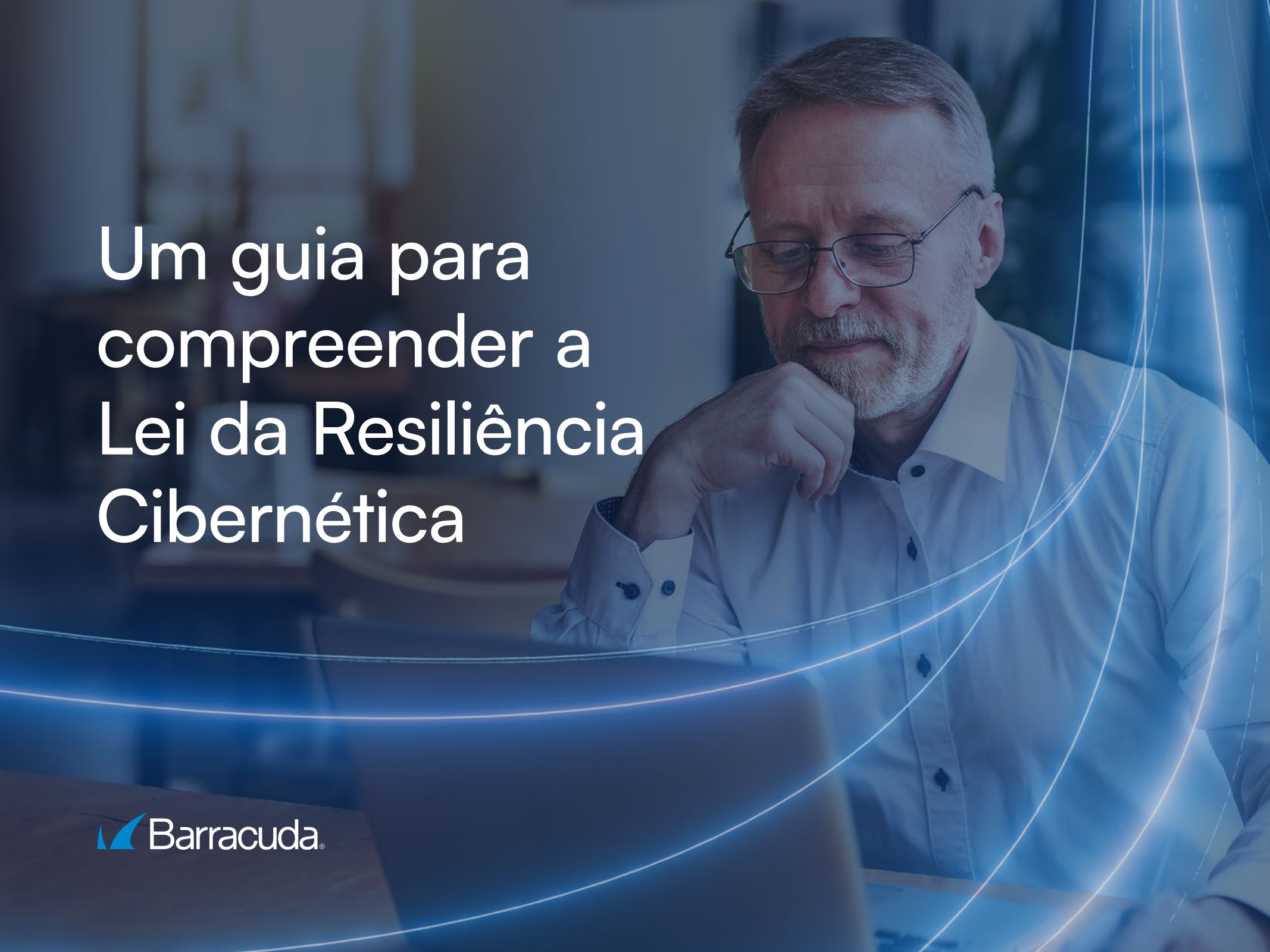

Um guia para compreender a Lei da Resiliência Cibernética

Barracuda

A compreensão da Lei da Ciberresiliência (CRA) da União Europeia (UE) é essencial para as organizações que fazem negócios na UE. Os fabricantes de produtos digitais oferecidos para venda na UE, bem como os importadores e distribuidores desses produtos, estão sujeitos à CRA. Este e-book apresenta alguns pontos importantes da CRA (Lei de Ciberresiliência) para os fabricantes, mas não substitui nem se destina a ser um aconselhamento jurídico para a sua empresa.

O Community Reinvestment Act (CRA, na sigla em inglês) entrou em vigor em dezembro de 2024, dando às organizações algum tempo para alcançar a conformidade. Aqui estão algumas datas importantes a saber:

- 11 de setembro de 2026 — Os fabricantes devem começar a comunicar incidentes graves de cibersegurança e vulnerabilidades que estão a ser exploradas ativamente.
- 11 de dezembro de 2027 — Todos os novos produtos e quaisquer produtos existentes "substancialmente modificados" colocados no mercado nesta data ou após esta data devem estar em conformidade com o CRA.

A lei pretende estabelecer um conjunto mais uniforme de requisitos de segurança para todos os produtos com elementos digitais vendidos na UE e fornecer aos consumidores e empresas que compram estes produtos mais informações sobre a sua segurança antes de os adquirirem. A lei espera retificar o que a UE descreve como o "nível inadequado" de cibersegurança encontrado em muitos produtos, incluindo a falta de atualizações de segurança.

A CRA complementa a Lei de Resiliência Operacional Digital (DORA) e a Diretiva de Segurança da Informação em Rede 2 (NIS2):

- O DORA está focado em melhorar a ciberresiliência da indústria financeira, e o NIS2 aplica-se a um conjunto mais amplo de entidades que fornecem serviços essenciais em setores-chave.
- Tanto a DORA como a NIS2 especificam requisitos de cibersegurança, incluindo medidas de segurança na cadeia de abastecimento, com o objetivo de aumentar a resiliência das empresas reguladas, devido ao impacto que as suas ofertas têm para terceiros.
- A CRA aplica-se ao nível do produto, fornecendo a estrutura obrigatória para produtos seguros com elementos digitais. Quando o cliente destes produtos é regulado pela DORA ou NIS2, a utilização de hardware e software compatíveis com a CRA pode auxiliar estas entidades a cumprir as suas obrigações.

O NIS2 e o DORA estão fora do âmbito deste e-book. Consulte Compreender o DORA: Um Guia para a Resiliência Operacional Digital. Atuar e Navegando NIS2: UM guia para o por vir europeu cibersegurança regulamentos para mais detalhes.

Porque é que a CRA é importante?

O CRA abrange todos os produtos que contenham "elementos digitais", o que significa que este regulamento abrange tanto o hardware como o software que está ligado a um dispositivo ou rede, além das soluções integradas de processamento remoto de dados desses produtos (ou seja, serviços cloud). A Comissão Europeia afirma: "O regulamento aplica-se a todos os produtos ligados direta ou indiretamente a outro dispositivo ou rede, com exceção de exclusões específicas, como certos produtos de software ou serviços de código aberto que já estão abrangidos por regras existentes, como é o caso dos dispositivos médicos, da aviação e dos automóveis."[1] Os produtos não conformes não poderão ser vendidos na UE. As organizações que forem apanhadas a fazê-lo serão sujeitas a coimas. Tal como o Regulamento Geral de Proteção de Dados (RGPD) alterou fundamentalmente a forma como as empresas tratam as informações pessoais, o CRA tem potencial para ter um efeito semelhante na forma como os fabricantes fabricam, vendem e apoiam os seus produtos com elementos digitais oferecidos no mercado da UE.

O CRA aborda um problema crescente com produtos de tecnologia moderna que recolhem, processam, partilham e armazenam dados do utilizador — muitas vezes sem segurança ou com segurança fraca — colocando esses dados em risco. À medida que estes produtos envelhecem, as soluções de segurança disponíveis podem tornar-se desatualizadas. Há pouca supervisão sobre como, quando ou se as atualizações de segurança são fornecidas aos utilizadores. O CRA procura aumentar a segurança dos produtos com elementos digitais e garantir que esses produtos permaneçam seguros durante todo o seu ciclo de vida. A lei também proporcionará maior transparência aos utilizadores, que terão uma melhor compreensão da segurança dos produtos com elementos digitais e como isso pode afetar os seus dados.

[1] Lei de Resiliência Cibernética | Moldando o Futuro Digital da Europa

Obrigações da CRA para os fabricantes

A CRA introduz requisitos obrigatórios de cibersegurança para os fabricantes que regem o planeamento, design, desenvolvimento, produção, entrega, documentação e manutenção de tais produtos. Estas obrigações devem ser cumpridas em cada etapa da cadeia de valor.

Ao abrigo da CRA, os produtos podem ser classificados como padrão (nível mais baixo), "Importantes" (com mais obrigações) — divididos em duas subcategorias: Importante Classe I e Importante Classe II — e "Críticos" (com o maior nível de risco e, portanto, obrigações).

Para os artigos normalizados, os fabricantes são obrigados a conceber, fabricar e testar bens e serviços quanto à conformidade com os "requisitos essenciais de segurança" especificados no Anexo I da CRA, documentar a avaliação e manter a documentação técnica disponível para as autoridades de fiscalização do mercado. A este nível, os fabricantes podem confiar numa avaliação interna de conformidade (autoavaliação).

De um modo geral, cerca de 90% dos produtos de hardware e software deverão enquadrar-se nesta categoria padrão, permitindo aos fabricantes realizar auto-testes e criar uma declaração de conformidade antes de afixar a marca CE que os produtos em conformidade irão receber.

Certos produtos com elementos digitais - como navegadores Web, firewalls e sistemas operativos - inserem-se na categoria "Importante", outros até na categoria "Crítica". Devem continuar a cumprir os requisitos técnicos do Anexo I, mas podem ser sujeitos a um processo de avaliação da conformidade mais rigoroso, incluindo a avaliação/certificação por terceiros, antes de serem vendidos na UE.

Além das obrigações no momento da venda, a CRA também exige que os fabricantes forneçam gestão de vulnerabilidades e atualizações de segurança, conforme descrito abaixo.

Obrigações de comunicação de segurança

A obrigatoriedade de comunicação de vulnerabilidades de segurança ativamente exploradas e incidentes graves, conforme previsto na Lei de Reinvestimento Comunitário (CRA), entra em vigor a 11 de setembro de 2026.

As obrigações de reporte são rigorosas. Os fabricantes deverão fornecer um aviso prévio às entidades reguladoras no prazo de 24 horas após tomarem conhecimento do problema. No prazo de 72 horas após a descoberta de uma vulnerabilidade explorada, os fabricantes deverão fornecer informações gerais sobre o produto afetado, uma descrição geral da vulnerabilidade explorada e quaisquer medidas de mitigação que o fabricante tenha tomado e que os utilizadores possam tomar, para além de indicar a gravidade do problema. No prazo de 14 dias após a implementação das medidas de mitigação, o fabricante terá obrigações de divulgação adicionais, como a apresentação de um relatório final.

As obrigações de comunicação incluem também informar os utilizadores afetados e aconselhá-los sobre formas de mitigar a exposição.

Os fabricantes devem familiarizar-se com estes requisitos de relatórios e desenvolver processos a cumprir até setembro Data de início em 2026.

Obrigações de suporte técnico

O apoio em cibersegurança, no sentido de fornecer atualizações de segurança, é também um tema importante na CRA e deve ser planeado de forma a abranger todo o ciclo de vida do produto. Os fabricantes devem especificar antecipadamente o período de suporte para os produtos com elementos digitais. Em geral, as empresas que colocam produtos com elementos digitais no mercado da UE devem apoiá-los por pelo menos cinco anos, a menos que a vida útil esperada do produto seja inferior a cinco anos. Nesse caso, o suporte deve durar a vida útil esperada do produto. Para produtos que geralmente têm uma vida útil superior a cinco anos (exemplos: motherboards, routers de rede, modems, switches e sistemas operativos), o período de suporte deve ser mais longo. As atualizações de segurança disponibilizadas durante o período de suporte devem permanecer disponíveis para os utilizadores durante o período mais longo entre o período de suporte ou 10 anos.

Como será garantida a conformidade?

A não conformidade pode resultar em penalizações, tanto financeiras — coimas até 15 milhões de euros ou 2,5% do total das receitas globais — como não financeiras. As entidades reguladoras podem obrigar uma empresa a recolher produtos que não cumpram as normas.

Barracuda

Seis passos para a conformidade dos fabricantes

Abaixo estão as etapas básicas para os fabricantes iniciarem o seu processo de conformidade para estarem prontos para o CRA quando estiver totalmente em vigor. Os vários anexos do CRA fornecem detalhes sobre o que é esperado em cada etapa.

1. Classifique os produtos e realize uma avaliação de risco cibernético. As organizações podem ter produtos em várias categorias. Por isso, é importante avaliar cada produto para determinar em que categoria se enquadra: padrão, importante ou crítico.

2. Elaborar a documentação técnica. Analisar o CRA Anexo I e os requisitos da cadeia de abastecimento para todos os produtos, identificando eventuais lacunas. Realizar e documentar uma avaliação de risco para cada produto, considerando os critérios aplicáveis e as normas, especificações comuns ou esquemas de certificação adequados identificados.

3. Determine a abordagem de avaliação de conformidade de cada produto. Se necessário, contrate um terceiro para realizar esta tarefa.

4. Prepare uma declaração de conformidade em conformidade com os anexos V/VI e complete a documentação técnica que abrange o conteúdo do anexo VII. Em seguida, o fabricante deve aplicar a marcação CE a um produto em conformidade, à sua embalagem ou documentação. A marcação CE indicará a conformidade dos produtos com elementos digitais com o CRA, para que possam circular livremente na UE.

Barracuda

5. Elaborar e fornecer informações/instruções ao utilizador conforme o Anexo II. A documentação é uma parte crucial da conformidade e tem como objetivo proporcionar transparência ao utilizador.

6. Monitorizar e lidar com vulnerabilidades. A CRA exige participação ativa e contínua dos fabricantes durante o período de cobertura de suporte, que inclui fornecer suporte de cibersegurança, monitorização de quaisquer vulnerabilidades, e relatórios e remediação, como atualizações de software que abordem questões de segurança.

A Barracuda está empenhada em confirmar as suas categorias de produtos e em definir os próximos passos. Forneceremos informações sobre o Centro de Confiança assim que estiverem disponíveis.

PASSO 1
Classificar os produtos e conduzir um risco cibernético avaliação para cada

PASSO 2
Prepare a documentação técnica

PASSO 3
Determinar a abordagem de avaliação da conformidade

PASSO 4
Aplicar a CE Marketing e rascunhar a Declaração de Conformidade

PASSO 5
Preparar e fornecer instruções ao utilizador

PASSO 6
Monitorizar e lidar com vulnerabilidades

Barracuda

Classe I importante e Classe II importante

Os produtos importantes de Classe I representam um risco de cibersegurança menor do que os produtos importantes de Classe II. Os fabricantes podem optar por declarar conformidade se cumprirem determinadas normas qualificadas da UE/especificações comuns/esquemas de certificação, desde que estejam disponíveis e sejam aplicáveis ao produto. Caso contrário, poderão exigir uma verificação por terceiros.

Produtos importantes da Classe II são considerados como apresentando um nível mais elevado de risco de cibersegurança, sendo necessária a certificação por uma terceira entidade autorizada.

A CRA, a DORA e a NIS2, em conjunto, constituem um conjunto complexo de regulamentos de cibersegurança para as empresas que operam na UE. A sua empresa pode estar sujeita a mais do que uma destas regulamentações Centro de Confiança Contém diversos recursos para ajudar os clientes a compreender o DORA, incluindo o nosso e-book Compreender o DORA: Um Guia para a Resiliência Operacional Digital Act e NIS2, incluindo o nosso e-book Navegando NIS2: UM guia para o por vir europeu cibersegurança regulamentos, para ajudar as empresas com as suas obrigações de conformidade.

Sobre a Barracuda

A Barracuda é uma empresa líder global em cibersegurança, que oferece proteção completa contra ameaças complexas para empresas de todas as dimensões. A nossa plataforma BarracudaONE, com AI, protege Emails, dados, aplicações e redes com soluções inovadoras, XDR gerido e um painel centralizado para maximizar a proteção e fortalecer a resiliência cibernética. Com a confiança de centenas de milhares de profissionais de TI e Provedores de serviços geridos em todo o mundo, a Barracuda oferece defesas robustas, fáceis de comprar, implementar e utilizar. Para mais informações, visite pt.barracuda.com.