AFEC
sociación de fabricantes
equipos de climatización

Webinar técnico

# Ley de Ciber Resiliencia

*Nuevas obligaciones de ciberseguridad para productos conectados en climatización*

14 de mayo de 2026

ontrol inteligente
limatización eficiente

# CRA en HVACR: requisitos para su implementación

Miriam Solana Ciprés

*HVAC/R Technical Knowledge Manager*

CAREL Industries S.p.A.

ontrol inteligente
limatización eficiente

AFEC
asociación de fabricantes
de equipos de climatización

CAREL

# Contenidos

1. CRA: calendario y ámbito de aplicación

2. Clasificación de productos

3. Obligaciones de los fabricantes

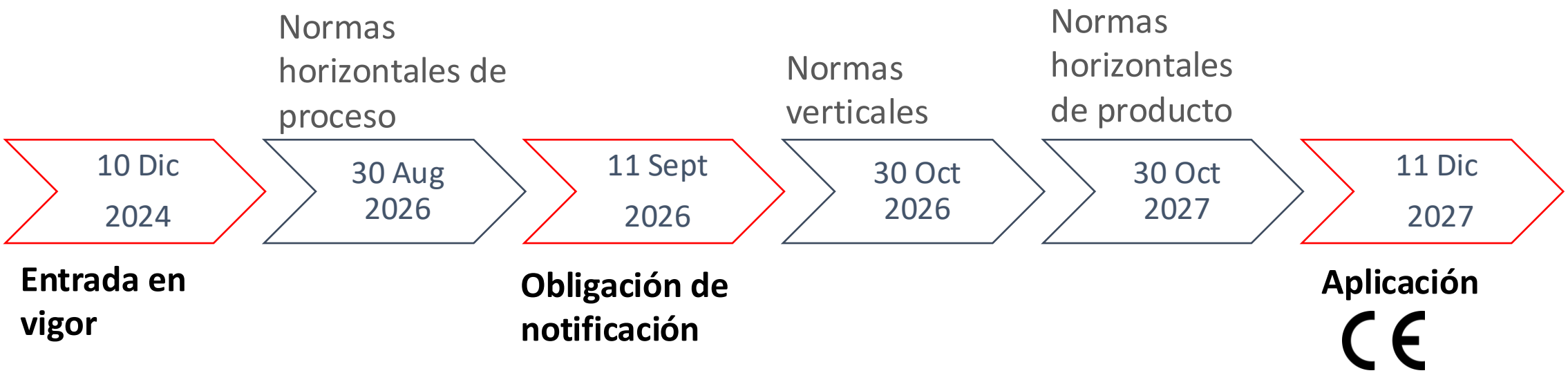
# Contenidos

1. CRA: calendario y ámbito de aplicación

2. Clasificación de productos

3. Obligaciones de los fabricantes

# Calendario: fechas clave




**Los Estados miembros deben designar autoridades y organismos para realizar evaluaciones de conformidad del CRA a partir del 11 de junio de 2026**

# Productos incluidos y excluidos

**DENTRO DEL ÁMBITO: «Productos con elementos digitales con una conexión de datos lógica o física a un dispositivo o red introducidos en el mercado de la UE»**

✓ Productos de hardware
✓ Productos de software

…incluidas sus soluciones de tratamiento de datos a distancia
…incluidos los componentes comercializados sujetos a una MODIFICACIÓN SUSTANCIAL

**FUERA DEL ÁMBITO**

X Productos no comerciales
X Software como servicio (SaaS), salvo las soluciones de tratamiento de datos a distancia relacionadas con un producto con elementos digitales
X Piezas de recambio puestas en el mercado para sustituir componentes idénticos
X Productos sanitarios y productos sanitarios para diagnóstico in vitro
X Seguridad de la aviación civil
X Vehículos de motor y remolques
X Productos con elementos digitales desarrollados exclusivamente para la seguridad nacional o la defensa

# Contenidos

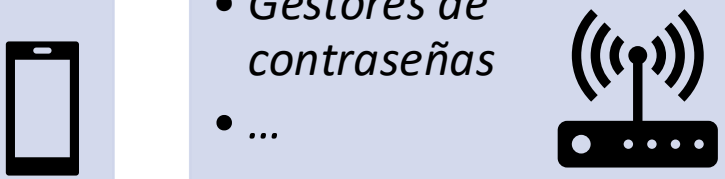
1. CRA: calendario y ámbito de aplicación

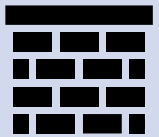
2. Clasificación de productos

3. Obligaciones de los fabricantes

# Categorías y requisitos

| **Predeterminada**<br>*Autoevaluación* | **Importante Clase I**<br>*Autoevaluación o evaluación por terceros* | **Importante Clase II**<br>*Evaluación por terceros* | **Crítica**<br>*Evaluación por terceros* |
|---|---|---|---|
| • *Aplicaciones móviles*<br>• *Altavoces inteligentes*<br>• *Videojuegos*<br>• *Impresoras*<br>• … | • *Navegadores independientes e integrados*<br>• *Routers, módems destinados a la conexión a Internet y conmutadores*<br>• *Gestores de contraseñas*<br>• … | • *Cortafuegos*<br>• *Microprocesadores y microcontroladores resistentes a la manipulación*<br>• *Sistemas de detección y prevención de intrusiones* | • *Dispositivos de hardware con módulos de seguridad*<br>• *Pasarelas de contadores inteligentes*<br>• *Tarjetas inteligentes* |





**Aproximadamente el 90 % de los productos pertenecen a la categoría predeterminada**

AFEC Control inteligente limatización eficiente

# Contenidos

1. CRA: calendario y ámbito de aplicación

2. Clasificación de productos

3. Obligaciones de los fabricantes

# Pasos clave para los fabricantes

## DISEÑO Y DESARROLLO

- **Análisis de riesgos** (Artículo 13)
- **Requisitos esenciales relacionados con el producto** (Anexo I, Parte I)
- **Requisitos esenciales para la gestión de vulnerabilidades**(Anexo I, Parte II)
- **Expediente técnico**, con información e instrucciones (Anexo VII, Anexo II)

## CONFORMIDAD

- **Marcado CE**
- **Declaración UE de Conformidad** (Anexo V, Anexo VI y Anexo VIII)

## MANTENIMIENTO

- **Cumplimiento** continuo de los requisitos esenciales para la gestión de vulnerabilidades durante el ciclo de vida previsto o >5 años (Artículo 13)
- Obligación de **informar** sobre vulnerabilidades explotadas o incidentes que afecten a la seguridad de los productos (Artículo 14)

# Pasos clave para los fabricantes

## DISEÑO Y DESARROLLO

- **Análisis de riesgos** (Artículo 13)
- **Requisitos esenciales relacionados con el producto** (Anexo I, Parte I)
- **Requisitos esenciales para la gestión de vulnerabilidades**(Anexo I, Parte II)
- **Expediente técnico**, con información e instrucciones (Anexo VII, Anexo II)

## CONFORMIDAD

- **Marcado CE**
- **Declaración UE de Conformidad** (Anexo V, Anexo VI y Anexo VIII)

## MANTENIMIENTO

- **Cumplimiento** continuo de los requisitos esenciales para la gestión de vulnerabilidades durante el ciclo de vida previsto o >5 años (Artículo 13)
- Obligación de **informar** sobre vulnerabilidades explotadas o incidentes que afecten a la seguridad de los productos (Artículo 14)

# Requisitos esenciales



- Sin vulnerabilidades aprovechables conocidas
  - ej.: Evitar credenciales por defecto: admin/admin
- Configuración segura por defecto
  - ej.: Actualizaciones de seguridad automáticas activadas
- Vulnerabilidades corregibles mediante actualizaciones de seguridad
  - ej.: Parche para una versión insegura del protocolo de comunicación
- Protección frente a accesos no autorizados
  - ej.: Proporcionar autenticación robusta
- Confidencialidad e integridad de datos
  - ej.: Métodos cifrados, arranque seguro
- Tratar únicamente los datos adecuados, pertinentes y limitados a lo necesario
  - ej.: No recopilar datos personales innecesarios
- Proteger la disponibilidad de las funciones esenciales
  - ej.: Control manual local
- 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
  - ej.: Incluir requisitos de aislamiento del dispositivo
- Limitar las superficies de ataque, incluidas las interfaces externas
  - ej.: Mantener los puertos físicos protegidos o deshabilitados si no se usan
- Uso de mecanismos y técnicas adecuadas de mitigación de la explotación
  - ej.: Implantar cortafuegos para las interfaces de red
- Registro y supervisión de la actividad interna relevante
  - ej.: Registrar intentos fallidos de inicio de sesión
- Posibilidad de que los usuarios eliminen todos los datos y ajustes
  - ej.: Botón u opción de menú de «restablecimiento de fábrica»

AFEC ontrol inteligente limatización eficiente

AFEC
asociación de fabricantes
de equipos de climatización

# Gracias

Miriam Solana Ciprés
CAREL Industries S.p.A.

CAREL

# Automatización, control y ecosistema europeo

Salvatore Cataldi

*Global Standards & Regulations Lead*

BELIMO Automation AG

BELIMO®

eu.bac european building automation controls association

ontrol inteligente limatización eficiente

AFEC asociación de fabricantes de equipos de climatización

# El CRA cambia el modelo de responsabilidad

## Si no lo tratamos como ciclo de vida, el cumplimiento se vuelve incompleto y reactivo.


La ciberseguridad deja de ser una función… y se convierte en una responsabilidad en el tiempo.

# Tres obligaciones que cambian la operación del fabricante

## Ya no basta “hacerlo seguro”: hay que demostrarlo y sostenerlo con procesos.

- Marcado CE con requisitos de ciberseguridad
- Gestión de vulnerabilidades (proceso continuo)
- Actualizaciones de seguridad durante el ciclo de vida

El producto ya no termina en la venta.

# El reto principal es organizativo, no tecnológico

## Sin roles y procesos claros, no hay respuesta consistente.

- Secure by design (desde el inicio)
- Proceso de vulnerabilidades (triage, priorización)
- Actualizaciones + soporte (a largo plazo)
- Documentación + notificación (evidencia)
- El producto ya no termina en la venta.

El reto no es técnico… es organizativo.

# El CRA también crea oportunidades de mercado

## Quien se prepare antes convierte cumplimiento en ventaja competitiva.

- Productos confiables → señal de mercado
- Requisitos armonizados → menos fragmentación
- Ventaja para los que se mueven primero

La confianza se convierte en ventaja competitiva.

# Cinco ideas clave sobre el impacto del CRA

## Esto es lo que deben empezar a hacer desde hoy.

1. La ciberseguridad es una responsabilidad en el tiempo, no una función.
2. El cumplimiento se basa en gestión del riesgo, no en soluciones únicas.
3. El sistema es responsable, no solo el producto.
4. La interoperabilidad requiere nuevas formas de gestionar la seguridad.
5. Empezamos ya a construir procesos, no solo productos.

asociación de fabricantes
de equipos de climatización

# Gracias

Salvatore Cataldi

BELIMO Automation AG

BELIMO®

eu.bac european building automation controls association

# CRA: Cómo prepararse

Marta Castro

*Directora del Área Digital Lab Services*

TECNALIA

ontrol inteligente
limatización eficiente

AFEC
asociación de fabricantes
de equipos de climatización

# Retos actuales de las empresas

¿Los equipos ya instalados son ciberseguros?
¿Cómo me protejo ante ciberataques?

¿Cómo adapto los equipos comercializados a los nuevos rediseños que cumplan con los requisitos de ciberseguridad?

¿Qué tiene que cumplir mi equipo a nivel de requisitos de ciberseguridad?

¿Cómo aseguro que mi equipo es ciberseguro?

## Entorno regulatorio fragmentado

- Múltiples normas, estándares, requisitos.
- Diferencias normativas dificultan el cumplimiento uniforme.

## Costos de cumplimiento

- Adaptación a nuevos requisitos para evitar sanciones y pérdidas de reputación

## Mantenimiento y despliegue

- Equilibrio entre ciberseguridad e innovación ágil.
- Cómo gestionar todo el ciclo de vida de los activos.
- Actualizaciones continuas
- Gestión de riesgos.

Exposure to cyber attacks

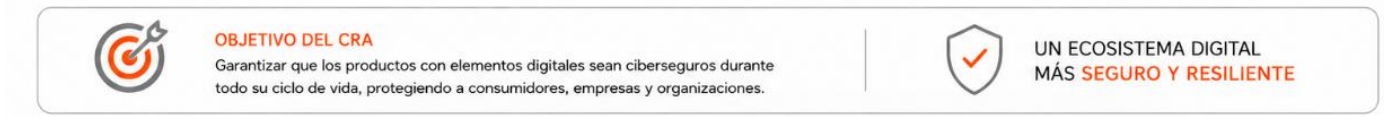
Access points

New technologies

Regulation

# CRA

Establece requisitos para la puesta en el mercado de productos con elementos digitales para garantizar la ciberseguridad de dichos productos


# CRA

## Cyber Resilience Act (Reglamento (UE) 2024/2847)

### 1. DEFINICIÓN DE LA CRA

El Reglamento (UE) 2024/2847 sobre ciberresiliencia (CRA) es adoptado y publicado en el Diario Oficial de la UE.

### 2. ÁMBITO

El CRA se aplica a los productos con elementos digitales durante todo su ciclo de vida.

- Desde el diseño y desarrollo hasta la comercialización, uso y retirada.
- Independientemente del sector o del tamaño de la organización.

### 3. OBJETIVO

Garantizar que los productos con elementos digitales sean ciberseguros durante todo su ciclo de vida, protegiendo a consumidores, empresas y organizaciones y reduciendo vulnerabilidades de origen (*security by design*).

### 4. ¿A QUIÉN AFECTA?

- Fabricantes de productos con elementos digitales
- Importadores y distribuidores

UN ECOSISTEMA DIGITAL MÁS **SEGURO Y RESILIENTE**

Menos vulnerabilidades. Más confianza.
Una Europa digital más resiliente.

Procedimientos de evaluación de la conformidad de los productos con elementos digitales


Análisis de riesgos

Procedimientos de evaluación de la conformidad de los productos con elementos digitales

## Tipos de evaluación posibles

- **Tipo A** (Módulo A) : Autodeclaración del fabricante
  - **Ruta típica para productos no importantes/no críticos (cuando aplique autoevaluación)**.
  - El fabricante documenta y declara que su producto cumple.

- **Tipo B+C** (Módulo B seguido de C)
  - El fabricante presenta el diseño a un organismo notificado (Módulo B).
  - Tras aprobación por el organismo notificado, el fabricante asegura que los productos fabricados son conformes (Módulo C).

- **Tipo H** (Módulo H)
  - Evaluación completa del sistema de gestión de calidad.
  - Requiere que un organismo notificado audite al fabricante.
  - **Ruta habitual para productos críticos o de alta exigencia, basada en aseguramiento de calidad total**.

Procedimientos de evaluación de la conformidad de los productos con elementos digitales

| Tipo de Evaluación | Composición de módulos | Quién interviene | Aplicación habitual (orientativa) |
|---|---|---|---|
| Tipo A | Módulo A | Fabricante | Productos no importantes /no críticos (ruta tipica) |
| Tipo B + C | Módulo B + Módulo C | Organismo notificado + Fabricante | Productos importantes (ruta típica) |
| Tipo H | Módulo H | Organismo notificado (audita QMS) | Productos criticos |

A mayor criticidad, mayor intervención de tercera parte y mayor evidencia exigida

# CRA

Cumplimiento de la CRA aplicando la norma IEC 62443-4-X

## REGLAMENTO DE CIBERRESILIENCIA (CRA)

- Los fabricantes deben garantizar la gestión de vulnerabilidades durante toda la vida útil del producto
- Extiende la responsabilidad por fallos de seguridad a toda la cadena de suministro
- Cada componente digital debe cumplir con los requisitos esenciales de ciberseguridad
- Los productos necesitarán una evaluación de conformidad antes de ser puestos en el mercado de la UE
- Las actualizaciones de software, el desarrollo seguro y la transparencia se convierten en obligaciones legales

**IEC 62443-4-1**
Cumplimiento con el ciclo de vida seguro del desarrollo (2)

**IEC 62443-4-2**
Cumplimiento del requisito de evaluación de productos (1)

**¿Tiene el equipo radio?**
Acta delegada de la Directiva RED + IEC 62443-4-1

## Cumplimiento de la CRA aplicando la norma IEC 62443-4-X

Para obtener la certificación de producto es requisito tener la certificación de la IEC 62443-4-1 y IEC 62443-4-2

### Pretest

- OBEJTIVO: conocer el estado de cumplimiento de los requisitos en fases tempranas de desarrollo, que permitan optimizar, adaptar y adecuar el desarrollo y el proceso a los requisitos de ciberseguridad requeridos al equipo, al caso de uso y al reglamento.
- Revisión documental con el objetivo de analizar el alcance de las pruebas y caracterizar el equipo
- Laboratorios de ensayos con pruebas críticas

### Certificación del proceso IEC 62443-4-1

- **Entidad Certificador** certifica que el fabricante ha desplegado un proceso de desarrollo de producto seguro acorde a la norma.
  - 4 Niveles de madurez
  - A través de una auditoría del proceso productivo en el que el fabricante aporta evidencias de la implantación de las prácticas establecidas por el estándar.
  - A través de una auditoría en fábrica.

### Certificación de requisitos de ciberseguridad IEC 62443-4-2

- **laboratorio acreditado** verifica que el producto cumple con los requisitos de ciberseguridad definidos en la norma
  - 4 niveles de seguridad (SL1, SL2, SL3 y SL4)
  - A través de la superación de un conjunto de pruebas funcionales realizadas en un laboratorio acreditado.
  - Con la aportación de evidencias por parte del fabricante que demuestren que el producto cumple con la IEC 62443-4-1 previamente certificado.
- Un **entidad Certificadora** evalúa el informe del laboratorio y certifica que el fabricante cumple con los requisitos de ciberseguridad acorde a la norma.

# CRA

Cumplimiento de la CRA aplicando la norma IEC 62443-4-X

| GAP Análisis - IEC 62443-4-1 Gestión de Vulnerabilidades | GAP Análisis - IEC 62443-4-2 SL1 | Trabajo Fabricante | Certificación IEC 62443-4-1 | Certificación IEC 62443-4-2 |
|---|---|---|---|---|
| Auditoría IEC 62443-4-1<br>Entregable: Informe de conclusiones | Revisión documental completa IEC 62443-4-2<br>1 prueba de cada una de las familias de la IEC 62443-4-2 SL1<br>Entregable: Informe de resultados | Resolución de incidencias tras análisis GAP IEC 62443-4-1<br>Resolución de incidencias tras análisis GAP IEC 62443-4-2 | Concesión del certificado de ciclo de vida para el desarrollo de productos seguros (acreditado por ENAC ISO 17065) | Laboratorio de ensayos<br>•Ensayos de laboratorio acreditado por ENAC bajo ISO 17025<br>•Entregable: Informe de resultados<br>Entidad certificadora:<br>•Entregable: Certificado IEC 62443-4-2 (acreditado por ENAC ISO 17065) |

El Grupo TECNALIA ofrece a los fabricantes una ventanilla única para obtener las certificaciones necesarias para cumplir con CRA

**Laboratorio de ensayos** acreditado por ENAC según norma UNE-EN ISO/IEC 17025:2017 para la realización de ensayos de **ciberseguridad basados en la norma IEC 62443-4-2**

Nº 4 / LE2793

ALCANCE DE ACREDITACIÓN

**Organismo de certificación** acreditado por ENAC según norma UNE-EN ISO/IEC 17065: 2012 para la **certificación del Ciclo de Vida (SPDL)** de acuerdo con **IEC 62443-4-1** y para la **certificación de Componentes (CSA)** de acuerdo con **IEC 62443-4-2**

CERTIFICACIÓN ISO 17065 Nº125 / C-PR481

ALCANCE DE ACREDITACIÓN

# CRA


[CYBER RESILIENCE ACT (CRA): Reglamento Europeo (UE) 2024/2847 de Ciberseguridad | Tecnalia]

Jornada

## CYBER RESILIENCE ACT ( CRA ):

### Reglamento Europeo (UE) 2024/2847 de Ciberseguridad

Buenos días {{Recipient.FirstName}},

TECNALIA y CERTINALIA organizan un encuentro clave para entender el impacto del **Reglamento (UE) 2024/2847** en productos con elementos digitales.

La entrada en vigor del **CRA en 2027** supondrá un cambio estructural para todos los productos con elementos digitales comercializados en la Unión Europea. Fabricantes, desarrolladores, integradores y operadores deberán garantizar seguridad por diseño, gestión continua de vulnerabilidades y conformidad técnica durante todo el ciclo de vida del producto.

La jornada te ofrecerá una **visión técnica, práctica y actualizada**, incluyendo:

- Qué exige realmente el Reglamento (UE) 2024/2847
- Cómo afectará a tus productos, procesos y responsabilidades
- El papel de **CERTINALIA** y **TECNALIA** en certificación y ensayos (incluida la familia **IEC 62443**)
- Casos reales de aplicación en la industria
- Networking con expertos, reguladores y empresas líderes del sector

**26**
**Mayo**
**09:00 h - 14:00 h**

**Más información e inscripciones**

### Una oportunidad única

El **programa detallado** estará disponible próximamente, pero te adelantamos que será un encuentro imprescindible para quienes deben garantizar la seguridad, la conformidad y la competitividad de sus productos en el nuevo marco europeo.

**** El aforo es limitado ****

asociación de fabricantes
de equipos de climatización

# Gracias

Marta Castro
marta.castro@tecnalia.com
TECNALIA

AFEC
sociación de fabricantes
equipos de climatización

Webinar técnico

# Ley de Ciber Resiliencia

*Nuevas obligaciones de ciberseguridad para productos conectados en climatización*

14 de mayo de 2026

ontrol inteligente
limatización eficiente