Cyber Resilience Act (CRA) na WEG

Motores Industriais

Motores Comerciais & Appliance

Automação & Sistemas

Energia

Transmissão & Distribuição

Tinta

Cibersegurança e Resiliência Digital

Driving efficiency and sustainability

Sumário

1. Visão Geral

Em uma era cada vez mais digital e interconectada, as infraestruturas industriais passam a depender fortemente de dispositivos de automação integrados, como inversores de frequência, controladores lógicos programáveis (CLPs), interfaces homem-máquina (IHMs), gateways industriais, sistemas de controle distribuídos, entre outros. Nesse cenário, a segurança cibernética deixa de ser uma opção e passa a ser um requisito essencial para a operação segura, confiável e contínua dos sistemas.

Com o avanço constante das ameaças cibernéticas, cada vez mais sofisticadas e direcionadas, as abordagens tradicionais e puramente reativas de segurança tornaram-se insuficientes. Novas técnicas de ataque surgem diariamente, exigindo que fabricantes, integradores e operadores industriais adotem medidas proativas e resilientes para proteger seus ativos.

A exposição de infraestruturas críticas conectadas à internet tem levado governos a estabelecer regulamentações que buscam reforçar a resiliência dos sistemas, isto é, a capacidade de se recuperar de um ataque, adaptar-se às ameaças em constante mudança e aprimorar seus mecanismos de defesa, minimizando os impactos e preservando a continuidade das operações. Isso envolve não apenas a implementação de medidas de segurança robustas, mas também a capacidade de antecipar e responder efetivamente a incidentes. Nesse contexto, adotar uma estratégia de resiliência cibernética robusta não é mais uma vantagem competitiva, é uma demanda real para os negócios e para a proteção das operações industriais e de missão crítica.

Diversas jurisdições ao redor do mundo têm desenvolvido regulamentações voltadas à segurança de sistemas industriais. Nos Estados Unidos, o conjunto de normas NERC-CIP estabelece requisitos rigorosos para a proteção de sistemas de automação em instalações críticas. Na União Europeia, tanto NIS2 quanto o Cyber Resilience Act (CRA) impõem obrigações diretas aos fabricantes de produtos digitais, incluindo equipamentos de automação industrial.

Essas iniciativas estão fundamentadas em normas e frameworks internacionalmente reconhecidos, como a série ISA/IEC 62443, o framework do NIST, a família ISO/IEC 27000, além de diretrizes específicas como a IEC 62351, voltada à segurança de protocolos de automação. A adoção dessas referências permite mitigar riscos relevantes, fortalecer a segurança dos dispositivos de automação e garantir a resiliência das operações industriais frente a ameaças complexas, assegurando a continuidade dos serviços essenciais e a integridade dos dados e sistemas envolvidos.

2. Muito Além da TI: A Nova Fronteira da Segurança Cibernética

Tradicionalmente, o termo "segurança cibernética" se refere ao conjunto de medidas adotadas para proteger sistemas computacionais e redes contra acessos não autorizados ou ataques maliciosos. No entanto, quando aplicado ao contexto das tecnologias de automação e energia, esse conceito se amplia significativamente. Nesse cenário, a segurança cibernética passa a abranger práticas destinadas a garantir a confiabilidade, a integridade e a disponibilidade dos sistemas de controle e automação, princípios amplamente conhecidos no universo da Tecnologia da Informação (TI) pela sigla "CIA" (Confidentiality, Integrity, Availability).

Em ambientes industriais, essas medidas são essenciais para prevenir uma série de riscos, como o vazamento de informações sensíveis, danos físicos a equipamentos ou sistemas, corrupção de dados e interrupções nas operações. Tais incidentes podem comprometer não apenas a eficiência, mas também a segurança de processos críticos.

Na TI, a prioridade costuma ser a confidencialidade dos dados, seguida da integridade e, por fim, da disponibilidade. Já na Tecnologia Operacional (OT), essa ordem se inverte: a disponibilidade é o fator mais importante, seguida da integridade e da confidencialidade. Isso se deve ao fato de que, em ambientes industriais, manter os sistemas em funcionamento contínuo e seguro é mais crucial do que proteger informações contra acessos indevidos.

3. Cyber Resilience Act (CRA)

O Cyber Resilience Act (CRA), formalmente denominado Regulamento (UE) 2024/2847, representa o primeiro marco regulatório horizontal da União Europeia voltado especificamente à cibersegurança de produtos com elementos digitais. Seu propósito é estabelecer um nível consistente de segurança em todo o mercado europeu, exigindo que fabricantes incorporem princípios de *Security by Design* e *Security by Default*, implementem processos estruturados de gestão de vulnerabilidades e garantam a disponibilização de atualizações de segurança durante todo o ciclo de vida do produto.

O regulamento entrou em vigor em 10 de dezembro de 2024, iniciando um período de transição para que fabricantes, importadores e distribuidores adaptem seus processos, produtos e estruturas de governança aos novos requisitos. Um marco importante ocorre em 11 de setembro de 2026, quando passam a ser obrigatórias as exigências de notificação de vulnerabilidades exploradas ativamente e de incidentes graves de segurança, demandando mecanismos formais de monitoramento, resposta e comunicação às autoridades competentes da União Europeia.

A partir de 11 de dezembro de 2027, o CRA torna-se plenamente aplicável. Nessa data, todos os produtos abrangidos pela regulamentação deverão demonstrar conformidade com os requisitos essenciais de segurança cibernética, manter documentação técnica adequada, operar processos efetivos de gestão de vulnerabilidades e concluir as avaliações de conformidade necessárias para obtenção da marcação CE antes de sua comercialização no mercado europeu.

Para os fabricantes, o desafio vai além da adequação regulatória. O CRA exige a consolidação de capacidades organizacionais permanentes relacionadas à segurança de produtos, incluindo desenvolvimento seguro, monitoramento contínuo de vulnerabilidades, coordenação de respostas a incidentes, gestão de atualizações de segurança e governança de cibersegurança ao longo de todo o ciclo de vida do produto. Por essa razão, a preparação prática deve ocorrer significativamente antes de 2027, permitindo que processos, ferramentas e responsabilidades estejam plenamente estabelecidos quando os requisitos passarem a ser mandatórios.

4. Construindo um Futuro Resiliente

Nossa missão de **“Crescimento contínuo e sustentável, mantendo a simplicidade**” reflete nosso compromisso em oferecer tecnologias e soluções que promovam um mundo mais eficiente, conectado e sustentável. Essa visão também orienta nossa atuação na criação de ambientes digitais e industriais mais seguros, resilientes e preparados para os desafios do futuro.

Reconhecemos que a **segurança cibernética** é essencial para garantir a confiabilidade, disponibilidade, integridade e resiliência de produtos, sistemas e soluções digitais. Em um cenário industrial cada vez mais integrado, a proteção cibernética deve ser considerada de forma contínua ao longo de todo o ciclo de vida dos produtos, desde a concepção e desenvolvimento até a operação, manutenção, atualização e suporte.

Nesse contexto, estamos evoluindo nossa estratégia de segurança cibernética com base em dois pilares complementares: de um lado, a adoção progressiva dos princípios de ***Security by Design*** e ***Security by Default*** nos requisitos e funcionalidades de nossos produtos e soluções; de outro, a consolidação de um processo estruturado de desenvolvimento seguro, com evolução contínua da maturidade em práticas de gestão de vulnerabilidades, resposta a incidentes e suporte à operação confiável ao longo de todo o ciclo de vida.

Diante da entrada em vigor do **Cyber Resilience Act (CRA)** da União Europeia, informamos que estamos ativamente engajados no desenvolvimento e implementação de um programa estruturado de **Tratamento de Vulnerabilidades**, com o objetivo de atender integralmente aos requisitos estabelecidos por essa regulamentação dentro dos prazos previstos para sua aplicação.

Entre as principais frentes de atuação da equipe de segurança cibernética em relação a CRA, destacam-se:

- Publicação de um canal de contato único e dedicado para reporte de vulnerabilidades;
- Condução do processo de gestão de vulnerabilidades;
- Resposta coordenada a incidentes de segurança cibernética;
- Comunicação transparente com clientes, parceiros, autoridades e demais partes interessadas;
- Evolução contínua de práticas relacionadas à divulgação coordenada de vulnerabilidades;
- Gestão de riscos em produtos conectados, componentes de terceiros e ecossistemas digitais industriais;
- Fortalecimento da resiliência operacional e cibernética ao longo do ciclo de vida dos produtos.

Nosso compromisso vai além da conformidade regulatória. Buscamos desenvolver tecnologias que apoiem operações mais seguras, resilientes, eficientes e sustentáveis, contribuindo para a construção da confiança digital necessária para a indústria e a sociedade do futuro. Essa evolução considera requisitos regulatórios, referências normativas e boas práticas amplamente reconhecidas no campo da segurança cibernética para produtos conectados e ambientes industriais.

Cada projeto, produto e solução WEG carrega o propósito de evoluir continuamente em confiabilidade, inovação e resiliência cibernética, apoiando nossos clientes e parceiros em um mundo cada vez mais conectado e digital.

O escopo de soluções do Grupo WEG não se limita aos produtos e soluções apresentados nesse catálogo.
Para conhecer nosso portfólio, consulte-nos.

Conheça as operações mundiais da WEG

www.weg.net

+55 47 3276.4000
cybersecurity@weg.net
Jaraguá do Sul - SC - Brasil

Cód: 10014764162 | Rev: 00 | Data (m/a): 06/2025.