

Para los incidentes graves, deberá presentarse un informe final en el plazo de un mes tras la presentación de la notificación de setenta y dos horas del incidente, que deberá incluir como mínimo lo siguiente:

- Descripción detallada del incidente, incluida su gravedad y repercusiones
- Tipo de amenaza o causa raíz que probablemente desencadenó el incidente
- Medidas de mitigación aplicadas y en curso

Notas importantes sobre el cumplimiento y el ciclo de vida del producto

Todos los productos aplicables en el mercado de la UE deben cumplir las obligaciones de información del CRA, incluidos los productos que estaban disponibles comercialmente antes del 11 de diciembre de 2027. Estos requisitos se aplican a todo el ciclo de vida de todos los productos que llevan la marca CE.

Por lo tanto, los equipos de desarrolladores deben vigilar y analizar continuamente las posibles vulnerabilidades de sus productos, documentarlas adecuadamente e informar de ellas a ENISA y al CSIRT. Para todas las vulnerabilidades identificadas, los desarrolladores deben crear u obtener parches y aplicarlos oportunamente. Esto significa que los fabricantes deben integrar la capacidad de acceder y actualizar cada dispositivo conectable a lo largo de la vida útil del producto para seguir cumpliendo la normativa.

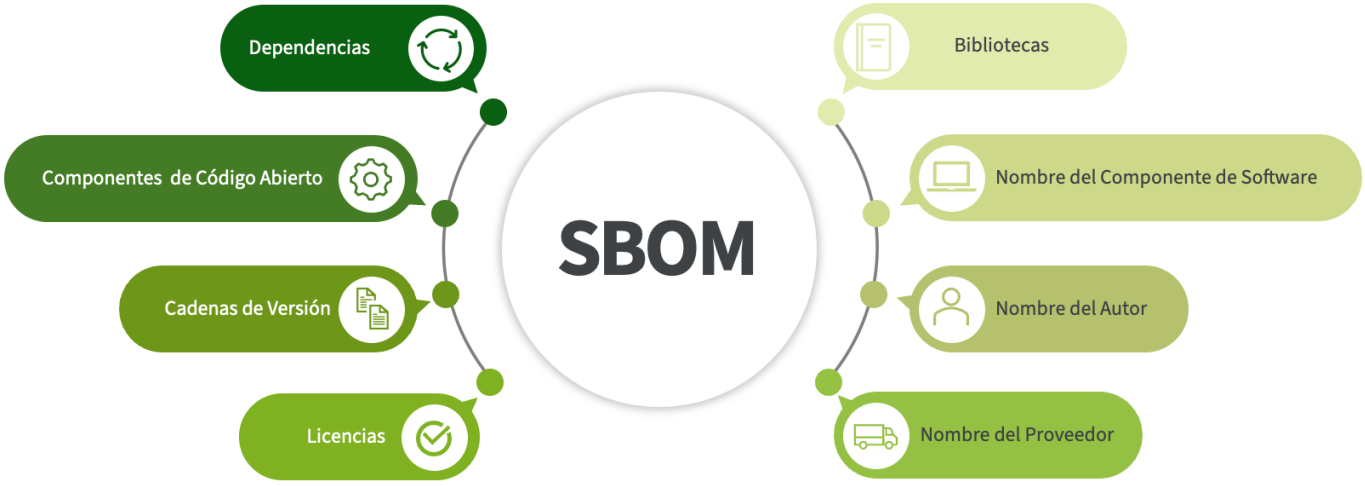
Consulte la sección **"Soporte integral de Digi para el cumplimiento del CRA" en la página 13** para saber cómo las soluciones de Digi ofrecen soporte en cuanto a estos requisitos.

Requisitos para la documentación técnica

Tal y como se menciona en el Artículo 31 y se describe en el Anexo VII del CRA, los fabricantes están obligados a mantener una documentación que incluya lo siguiente:

- Una descripción general de su producto junto a su finalidad prevista, información sobre la versión del software, fotografías que muestren las características y marcas externas, así como la disposición interna, y la información para el usuario y las instrucciones enumeradas en el Anexo II
- Detalles sobre los procesos de diseño, desarrollo, producción y gestión de vulnerabilidades
- Información sobre el diseño y desarrollo del producto: planos/esquemas y una descripción de la arquitectura del sistema que explique cómo los componentes de software interoperan y se integran en el procesamiento global
- Especificaciones sobre los procesos de gestión de vulnerabilidades, incluida la lista de materiales del software, la política coordinada de divulgación de vulnerabilidades, una dirección de contacto para la notificación de vulnerabilidades y una descripción de las soluciones seleccionadas para la distribución segura de actualizaciones
- Información sobre los procesos de producción y supervisión, y la validación de dichos procesos
- La evaluación de los riesgos de ciberseguridad mencionada en el Artículo 13, incluida la forma en que son aplicables los requisitos esenciales de ciberseguridad formulados en la Parte I del Anexo I
- Información sobre cómo determinó el fabricante el período de soporte de su producto de conformidad con el apartado 8 del Artículo 13
- Cualquier norma armonizada publicada por la UE que se aplique total o parcialmente al producto, incluidos los esquemas de certificación de la ciberseguridad y las especificaciones comunes
- Informes de las pruebas realizadas para verificar la conformidad del producto y de los procesos de gestión de las vulnerabilidades con los requisitos esenciales de ciberseguridad aplicables
- Una copia de la declaración de conformidad de la UE del producto, y una SBOM, si procede, a petición de una autoridad de vigilancia del mercado

Entre los requisitos de la documentación técnica se incluyen las descripciones de los productos, los procesos de vulnerabilidades, las evaluaciones de riesgos y las SBOMs, que se mantienen a disposición de las autoridades de vigilancia del mercado durante al menos diez años.



Categorías de productos y procedimientos de evaluación de la conformidad

Productos por defecto y de código abierto	Productos importantes Clase I	Productos importantes Clase II	Productos críticos
Productos no incluidos en otras categorías	• Gestores de arranque • Interfaces de red físicas y virtuales • Sistemas operativos • **MCU/MPU/ASIC/FPGA con funcionalidades relacionadas con la seguridad** • ...	• Hipervisores • Cortafuegos, sistemas de detección y prevención de intrusiones • **MCU/MPU resistentes a manipulaciones**	• Dispositivos de hardware con módulos de seguridad • Pasarelas de contadores inteligentes según la Directiva (UE) 2019/944 • Tarjetas inteligentes, que incluyan elementos seguros
Autoevaluación (Módulo A)			
Autoevaluación únicamente si se realiza conforme a norma(s) armonizada(s) (Módulo A)			
Tercero independiente - Examen de tipo UE y control interno de la producción (Módulo B + C) *(evaluación del producto)*			
Tercero independiente - Garantía total de calidad (Módulo H) *(evaluación del proceso)*			
Tercero independiente - Esquema de certificación de la ciberseguridad de la UE (EUCC) *(evaluación del producto y del proceso)*			

Procedimientos de evaluación de la conformidad (Artículo 32)

Según el Artículo 32, todos los productos incluidos en el ámbito de aplicación del CRA deben someterse a una evaluación de conformidad para demostrar que cumplen los requisitos esenciales de ciberseguridad descritos en el Anexo I.

Los fabricantes deben aplicar al menos uno de los procedimientos de evaluación de la conformidad establecidos por el CRA. Esto incluye tener en cuenta los cambios en los productos, las actualizaciones de las normas armonizadas y la evolución de las certificaciones de ciberseguridad.

El tipo y el alcance de esta evaluación dependen de la clasificación del producto. En la actualidad, la información disponible sobre las categorías de productos sigue siendo incompleta. Acorde con el apartado 4 del Artículo 7, se espera que la Comisión Europea adopte un acto de ejecución a más tardar el 11 de diciembre de 2025 para definir las descripciones técnicas de las Clases I y II de productos importantes que figuran en el Anexo III, así como la categoría de productos críticos que figura en el Anexo IV. Actualmente se está elaborando un **borrador** de dicha ley.

Por defecto

Si el producto no figura en la lista como importante o crítico, el fabricante puede realizar una evaluación interna de la conformidad. La mayoría de los productos cubiertos entran dentro de esta categoría. Esto también se aplica al software libre y de código abierto asociado a productos comerciales.

Tenga en cuenta que los servicios están exentos del CRA, a menos que sean parte integral de la funcionalidad de un producto.

Productos importantes, Clase I

El fabricante puede realizar una evaluación interna solo si aplica normas armonizadas, especificaciones comunes o esquemas europeos de certificación de ciberseguridad. Algunos ejemplos de productos de la Clase I son los gestores de contraseñas, los productos con la función de red privada virtual (VPN), los sistemas de gestión de redes y los asistentes virtuales de propósito general para hogares inteligentes.

Productos importantes, Clase II

Los productos de Clase II siempre requieren una evaluación de conformidad por parte de un tercero. Incluyen hipervisores, microprocesadores y microcontroladores resistentes a las manipulaciones.

Productos críticos

Los productos críticos deben obtener un certificado europeo de ciberseguridad de conformidad con el Reglamento (UE) 2019/881, la Ley de Ciberseguridad de la UE de 2019, o seguir los mismos procesos de evaluación de la conformidad que los productos de Clase II.

Una vez que el fabricante ha completado la evaluación de la conformidad de su producto, debe redactar una declaración de conformidad en las lenguas del estado miembro donde se vende el producto. A continuación, pueden colocar el marcado CE en su producto, su embalaje, la documentación que lo acompaña y su sitio web.

Trabajando juntos para el cumplimiento

El CRA ha alterado fundamentalmente el panorama del cumplimiento normativo de los productos en la UE. Navegar por el CRA y sus complejos requisitos representa uno de los mayores retos a los que se enfrentan los OEMs a la hora de comercializar en la Unión Europea productos seguros que tienen la capacidad de conectarse a Internet.

La combinación de los avanzados procesadores seguros de NXP y las soluciones integrales de Digi ofrece bloques de seguridad que permiten a los OEMs cumplir los requisitos del CRA.

NXP y Digi: Desarrollando procesadores de última generación y soluciones SOM

Digi International colabora con fabricantes como NXP Semiconductors para ofrecer bloques para desarrolladores que aprovechan procesadores avanzados y métodos de seguridad, y ofrecer así apoyo a los OEMs en la creación de productos seguros por diseño que cumplan requisitos como los del CRA y otras normativas.

Postura de NXP en materia de seguridad: Preparación para el CRA

El programa EdgeLock® Assurance de NXP fue creado por NXP para abordar la madura postura en materia de seguridad de la empresa. Sirve de base para que los clientes cumplan las normas y reglamentos de seguridad, apoyando el proceso de seguridad del desarrollador del producto además de ofrecer capacidades de seguridad para el producto.

Este programa incluye la aplicación de las mejores prácticas del sector para un desarrollo seguro y una sólida cultura empresarial que aborda la seguridad física y lógica, así como la formación continua del personal. Los procesos de desarrollo de productos seguros son una parte integral del programa, certificados por terceras partes externas según normas industriales como ISO 21434, IEC 62443-4-1 e IEC 80001-5-1.

Los productos de NXP con funcionalidades de seguridad son verificados durante el proceso de desarrollo por un grupo de expertos del laboratorio interno de Análisis de Vulnerabilidades para garantizar que los productos de NXP están protegidos contra los escenarios de riesgo más comunes. Además, NXP garantiza que sus declaraciones sobre seguridad sean verificadas por terceros independientes, siguiendo estrictas normas industriales como SESIP (EN 17927) y Common Criteria (ISO 15408), garantizando que los componentes de NXP cumplen los más altos estándares de seguridad y resiliencia. Las terceras partes independientes verifican las afirmaciones de seguridad de los productos de NXP, la solidez de dichas implementaciones frente a potenciales ataques específicos, así como la verificación frente a vulnerabilidades conocidas públicamente, ofreciendo una seguridad de vanguardia para cada nivel de riesgo aplicable.

Arquitectura de seguridad escalable y mapeo de requisitos CRA

Para apoyar aún más el cumplimiento del CRA, las capacidades de seguridad de los productos de NXP se pueden asignar a los Requisitos Esenciales de Ciberseguridad del CRA, incluyendo la configuración del producto, la autenticación, el control de acceso, la protección de datos, la supervisión, la gestión de vulnerabilidades y la respuesta a incidentes. Las soluciones de seguridad de NXP están disponibles en una amplia gama de funcionalidades de seguridad, desde el nivel básico hasta el avanzado, lo que permite a los OEMs ampliar las protecciones en función de los niveles de riesgo. Tecnologías clave como los servicios **EdgeLock Secure Enclave**, y **EdgeLock 2GO** proporcionan una sólida protección de credenciales, gestión de la seguridad del ciclo de vida y aprovisionamiento llave en mano.

Soluciones de seguridad de NXP para aplicaciones conformes con el CRA

Para crear un sistema seguro y robusto, en primer lugar, tenemos que poner el ancla de todo el sistema a algo en lo que confiemos. Un silicio con protección de seguridad basada en hardware es difícil de atacar porque es intrínsecamente fiable. El silicio es la base dónde se ejecuta todo el software. Software: el firmware, los protocolos de comunicación, el sistema operativo y otras aplicaciones, pueden ser modificados y puestos en riesgo, pero el silicio no es fácil de comprometer. Llamamos al silicio la Raíz de Confianza (RoT) del sistema.

No existe una seguridad absoluta, dado el amplísimo espectro de ataques posibles, pero además la creciente complejidad de las aplicaciones aumenta significativamente la superficie de ataque.

Como resultado, es importante trabajar con un proveedor de soluciones como Digi que integra los procesadores seguros de NXP en su **sistema sobre módulos Digi ConnectCore®** y ofrece soluciones completas y seguras por diseño y bloques como **Digi ConnectCore Cloud Services** y **Digi ConnectCore Security Services** que permiten a los OEMs diseñar y ofrecer productos finales seguros, junto con la capacidad de supervisar y gestionar de forma remota sus soluciones, cumplir los requisitos del CRA e incluso sumar ingresos adicionales al modelo de negocio de su empresa.

Soporte integral de Digi para el cumplimiento del CRA

Tanto las empresas europeas como las internacionales necesitan orientación práctica y aplicable acerca del CRA y sobre cómo diseñar productos para lograr el cumplimiento desde el principio.

Digi tiene **un gran interés en la ciberseguridad** y ha estado siguiendo el CRA desde que se anunció por primera vez, aprovechando nuestra experiencia en seguridad, y mapeando nuestros bloques de seguridad a los requisitos de esta importante regulación. También adoptamos un enfoque único en nuestros servicios que aborda cada aspecto del CRA, con una orientación detallada paso a paso sobre su aplicación.

"Cuando hablamos con Digi, fue la primera vez que alguien nos habló realmente de lo que teníamos que hacer para cumplir con el CRA", afirma un cliente. "Cuando nos reunimos con otros proveedores, solo nos dieron una visión general de la ley".

Las soluciones y servicios integrados de Digi están diseñados específicamente para ayudar a los clientes a cumplir con los requisitos y obligaciones del CRA, y Digi trabaja con cada cliente para crear un paquete de servicios que satisfaga sus necesidades concretas.

El ecosistema de Digi centrado en el cumplimiento normativo

Digi ofrece **una gama completa** de servicios de conectividad en la nube, incluyendo **sistemas sobre módulos (SOMs) Digi ConnectCore**, software y herramientas, así como **Digi ConnectCore Security Services** y **Digi ConnectCore Cloud Services** que constituyen un ecosistema integrado con seguridad incorporada. Nuestras soluciones ayudan a crear productos digitales conformes y seguros por diseño con una gestión proactiva de las vulnerabilidades, actualizaciones de software seguras y configuración, supervisión y mantenimiento remotos.

Con el ecosistema completo de Digi, los OEMs pueden mantener con confianza el cumplimiento del CRA durante todo el ciclo de vida de sus productos, al tiempo que reducen tanto la complejidad como el tiempo de comercialización. Nuestro enfoque integrado no solo ayuda a abordar los requisitos actuales, sino que también posiciona a las organizaciones para adaptarse sin problemas a futuros cambios normativos.

Junto a nuestro portfolio de productos y servicios especialmente diseñados, Digi también ofrece varios recursos educativos, incluido un seminario web de una hora de duración que aborda **cómo los ingenieros pueden superar los desafíos del CRA**.

Digi TrustFence

Diseñado para aplicaciones de misión crítica, **Digi TrustFence®** ayuda a los desarrolladores a crear una seguridad dinámica y adaptable directamente en los dispositivos IoT, soportando tanto la seguridad por diseño como la configuración segura a través de características como arranque seguro, consola segura, actualizaciones de software seguras, sistema de archivos cifrado, y hardware y pines protegidos.

TrustFence está completamente integrado en los **routers móviles de Digi**, **los módulos RF y módems móviles XBee®**, **los dispositivos de gestión de infraestructura**, y **SOMs Digi ConnectCore**. Digi Embedded Yocto (DEY) también incorpora TrustFence.

Digi ConnectCore Security Services

Digi ConnectCore Security Services ofrece una serie de herramientas para ayudar a las organizaciones a cumplir los requisitos de gestión y divulgación de vulnerabilidades del CRA, incluida la obligación de informar en 24 horas sobre vulnerabilidades aprovechadas activamente e incidentes graves.

Esto analizar y supervisar constantemente una SBOM personalizada que se ejecuta en los SOMs Digi ConnectCore en busca de vulnerabilidades de seguridad. Para ayudar a solucionar los problemas críticos, los servicios proporcionan un informe preciso de vulnerabilidades, una capa de software de seguridad con parches y correcciones para las vulnerabilidades más comunes, y servicios de consultoría y soporte especializados.

Digi ConnectCore Cloud Services

Digi ConnectCore Cloud Services está basado en la plataforma **Digi Remote Manager®** (Digi RM) y ayuda a los fabricantes a mantener sus dispositivos actualizados y proporciona amplias capacidades de automatización de procesos, supervisión y gestión remota de dispositivos.

Al combinar hardware verificado con el conocimiento y la experiencia líderes en el sector, ConnectCore Cloud Services permite a los OEMs desarrollar dispositivos conectados conformes que ofrecen a los clientes una calidad superior y una experiencia de uso sencilla, gracias a actualizaciones automáticas a gran escala de firmware y software, comunicación bidireccional, alertas en tiempo real, e informes detallados sobre el estado de los dispositivos y la salud de la red.

Digi Wireless Design Services

Si está trabajando con soluciones integradas de Digi y necesita soporte de ingeniería, nuestro equipo **Wireless Design Services** (WDS) puede ayudarle. WDS puede apoyar a su equipo de desarrollo en cualquier punto a lo largo del camino, tanto si necesita servicios de diseño y fabricación de productos, certificaciones, desarrollo de software, soporte para una rápida comercialización o compromiso continuo para garantizar que sus productos sigan cumpliendo la normativa.;;p

Este equipo de ingenieros y gestores de proyectos de gran talento cuenta con una amplia experiencia en todos los aspectos del desarrollo de productos, incluidos los rediseños de placas y los recuperación de productos, y dispone de un laboratorio totalmente equipado para tareas de ingeniería, pruebas y soporte para la fabricación.

Digi Embedded Yocto (DEY)

Una distribución Linux de código abierto basada en el Yocto Project™, **Digi Embedded Yocto** (DEY) está diseñado específicamente para nuestros SOMs. Ayuda a los desarrolladores de sistemas embebidos a cumplir con sus obligaciones de conformidad con el CRA mediante una combinación de mantenimiento de software propiedad de Digi, una sólida **política de parches**, y una integración total con Digi TrustFence, Digi ConnectCore Security Services y Digi ConnectCore Cloud Services.

Digi ofrece un soporte completo para el cumplimiento del CRA que incluye la supervisión automatizada de vulnerabilidades, actualizaciones remotas seguras y asesoramiento de expertos durante todo el ciclo de vida del producto.

Cumplir con el CRA: Aprovechar los bloques de seguridad de Digi

Veamos exactamente cómo la solución Digi ConnectCore le ayuda a cumplir con los requisitos del CRA.

Parte I: Requisitos de ciberseguridad relacionados con el producto

En la tabla de la página siguiente hemos incluido los catorce requisitos de ciberseguridad relativos a las propiedades de los productos, según el Anexo I, Parte I. Nos hemos puesto manos a la obra y hemos asignado cada uno de los requisitos a Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services y, por supuesto, nuestro sistema operativo DEY. Echemos un vistazo más de cerca a un par de requisitos.

- **Anexo I, Parte I.2(a).** Los productos se suministrarán sin vulnerabilidades aprovechables conocidas. Digi ConnectCore Security Services facilita el análisis de listas de materiales de software (SBOMs) personalizadas para clasificar vulnerabilidades y exposiciones comunes (CVEs), eliminando falsos positivos y permitiendo a los OEMs centrarse en los problemas más críticos. Además, los OEMs pueden aprovechar nuestra capa meta-digi-security que incluye un conjunto de parches de seguridad preintegrados para DEY, el paquete de soporte de placa (BSP), el kernel de Linux y el gestor de arranque.
- **Anexo I, Parte I.2(c).** Las vulnerabilidades pueden abordarse aprovechando la función de actualización segura de software incluida en Digi TrustFence y Digi ConnectCore Cloud Services para desplegar de forma segura y fiable dichos parches y correcciones remotamente over-the-air (OTA).

Se trata de una evaluación exhaustiva y cuidadosa que detalla nuestro software, herramientas, funcionalidades y procedimientos disponibles para ayudar a los clientes OEM a cumplir con confianza esta legislación, reduciendo el tiempo de comercialización y, lo que es más importante, manteniendo la conformidad durante el ciclo de vida del producto.

Hay algunos requisitos que no aplican a los bloques de seguridad de Digi, pero que podrían aplicar a un producto final basado en ConnectCore. Por ejemplo, un OEM que desarrolle una aplicación utilizando un SOM Digi ConnectCore debe cumplir los requisitos del CRA en el producto final. De hecho, los clientes OEMs son los responsables de productos finales con hardware y software potencialmente vulnerables, por lo que tendrán que considerar cuidadosamente qué trabajo deberán realizar durante su proceso de adopción del CRA.

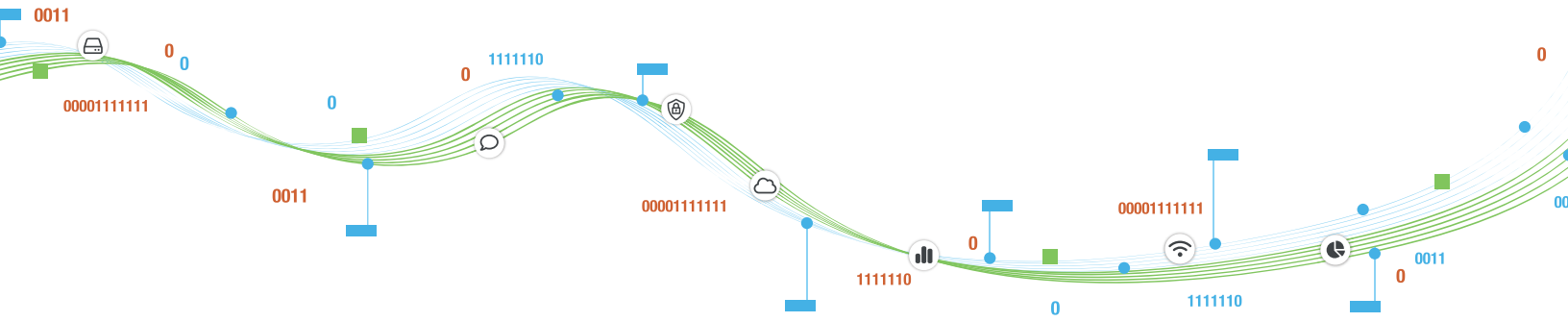
Parte II: Requisitos para la gestión de vulnerabilidades

La última tabla incluye los ocho requisitos de gestión de las vulnerabilidades del Anexo I, Parte II. Siguiendo el mismo enfoque que en la Parte I, hemos asignado meticulosamente cada uno de los requisitos a nuestros bloques de seguridad. Profundicemos en un par de requisitos.

- **Anexo I, Parte II.1.** Nuestra probada metodología, junto con DEY y Digi ConnectCore Security Services, facilita a los fabricantes la identificación y documentación de las vulnerabilidades y los componentes contenidos en los productos mediante la elaboración de una SBOM personalizada que cubre, como mínimo, las dependencias de primer nivel.
- **Anexo I, Parte II.7.** Digi TrustFence y Digi ConnectCore Cloud Services también proporcionan mecanismos para distribuir de forma segura las actualizaciones de los productos para garantizar que se corrigen las vulnerabilidades o mitigan de forma oportuna y, en su caso para las actualizaciones de seguridad, de forma automatizada. Nuestros servicios en la nube garantizan comunicaciones seguras de extremo a extremo con soporte de TLS (Transport Layer Security), autenticación basada en certificados y cifrado. Además, con la funcionalidad de plantillas, las flotas de dispositivos OEM pueden analizarse, actualizarse y mantenerse automáticamente de acuerdo con la configuración establecida. Al aprovechar las plantillas, los clientes OEM pueden ahorrar tiempo, reducir errores, minimizar el esfuerzo y gestionar su crecimiento cuando se necesitan actualizaciones de la configuración, así como garantizar la concordancia y la estandarización en todos los dispositivos desplegados sobre el terreno.

El alcance de esta revisión se centra en Digi ConnectCore. Los clientes OEM que diseñen productos basados en nuestros SOMs podrán aprovechar nuestras soluciones de valor añadido, pero tendrán que dedicar ciertos esfuerzos a cumplir las obligaciones y requisitos del CRA y sus hitos para lanzar un producto al mercado o seguir vendiendo los productos ya existentes.

Por supuesto, podemos concertar una llamada con su representante de ventas para profundizar en estos requisitos y en cómo implementar los bloques de seguridad de Digi para un proyecto específico.

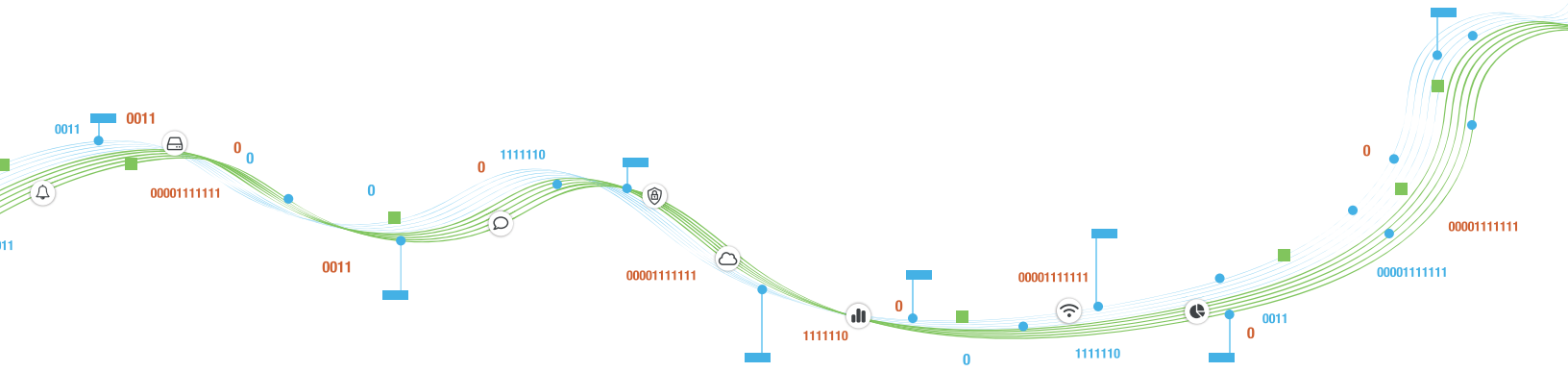


Cumplir con el CRA: Aprovechar los bloques de seguridad de Digi (I)

Parte I	Descripción	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Los productos se diseñarán, desarrollarán y producirán garantizando un nivel adecuado de ciberseguridad basado en los riesgos	TrustFence en general	Security Services en general	Cloud Services en general	DEY en general
(2) (a)	Los productos deberán estar disponibles sin vulnerabilidades aprovechables conocidas	N/A	Análisis SBOM personalizadas, meta-digi-security	**Política de parches de vulnerabilidades de Digi RM**	**Mantenimiento de software propiedad de Digi**
(2) (b)	Los productos estarán disponibles con una configuración segura por defecto	TrustFence en general	N/A	N/A	DEY reforzado
(2) (c)	Los productos garantizarán que las vulnerabilidades puedan abordarse mediante actualizaciones de seguridad	Actualización segura del software	meta-digi-security, consultoría y soporte	Actualizaciones de software OTA seguras y en remoto	Actualización segura del software, configuración de arranque dual
(2) (d)	Los productos garantizarán la protección contra el acceso no autorizado	Consola segura, JTAG segura	N/A	N/A	SSH/TLS
(2) (e)	Los productos protegerán la confidencialidad de los datos almacenados, transmitidos o procesados de cualquier otra forma, ya sean personales o de otro tipo	Sistema de archivos / archivos encriptados (vinculados al hardware)	N/A	Acceso al sistema de archivos, TLS, autenticación basada en certificados y cifrado	Cifrado, WPA3, FIPS 140-2/3 (coste adicional)
(2) (f)	Los productos deberán proteger la integridad de los datos almacenados, transmitidos o procesados de otro modo, personales o de otro tipo, comandos, programas y configuración	Arranque seguro / sistema de archivos autenticado	N/A	Acceso al sistema de archivos, TLS, autenticación basada en certificados y cifrado	TLS, sistema de archivos de solo lectura
(2) (g)	Los productos solo tratarán datos, personales o de otro tipo, que sean adecuados, pertinentes y limitados a lo necesario	N/A	N/A	Flujos de datos personalizados	N/A
(2) (h)	Los productos deberán proteger la disponibilidad de las funciones esenciales y básicas contra los ataques de denegación de servicio	N/A	N/A	N/A	Mejores prácticas de seguridad para sistemas embebidos
(2) (i)	Los productos deberán minimizar el impacto negativo de los propios productos o de los dispositivos conectados sobre la disponibilidad de los servicios prestados por otros dispositivos o redes	N/A	N/A	N/A	Mejores prácticas de seguridad para sistemas embebidos
(2) (j)	Los productos se diseñarán, desarrollarán y producirán para limitar las superficies de ataque, incluidas las interfaces externas	Arranque seguro, consola segura, JTAG segura, detección de manipulaciones	meta-digi-security, consultoría y soporte	N/A	N/A
(2) (k)	Los productos se diseñarán, desarrollarán y producirán para reducir el impacto de un incidente utilizando mecanismos y técnicas de mitigación del aprovechamiento adecuados	Detección de manipulaciones	N/A	Plantillas	N/A
(2) (l)	Los productos proporcionarán información relacionada con la seguridad mediante el registro y la supervisión de la actividad interna pertinente	Detección de manipulaciones	N/A	Agente de supervisión de la seguridad	N/A
(2) (m)	Los productos ofrecerán a los usuarios la posibilidad de eliminar de forma segura y sencilla, y de manera permanente, todos los datos y ajustes y, cuando dichos datos puedan transferirse a otros productos o sistemas, garantizarán que se haga de forma segura	N/A	N/A	Acceso al sistema de archivos, gestión de datos/ajustes en Digi RM	N/A

Cumplir con el CRA: Aprovechar los bloques de seguridad de Digi (II)

Parte II	Descripción	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Los fabricantes elaborarán una lista de materiales de software en un formato de uso común y legible por máquina	N/A	Creación de SBOMs personalizadas	N/A	SBOM DEY
(2)	Los fabricantes abordarán y subsanarán las vulnerabilidades sin demora	N/A	meta-digi-security, consultoría y soporte	Actualizaciones de software OTA seguras y en remoto, plantillas	Versiones periódicas de DEY
(3)	Los fabricantes llevarán a cabo exámenes y pruebas eficaces y periódicas de la seguridad del producto	N/A	Análisis SBOM personalizadas	Política de parches de vulnerabilidades de Digi RM	Política de parches de DEY
(4)	Los fabricantes compartirán y divulgarán públicamente información sobre las vulnerabilidades corregidas	N/A	Security Services en general	Digi Security Center	Digi Security Center
(5)	Los fabricantes establecerán y aplicarán una política de divulgación coordinada de vulnerabilidades	N/A	N/A	Política de parches de vulnerabilidades de Digi RM, Digi Security Center	Política de parches de DEY, Digi Embedded GitHub, Digi Security Center
(6)	Los fabricantes facilitarán el intercambio de información sobre vulnerabilidades potenciales, entre otras cosas, proporcionando una dirección de contacto para notificar las vulnerabilidades descubiertas	N/A	N/A	Formulario de seguridad de Digi	Formulario de seguridad de Digi
(7)	Los fabricantes preverán mecanismos para distribuir de forma segura las actualizaciones con el fin de garantizar que las vulnerabilidades se corrijan o mitiguen de forma oportuna	Actualización segura del software	N/A	Actualizaciones de software OTA seguras y en remoto, plantillas, TLS, autenticación basada en certificados y cifrado	N/A
(8)	Los fabricantes deberán asegurarse de que, cuando existan actualizaciones de seguridad, estas se difundan sin demora y de forma gratuita, acompañadas de mensajes de aviso que proporcionen a los usuarios la información pertinente, incluida incluidas posibles medidas que deban adoptarse	N/A	N/A	Actualizaciones de software OTA seguras y en remoto, plantillas	Política de parches de DEY, Digi Embedded GitHub



El ecosistema de Digi: Cumplimiento integrado del CRA

Uno de los puntos más fuertes del portfolio de Digi es su enfoque integrado del cumplimiento del CRA. Las soluciones de Digi son seguras por diseño y están respaldadas por Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services, y Digi Embedded Yocto (DEY). Estos constituyen una solución integrada de hardware y software con seguridad incorporada desde el principio.

El ecosistema de Digi proporciona una cobertura completa para los requisitos clave del CRA:

- ✓ **Gestión de SBOM:** Herramientas para crear y mantener una lista de materiales de software
- ✓ **Gestión de vulnerabilidades:** Análisis frecuente de vulnerabilidades que surgen tras el lanzamiento inicial del producto
- ✓ **Herramientas de información:** Se incluyen informes precisos sobre vulnerabilidades resaltando los problemas críticos
- ✓ **Subsanación de vulnerabilidades:** Capa de software de seguridad que incluye parches y correcciones para vulnerabilidades comunes
- ✓ **Mantenimiento de la seguridad:** Actualizaciones de software remotas OTA, seguras y fiables
- ✓ **Gestión de flotas de dispositivos:** Permitiendo la automatización de procesos, la supervisión, la gestión remota de dispositivos y la reducción de costes
- ✓ **Soporte de expertos:** Servicios de consultoría y soporte para la integración de parches y correcciones

Con el ecosistema completo de SOMs, software, herramientas y servicios de Digi, los OEMs pueden acelerar con confianza el cumplimiento de esta legislación, reduciendo el tiempo de comercialización y, lo que es más importante, manteniendo la conformidad durante todo el ciclo de vida de sus productos. Este enfoque integrado no solo aborda los requisitos actuales del CRA, sino que posiciona a las organizaciones para adaptarse sin problemas a futuros cambios normativos.

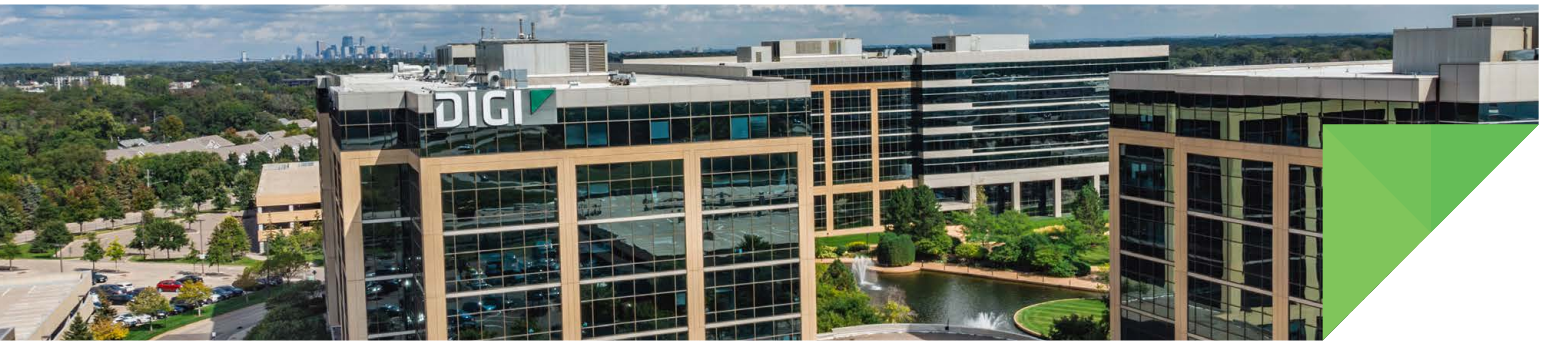
Conclusión

El CRA representa un cambio fundamental en el panorama de los productos digitales. Establece la ciberseguridad como un elemento fundamental y no negociable del diseño y de la gestión del ciclo de vida del producto.

Aunque el CRA se originó en Europa, su influencia ya se está extendiendo por todo el mundo. Adoptando sus principios ahora, las organizaciones pueden prepararse para las normativas emergentes en otras regiones, transformando el cumplimiento normativo de un reto a una oportunidad para el crecimiento sostenible y el liderazgo del mercado a largo plazo.

Las organizaciones que aborden el cumplimiento del CRA de forma estratégica también descubrirán oportunidades más allá de la adhesión a la normativa. Al integrar la seguridad en todo el ciclo de vida del producto, desde la idea hasta el desarrollo, la producción, el despliegue y el mantenimiento, los fabricantes pueden generar una mayor confianza en los clientes, reducir los costosos incidentes de seguridad, y crear productos más resilientes que superen la prueba del tiempo.

Solicite una hora gratuita de consultoría de seguridad con Digi



¿Por qué Digi?

Digi es un proveedor completo de soluciones IoT, que respalda todos los aspectos de su proyecto, desde los equipos de comunicaciones de misión crítica hasta los servicios de diseño y despliegue para que su aplicación se diseñe, instale, pruebe y funcione de forma segura, fiable y con el máximo rendimiento.

Digi crea sus productos de forma que ofrezcan alta fiabilidad, alto rendimiento, seguridad, escalabilidad y versatilidad, de modo que los clientes puedan esperar una vida útil prolongada, adaptarse rápidamente a la evolución de los requisitos del sistema y adoptar tecnologías futuras a medida que surjan. Los módulos embebidos, los routers, los gateways y las soluciones de gestión de infraestructuras de Digi son compatibles con las últimas aplicaciones conectadas en todos los sectores verticales, desde la empresa hasta los casos de uso en el transporte, la energía, la industria y las ciudades inteligentes.

Nuestras soluciones permiten la conectividad con equipos propietarios y basados en estándares, dispositivos, y sensores, y garantizan una comunicación fiable a través de prácticamente cualquier forma de sistema inalámbrico o por cable. Nuestra plataforma integrada de gestión remota ayuda a acelerar el despliegue y a proporciona una seguridad óptima mediante operaciones de red altamente eficientes para funciones de misión crítica, como la configuración en bloque y las actualizaciones de firmware, así como la supervisión de todo el sistema con paneles de control, alarmas, y métricas de rendimiento.

Antecedentes de la empresa

- Digi lleva conectando el "Internet de las cosas", dispositivos, vehículos, equipos y activos, desde 1985
- Digi cotiza públicamente en la bolsa de valores NASDAQ: DGII
- Con sede en las Ciudades Gemelas de Minnesota, Digi emplea a más de 800 personas en todo el mundo y ha conectado más de 100 millones de dispositivos en todo el mundo

Como proveedor de soluciones IoT, Digi pone tecnología probada al servicio de nuestros clientes para que puedan encender redes y lanzar nuevos productos. Una conectividad entre máquinas implacablemente fiable, segura, escalable y gestionada, y que siempre está ahí cuando más la necesita. Eso es Digi.

Próximos pasos

- ¿Listo para hablar con un experto de Digi?
  Contacte con nosotros
- ¿Quiere saber más sobre Digi?
  Suscríbase a nuestro boletín informativo
- Compre ahora soluciones Digi: **Cómo comprar**

Póngase en contacto con un experto de Digi y empiece hoy mismo

TEL.: 877-912-3444
www.digi.com

Sede Mundial de Digi International
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international @DigiDotCom /digi-international