SE

EMBEDDED SYSTEMS ENGINEERING

SCHMITT CONSULTING S.A.R.L. · SC-SARL.COM

Verificação rápida CRA para fabricantes de dispositivos

A nova lei da UE sobre a cibersegurança dos produtos conectados — o que tem de estar pronto até setembro de 2026, em linguagem clara.

Primeiro prazo vinculativo: 11 de setembro de 2026

Não em 2027. Quem não se preparar agora ficará sem tempo.

1 Do que se trata

O **Cyber Resilience Act** — em resumo **CRA** — está em vigor desde dezembro de 2024. Define quão seguros os produtos conectados devem ser contra ataques vindos da internet. Abrange tudo o que contém software ou se liga a uma rede: do termostato inteligente aos autómatos industriais e à aplicação.

Muitos fabricantes acreditam ter tempo até ao final de 2027. Isso só é verdade para parte das obrigações. O **primeiro prazo vinculativo ocorre já em setembro de 2026** — e abrange também produtos há muito no mercado e ainda mantidos.

11 de setembro de 2026

Obrigação de notificação. Se uma vulnerabilidade for comprovadamente explorada por atacantes, deve ser comunicada às autoridades **no prazo de 24 horas**.

11 de dezembro de 2027

Todas as restantes obrigações. Produto seguro desde a conceção, atualizações de segurança ao longo de toda a vida útil, lista de materiais de software completa, avaliação formal e marcação CE.

As coimas possíveis chegam a **15 milhões de euros ou 2,5 % do volume de negócios anual mundial** — consoante o valor mais elevado. E: a lei aplica-se expressamente também a pequenos fabricantes e fornecedores individuais, não apenas às grandes empresas.

2 Os termos mais importantes — em breve

Firmware

O software de controlo integrado de forma permanente num dispositivo e que o faz funcionar — por exemplo, o código de programa numa máquina, num sensor ou num controlador.

Vulnerabilidade (falha de segurança)

Um erro ou uma fraqueza no software através do qual um atacante pode penetrar no dispositivo ou manipulá-lo.

Lista de materiais de software (SBOM)

Uma lista completa de todos os componentes de software de um produto — comparável à lista de peças de um componente, mas para o código de programa. Sem ela não é possível saber se o produto é afetado por uma falha conhecida.

ENISA / CSIRT

A ENISA é a agência de cibersegurança da UE, o organismo central para a segurança informática na Europa. Os CSIRT são os «bombeiros informáticos» nacionais que coordenam em caso de incidentes. É para eles que vai a notificação de 24 horas.

Segurança funcional

A proteção de um dispositivo contra *avarias e falhas* técnicas — prática estabelecida, por exemplo, no setor automóvel. O CRA acrescenta-lhe a proteção contra *ataques intencionais*.

Marcação CE

A conhecida marcação CE nos produtos. Confirma que um produto cumpre os requisitos da UE e pode ser vendido no mercado europeu.

3 Está preparado para o CRA? A lista de verificação

Percorra os pontos seguintes. Cada caixa que **não** consiga assinalar de consciência tranquila é uma tarefa em aberto até setembro de 2026.

VISÃO GERAL E ORGANIZAÇÃO

- ☐ Sabemos quais dos nossos produtos estão abrangidos pela lei.
- ☐ Sabemos quais produtos mais antigos ainda mantemos (e que estão, por isso, também abrangidos).
- ☐ Existe uma pessoa responsável pelo tema CRA na empresa.

LISTA DE MATERIAIS DE SOFTWARE

- ☐ Para cada produto existe uma lista completa de todos os componentes de software integrados.
- ☐ Nela reconhecemos também os componentes obsoletos que o fornecedor já não mantém.
- ☐ Esta lista é mantida continuamente atualizada, não criada uma única vez.

PROCESSO DE NOTIFICAÇÃO (OBRIGATÓRIO A PARTIR DE 09/2026)

- ☐ Está definido quem deteta uma vulnerabilidade explorada.
- ☐ Está definido quem a avalia e quem a notifica.
- ☐ Conseguimos cumprir realmente o prazo de 24 horas a nível organizacional — incluindo ao fim de semana.

PROTEÇÃO TÉCNICA DO DISPOSITIVO

- ☐ O software no dispositivo está armazenado cifrado e não pode ser simplesmente lido.
- ☐ As atualizações são à prova de adulteração — ninguém pode injetar software introduzido de forma fraudulenta.
- ☐ O dispositivo pode receber atualizações de segurança durante toda a sua vida útil.
- ☐ No arranque, o dispositivo verifica que só é executado software autêntico e inalterado.

PROVAS E DOCUMENTAÇÃO

- ☐ Conseguimos demonstrar que o desenvolvimento seguiu normas de programação reconhecidas.
- ☐ Fiabilidade e resistência a ataques são pensadas num conceito comum, não em separado.
- ☐ Os documentos necessários para a posterior avaliação de conformidade são mantidos desde o início.

4 Como prosseguir

Os próximos meses decidirão se em setembro de 2026 haverá um processo ordenado ou se será preciso improvisar à pressa. Quem começa cedo distribui o trabalho — e evita correções dispendiosas mesmo antes do prazo. A maior alavanca não está, em regra, apenas na técnica, mas na boa articulação entre lista de materiais, processo de notificação e proteção do dispositivo.

→ Aprofundar e apoio

Não quer apenas ter uma visão geral dos requisitos, mas implementá-los? Três caminhos:

Livros técnicos e software

Conhecimento prático de mais de 35 anos de desenvolvimento embarcado — a base técnica por trás dos requisitos do CRA. Disponível em **sc-sarl.com/pt/produkte.html**

De oferta: «Coletânea de fórmulas para informáticos e engenheiros»

Coletânea de fórmulas HTML interativa, 56 capítulos, bilingue DE/EN, utilizável offline — grátis na área de downloads.

Apoio personalizado

Da lista de materiais de software ao endurecimento do firmware. Consulta em **sc-sarl.com/pt/kontakt.html**

Para os produtos e downloads →

Este guia dá uma visão prática e não substitui aconselhamento jurídico. O texto de referência é o Regulamento (UE) 2024/2847. Estado dos prazos: obrigação de notificação a partir de 11/09/2026, plena aplicabilidade a partir de 11/12/2027.