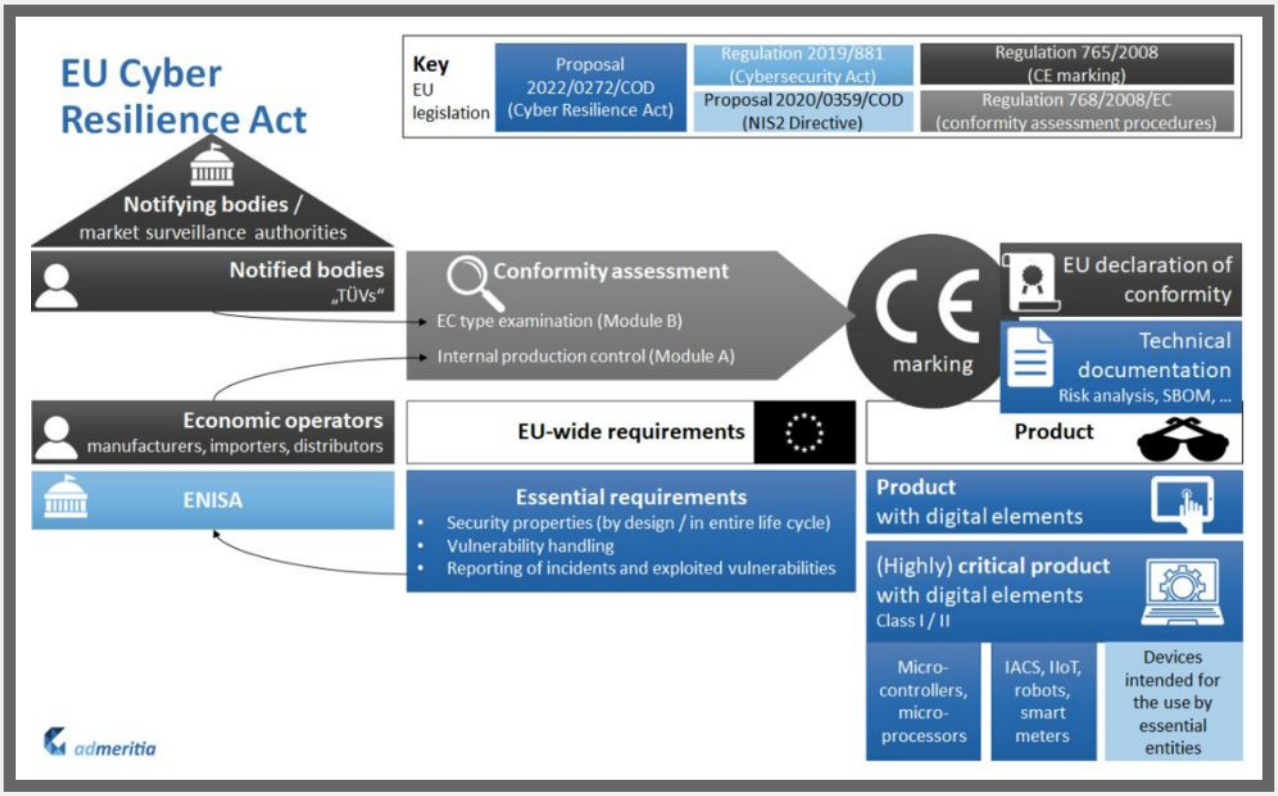
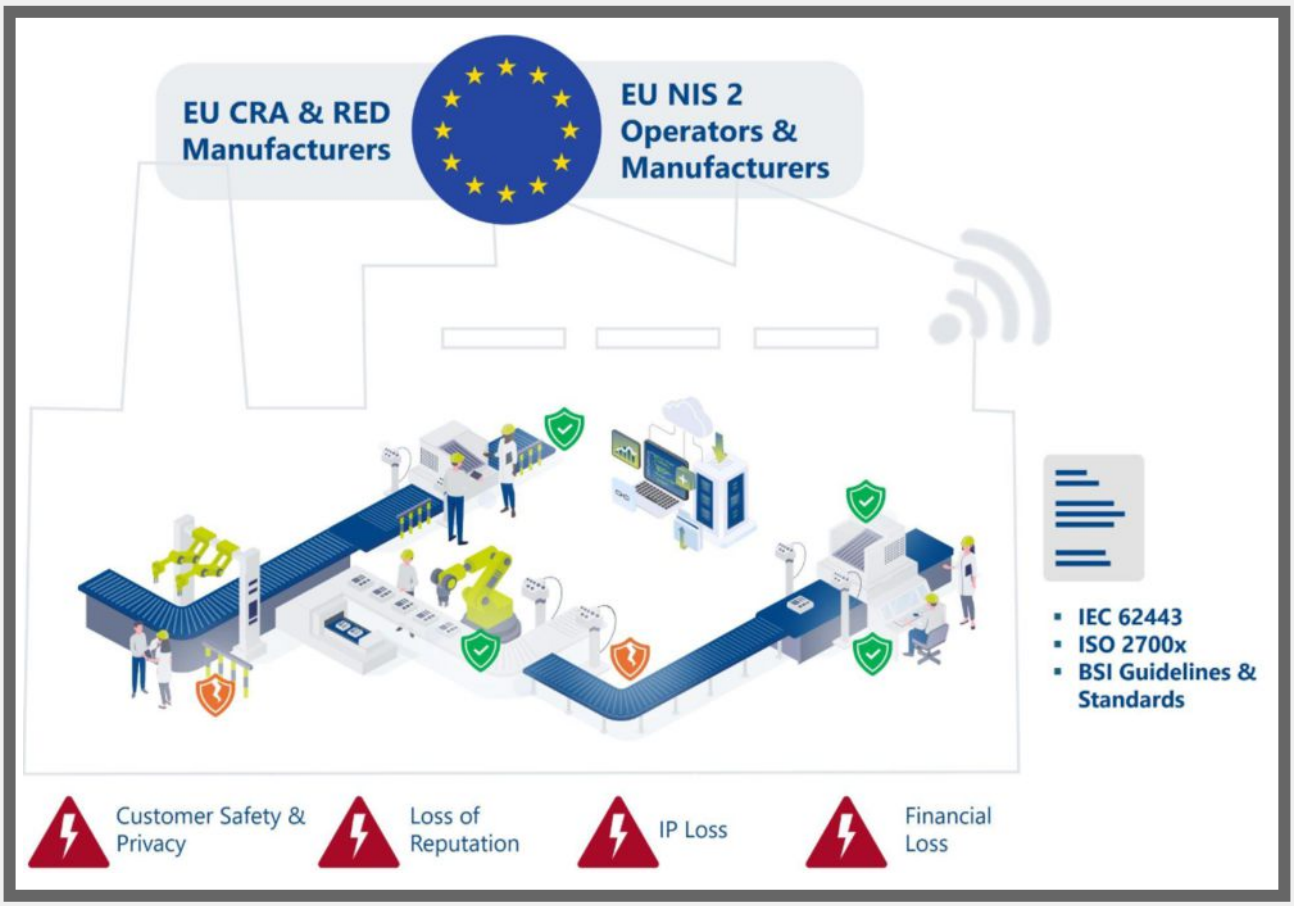
Impacto del Cyber Resilience Act en la industria de la seguridad: hoja de ruta de cumplimiento para los fabricantes

Contenido





Intro

Durante años, en la industria de la seguridad hemos trabajado con una idea bastante asentada: si un producto incorporaba mecanismos sólidos, seguía buenas prácticas y había sido diseñado con criterio, podía considerarse razonablemente seguro. Ese enfoque ha permitido construir soluciones robustas y técnicamente maduras. El problema es que, con la llegada del **Cyber Resilience Act (CRA)**, esa lógica deja de ser suficiente. El mercado europeo ya no se conforma con que la seguridad esté implementada; ahora exige que pueda **demostrarse**. Y eso cambia mucho más de lo que parece. El CRA entró en vigor el **10 de diciembre de 2024**, las obligaciones de reporte arrancan el **11 de septiembre de 2026** y la aplicación plena de las obligaciones principales llega el **11 de diciembre de 2027**.

El CRA no es simplemente una norma más en el panorama regulatorio europeo. Introduce requisitos obligatorios para productos con elementos digitales que se comercialicen en la UE y los convierte en una condición real de acceso al mercado. Eso significa que un fabricante no solo debe diseñar productos técnicamente solventes, sino también estar en condiciones de demostrar su conformidad, emitir su declaración UE y colocar el marcado CE. Sin eso, el producto no debería ponerse en el mercado. Por eso, más que una cuestión puramente técnica, el CRA obliga a conectar seguridad, validación, evidencia y estrategia de producto.

Lo que cambia de verdad con el CRA

Lo más importante del CRA no es que introduzca mecanismos de seguridad desconocidos. Gran parte de lo que exige ya está presente en la conversación habitual de cualquier fabricante con algo de madurez: control de acceso, autenticación, protección de datos, actualizaciones seguras, gestión de vulnerabilidades o trazabilidad. Lo que cambia de verdad no es tanto el "Qué" sino el "Cómo" Hasta ahora muchas organizaciones trabajaban con una lógica de implementación: se aplicaban controles y se asumía que, si estaban bien planteados, el producto estaba razonablemente cubierto. El CRA rompe con esa comodidad. No se fija solo en lo que el fabricante dice haber hecho. Se fija en **cómo se comporta el producto en la práctica**.

Y ahí aparece una de las mayores fricciones para la industria. Muchos productos están bien resueltos sobre el papel y, sin embargo, muestran debilidades cuando se analizan con detalle. Un equipo puede incorporar autenticación y seguir permitiendo accesos indirectos. Puede cifrar comunicaciones, pero hacerlo de forma incorrecta o insuficiente. Puede permitir actualizaciones, pero sin garantizar la integridad del paquete o sin controlar adecuadamente el proceso completo. El problema no siempre es la falta de seguridad; muy a menudo es la falta de **validación real** de esa seguridad. Eso es exactamente lo que el CRA obliga a cambiar.

Por qué el impacto en la industria de la seguridad es tan directo

Este cambio afecta especialmente al sector de la seguridad porque muchos de los fabricantes que llevan años construyendo productos para proteger a terceros son ahora, al mismo tiempo, objeto directo de evaluación. Firewalls, plataformas de virtualización, software de seguridad, gateways, sistemas OT, soluciones cloud o componentes conectados pasan a estar bajo el mismo nivel de exigencia que antes aplicaban a otros entornos. En otras palabras: la industria de la seguridad deja de limitarse a vender confianza y tiene que empezar a demostrarla de forma verificable.

Eso tiene dos consecuencias muy claras. La primera es regulatoria: sube el nivel de exigencia para entrar y mantenerse en el mercado europeo. La segunda es competitiva: los fabricantes que sean capaces de demostrar seguridad con una base técnica sólida y evidencias bien estructuradas estarán mejor posicionados no solo frente a autoridades, sino también frente a clientes, integradores y procesos de compra más exigentes. En un mercado donde todos dirán que su producto es seguro, destacarán los que puedan sostenerlo.

Una hoja de ruta realista para cumplir

El principal error al abordar el CRA es pensar que el cumplimiento se parece a una checklist. No funciona así. En la práctica, lo que necesitan los fabricantes es una **hoja de ruta** que conecte bien el producto, su arquitectura, su comportamiento y la evidencia que va a sostener la evaluación.

El primer paso es **entender el producto** de verdad. No en términos comerciales, sino técnicos. Hay que saber qué expone, qué interfaces utiliza, qué datos trata, qué dependencias tiene, qué activos son críticos y qué pasaría si alguno de esos activos se ve comprometido. Sin este análisis inicial, cualquier control que se implemente después tendrá algo de arbitrario. La seguridad empieza mucho antes de decidir qué mecanismo poner. Empieza por entender qué hay que proteger.

El segundo paso es **definir los mecanismos que realmente aplican**. Aquí es donde marcos como **EN 18031** ayudan a aterrizar la seguridad de producto, porque fuerzan a relacionar activos, exposición y requisitos técnicos. No todos los productos necesitan lo mismo, y precisamente por eso el trabajo no consiste en aplicar todos los controles posibles, sino en aplicar los que corresponden y poder justificar por qué. Este enfoque evita otra desviación muy habitual: diseñar “ara cumplir”en lugar de diseñar para proteger correctamente.

El tercer paso es **entender el contexto en el que el producto va a operar**. Cuando el producto forma parte de un entorno industrial, de un sistema OT o de una arquitectura distribuida, no basta con analizarlo de forma aislada. Aquí es donde **IEC 62443** aporta una base muy útil, porque no se limita al componente, sino que cubre producto, sistema, desarrollo seguro e integración operativa. **IEC 62443-4-1** aporta la base de desarrollo seguro y gestión de vulnerabilidades, mientras que **IEC 62443-4-2** y **IEC 62443-3-3** ayudan a convertir los requisitos de alto nivel del CRA en capacidades técnicas verificables a nivel de componente y sistema.

El cuarto paso es **validar el comportamiento real**. Y éste es probablemente el núcleo más exigente del CRA. No basta con que el mecanismo exista; hay que comprobar que funciona. Eso implica revisar autenticación, control de acceso, comunicaciones, actualizaciones, almacenamiento, gestión de credenciales y todo aquello que define el comportamiento real del producto. En esta fase es donde suelen aparecer las desviaciones más incómodas, no porque el diseño sea necesariamente malo, sino porque nadie había sometido el producto a una validación seria y estructurada.

El quinto paso es **convertir esa validación en evidencia técnica**. Aquí muchas organizaciones subestiman el problema. La documentación por sí sola no basta, pero la ausencia de documentación estructurada tampoco permite sostener una evaluación formal. La evidencia técnica es lo que traduce seguridad implementada en seguridad demostrable: resultados de prueba, trazabilidad, justificación de decisiones, correlación entre riesgos y mecanismos, y una narrativa técnica coherente que permita a un tercero entender por qué el producto se comporta como se espera.

Dónde encajan ETSI, EUCC y Common Criteria

A partir de esa base es donde encajan otros marcos. En algunos casos, el fabricante necesitará aterrizar requisitos muy concretos en función de la naturaleza del producto. Ahí aparece la utilidad

de los estándares **verticales**, como los desarrollados por **ETSI**, especialmente para tipologías concretas: red, virtualización, componentes software, dispositivos conectados o categorías específicas de producto.

En ese punto, la familia **EN 3046xx** puede actuar como referencia vertical para productos de **Clase 1**, al concretar requisitos técnicos sobre categorías específicas. No obstante, la aplicabilidad debe evaluarse caso por caso, en función del tipo de producto, su superficie de exposición y su contexto de uso.

Cuando el nivel de exigencia es mayor o el producto necesita una vía de evaluación más formal, entran en juego esquemas como **EUCC** y **Common Criteria**. EUCC es el esquema europeo basado en Common Criteria que permite certificar productos TIC bajo un proceso común dentro de la UE, y está ya operativo. Common Criteria, por su parte, sigue siendo la base metodológica internacional para muchas evaluaciones de garantía. Ninguno de los dos sustituye el trabajo técnico previo. Al contrario: se apoyan en él. Si el producto no está bien estructurado, bien validado y documentado, será muy difícil recorrer con éxito un proceso formal de certificación.

Lo técnico no lo resuelve todo

Éste es un punto que conviene no perder de vista. Aunque marcos como EN 18031, IEC 62443 o ETSI ayudan a construir una base técnica sólida, el CRA incorpora además obligaciones que son puramente regulatorias y que no se resuelven solo diseñando bien el producto. Entre ellas están la clasificación del producto, los procedimientos de evaluación de la conformidad, la declaración UE, el marcado CE, la vigilancia de mercado y las obligaciones de notificación.

Por eso conviene separar dos planos que a veces se mezclan demasiado: una cosa es la **base técnica del cumplimiento** y otra la **ruta regulatoria completa**. El error más habitual es pensar que si se ha hecho bien la parte técnica, el cumplimiento viene dado por añadidura. No es así. Cumplir significa recorrer bien ambos caminos a la vez.

El error más común: tratar el CRA como una checklist

Si hubiera que resumir en una frase el principal riesgo para fabricantes, sería ésta: **abordar el CRA como una checklist es la forma más rápida de quedarse corto**. El CRA no premia la suma de controles. Premia la coherencia entre análisis, arquitectura, mecanismos, validación y evidencia.

Y aquí es donde aparecen muchos problemas reales:

- Controles aplicados sin relación clara con los activos.
- Requisitos marcados como no aplicables sin justificación.
- Documentación extensa, pero con poca evidencia útil.
- Productos técnicamente correctos que nunca se validaron con suficiente profundidad o sistemas bien estructurados en papel, pero sin una integración realista en operación.

Conclusión: del cumplimiento a la ventaja competitiva

El CRA cambia las reglas del juego porque obliga a la industria de la seguridad a dar un paso más allá de la implementación. Ya no basta con construir productos con mecanismos de protección. Hay que construir productos que puedan ser entendidos, evaluados, validados y defendidos.

Eso exige más disciplina, más trazabilidad y una forma distinta de pensar el producto. Pero también abre una oportunidad clara.

En un mercado donde cada vez más fabricantes van a afirmar que su producto es seguro, destacarán aquellos que puedan demostrarlo con claridad. Los que conviertan la conformidad en una capacidad estructurada — no en una reacción de última hora—no solo estarán mejor preparados para cumplir con el CRA. También estarán mejor preparados para competir.

Y, probablemente, ésa sea la lectura más útil del momento que vive ahora la industria: el CRA no solo obliga a elevar el nivel de seguridad. Obliga a profesionalizar la forma en la que esa seguridad se diseña, se valida y se demuestra. Y en ese escenario, quien mejor entienda el proceso tendrá ventaja real.

Rafael Rodríguez Muñoz
Miembro del área de ciberseguridad de AE