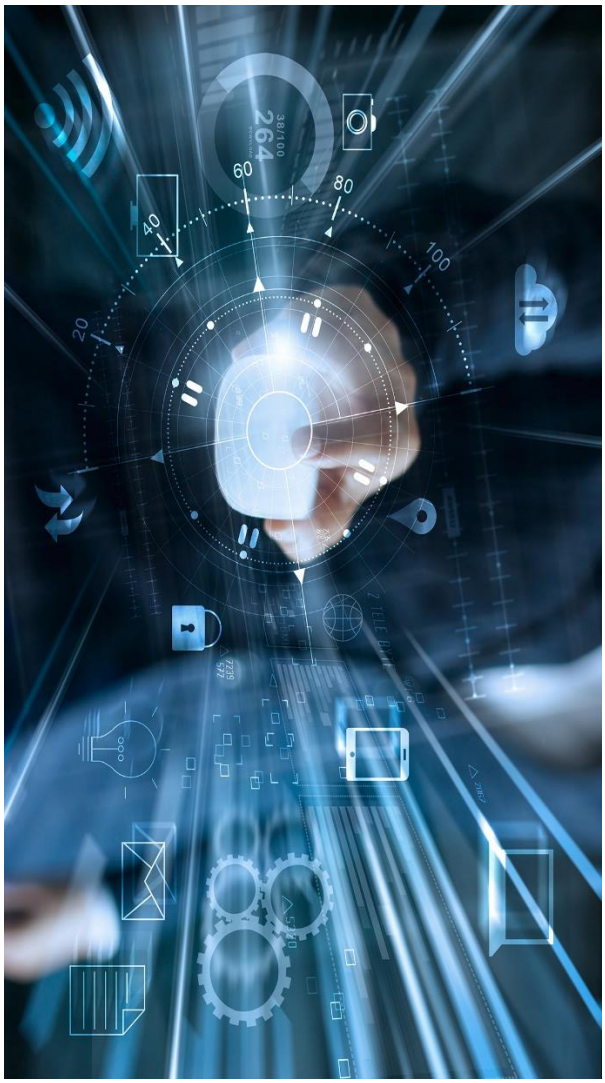
CUATRECASAS

Regulamento da Ciber-Resiliência

Publicado o Regulamento da Ciber-Resiliência que estabelece normas unificadas de cibersegurança para os produtos digitais em todo o mercado da UE

Legal Flash

20 de novembro de 2024



Aspetos chave

Foi hoje publicado no Jornal Oficial da UE o Regulamento da Ciber-Resiliência (Regulamento (EU) 2024/2847 do Parlamento Europeu e do Conselho), concluindo-se assim o processo legislativo de aprovação deste regulamento, em curso desde meados de 2022, na sequência da proposta da Comissão Europeia. Destacamos alguns dos seus aspetos chave:

- Os fabricantes devem adotar **medidas de segurança** desde a fase de conceção e garantir a marcação CE;
- Os importadores e distribuidores são responsáveis pela verificação das **normas de cibersegurança dos produtos**;
- Os fabricantes devem comunicar atempadamente as **vulnerabilidades e os incidentes**;
- São impostas sanções significativas em caso de incumprimento, com exceções para as pequenas empresas.

Regulamento da Ciber-Resiliência

O Regulamento (EU) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (EU) n.º 168/2013 e (EU) 2019/1020 e a Diretiva (EU) 2020/1828 (doravante, "**CRA**") estabelece requisitos abrangentes de cibersegurança para todos os produtos de *hardware* e *software* com elementos digitais comercializados na União Europeia ("**UE**"). Entre outros produtos com elementos digitais abrangidos pelo âmbito de aplicação do CRA, o regulamento aplica-se a sistemas de gestão de redes, sistemas operativos ou de palavras-passe, assistentes virtuais domésticos inteligentes de uso geral, *smartcards* ou dispositivos semelhantes, juntamente com dispositivos de *hardware* com caixas de segurança.

Antes do CRA ser aprovado, várias iniciativas nacionais e a nível da UE abordavam os desafios da cibersegurança de forma fragmentada, criando um quadro regulamentar incoerente em todo o mercado interno. Embora a legislação da UE em vigor (por exemplo, a Diretiva (UE) 2022/2555 [Diretiva NIS2] e o Regulamento (UE) 2019/881 [Regulamento Cibersegurança]) aborde vários aspetos da cibersegurança de diferentes perspetivas, atualmente nenhuma impõe requisitos de segurança obrigatórios especificamente para produtos com elementos digitais.

O CRA é particularmente importante devido à natureza transfronteiriça dos riscos de cibersegurança. Os produtos desenvolvidos num país são frequentemente utilizados por empresas e consumidores em toda a UE, o que sublinha a necessidade de um quadro regulamentar unificado.

De acordo com o acima exposto, os operadores económicos (ou seja, fabricantes, importadores, distribuidores e representantes autorizados) têm papéis específicos na garantia de que os produtos com elementos digitais são seguros e cumprem com o CRA antes de serem vendidos na UE. Os requisitos são diferentes entre fabricantes e importadores ou distribuidores, e consoante os produtos com elementos digitais sejam definidos como produtos importantes (Anexo III do CRA) ou produtos críticos (Anexo IV do CRA).

Fabricantes, importadores e distribuidores

Os fabricantes[1] são obrigados a introduzir medidas de cibersegurança desde o início, garantindo que os produtos são desenhados, desenvolvidos e produzidos de forma segura. Estas medidas incluem:

[1] Nos termos previstos no n.º 13, do artigo 3.º do CRA, como a "pessoa singular ou coletiva que desenvolva ou fabrique produtos com elementos digitais, ou que os mande conceber, desenvolver ou fabricar e os comercialize em seu nome ou sob a sua marca, a título oneroso, gratuito ou com fins lucrativos".

- promover avaliações rigorosas de cada produto para identificar e atenuar eventuais riscos de cibersegurança durante a conceção e o desenvolvimento;
- manter registos pormenorizados que apresentam a forma como os riscos de cibersegurança foram tratados, disponibilizando essas informações às entidades reguladoras, se necessário;
- manter as informações e instruções ao utilizador previstas no Anexo II à disposição dos utilizadores e das autoridades de fiscalização do mercado durante, pelo menos, 10 anos após a colocação no mercado do produto com elementos digitais ou durante o período de suporte, consoante o que for mais longo[2];
- garantir que os produtos ostentem a marcação CE, indicando que cumprem as normas necessárias e podem ser vendidos com segurança em toda a UE; e
- estabelecer processos para lidar com potenciais problemas de cibersegurança que surjam após o lançamento do produto, tais como, fornecer atualizações de segurança e aconselhar os utilizadores sobre a forma de gerir as vulnerabilidades.

O CRA introduz o papel do representante autorizado, que deve ser nomeado e autorizado pelo fabricante a desempenhar as funções especificadas no mandato escrito recebido do fabricante, o que permitirá ao representante autorizado (i) manter a declaração de conformidade da UE e a documentação técnica à disposição das autoridades de fiscalização do mercado durante, pelo menos, 10 anos após a colocação no mercado do produto com elementos digitais ou durante o período de suporte, consoante o que for mais longo; (ii) fornecer a essa autoridade toda a informação e documentação necessárias para demonstrar a conformidade do produto com elementos digitais, e (iii) cooperar com as autoridades de fiscalização do mercado, a pedido destas.

Quanto aos importadores[3] e distribuidores[4], a responsabilidade recai sobre a necessidade de verificar, avaliar e garantir que os produtos que estão a ser vendidos são seguros e cumprem as normas de cibersegurança. Por exemplo, os importadores devem verificar se os produtos cumprem todos os requisitos de cibersegurança antes de serem comercializados, incluindo a verificação da marcação CE e da documentação adequada. Os distribuidores devem estar atentos a quaisquer problemas de segurança emergentes e garantir que os produtos que manuseiam se mantêm em conformidade ao longo do tempo.

O CRA identifica um conjunto de medidas de cibersegurança que devem ser aplicadas pelos fabricantes e verificadas pelos importadores e distribuidores, incluindo as seguintes:

[2] Se essas informações e instruções forem fornecidas online, os fabricantes devem garantir que sejam acessíveis, de fácil utilização e estejam disponíveis online durante, pelo menos, dez anos após a colocação no mercado do produto com elementos digitais ou durante o período de suporte, consoante o que for mais longo.
[3] Nos termos do n.º 16 do artigo 3.º do CRA como "a pessoa singular ou coletiva estabelecida na União que coloque no mercado um produto com elementos digitais que ostente o nome ou a marca de uma pessoa singular ou coletiva estabelecida fora da UE".
[4] Nos termos do n.º 17 do artigo 3.º do CRA como a "pessoa singular ou coletiva inserida na cadeia de abastecimento, distinta do fabricante ou o importador, que disponibiliza um produto com elementos digitais no mercado da União sem alterar as suas propriedades".

- **Segurança desde a conceção:** Desde o início da conceção, os produtos devem ser desenvolvidos tendo em conta a segurança. Inclui a incorporação de medidas de proteção para impedir o acesso não autorizado e garantir a integridade e a confidencialidade de quaisquer dados processados.

- **Proteção de produtos críticos:** Os produtos que desempenham funções essenciais de cibersegurança ou que representam um risco elevado se forem comprometidos - como *firewalls* ou sistemas de prevenção de intrusões - enfrentam requisitos de segurança mais rigorosos. Estes produtos devem ser objeto de avaliações mais exaustivas para garantir a sua robustez.

- **Gestão de vulnerabilidades:** Todos os produtos devem ter um plano para gerir as vulnerabilidades durante todo o seu ciclo de vida. Espera-se que os fabricantes forneçam atualizações de segurança, correções e instruções para mitigar os riscos à medida que estes surgem. Isto é especialmente importante para os produtos críticos (enumerados no Anexo IV do CRA), em que as atualizações atempadas são essenciais para manter a segurança.

- **Segurança da cadeia de abastecimento:** Os operadores económicos devem gerir cuidadosamente os riscos de cibersegurança associados a componentes de terceiros utilizados nos seus produtos, incluindo *software* de código aberto. O nível de controlo depende da natureza do componente e dos riscos que lhe estão associados. Os fabricantes devem garantir que todos os componentes de terceiros, incluindo o *software*, são seguros, atualizados regularmente e não apresentam vulnerabilidades.

- **Atualizações e suporte de segurança:** As modificações a um produto, seja através de atualizações de software ou alterações de *hardware*, podem afetar o seu estado de cibersegurança. Por exemplo, uma atualização de caraterísticas que introduza novas funcionalidades pode aumentar a potencial exposição do produto a ciberameaças, exigindo uma nova avaliação do risco. No entanto, nem todas as atualizações são consideradas substanciais. As pequenas correções, tais como as correções de erros ou as melhorias na interface, normalmente não alteram o risco global de segurança de um produto. No entanto, as alterações mais significativas, especialmente as que afetam as funcionalidades principais, exigem um exame mais minucioso para garantir que não introduzem novas vulnerabilidades. Nas situações em que a modificação de um produto altera significativamente o objetivo pretendido ou o perfil de risco, pode ser necessário submetê-lo a uma nova avaliação de conformidade. Deste modo, garante que o produto continua a cumprir as normas de segurança exigidas após grandes atualizações ou alterações.

No que diz respeito ao ***software* de código aberto**, os operadores económicos devem ter especial atenção quando integram este tipo de *software* em produtos comerciais. Embora os projetos de código aberto não destinados a utilização comercial possam estar isentos de certas obrigações, qualquer produto que incorpore componentes de código aberto num contexto comercial deve garantir que esses componentes cumprem as normas de cibersegurança. Para os administradores de *software* de fonte aberta -

organizações que prestam apoio a longo prazo a esses projetos - aplica-se uma abordagem mais flexível. No entanto, os produtos comerciais que incorporam estes componentes devem continuar a cumprir todos os requisitos de segurança.

Para além do acima exposto, vale a pena sublinhar que o CRA introduz alguns casos em que as obrigações dos fabricantes se aplicam aos importadores e aos distribuidores. Nomeadamente, quando o importador ou o distribuidor coloca um produto com elementos digitais no mercado em seu nome ou marca registada ou efetua uma modificação substancial de um produto com elementos digitais já colocado no mercado. Nesses casos, nos termos do CRA, o importador ou o distribuidor ficarão sujeitos às obrigações dos fabricantes estabelecidas no CRA.

Resposta a incidentes e notificações

Os requisitos de notificação no âmbito do CRA visam garantir a transparência, a resposta rápida e os esforços de colaboração entre os fabricantes, a Agência da União Europeia para a Cibersegurança ("ENISA") e a rede de Equipas de Resposta a Incidentes de Segurança Informática ("CSIRT"). O CRA exige que os fabricantes de produtos com elementos digitais notifiquem as entidades pertinentes sobre **vulnerabilidades ativamente exploradas** e **incidentes de cibersegurança classificados como graves**. Os incidentes serão classificados como graves se afetarem negativamente a capacidade do produto para proteger dados ou funções sensíveis ou se conduzirem à introdução ou execução de código malicioso num sistema, causando riscos de cibersegurança para o produto com elementos digitais.

O processo e os prazos para notificar tanto as vulnerabilidades exploradas como os incidentes graves seguem o atual modus operandi da maior parte da legislação em matéria de cibersegurança, ou seja, através das seguintes notificações principais:

- **No prazo de 24 horas após o conhecimento** da vulnerabilidade ou do incidente, deve ser apresentada uma **notificação de alerta precoce** especificando informações relevantes como, por exemplo, se o incidente resultou de atos ilícitos ou maliciosos.
- N**o prazo de 72 horas**, deve seguir uma **notificação** provisória e mais detalhada do incidente, fornecendo um contexto mais amplo, incluindo a natureza da vulnerabilidade ou do incidente, as medidas corretivas já tomadas e as potenciais medidas de atenuação que os utilizadores podem adotar.
- No prazo de **um mês**, deve ser apresentado um **relatório final** que descreva em pormenor a gravidade da vulnerabilidade, os potenciais agentes maliciosos envolvidos e as medidas de atenuação abrangentes.

Em circunstâncias excecionais, os fabricantes podem solicitar uma prorrogação do prazo para a difusão da notificação, principalmente se uma vulnerabilidade for objeto de uma divulgação coordenada de

vulnerabilidades em curso. No entanto, esta prorrogação é estritamente limitada no tempo e depende de motivos relacionados com a cibersegurança.

Os fabricantes devem notificar simultaneamente a **CSIRT** designada como coordenadora e a **ENISA**. A notificação deve ser apresentada através de uma **plataforma única de comunicação** gerida pela ENISA, facilitando a comunicação simplificada com todas as CSIRT da UE.

Nos casos de vulnerabilidades ativamente exploradas ou de incidentes graves, os fabricantes são obrigados a informar os utilizadores afetados, fornecendo pormenores sobre os riscos e as medidas de atenuação. Se o fabricante não informar os utilizadores, as CSIRT notificadas podem assumir a responsabilidade pela comunicação, garantindo a divulgação de informações de segurança cruciais.

Além disso, na sequência de outra legislação sobre cibersegurança e de quadros de referência, a partilha voluntária de ameaças, vulnerabilidades e incidentes de cibersegurança deve ser mantida no CRA. Por conseguinte, os fabricantes e outras partes interessadas podem notificar voluntariamente vulnerabilidades ou incidentes à ENISA ou à rede de CSIRT. Esta abordagem voluntária incentiva um ambiente de colaboração em matéria de cibersegurança, reforçando a transparência e a resiliência em todo o sector.

Notificação dos organismos de avaliação da conformidade

Os Estados-Membros estão especificamente mandatados para designar e informar a Comissão Europeia e os demais Estados-Membros dos organismos de avaliação da conformidade que reconhecem como competentes para efetuar avaliações de cumprimento do CRA.

Estes organismos são responsáveis por avaliar se os produtos com elementos digitais cumprem os critérios de cibersegurança exigidos pelo CRA. Este processo de notificação tem como objetivo criar uma abordagem normalizada em toda a UE, assegurando que todos os organismos designados cumprem os mesmos padrões elevados de avaliação.

Para poderem ser notificados, os organismos de avaliação da conformidade devem satisfazer determinados critérios rigorosos, que incluem os seguintes:

- **Independência e imparcialidade:** Os organismos devem funcionar de forma independente dos fabricantes, evitando assim quaisquer conflitos de interesses e assegurando avaliações imparciais.

- **Competência técnica:** Devem possuir as competências e os recursos necessários para avaliar com exatidão os produtos em função dos requisitos estabelecidos no CRA.

- **Gestão da qualidade:** Espera-se que os organismos designados apliquem sistemas sólidos de gestão da qualidade que garantam a coerência e a fiabilidade das suas avaliações.

Cumprimento e fiscalização do mercado

Do mesmo modo, os Estados-Membros devem nomear autoridades de fiscalização do mercado responsáveis pelo controlo do cumprimento do CRA - atualmente, os organismos governamentais portugueses ainda não designaram quaisquer autoridades. Estas autoridades são fundamentais para garantir que os produtos colocados no mercado cumprem de forma consistente as normas de cibersegurança exigidas.

As suas responsabilidades incluem a **monitorização ativa do mercado** para garantir o cumprimento dos regulamentos de cibersegurança, o que envolve inspeções regulares, testes e avaliações dos produtos disponíveis para venda.

As respetivas autoridades têm também **poderes para investigar produtos** suspeitos de incumprimento, efetuar auditorias, analisar documentação técnica e avaliar a marcação CE e a declaração de conformidade da UE.

Se um incumprimento for identificado, as autoridades de fiscalização do mercado têm autoridade para tomar **medidas corretivas**. Para tal, os fabricantes podem ter de cessar a venda de produtos em incumprimento, retirá-los do mercado ou recolhê-los junto dos consumidores.

Para identificar e resolver sistematicamente os incumprimentos, as autoridades de fiscalização do mercado são encorajadas a realizar ações de controlo coordenadas, geralmente designadas por ***sweeps***. Estas envolvem predominantemente inspeções simultâneas de produtos ou categorias específicas em vários Estados-Membros, sendo os resultados agregados e disponibilizados ao público.

Confidencialidade e sanções

Note-se que o CRA coloca uma ênfase significativa na confidencialidade e na aplicação de sanções. Os principais objetivos destas disposições em matéria de confidencialidade consistem em salvaguardar as informações sensíveis, garantindo simultaneamente que o quadro regulamentar funcione eficazmente sem comprometer os direitos de propriedade intelectual ou a segurança nacional.

Em termos de aplicação, o CRA exige que os Estados-Membros estabeleçam sanções efetivas e proporcionadas para as infrações, nomeadamente:

- **Infrações dos requisitos essenciais de cibersegurança:** Até €15 milhões ou 2,5% do volume de negócios anual total a nível mundial do infrator, consoante o montante mais elevado.
- **Infrações das obrigações gerais:** Até €10 milhões ou 2% do volume de negócios anual total a nível mundial do infrator, consoante o montante mais elevado.

- **Fornecer informação enganosa:** Até €5 milhões ou 1% do volume de negócios anual total a nível mundial do infrator, consoante o montante mais elevado.

Naturalmente, ao determinar o montante da coima administrativa, devem ser cuidadosamente consideradas as circunstâncias relevantes, tais como a natureza, a gravidade e a duração da infração. Algumas disposições específicas também isentam certas entidades de sanções. Por exemplo, os fabricantes classificados como microempresas ou pequenas empresas podem ser isentos de sanções para certas questões de incumprimento relacionadas com os prazos. Esta mesma isenção também se aplica aos administradores de *software* de código aberto por quaisquer infrações ao CRA.

Próximos passos para as empresas

Para ajudar a implementar o CRA, a Comissão Europeia fornecerá orientações, especialmente destinadas às pequenas e médias empresas (PME). Este apoio ajudará os operadores económicos a compreender como aplicar eficazmente as medidas de cibersegurança necessárias. As empresas dispõem igualmente de um período de transição para adaptar os produtos já existentes no mercado aos novos requisitos de cibersegurança, permitindo-lhes continuar a funcionar sem perturbações imediatas enquanto efetuam os ajustamentos necessários.

Os próximos passos para os operadores económicos, em particular os fabricantes, serão a realização de uma análise das lacunas nas medidas de cibersegurança em vigor, não só a nível organizacional, mas também para o fabrico dos seus produtos com elementos digitais. Esta análise das lacunas deve centrar-se numa abordagem baseada no risco, incluindo o risco da cadeia de abastecimento, e nas capacidades dos fabricantes para detetar e responder às vulnerabilidades que possam surgir.

O Regulamento será aplicável a partir de 11 de dezembro de 2027, embora o artigo 14, referente às obrigações de informação dos fabricantes, seja aplicável a partir de 11 de setembro de 2026; e o capítulo IV, relativo à notificação dos organismos de avaliação da conformidade, será aplicável a partir de 11 de junho de 2026.

Para obter informação adicional sobre o conteúdo deste documento, por favor dirija-se ao seu contacto habitual na *Cuatrecasas.*