# APRESENTANDO A LEI DE RESILIENCIA CIBERNETICA (CRA)

O cenário regulatório europeu está passando por uma grande transformação com a adoção da Lei de Resiliência Cibernética (CRA). Este regulamento entrou em vigor em dezembro de 2024 e representa um passo decisivo na segurança dos produtos digitais comercializados na União Europeia. Para os fabricantes de máquinas, equipamentos industriais e produtos conectados, este regulamento introduz novas obrigações que transformam profundamente as práticas de design e marketing.

## O que é o CRA?

A Lei de Resiliência Cibernética (Regulamento da UE 2024/2847) é um regulamento europeu diretamente aplicável que estabelece requisitos harmonizados de segurança cibernética para todos os "produtos com elementos digitais" disponibilizados no mercado da União Europeia. Ao contrário das directivas que exigem a transposição nacional, a ANR aplica-se uniformemente em todos os Estados-Membros a partir do momento da sua entrada em vigor.

### Um regulamento diretamente aplicável

A natureza directamente aplicável da ANR significa que não é necessária uma transposição nacional. Os fabricantes, estabelecidos na UE ou em países terceiros, devem cumprir os mesmos requisitos para comercializar os seus produtos no mercado europeu. Essa padronização visa criar um nível homogêneo de segurança e evitar a fragmentação regulatória.

### Âmbito de aplicação

O ARC aplica-se a qualquer produto com elementos digitais, ou seja, qualquer hardware ou software capaz de processar dados digitais. Isso inclui:

- Produtos de consumo (smartphones, laptops, objetos conectados, automação residencial)
- Equipamentos industriais conectados (máquinas, robôs, PLCs)
- Sistemas de controle (PLC, SCADA, DCS)
- Dispositivos IoT e IIoT
- Software e firmware incorporados
- Os próprios componentes de segurança cibernética

O regulamento abrange todo o ciclo de vida do produto, desde seu design até seu descomissionamento, distribuição e uso.

## Quais são os objetivos do CRA?

A Lei de Resiliência Cibernética persegue vários objetivos estratégicos que refletem os desafios atuais de segurança cibernética em um contexto de crescente interconexão de sistemas industriais e de consumo.

### Fortaleça a segurança por design

O objetivo central da CRA é impor uma abordagem de "segurança por design" para todos os produtos digitais. Essa filosofia exige que a segurança cibernética seja integrada desde os primeiros estágios de desenvolvimento, não adicionada como uma camada adicional após o fato. Os fabricantes devem antecipar ameaças, avaliar riscos e implementar mecanismos de proteção adequados antes mesmo de serem lançados no mercado.

### Melhorando a transparência e a confiança

O ARC visa criar um ambiente de confiança, exigindo que os fabricantes comuniquem claramente os recursos de segurança de seus produtos. Os utilizadores e integradores devem ser capazes de identificar facilmente os produtos conformes com a marca CE e dispor de informações pormenorizadas sobre as medidas de segurança aplicadas, as

vulnerabilidades conhecidas e as atualizações disponíveis.

### Criando uma cadeia de responsabilidade

Ao responsabilizar todos os agentes económicos (fabricantes, importadores, distribuidores), o regulamento estabelece uma cadeia de responsabilidade clara. Cada parte interessada deve garantir que os produtos que disponibilizam atendam aos requisitos do ARC, criando um ecossistema onde a segurança cibernética se torne uma preocupação compartilhada.

### Harmonização de requisitos a nível europeu

A harmonização regulatória evita a proliferação de padrões nacionais divergentes que complicariam o marketing transfronteiriço. Um produto compatível com a CRA pode ser comercializado livremente em toda a União Europeia, simplificando o processo para os fabricantes e garantindo um nível uniforme de proteção para os usuários.

## O que está mudando com o CRA?

A entrada em vigor da Lei de Resiliência Cibernética marca uma mudança de paradigma para a indústria manufatureira e as empresas de software. As obrigações impostas transformam profundamente as práticas estabelecidas.

### Uma abordagem regulamentar restritiva

Ao contrário das recomendações e boas práticas voluntárias que prevaleciam até agora, a ANR impõe obrigações juridicamente vinculativas. Os fabricantes não podem continuar a optar por ignorar a cibersegurança: está a tornar-se uma condição legal para aceder ao mercado europeu, da mesma forma que a segurança funcional ou a compatibilidade eletromagnética.

### Gerenciamento proativo de vulnerabilidades

Uma das grandes inovações do CRA diz respeito à gestão de vulnerabilidades. O regulamento distingue entre dois tipos de vulnerabilidades que exigem uma resposta rápida:

- **Vulnerabilidades exploradas ativamente** : quando um fabricante descobre que uma vulnerabilidade em seu produto está sendo explorada maliciosamente em condições do mundo real, ele tem 24 horas para fazer uma notificação inicial, 72 horas para fornecer ações corretivas iniciais e 14 dias para enviar um relatório final.
- **Vulnerabilidades exploráveis** : essas vulnerabilidades têm o potencial de serem exploradas em condições operacionais práticas. Embora a ANR não imponha prazos rígidos para o seu processamento, eles não devem mais estar presentes em produtos comercializados após a data de aplicação integral do regulamento.

### A obrigação de apoiar a longo prazo

O ARC exige que os fabricantes forneçam atualizações de segurança por um período mínimo de 5 anos após a colocação no mercado. Essa obrigação transforma o modelo de negócios de muitos fabricantes que estão acostumados a uma única lógica de vendas, obrigando-os a manter um relacionamento contínuo com seus produtos e clientes.

### Rastreabilidade e documentação

Os requisitos documentais tornam-se consideravelmente mais importantes. Os fabricantes devem compilar e manter documentação técnica detalhada, incluindo:

- Análise de risco de segurança cibernética
- Descrição dos recursos de segurança
- Resultados de testes e avaliações
- O processo de gerenciamento de vulnerabilidades
- Instruções de instalação e uso seguro

Esta documentação deve ser conservada durante 10 anos e disponibilizada às autoridades de controlo mediante pedido.

## Quem está preocupado com o CRA?

O âmbito de aplicação do Regulamento Ciber-Resiliência é deliberadamente amplo para abranger todos os agentes económicos envolvidos no fornecimento de produtos digitais.

### Fabricantes

Os fabricantes são a categoria de intervenientes mais directamente afectados. São considerados fabricantes:

- Empresas que projetam e produzem produtos com elementos digitais
- Empresas que têm esses produtos projetados ou fabricados e os comercializam sob seu nome ou marca
- Importadores que introduzem produtos de fabricantes estabelecidos fora da UE no mercado europeu
- Distribuidores que se tornam responsáveis quando alteram substancialmente um produto ou o disponibilizam quando este não está manifestamente conforme

Esta definição ampla inclui grandes grupos industriais, bem como PMEs e startups que desenvolvem soluções conectadas.

### Setores industriais particularmente afetados

Vários setores estão particularmente preocupados com o CRA:

**Fabricação** : Fabricantes de máquinas-ferramentas, equipamentos de produção, robôs industriais e controladores lógicos programáveis estão na linha de frente. Seus produtos, que estão cada vez mais conectados e integrados às arquiteturas IIoT, estão totalmente dentro do escopo do regulamento.

**Automação industrial** : Os fabricantes de sistemas de controle (SCADA, DCS, PLC), sensores inteligentes e interfaces homem-máquina (HMI) devem adaptar seus processos de desenvolvimento para atender aos requisitos do CRA.

**IoT e eletrônicos de consumo** : Produtos conectados para indivíduos (objetos conectados, equipamentos de automação residencial, dispositivos de vigilância) também estão sujeitos à regulamentação.

**Fornecedores de software** : os desenvolvedores de sistemas operacionais, firmware, aplicativos industriais e soluções de segurança cibernética devem estar em conformidade com o CRA.

### Classificação do produto

O CRA estabelece uma classificação dos produtos de acordo com sua criticidade, com requisitos e procedimentos de avaliação diferenciados:

**Produtos padrão** : A maioria dos produtos com elementos digitais se enquadra nessa categoria. Estão sujeitos a uma avaliação da autoconformidade pelo fabricante (módulo A), que pode basear-se em normas harmonizadas após a sua publicação.

**Produtos Classe I (Importante):** Esta categoria inclui determinados produtos para gerenciamento de identidade, controle de acesso, redes privadas virtuais e sistemas que detectam vulnerabilidades. Exigem uma autoavaliação com a conformidade com as normas harmonizadas, caso existam.

**Produtos de Classe II (Importantes):** Inclui, mas não se limita a, sistemas operacionais, microprocessadores seguros e alguns sistemas de detecção de intrusão. Exigem um exame de tipo por um organismo notificado (módulo B+C).

**Produtos críticos** : Os produtos mais sensíveis (por exemplo, certos componentes de segurança para infraestruturas críticas) podem estar sujeitos a um sistema europeu de certificação de cibersegurança.

### Os intervenientes indirectamente afectados

Além dos fabricantes, outras partes interessadas são impactadas:

- **Os integradores de sistemas** que montam produtos digitais em instalações complexas devem garantir que os componentes usados estejam em conformidade
- **É** do interesse dos operadores industriais exigir a conformidade com a ANR de seus fornecedores para proteger suas instalações

- **Os subcontratantes e fornecedores** envolvidos na cadeia de desenvolvimento devem adaptar as suas práticas para permitir que o produto final cumpra

## Quais são as principais obrigações das organizações industriais?

O CRA impõe um conjunto de obrigações que estruturam a abordagem de segurança cibernética ao longo do ciclo de vida do produto. Esses requisitos são divididos em várias categorias complementares.

### Requisitos essenciais de segurança cibernética

Os requisitos essenciais estabelecidos no Anexo I da ANR constituem o quadro de segurança que todos os produtos devem cumprir. Eles incluem:

**Segurança desde a concepção** : Os produtos devem ser projetados, desenvolvidos e produzidos de forma a garantir um nível adequado de segurança cibernética baseada em risco. Tal implica uma análise de risco formalizada, a identificação de ativos críticos e potenciais ameaças e a aplicação de medidas de proteção proporcionadas.

**Defesa em profundidade** : A regulamentação incentiva a adoção de arquiteturas de segurança multicamadas, onde vários mecanismos de proteção se reforçam mutuamente. Essa abordagem, bem conhecida em ambientes de OT como "defesa em profundidade", limita o impacto de um compromisso único.

**Superfície de ataque reduzida**: os fabricantes devem minimizar funcionalidades desnecessárias, desabilitar serviços não essenciais e limitar os privilégios de acesso ao estritamente necessário. Os componentes de software e hardware devem ser escolhidos com o menor número de vulnerabilidades conhecidas em mente.

**Gerenciamento de atualizações** : os produtos devem ser capazes de receber atualizações de segurança durante todo o período de suporte. Essas atualizações devem ser seguras (assinadas, autenticadas), fáceis de aplicar e não degradar a funcionalidade do produto.

### Gerenciamento de vulnerabilidades

O gerenciamento de vulnerabilidades é uma das obrigações mais exigentes do ARC. Os fabricantes devem estabelecer e manter um processo abrangente que inclua:

**Identificação e recepção** : Estabelecimento de um único ponto de contato para receber relatórios de vulnerabilidade (security.txt de acordo com a RFC 9116). Os fabricantes devem monitorar ativamente os bancos de dados de vulnerabilidades (CVEs, NVDs) para os componentes que incorporam.

**Análise e avaliação** : Cada vulnerabilidade deve ser analisada para determinar sua exploração Esta avaliação deve ter em conta o ambiente de utilização previsto, as medidas de proteção existentes e as condições práticas de funcionamento. Uma vulnerabilidade teórica em um componente pode não ser explorável se esse componente estiver isolado da rede ou protegido por outros mecanismos.

**Processamento e correção** : dependendo da criticidade e da operabilidade, o fabricante deve desenvolver e implantar patches, soluções alternativas ou medidas compensatórias. O regulamento reconhece o conceito de "correção virtual", que é particularmente relevante para ambientes OT onde as atualizações de software podem ser difíceis de aplicar.

**Comunicação** : Os fabricantes devem se comunicar de forma transparente sobre vulnerabilidades e correções. Esta comunicação deve ser simultaneamente proativa (notificações aos utilizadores) e reativa (respostas aos pedidos de informação).

**Técnica de documentação**

A constituição de documentação técnica completa e atualizada é obrigatória. Esta documentação deve incluir:

- Uma declaração de conformidade da UE atestando a conformidade com os requisitos essenciais
- Documentação da análise de risco de segurança cibernética

- Descrição detalhada das propriedades de segurança do produto
- Instruções para instalação, configuração e uso seguros
- A política de gerenciamento de vulnerabilidades e atualizações
- Os resultados dos testes e avaliações de segurança realizados

### Marcação CE e declaração de conformidade

Antes de comercializar um produto, o fabricante deve:

- Realizar a avaliação da conformidade de acordo com o procedimento aplicável (Módulo A, A com norma harmonizada ou B+C dependendo da classe)
- Elabore a declaração de conformidade da UE
- Afixe a marca CE no produto
- Forneça as instruções e informações de segurança necessárias

### Obrigações de apoio e alimentos

As obrigações principais não entrarão em vigor até 11 de dezembro de 2027, mas os fabricantes devem planejar sua estratégia de suporte de longo prazo agora. A exigência de fornecer atualizações de segurança por pelo menos 5 anos transforma o modelo de relacionamento com o cliente e requer uma organização dedicada para suporte pós-venda.

## Quais são as penalidades previstas pela CRA?

O Regulamento Ciber-Resiliência prevê um regime de sanções dissuasivo para garantir a eficácia das obrigações impostas. As autoridades nacionais de controlo dispõem de amplos poderes de investigação, injunção e sanção.

### Sanções financeiras

As multas podem chegar a € 15 milhões ou 2,5% do faturamento anual mundial. Esta dupla abordagem permite adaptar a sanção à dimensão da empresa: as grandes organizações incorrem em coimas proporcionais ao seu volume de negócios, enquanto um limite mínimo de 15 milhões de euros garante um efeito dissuasor mesmo para as empresas mais pequenas.

A proporcionalidade das sanções depende de vários critérios:

- Natureza, gravidade e duração da violação
- Se a ofensa foi intencional ou negligente
- Medidas tomadas para atenuar os danos
- O grau de cooperação com as autoridades
- Quaisquer violações anteriores
- As consequências da violação para os usuários e a sociedade

### Sanções administrativas

Além das multas financeiras, os supervisores podem tomar várias medidas:

**Injunções** : Obrigação de colocar o produto em conformidade dentro de um período especificado, fornecer informações adicionais ou corrigir práticas não conformes.

**Recolha e recolha** : Em caso de violação grave, a autoridade pode exigir que o produto seja retirado do mercado e recolhido junto dos utilizadores finais. Esta medida, particularmente dispendiosa e prejudicial para a imagem da empresa, constitui uma importante sanção dissuasora.

**Proibição de comercialização** : Os produtos não conformes podem ser banidos do mercado europeu até que sua conformidade seja demonstrada.

**Publicação das** sanções: As autoridades podem tornar públicas as sanções emitidas, com um impacto significativo na reputação das empresas em causa.

### Responsabilidade civil e comercial

Além das penalidades administrativas, os fabricantes também estão expostos a:

- Ações de responsabilidade civil por usuários que sofreram danos
- Perda de confiança e imagem de marca

- Exclusão de contratos públicos ou certificações setoriais
- Desafios de negócios com clientes que exigem conformidade

## Como se preparar para a aplicação do ARC?

A preparação para a conformidade com o CRA requer uma abordagem metódica e em fases. Embora as principais obrigações se apliquem a partir de 11 de dezembro de 2027, é essencial começar já, dada a dimensão das transformações a efetuar.

### Etapa 1: Avaliação da condição

O primeiro passo é realizar um diagnóstico preciso da situação atual:

**Inventário de produtos** : Identifique todos os produtos com elementos digitais que são comercializados ou estão em desenvolvimento. Para cada produto, determine sua classificação potencial (padrão, classe I, classe II, crítica).

**Análise de lacunas** : Compare as práticas atuais com os requisitos do ARC. Identifique os processos existentes (desenvolvimento seguro, gerenciamento de vulnerabilidades, suporte) e as lacunas que precisam ser abordadas.

**Avaliação de impacto** : Estime os recursos necessários (humanos, técnicos, financeiros) para alcançar a conformidade, bem como cronogramas realistas para implementação.

### Etapa 2: Implementação do gerenciamento de riscos de segurança cibernética

O gerenciamento de riscos é a base da abordagem de conformidade. Trata-se de adotar uma abordagem estruturada, idealmente baseada em padrões reconhecidos, como o padrão IEC 62443-4-1 para o desenvolvimento de produtos seguros:

**Defina o sistema em consideração** : Delimite com precisão o escopo da análise (componentes de hardware, software, interfaces, ambiente de uso pretendido).

**Identifique ativos e interfaces** : liste todos os elementos do sistema que provavelmente serão alvo de um ataque (dados, funções críticas, componentes de comunicação).

**Analise** os impactos: Avalie a criticidade de cada ativo em termos de confidencialidade, integridade, disponibilidade e segurança.

**Identifique ameaças** : Use metodologias estruturadas (Microsoft STRIDE, MITRE ATT&CK para ICS) para identificar ameaças relevantes de acordo com o contexto de uso.

**Avalie a plausibilidade** : determine a probabilidade de cada ameaça ocorrer com base na motivação do invasor, nas oportunidades de ataque e nas medidas de proteção existentes.

**Calcule e priorize os riscos** : Cruze o impacto e a probabilidade de obter um nível de risco e, em seguida, priorize os riscos a serem abordados.

**Defina e implemente medidas de mitigação** : Selecione medidas técnicas e organizacionais apropriadas para reduzir os riscos a um nível aceitável.

**Avalie o risco residual** : Verifique se os riscos remanescentes após o tratamento são aceitáveis em relação ao contexto de uso.

### Etapa 3: Integrar a segurança ao ciclo de vida de desenvolvimento

A segurança deve ser integrada em todas as fases do ciclo de vida do produto, usando uma abordagem de SDL (Ciclo de Vida de Desenvolvimento Seguro):

**Design** : Defina os requisitos de segurança, projete uma arquitetura segura, selecione componentes com a segurança em mente.

**Desenvolvimento** : Aplique práticas de codificação seguras, use ferramentas de análise estática e dinâmica, execute revisões de código orientadas à segurança.

**Teste e validação** : Realizar testes de segurança (testes de penetração, fuzzing), verificar a resistência a ataques identificados na análise de risco.

**Colocação no mercado** : Compilar a documentação técnica, realizar a avaliação da conformidade, estabelecer a declaração UE de conformidade.

**Suporte e manutenção** : monitore vulnerabilidades, desenvolva e implante patches, comunique-se com os usuários.

**Fim da vida útil** : notifique os usuários sobre o fim do suporte de segurança, forneça recomendações para migração ou desativação segura.

## Etapa 4: Configurando o processo de gerenciamento de vulnerabilidades

Um processo robusto de gerenciamento de vulnerabilidades é essencial:

**Crie um ponto de contato** : Publique um arquivo security.txt (RFC 9116) na raiz do site da empresa, indicando como relatar vulnerabilidades com responsabilidade.

**Inteligência de vulnerabilidade** : monitore bancos de dados CVE/NVD em busca de componentes de terceiros usados, rastreie avisos de segurança de fornecedores, participe de comunidades de troca de ameaças (ISAC).

**Verificação contextual** : Para cada vulnerabilidade identificada, avalie sua exploração real no contexto específico do produto. Uma vulnerabilidade que afeta um componente que não está exposto ou protegido por medidas compensatórias pode não exigir patches urgentes.

**Desenvolvimento de patches** : priorize o desenvolvimento de patches com base na criticidade e na capacidade de exploração, teste patches para evitar regressões, prepare documentos VEX (Vulnerability Exploitability eXchange) especificando o status de cada vulnerabilidade.

**Implantação e comunicação** : notifique os clientes sobre a disponibilidade de patches, forneça instruções claras para seus aplicativos, proponha soluções alternativas, se necessário.

**Conformidade com CRA** : Implementar procedimentos de contingência para cumprir prazos rígidos para vulnerabilidades exploradas ativamente (notificação inicial em 24 horas, relatório completo em 14 dias).

## Etapa 5: Organização e habilidades

A conformidade com o CRA requer habilidades específicas e uma organização adaptada:

**Designe um gerente de produto de segurança** : Identifique uma pessoa responsável pelo assunto no nível executivo, com a autoridade e os recursos necessários.

**Treine equipes** : Aumente a conscientização entre todas as equipes de desenvolvimento, treine em práticas de desenvolvimento seguro, desenvolva experiência em análise de riscos e gerenciamento de vulnerabilidades.

**Criar ou fortalecer o PSIRT** : Estabeleça uma Equipe de Resposta a Incidentes de Segurança do Produto (PSIRT) responsável pelo gerenciamento de vulnerabilidades e incidentes de segurança.

**Governança estrutural** : Defina funções e responsabilidades, estabeleça processos de tomada de decisão e estabeleça indicadores de monitoramento de conformidade.

## Etapa 6: Colabore com o ecossistema

O cumprimento não pode ser alcançado isoladamente:

**Requisitos do fornecedor** : Incluir cláusulas de segurança nos contratos com fornecedores de componentes, exigir o fornecimento de informações de vulnerabilidade e patch (SBOM, VEX).

**Comunicação com os clientes** : forneça documentação de segurança abrangente, apoie os integradores na implantação segura, estabeleça canais de comunicação para problemas de segurança.

**Participação em iniciativas setoriais** : Participar de grupos de trabalho profissionais (VDMA, outras associações industriais), participar do trabalho de padronização, trocar as melhores práticas.

# Lista de verificação operacional de OT/IoT: 10 ações-chave

Para estruturar sua abordagem de conformidade, aqui está uma lista de verificação pragmática de ações prioritárias a serem implementadas:

## 1. Efectuar um inventário exaustivo dos produtos em causa

Identifique todos os seus produtos com elementos digitais para o mercado europeu. Para cada um, documente os componentes de hardware e software, interfaces de comunicação, versões de firmware e determine a classificação CRA aplicável.

## 2. Realize análises de risco de segurança cibernética produto por produto

Aplicar uma metodologia estruturada (IEC 62443-4-1, ISO/SAE 21434 para produtos conectados a veículos) para identificar ativos críticos, ameaças relevantes, avaliar riscos e definir medidas de proteção apropriadas. Documente formalmente esta análise.

## 3. Implemente defesa em profundidade e segmentação

Adote uma arquitetura de segurança em várias camadas: segmentação de rede para isolar áreas críticas, firewalls e IPS para controlar fluxos, controle de acesso rigoroso, autenticação forte. Essa abordagem reduz significativamente a superfície de ataque e a capacidade de exploração de vulnerabilidades.

## 4. Implante soluções nativas de segurança cibernética de OT

Os ambientes de OT exigem soluções específicas que são diferentes das ferramentas tradicionais de TI. Escolher:

- Soluções de proteção de endpoint adaptadas a sistemas industriais (suporte para sistema operacional legado, sem necessidade de reinicialização, lista de permissões de OT)
- IPS com inspeção profunda de protocolos industriais (DPI sobre Modbus, Profinet, EtherNet/IP, etc.)
- Soluções de aplicação de patches virtuais para proteger sistemas não patcháveis
- Ferramentas de controle de mídia removível (USB) para ambientes de produção

## 5. Estabeleça o processo de gerenciamento de vulnerabilidades

Implemente a infraestrutura necessária: ponto de contato (security.txt) seguro, processos automatizados de monitoramento, análise e priorização de CVE, capacidade de desenvolver e implantar patches em caso de emergência e comunicação estruturada com os clientes.

## 6. Implemente um sistema de atualização seguro

Projete um mecanismo para implantar atualizações de segurança de maneira segura (assinatura criptográfica, canal autenticado), simples (automação possível) e sem interrupção prolongada da produção. Forneça mecanismos de reversão em caso de problemas.

## 7. Compilar a documentação técnica de conformidade

Reúna e formalize toda a documentação necessária: análise de risco, especificações de segurança, resultados de testes, procedimentos de configuração segura, política de gerenciamento de vulnerabilidades, manual do usuário seguro. Esta documentação deve ser mantida atualizada durante todo o ciclo de vida.

## 8. Defina as condições de uso seguro e responsabilidades

Especifique na documentação do produto o contexto de uso pretendido, as suposições de segurança (ambiente de rede, controles de acesso físico esperados) e os limites de responsabilidade. Algumas medidas de segurança são de responsabilidade do operador final: esclareça essas responsabilidades contratualmente.

## 9. Treine e estruture equipes

Investir no desenvolvimento de competências: formação em desenvolvimento seguro, certificação em cibersegurança industrial (ISA/IEC 62443 Cybersecurity Expert), recrutamento de perfis especializados se necessário. Estruturar a organização com funções dedicadas (oficial de segurança do produto, PSIRT).

### 10. Antecipe o suporte de longo prazo

Planeje a estratégia de suporte por design por um período mínimo de 5 anos: arquitetura permitindo atualizações, provisionamento de recursos humanos e técnicos para suporte pós-venda, modelo econômico incluindo o custo do suporte de segurança. Antecipe o gerenciamento de obsolescência de componentes.

## Como a AKENATECH o apoia?

Diante da complexidade e escala dos requisitos da Lei de Resiliência Cibernética, desenvolvemos uma abordagem de suporte abrangente que cobre toda a sua jornada de conformidade.

### Experiência reconhecida em segurança cibernética OT e conformidade regulatória

Nosso posicionamento exclusivo combina profundo conhecimento técnico em segurança cibernética de ambientes industriais (OT/IoT) com um domínio das questões de conformidade regulatória. Estamos familiarizados com as especificidades dos sistemas de controle, as restrições de disponibilidade dos ambientes de produção e os requisitos das normas IEC 62443 e ISO 27001, que constituem a base técnica da conformidade com o CRA.

### Suporte de ponta a ponta: Estratégia → Implementação → Operações

Nossa abordagem em três fases garante uma transformação sustentável e eficaz:

### Fase de Estratégia - GRC Consulting

Começamos com uma análise aprofundada da sua situação:

- Diagnóstico de conformidade com a CRA: identificação dos produtos em causa, avaliação dos desvios em relação aos requisitos
- Definição da estratégia de compliance: priorização de ações, planejamento de recursos, estimativa de custos
- Implementação do gerenciamento de riscos de segurança cibernética de acordo com IEC 62443-4-1: metodologia de análise de risco do produto, suporte em seus primeiros produtos piloto
- Apoio na elaboração de documentação técnica e procedimentos de avaliação da conformidade
- Suporte para marcação CE para produtos com elementos digitais

Esta fase de consultoria permite que você construa um roteiro claro e realista, alinhado com suas restrições de negócios e seus objetivos de negócios.

### Fase de Implementação - Integração da Solução

Uma vez definida a estratégia, passamos à implementação concreta:

- **Proteção de endpoint** : implantação de soluções nativas de segurança cibernética para OT, adaptadas a sistemas industriais e legados (suporte a Windows 2000/XP e Linux, sem necessidade de reinicialização, lista de permissões automática de aplicativos OT)
- **Visibilidade e detecção** : implementação de soluções de monitoramento de rede com inspeção aprofundada de protocolos industriais (DPI em 200+ protocolos OT), detecção de anomalias e intrusão
- **Sistemas de proteção** : aplicação de práticas recomendadas de configuração segura, desativação de serviços desnecessários, controle de acesso aprimorado
- **Vedação e integridade** : soluções para proteção contra modificações não autorizadas, controle de mídia removível (USB) adequado para ambientes de produção
- **Segmentação e defesa em profundidade** : arquitetura de rede segura com IPS/IDS, firewalls industriais, isolamento de áreas críticas

Privilegiamos soluções comprovadas em ambientes OT, com parceiros tecnológicos reconhecidos, como a TXOne Networks, que oferecem mecanismos de patch

virtual que são particularmente adaptados às restrições do CRA.

### Fase de Operações - Serviços Gerenciados

A conformidade com o CRA não é um projeto único, mas um compromisso de longo prazo. Garantimos a continuidade da sua conformidade:

- **CISO de compartilhamento de tempo** : fornecimento de um gerente de segurança de sistemas de informação experiente para gerenciar a abordagem de segurança do seu produto sem recrutar internamente
- **PSIRT semi-terceirizado** : gerenciamento operacional de suas vulnerabilidades, monitoramento automatizado de CVE, análise de explorabilidade, coordenação do desenvolvimento e implantação de patches, comunicação com clientes e autoridades
- Suporte contínuo para a evolução de sua documentação e processos

### Uma abordagem pragmática e operacional

Nossa metodologia é projetada para ser pragmática e adaptada às realidades industriais:

- Consideração de restrições de produção (disponibilidade, legado, ambientes isolados)
- Abordagem faseada e priorizada para controlar os investimentos
- Transferência de habilidades para capacitar suas equipes
- Reutilização de análises e investimentos existentes (ISO 27001, NIS2, IEC 62443)

### Sinergia com outros regulamentos

A ANR não se aplica isoladamente. Ajudamos você a criar sinergias com seus outros esforços de conformidade:

- **Regulamento de Máquinas 2023/1230** : coordenação dos requisitos comuns de cibersegurança com a ANR
- **NIS2** : Alinhamento de Medidas Organizacionais e Técnicas para Operadores Críticos
- **ISO 27001** : Integrando a segurança do produto em seu sistema de gestão de segurança da informação
- **IEC 62443** : um padrão técnico de referência para segurança cibernética industrial, reconhecido como uma base sólida para conformidade com CRA

## Perguntas Freqüentes

### Quando é que a ANR entra realmente em vigor?

A Lei de Resiliência Cibernética entrou em vigor em 10 de dezembro de 2024. No entanto, as obrigações estão sendo aplicadas gradualmente:

- **11 de setembro de 2026** : Obrigação de relatar vulnerabilidades exploradas ativamente e incidentes graves de segurança
- **11 de dezembro de 2027:** aplicação total de todos os requisitos, incluindo a proibição de comercializar produtos com vulnerabilidades exploráveis conhecidas

Portanto, é crucial iniciar seu processo agora, porque as transformações necessárias levam tempo.

### Meu produto está coberto pelo CRA?

Se o seu produto tiver elementos digitais (hardware ou software capaz de processar dados digitais) e se destinar a ser comercializado na União Europeia, é mais provável que seja afetado. Isso inclui:

- Produtos de consumo que incorporam elementos digitais
- Máquinas industriais com controladores lógicos programáveis
- Equipamentos conectados (IoT/IIoT)
- Sistemas de controle (SCADA, DCS, PLC)
- Componentes eletrônicos com firmware
- Software embarcado e aplicações industriais

Existem algumas isenções (dispositivos médicos, veículos, aeronáutica já abrangidas por outros regulamentos específicos), mas são limitadas.

## Qual é a diferença entre o ARC e o Regulamento de Máquinas?

O **Regulamento de Máquinas (UE) 2023/1230** aplica-se especificamente a máquinas e estabelece requisitos de segurança funcional que agora incluem aspectos de segurança cibernética. O **ARC** aplica-se horizontalmente a todos os produtos com elementos digitais, independentemente de serem máquinas ou não.

Para um fabricante de máquinas, os dois regulamentos se aplicam de forma complementar:

- O Regulamento de Máquinas cobre a segurança funcional geral da máquina (riscos mecânicos, elétricos, de segurança cibernética que afetam a segurança)
- O ARC cobre todos os aspectos da segurança cibernética dos elementos digitais da máquina

Os requisitos se sobrepõem até certo ponto, e uma análise de risco bem conduzida torna possível atender a ambos os regulamentos simultaneamente.

## Preciso resolver todas as vulnerabilidades de CVE que afetam meus componentes?

Não, a abordagem ARC é baseada no risco e na operabilidade em condições do mundo real. Uma vulnerabilidade de CVE que afeta um componente que você usa pode não ser explorável em seu produto, dependendo de:

- Sua arquitetura de segurança (segmentação, defesa em profundidade)
- O contexto de uso (componente não exposto à rede, acesso físico necessário para operação)
- Recursos realmente usados (vulnerabilidade em uma função de servidor quando você usa apenas o modo cliente)

É precisamente a análise de risco que permite determinar a real operacionalidade e priorizar as ações de remediação. Os documentos VEX (Vulnerability Exploitability eXchange) ajudam a comunicar claramente o status de cada vulnerabilidade.

## E se eu não conseguir corrigir um sistema legado?

Os ambientes OT geralmente têm sistemas legados que não podem ser atualizados sem o risco de mau funcionamento. A CRA reconhece esta realidade e permite o recurso a **medidas compensatórias** :

- **Correção virtual** : uso de IPS/IDS que pode bloquear tentativas de explorar vulnerabilidades conhecidas, sem modificar o sistema vulnerável
- **Segmentação de rede** : isolamento do sistema legado em uma área segura com controle de fluxo rigoroso
- **Controle de acesso aprimorado** : limitando o acesso físico e lógico ao sistema
- **Monitoramento intensivo** : monitoramento aumentado para detectar qualquer tentativa de exploração

Essas abordagens de defesa em profundidade ajudam a reduzir a capacidade de exploração de vulnerabilidades sem corrigir o próprio sistema.

## Como faço para gerenciar o suporte de segurança ao longo de 5 anos?

A obrigação de suporte mínimo de 5 anos representa uma mudança significativa. Várias estratégias são possíveis:

- **Antecipe por design** : escolha componentes com suporte de longo prazo, projete uma arquitetura modular que facilite as atualizações
- **Integre o custo ao modelo de negócios** : cobre explicitamente pelo suporte de segurança, ofereça contratos de manutenção que incluam patches
- **Terceirize o PSIRT** : use um provedor de serviços especializado para gerenciamento de vulnerabilidades operacionais e desenvolvimento de patches

- **Partilha de recursos** : para as PME, começam a surgir soluções de mutualização específicas para cada setor

## A ANR se aplica a produtos que já estão no mercado?

O regulamento prevê um princípio de não retroatividade: os produtos já colocados no mercado antes de 11 de dezembro de 2027 não estão sujeitos aos requisitos iniciais de conformidade. Contudo:

- A obrigação de comunicar vulnerabilidades exploradas ativamente aplica-se a partir de 11 de setembro de 2026, **incluindo para produtos já existentes no mercado**
- Os fabricantes mantêm uma obrigação geral de segurança para os produtos em serviço
- É altamente recomendável fornecer patches de segurança mesmo para produtos anteriores, por motivos de responsabilidade e imagem

## Posso confiar em padrões para demonstrar conformidade?

Sim, a ANR prevê explicitamente a utilização de **normas harmonizadas**. Quando uma norma harmonizada é publicada no Jornal Oficial da União Europeia, o cumprimento da mesma cria uma presunção de conformidade com os requisitos essenciais correspondentes.

Os padrões da série IEC **62443** (segurança cibernética de sistemas de controle e automação industrial) são particularmente relevantes e devem ser harmonizados sob o ARC:

- IEC 62443-4-1: Requisitos para o desenvolvimento de produtos seguros
- IEC 62443-4-2: Requisitos técnicos para segurança de componentes

Outras normas, como **a ISO/IEC 27001** (sistema de gestão de segurança da informação), também podem ajudar a demonstrar a conformidade organizacional.

## Quais são as primeiras ações a serem tomadas agora?

Para começar de forma eficaz:

1. **Faça um inventário de seus produtos afetados** e determine sua classificação CRA
2. **Configure seu ponto de contato de segurança** (security.txt) para ser acessível a partir de setembro de 2026
3. **Inicie a análise de risco** em seus produtos prioritários para identificar vulnerabilidades e ameaças
4. **Treine suas equipes** nos desafios do ARC e práticas de desenvolvimento seguras
5. **Avalie seus fornecedores** e integre cláusulas de segurança em seus contratos

Recomendamos que você obtenha suporte para estruturar esse processo e evitar erros dispendiosos.

# Conclusão

A Lei de Resiliência Cibernética representa um grande ponto de virada na abordagem da segurança cibernética de produtos industriais e conectados. Além da restrição regulatória, é uma oportunidade de diferenciação comercial para os fabricantes que poderão transformar esse requisito em vantagem competitiva.

A conformidade com o CRA requer uma profunda transformação das práticas de design, desenvolvimento e suporte do produto. Essa transformação é de longo prazo e requer investimentos significativos em habilidades, processos e tecnologias. No entanto, é essencial continuar a comercializar no mercado europeu, que representa uma saída fundamental para a indústria transformadora global.

Os prazos estão se aproximando rapidamente: setembro de 2026 para relatórios de vulnerabilidade, dezembro de 2027 para todos os requisitos. Os fabricantes precisam agir agora para se preparar de forma eficaz. Uma abordagem estruturada, baseada em análise de risco e padrões reconhecidos, como IEC

62443, permite progredir metodicamente e otimizar os investimentos.

Na AKENATECH, apoiamos os fabricantes nessa transformação, combinando experiência técnica em segurança cibernética OT, conhecimento dos ambientes de produção e domínio das questões regulatórias. Nossa abordagem de ponta a ponta – da estratégia à operação e à implementação – permite que você crie conformidade sustentável, mantendo o desempenho dos negócios.

**Não deixe o tempo escapar. A conformidade com o CRA é construída hoje para estar pronta amanhã.**

Entre em contato conosco para discutir sua situação específica e construir seu roteiro de conformidade com a Lei de Resiliência Cibernética juntos.