

REGRA DA UE · SEGURANÇA DE PRODUTOS

Cyber Resilience Act: segurança para produtos conectados

Quem vende na UE hardware ou software com elementos digitais é fabricante segundo o Cyber Resilience Act, mesmo sem estabelecimento na Europa. As obrigações de notificação de vulnerabilidades exploradas já valem desde 11/09/2026.

BASE LEGAL	NOTIFICAÇÕES DESDE	TODAS AS OBRIGAÇÕES A PARTIR DE	AFETA
Regulamento (UE) 2024/2847	11/09/2026	11/12/2027	Fabricantes de hardware e software conectados

Em resumo

O Cyber Resilience Act, ou CRA (na versão portuguesa oficial, Regulamento de Ciber-Resiliência), é um regulamento da UE sobre requisitos de cibersegurança para “produtos com elementos digitais”. Isso abrange hardware e software que se conectam, direta ou indiretamente, a um dispositivo ou a uma rede: roteadores, câmeras, controladores, sensores industriais, dispositivos de casa inteligente e também software comercial, como aplicativos, sistemas operacionais ou firmware. Ficam de fora áreas com regras próprias, como dispositivos médicos, veículos e aviação.

O CRA vale durante todo o ciclo de vida. Na entrega, o produto precisa cumprir os requisitos essenciais do Anexo I: nenhuma vulnerabilidade explorável conhecida, configurações padrão seguras, proteção contra acesso não autorizado e possibilidade de atualizações de segurança. Depois disso, o fabricante precisa tratar vulnerabilidades e fornecer atualizações durante um período de suporte que, em regra, é de pelo menos cinco anos (art. 13). No fim do processo está a marcação CE, que passa a cobrir também a cibersegurança.

Para a maioria dos produtos basta uma autoavaliação do fabricante. Para certos produtos importantes e críticos, como firewalls, equipamentos de rede ou cartões inteligentes, é preciso, conforme a classe, uma norma harmonizada ou um organismo notificado.

Quem é afetado na América do Sul

Um fabricante de fora da UE é fabricante nos termos do CRA assim que o seu produto é disponibilizado no mercado da UE. Uma empresa de Manaus que fornece eletrônica de controle para um fabricante de máquinas na Itália assume, portanto, as obrigações de fabricante, desde que coloque o produto no mercado com o próprio nome. Ela pode nomear um mandatário na UE (art. 18),

que assume algumas tarefas.

Também são afetadas as software houses com produtos comerciais: um aplicativo de contabilidade de Santiago, um software de segurança de Buenos Aires, um firmware para sensores agrícolas de Rosário. No desenvolvimento sob encomenda, em que o cliente da UE vende o produto com o nome dele, quem vira fabricante é o cliente. Ele vai então repassar os requisitos a você por contrato.

Há ainda o caminho pelo importador. Pelo artigo 19, um importador só pode colocar no mercado produtos que cumpram os requisitos. Por isso ele verifica se existem avaliação de conformidade, documentação técnica, marcação CE e os dados de contato do fabricante. Se faltar algo, ele não compra.

Os distribuidores têm, pelo artigo 20, deveres de verificação parecidos, um pouco mais leves. Se um importador ou distribuidor souber de uma vulnerabilidade, precisa informar o fabricante. Em caso de risco grave, a fiscalização do mercado pode exigir que os produtos sejam recolhidos ou retirados do mercado. Para um exportador, isso quer dizer que um problema em um produto pode travar um lote inteiro em um armazém na UE.

Software de código aberto gratuito, fora de uma atividade comercial, não está sujeito ao CRA. Mas, assim que você o incorpora a um produto que vende, passa a responder pela segurança desses componentes.

Prazos

A PARTIR DE	O QUE VALE
11/06/2026	Regras sobre os organismos de avaliação da conformidade
11/09/2026	Obrigações de notificação do art. 14 para vulnerabilidades ativamente exploradas e incidentes graves, inclusive para produtos que já estão no mercado
11/12/2027	Todas as demais obrigações, entre elas os requisitos do Anexo I, a avaliação de conformidade e a marcação CE

As obrigações de notificação já estão valendo. Se um fabricante souber de uma vulnerabilidade ativamente explorada no seu produto, precisa enviar um alerta precoce em até 24 horas, uma notificação em até 72 horas e um relatório final no máximo 14 dias depois de disponibilizar uma correção. Para incidentes graves, o prazo do relatório final é de um mês. As notificações são feitas pela plataforma única de notificação da ENISA (art. 16), em operação desde 11/09/2026.

A obrigação de notificar vale também para produtos que você vendeu há anos, enquanto estiverem no mercado da UE. Quem ainda não tem um processo para receber avisos de vulnerabilidades deve criá-lo agora.

O que os clientes da UE pedem na prática

- Uma declaração UE de conformidade, a partir de 11/12/2027 para todos os produtos com elementos digitais.
- A documentação técnica, com avaliação de riscos e descrição das medidas de segurança.
- Uma lista de materiais de software (SBOM) com todos os componentes e bibliotecas.
- Uma política de divulgação coordenada de vulnerabilidades (CVD), com um endereço de contato para avisos.
- A indicação do período de suporte e uma comprovação de como as atualizações são entregues.
- Para produtos importantes ou críticos, o resultado da avaliação de conformidade exigida e, se for o caso, um certificado de um organismo notificado.
- Para produtos industriais, muitas vezes comprovações segundo a série de normas IEC 62443.

Muitos importadores e distribuidores já perguntam por isso hoje, embora a maior parte das obrigações só valha a partir do fim de 2027. Eles não querem ter em estoque mercadoria que depois não poderão mais vender.

Grandes compradores também colocam os requisitos nas suas condições de compra: garantia de conformidade com o CRA a partir de uma data, aviso de vulnerabilidades ao cliente, entrega de atualizações por um prazo mínimo combinado e responsabilidade em caso de recall. Leia essas cláusulas com atenção antes de assinar contratos de fornecimento que vão além de 2027.

Primeiros passos

1. Faça uma lista de todos os produtos que você fornece à UE e que contêm software ou podem ser conectados.
2. Verifique, para cada produto, se ele se enquadra nas classes de produtos importantes ou críticos (Anexos III e IV).
3. Crie já um processo de notificação: quem recebe avisos de vulnerabilidades, quem avalia, quem notifica em até 24 horas?
4. Gere uma SBOM para cada versão do produto. Muitas ferramentas de build fazem isso automaticamente.

5. Verifique quais dos seus sistemas são acessíveis pela internet, como servidores de atualização e acessos de manutenção remota. Ferramentas como o [veyrisk](#) mostram isso de fora.
6. Planeje a avaliação de conformidade e a documentação para que estejam prontas antes de 11/12/2027.

O [Diagnóstico UE](#) gratuito oferece uma primeira avaliação.

Relação com certificações

O CRA não exige certificação de sistema de gestão. Mas um certificado [ISO/IEC 27001](#) mostra que seu desenvolvimento, seu ambiente de build e sua resposta a incidentes estão organizados, e ajuda com os requisitos de processo. Para produtos industriais, a IEC 62443 é comum. Fornecedores da indústria automotiva costumam precisar do [TISAX](#), mesmo que os veículos em si não estejam sujeitos ao CRA. Uma gestão da qualidade segundo a [ISO 9001](#) facilita a documentação. Se você fornece produtos a operadores de serviços críticos, entra a [NIS2](#), e funções de IA em produtos ficam sujeitas também ao [Regulamento da IA](#).

Para fabricantes do [Brasil](#), onde se produz muita eletrônica e tecnologia de automação, o CRA é uma das novas regras da UE mais importantes. Os requisitos são os mesmos, quer a mercadoria vá por um importador, quer vá direto para um cliente industrial.

FAQ

O Cyber Resilience Act vale para software?

Sim, para software comercial disponibilizado na UE, inclusive aplicativos e firmware. Ficam de fora, entre outros, serviços puramente em nuvem sem vínculo com um produto e software de código aberto gratuito fora de uma atividade comercial.

O que preciso fazer desde 11/09/2026?

Notificar pela plataforma da ENISA vulnerabilidades ativamente exploradas e incidentes graves nos seus produtos: alerta precoce em até 24 horas, notificação em até 72 horas.

Preciso de um estabelecimento na UE?

Não. Você pode nomear um mandatário na UE (art. 18). Seu importador na UE precisa conhecer seus dados de contato e verificar a conformidade.

O que é uma SBOM?

Uma lista de materiais de software que relaciona todos os componentes e bibliotecas de um produto. O CRA a exige como parte da documentação técnica.

Qual ferramenta ajuda a preparar a documentação do CRA?

O Sightadel não traz o CRA como marco próprio. Como ferramenta GRC, o [Sightadel](#) ajuda a distribuir tarefas, controlar documentos como a política de divulgação de vulnerabilidades e guardar comprovações. Para ver quais servidores de atualização e acessos remotos estão expostos na internet, o [veyrisk](#) verifica sua superfície de ataque de fora.

Fontes · Atualizado em: 11 de outubro de 2026

Regulamento (UE) 2024/2847 (Regulamento de Ciber-Resiliência), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

Comissão Europeia: Cyber Resilience Act: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

Comissão Europeia: obrigações de notificação do CRA: <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

Informações gerais, sem caráter de consultoria jurídica. Valem os textos oficiais.

COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



O Sightadel conduz sua equipe por a ISO 27001: modelos, tarefas, evidências e preparação para auditoria em um só lugar. Desenvolvido e hospedado na Alemanha, com pacote de consultoria opcional.

[Conhecer o Sightadel →](#)



O veyrisk mostra o que um atacante enxerga da sua empresa por fora: serviços abertos, certificados, vulnerabilidades conhecidas. Você pode apresentar o relatório a clientes europeus e auditores.

[Conhecer o veyrisk →](#)

Sightadel, veyrisk e Valar são produtos da neonotu GmbH, empresa que opera o MercoEU.

O que disso se aplica à sua empresa?

O Diagnóstico UE gratuito mostra isso por setor e país em 10 minutos.

<https://www.mercoeu.com/pt/diagnostico-ue>