

AMOSTRA DO MAPA ESSENCIAL

Cyber Resilience Act.

Da incerteza ao plano.

Um exemplo de como organizamos sinais comerciais, hipóteses de escopo, lacunas prioritárias e próximos passos para uma empresa brasileira de produto conectado.

EMPRESA E PRODUTO FICTÍCIOS - AMOSTRA EDUCACIONAL

01 - RESUMO EXECUTIVO

A decisão não é 'estamos conformes?'.

É o que provar primeiro.

A Aurora Controls Ltda. e o controlador AX-100 são fictícios. Os fatos simulam as informações que uma empresa forneceria em um pedido real.

ROTA PRIORITÁRIA

CRA

Hipótese forte: hardware com firmware e conectividade, ofertado comercialmente na União Europeia.

GATILHO

14 dias

Prazo simulado de um distribuidor alemão para receber um plano de evidências.

NÍVEL ATUAL

3/10

Três grupos de evidência foram descritos. Sete precisam de confirmação documental.

DECISÃO RECOMENDADA

Frente CRA de 30 dias

Confirmar escopo e papel econômico, estabelecer responsável de reporte, inventariar versões e componentes e abrir um índice mínimo de evidências.

O QUE NÃO AFIRMAMOS

Nenhuma conclusão jurídica

Não avaliamos documentos reais, arquitetura, código, vulnerabilidades, classificação, procedimento de avaliação ou contrato. Não concluímos aplicabilidade nem conformidade.

Valor desta etapa

Em poucos dias, a equipe recebe uma ordem de trabalho: o que já está declarado, o que ainda precisa de prova, quem deve responder e qual decisão depende de especialista. Isso reduz retrabalho antes de contratar jurídico, teste ou avaliação de conformidade.

02 - FATOS E HIPÓTESES

Separar o que foi dito do que ainda precisa de prova.

ITEM	INFORMAÇÃO SIMULADA	TRATAMENTO
Empresa	Aurora Controls Ltda., fabricante brasileiro.	FATO DECLARADO
Produto	AX-100: controlador industrial com Ethernet, MQTT, firmware e painel web local.	FATO DECLARADO
Mercado	Venda por distribuidor alemão, sob a marca da fabricante.	FATO DECLARADO
Versões	Duas variantes de hardware e firmware em manutenção.	CONFIRMAR
Atualizações	Pacotes assinados seriam oferecidos por portal de suporte.	VER EVIDÊNCIA
Componentes	Há bibliotecas de terceiros, sem inventário apresentado.	LACUNA
Vulnerabilidades	Suporte recebe e-mail; fluxo formal não descrito.	LACUNA
Reporte CRA	Sem titular, suplente ou procedimento de 24 e 72 horas.	URGENTE
Suporte	Sem data final de suporte informada ao comprador.	LACUNA
Documentação	Manuais e relatórios em pastas distintas, sem índice.	ORGANIZAR

Regra de qualidade

Uma declaração vira evidência somente quando tem artefato identificável, proprietário, versão e data. Onde não há prova, mantemos 'não confirmado' em vez de completar a história.

03 - PORTA DE ENTRADA E CALENDÁRIO

Por que o CRA apareceu e qual prazo muda a prioridade.

SINAL 1

Produto digital

O cenário descreve hardware e firmware. A Comissão resume o CRA como aplicável a hardware e software, inclusive componentes vendidos separadamente.

SINAL 2

Conexão de dados

O uso previsto inclui conexão lógica a rede, teste central indicado no resumo oficial para a possível entrada no escopo.

SINAL 3

Mercado da União

O produto é ofertado a parceiro europeu. Os papéis de fabricante, importador e distribuidor precisam ser confirmados.

PERGUNTA DE CORTE

Existe exclusão?

Não verificamos exclusão, regra setorial, modificação substancial nem classificação como produto importante ou crítico.

10 dez. 2024**Entrada em vigor**

Início do período de preparação.

11 set. 2026**Reporte do artigo 14**

Início do reporte de vulnerabilidades exploradas e incidentes graves.

24 horas**Alerta inicial**

Prazo contado do conhecimento do evento reportável.

72 horas**Notificação principal**

Produto, versões, impacto, responsáveis e informação disponível.

11 dez. 2027**Aplicação geral**

Principais disposições passam a ser aplicáveis.

04 - DEZ LACUNAS PRIORITÁRIAS

O que localizar antes de contratar trabalho especializado.

1

Dono do reporte

URGENTE

Nomear titular e suplente; definir escalonamento e relógio de 24 e 72 horas.

2

Inventário de produto

ALTA

Relacionar modelos, hardware, firmware, mercados e datas.

3

Fluxo de vulnerabilidade

ALTA

Documentar recebimento, triagem, severidade, correção e comunicação.

4

Componentes

CONFIRMAR

Localizar inventário versionado de componentes próprios e de terceiros.

5

Risco cibernético

ALTA

Identificar avaliação vinculada ao produto, versões e desenvolvimento.

6

Atualização segura

CONFIRMAR

Reunir prova de integridade, distribuição e resposta a falha.

7

Período de suporte

ALTA

Definir critério, data final e comunicação ao comprador e usuário.

8

Instruções ao usuário

CONFIRMAR

Verificar instalação, uso seguro, contato, atualização e limitações.

9

Arquivo técnico

ALTA

Montar índice com dono, versão, local e validade de cada evidência.

10

Relação com importador

CONFIRMAR

Definir responsabilidades, troca de informação e bloqueio de venda.

05 - PLANO DE 30 DIAS

Quatro saídas pequenas, verificáveis e com responsável.

Semana 1

Delimitar produto, versões e papéis

Reunir comercial, produto e suporte por formulário escrito. Confirmar fabricante, marca, importador, distribuidor, países e datas.

SAÍDA

Ficha de escopo v1

Semana 2

Abrir o índice de evidências

Listar risco, arquitetura, componentes, desenvolvimento, atualização, suporte, instruções e documentação. Para cada item: dono, versão, data, link e estado.

SAÍDA

Índice rastreável

Semana 3

Ensaiai reporte de 24 e 72 horas

Usar cenário fictício para testar detecção, escalonamento, classificação, fontes, aprovação e ausência do titular.

SAÍDA

Registro do exercício

Semana 4

Decidir o próximo investimento

Levar escopo, lacunas e evidências a profissional adequado. Pedir proposta por resultado e separar obrigação de melhoria.

SAÍDA

Briefing comparável

Critério de parada

Se a empresa não confirma produto, mercado, responsável interno ou acesso mínimo às evidências, interromper a ampliação e resolver primeiro a governança básica.

06 - ÍNDICE DE EVIDÊNCIAS

Um mapa útil mostra o artefato, o dono e o próximo teste.

#	EVIDÊNCIA	ESTADO	RESPONSÁVEL	PRÓXIMA AÇÃO
01	Lista de modelos e versões em mercado	Parcial	Produto + comercial	Cruzar catálogo e vendas UE
02	Avaliação de risco do AX-100	Ausente	Engenharia	Procurar análise equivalente
03	Arquitetura e limites de confiança	Parcial	Engenharia	Identificar desenho vigente
04	Inventário de componentes	Ausente	Firmware	Gerar inventário inicial
05	Recebimento de vulnerabilidades	Ausente	Segurança + suporte	Definir canal e triagem
06	Histórico de correções e avisos	Parcial	Suporte	Relacionar tickets e versões
07	Procedimento de atualização segura	Parcial	Firmware	Vincular assinatura e rollback
08	Critério e data do suporte	Ausente	Direção + produto	Propor política
09	Procedimento de reporte	Ausente	Segurança + jurídico	Nomear dono e ensaiar
10	Instruções de instalação e uso	Localizada	Documentação	Revisar versão e idioma

ESTADO CORRETO

'Ausente' é dado útil

Permite priorizar criação, definir orçamento e impedir que uma planilha verde esconda a falta de prova.

CONTROLE MÍNIMO

Nome, versão, data, dono e link

Esses cinco campos tornam a evidência encontrável e reduzem retrabalho.

07 - PERGUNTAS AO PARCEIRO EUROPEU

Transformar pressão comercial em respostas para decidir.

1

Qual entidade colocará o produto no mercado e em quais países?

Pedir razão social, função na cadeia e mercados. Não presumir que todo parceiro é apenas distribuidor.

2

O pedido vem de lei, política interna ou exigência de cliente?

Pedir referência e prazo para separar obrigação, contrato e preferência comercial.

3

Quais modelos, versões e configurações estão no pedido?

Confirmar família, variante, firmware ou combinação específica.

4

Há questionário, formato de evidência ou portal obrigatório?

Receber o artefato antes de produzir documentação que talvez não seja aceita.

5

Como serão trocadas informações de vulnerabilidade e incidente?

Definir canal, contatos, horário, suplentes, confidencialidade e encaminhamento.

6

O que o parceiro espera antes da aplicação geral em 2027?

Registrar entregas transitórias sem prometer avaliação completa antes do escopo.

7

Quem decide se a evidência é suficiente?

Nomear aprovador e obter critério escrito para reduzir ciclos de revisão.

Modelo de resposta curta

Recebemos o pedido e estamos consolidando produto, versões, papéis e evidências. Para devolver um plano rastreável, confirme os pontos abaixo. O mapa manterá os itens não comprovados como lacunas e indicará o que depende de especialista.

08 - LIMITES E FONTES

O mapa começa em fonte oficial e termina em decisão honesta.

Comissão Europeia - resumo do CRA

Escopo, operadores econômicos, fabricantes, suporte, documentação e calendário.

digital-strategy.ec.europa.eu/en/policies/cra-summary

Comissão Europeia - reporte do CRA

Início em 11/09/2026, plataforma única e prazos de alerta, notificação e relatório final.

digital-strategy.ec.europa.eu/en/policies/cra-reporting

Comissão Europeia - implementação

Atos, orientações, FAQ e trabalho de implementação.

digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

EUR-Lex - Regulamento (UE) 2024/2847

Texto legal no Jornal Oficial. Em caso real, prevalece sobre resumos e material comercial.

eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

INCLUÍDO

Organizar a decisão

Triagem de sinais, fatos e hipóteses, dez lacunas, plano de 30 dias, índice de evidências e perguntas de handoff.

LIMITES DESTA ENTREGA

Encaminhamento seguro

Parecer, classificação definitiva, auditoria, teste, documentação formal, declaração UE, marcação CE, certificação ou representação.

Próximo passo

Use a triagem gratuita do Ponte Segura Radar. Se a rota fizer sentido para sua decisão, solicite um pacote por escrito. Nenhum pagamento é cobrado na triagem e nenhuma reunião inicial é obrigatória.