



## Cyber RED: El cambio normativo que pone en riesgo miles de productos conectados

El nuevo marco normativo derivado de la Directiva RED 2014/53/UE, *relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos*, y el Reglamento Delegado (UE) 2022/30, *que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, apartado 3, letras d), e) y f)*, supone un punto esencial para el mercado europeo de equipos radioeléctricos. A partir del 1 de agosto de 2025, todo dispositivo que se conecte a redes, procese datos personales o permita transacciones electrónicas estará sujeto a un escrutinio más estricto: solo quienes demuestren cumplimiento de los nuevos y exigentes requisitos de ciberseguridad podrán obtener el marcado CE. Las empresas que no se adapten a tiempo podrían enfrentarse a retrasos críticos, incertidumbre regulatoria y riesgos para su continuidad en el mercado.

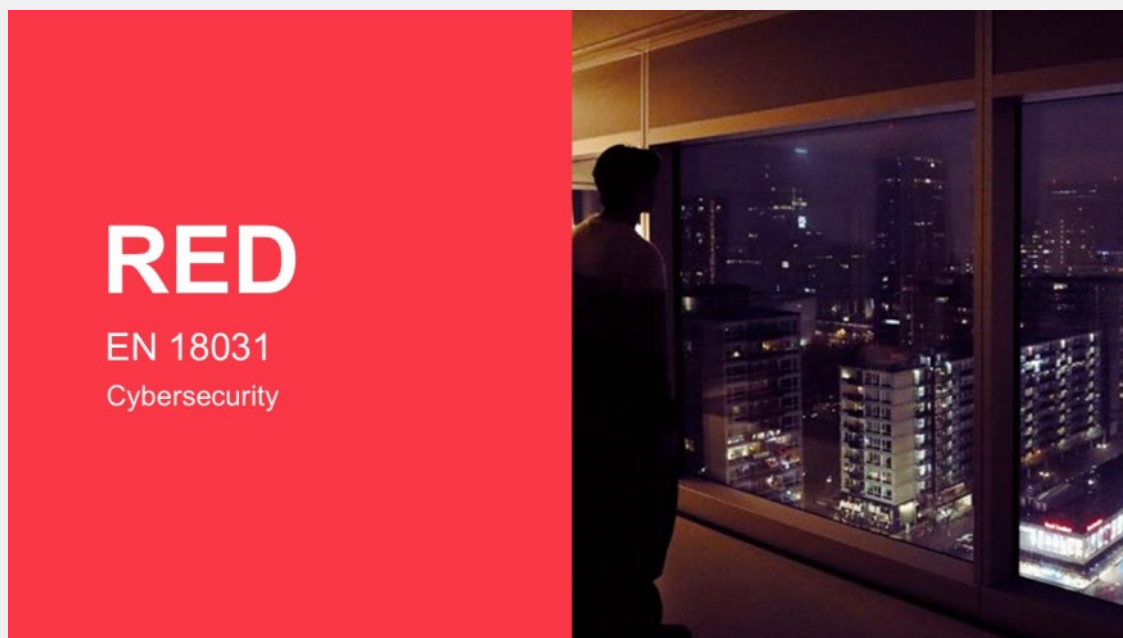
Este cambio es significativo: muchos productos quedarán fuera de cumplimiento si los fabricantes no actúan a tiempo. La mayoría de las empresas aún desconoce el alcance real de estas obligaciones, y se arriesgan a ver detenida su comercialización, rediseños urgentes o incluso la retirada de productos del mercado.

Este documento ofrece una visión clara y necesaria de lo que ya está en vigor. Explicamos los nuevos requisitos técnicos, las normas armonizadas, los desafíos en la presunción de conformidad y cómo el proceso de certificación puede convertirse en un retraso crítico para quienes no se hayan preparado. En un entorno regulatorio que evoluciona rápidamente, comprender y anticipar estos requisitos no es una opción, es una condición indispensable para seguir operando.

### Introducción a la Directiva RED

La Directiva RED (2014/53/UE) regula la comercialización de equipos radioeléctricos en la Unión Europea, garantizando que sean seguros, eficientes y compatibles con el entorno electromagnético. Desde su entrada en vigor en 2016, es el marco legal de referencia para dispositivos *eléctricos o electrónicos que emite o recibe intencionadamente ondas radioeléctricas para radiocomunicación o radiodeterminación, así como para productos que requieren accesorios para dichas funciones* como móviles, routers, wearables y otros productos que utilizan tecnologías inalámbricas como puedan ser los productos de intrusión y control de accesos para sistemas de seguridad, o para sistemas de incendios.

Con la publicación del Reglamento Delegado (UE) 2022/30, la Directiva se amplía para incluir requisitos nuevos y fundamentales. Estos requisitos van dirigidos a fortalecer la ciberseguridad, la protección de datos y la resistencia de los dispositivos conectados. Tales modificaciones pretenden asegurar que los equipos radioeléctricos conserven un grado suficiente de defensa ante amenazas digitales que van apareciendo.



### **Nuevos Requisitos de Ciberseguridad**

El Reglamento Delegado (UE) 2022/30, incorpora tres requisitos esenciales de ciberseguridad al artículo 3.3 de la Directiva RED. Estos requisitos son obligatorios a partir del 1 de agosto de 2025 para todos los equipos radioeléctricos conectados a redes públicas o que traten datos personales o transacciones electrónicas.

Requisitos clave:

- Artículo 3.3 (d): Protección de redes
- Artículo 3.3 (e): Protección de datos personales
- Artículo 3.3 (f): Prevención del fraude

Estos requisitos refuerzan la seguridad digital en el mercado europeo, alinean los productos con las expectativas de protección frente a ciber amenazas, y aumentan la confianza del consumidor.

### **Aplicabilidad a Equipos de Radio**

La aplicabilidad de los nuevos requisitos depende de las funcionalidades del equipo radioeléctrico.

No todos los dispositivos están sujetos a ellos, pero es imprescindible realizar un análisis de riesgos para determinar si aplican.



### Presunción de Conformidad y Normas Técnicas

Para facilitar el cumplimiento de los requisitos de ciberseguridad, la Comisión Europea ha armonizado la serie de normas **EN 18031**, que permiten la presunción de conformidad bajo la Directiva RED.

Normas armonizadas:

- EN 18031-1: Protección de redes
- EN 18031-2: Protección de datos personales
- EN 18031-3: Prevención del fraude

Otras normas relevantes:

- ISO/IEC 62443: –Enfocada en la ciberseguridad en sistemas de automatización y control industrial (ICS)
- ETSI EN 303 645: Este es el referente en ciberseguridad para dispositivos IoT de consumo.

### Restricciones y consecuencias

A partir de la fecha en que el Reglamento Delegado (UE) 2022/30 es de obligado cumplimiento, los equipos radioeléctricos que no muestren que cumplen con los nuevos requisitos de ciberseguridad no se podrán comercializar ni usar en el mercado europeo. La falta de cumplimiento podría conllevar la retirada o prohibición de venta de los productos afectados, y también a sanciones administrativas o económicas impuestas por las autoridades que correspondan.

## Estructura y Evaluación de las Normas EN 18031

La serie de normas EN 18031 ha sido publicada en el Diario Oficial de la Unión Europea y se convierte en referencia para demostrar el cumplimiento de los requisitos de ciberseguridad de la Directiva RED. Cada norma aborda un apartado específico del artículo 3.3 y define mecanismos técnicos como autenticación, cifrado, control de acceso, actualizaciones seguras, etc.

Documento	Cubre el requisito esencial	Aborda los activos y riesgos de seguridad	Aborda los activos y riesgos de la red	Aborda los activos y riesgos de privacidad	Aborda los activos y riesgos financieros
EN 18031-1	3.3.(d)	✓	✓	✗	✗
EN 18031-2	3.3.(e)	✓	✗	✓	✗
EN 18031-3	3.3.(f)	✓	✗	✗	✓

Para cumplir con cada uno de los requisitos, la norma establece un conjunto de mecanismos, que son:

Requirements	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] Access Control Mechanism	✓	✓	✓
[AUM] Authentication Mechanism	✓	✓	✓
[SUM] Secure Update Mechanism	✓	✓	✓
[SSM] Secure Storage Mechanism	✓	✓	✓
[SCM] Secure Communication Mechanism	✓	✓	✓
[LGM] Logging Mechanism	-	✓	✓
[DLM] Deletion Mechanism	-	✓	-
[UNM] User Notification Mechanism	-	✓	-
[RLM] Resilience Mechanism	✓	-	-
[NMM] Network Monitoring Mechanism	✓	-	-
[TCM] Traffic Control Mechanism	✓	-	-
[CCK] Confidential Cryptographic Keys	✓	✓	✓
[GEC] General Equipment Capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

### Evaluaciones requeridas:

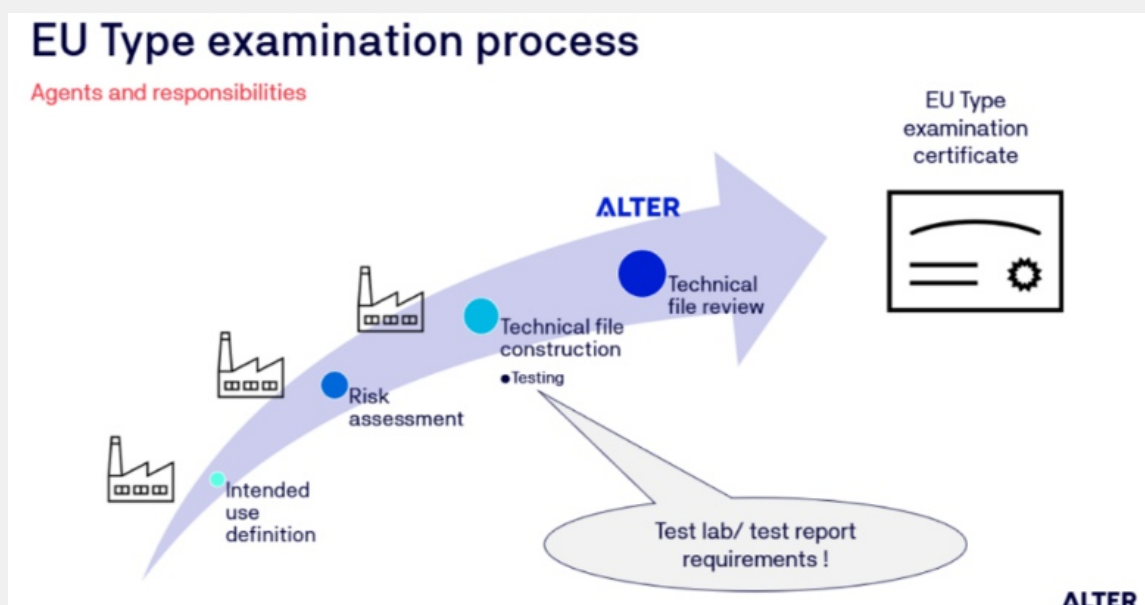
1. Evaluación conceptual: Verifica que el diseño del equipo o del sistema integre de manera consistente los principios de ciberseguridad que se requieren. De esta forma, la arquitectura que se propone maneja de forma apropiada los riesgos que se esperan.
2. Evaluación de integridad funcional: Revisa que las funciones de seguridad que se han puesto en marcha, como el cifrado, la autenticación o el control de acceso, funcionen bien y no interfieran con el resto de las operaciones del sistema.
3. Evaluación de suficiencia funcional: Evalúa si el grado de protección que ofrecen las medidas de seguridad resulta suficiente ante el tipo de amenaza que se prevé. Toma en cuenta la clase de dispositivo y el ambiente en el que opera.

### Proceso de Certificación de Examen UE de Tipo

Este proceso para equipos radioeléctricos bajo la Directiva RED y el Reglamento Delegado 2022/30 sigue una secuencia estructurada que permite validar la seguridad del producto y obtener el mercado CE.

#### Fases del proceso:

1. Solicitud
2. Workshop
3. Definición de activos y alcance
4. Entrega de muestras y documentación
5. Evaluaciones funcionales
6. Certificación



## Restricciones en la Armonización

Aunque las normas EN 18031 permiten la presunción de conformidad, existen restricciones técnicas que pueden limitar su aplicación directa. Si el producto no cumple con estas restricciones, será necesario recurrir a un Organismo Notificado para validar el cumplimiento.

*Principales restricciones:*

- Fortaleza de contraseñas
- Control parental
- Actualizaciones seguras

## Estrategia de Cumplimiento para Empresas

La adaptación a los nuevos requisitos de ciberseguridad exige una estrategia clara, proactiva y alineada con el ciclo de vida del producto.

*Recomendaciones clave:*

- Seguridad desde el diseño
- Análisis de riesgos
- Selección de normas aplicables
- Documentación técnica
- Roadmap de certificación

## Conclusiones y Recomendaciones Finales

La incorporación de requisitos de ciberseguridad en la Directiva RED representa un cambio significativo en la regulación de equipos radioeléctricos en Europa. Las empresas deben prepararse para este nuevo escenario normativo mediante:

- Integración de la seguridad como parte del diseño del producto
- Adopción de normas armonizadas o equivalentes
- Planificación de procesos de evaluación y certificación
- Formación interna sobre requisitos técnicos y regulatorios

Rafael Rodríguez Muñoz

Miembro del área de ciberseguridad de AES