Infraestrutura antiga não oferece recursos necessários para segurança cibernética

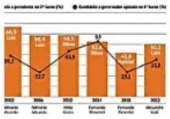
Serviços como os de fornecimento de energia ou água têm o desafio de modernizar equipamentos de uma forma que não aumente o risco de interrupções em operações essenciais à população

Por Emilio Sant'Anna — De São Paulo
30/06/2026 05h02 · Atualizado 30/06/2026 05h03

Sistemas de automação, plataformas de supervisão, redes de telecomunicações e equipamentos industriais são projetados para funcionar por décadas. Parte dessa infraestrutura em operação, porém, vem de uma época e de ambientes com pouca conectividade e sem mecanismos nativos de segurança cibernética. A atualização dessa infraestrutura é um processo que exige planejamento e cautela, pois sustenta operações essenciais que não podem ser simplesmente interrompidas, como o fornecimento de energia ou água.

O caminho, dizem especialistas do setor, combina a realização de inventários, manutenção, controles de acesso, segmentação, monitoramento e renovação por etapas. O tempo de uso, sozinho, não define se um ativo deve ser descartado. O que pesa é a capacidade de mantê-lo confiável e protegido.

Leia também:



Lula precisa mesmo de palanque em Minas?

FT: Uma adolescente se encaminha para ser a próxima ditadora da Coreia do Norte

"O desafio não está necessariamente na idade do equipamento, mas em garantir que ele continue operando de forma segura, integrada e aderente aos requisitos regulatórios e operacionais do setor", afirma Luís Henrique Ferreira Pinto, vice-presidente de operações reguladas da CPFL Energia.

A substituição não depende apenas da disponibilidade de uma tecnologia mais nova. Sistemas operacionais estão ligados a equipamentos físicos que executam funções críticas e qualquer mudança exige testes, compatibilidade tecnológica, planejamento regulatório e redução do risco de interrupção. Na CPFL, segundo Pinto, a modernização ocorre de forma gradual e estruturada, por etapas, para permitir validações técnicas e operacionais. A companhia considera o quão crítico é o ativo, os riscos operacionais e cibernéticos, a defasagem, os ganhos de eficiência, as exigências regulatórias e o impacto para os clientes. "A segurança precisa caminhar junto com a continuidade operacional."

> **"A segurança precisa caminhar junto com a continuidade operacional"**
>
> — Luís Pinto

No saneamento, o dilema é semelhante e se espalha por uma infraestrutura extensa de estações de tratamento, elevatórias, redes de distribuição e coleta, centros de controle e equipamentos eletromecânicos. Eduardo Mendes, diretor de tecnologia da Aegea, diz que tecnologias antigas e recentes convivem em ambientes híbridos porque a renovação precisa ser compatível com a continuidade da operação. "Trata-se de um serviço que não pode parar", afirma.

Diferentemente de outros setores, em que a substituição tecnológica pode ocorrer em ciclos mais curtos, no saneamento é comum que equipamentos mais antigos convivam com tecnologias mais recentes. "Na Aegea, essa evolução ocorre de forma estruturada, temos ciência da importância de mantermos a população abastecida e não causar grandes pausas ou riscos na operação", afirma Mendes. "O plano leva em consideração o mapa de ativos críticos e riscos de ruptura operacional. Com base nele priorizamos as trocas."

O ponto de partida para proteger o legado é saber exatamente o que está conectado e qual função cada equipamento exerce. "Nós só protegemos o que conseguimos enxergar", afirma Caio Colman, diretor de segurança da informação (CISO) da Siemens Brasil. Segundo ele, os sistemas industriais antigos eram concebidos sem segurança nativa, operavam de forma isolada e priorizavam disponibilidade e durabilidade. Muitos ainda usam sistemas operacionais obsoletos e protocolos de comunicação inseguros, enquanto seu ciclo de vida foi projetado para cerca de 20 anos, bem mais longo do que o dos sistemas corporativos.

O inventário de ativos e a avaliação de riscos vêm antes da escolha de uma ferramenta. A partir desse diagnóstico, as empresas podem priorizar vulnerabilidades e adotar segmentação de rede, endurecimento de sistemas e monitoramento contínuo, explica.

Nem sempre, porém, é possível corrigir diretamente a falha. Quando um sistema não recebe mais atualizações, entram em cena os chamados controles compensatórios, também chamados de correções virtuais. Firewalls industriais, segmentação e monitoramento formam uma barreira externa ao equipamento vulnerável. Colman ressalta que esses mecanismos ajudam a mitigar uma possível exploração, mas "não eliminam a vulnerabilidade".

Operadores precisam de monitoramento remoto, dados em tempo real e integração entre unidades. O desafio é conectar apenas o necessário. Ao mesmo tempo em que cria novas exposições, a conectividade também traz resiliência. Na Aegea, sensores, telemetria e plataformas de supervisão acompanham os ativos em tempo real e ajudam a antecipar falhas.

‹ Mais recente

Próxima **Banco mira comportamentos, não s...** ›

Conteúdo Publicitário

Perda de memória não é causado pela idade: basta parar de comer esses 3 alimentos

Portal + Saúde | Patrocinado

Facas ultraafiadas: 10x mais poder de corte em apenas segundos

Facas sem corte nunca mais. Com o Afiador Kenshin Pro, você recupera o fio …

Afiador Japonês Potente | Patrocinado

Leia mais

Gigante japonesa faz liquidação histórica no Brasil.

Nimbus gel 27 reúne leveza, amortecimento avançado e visual moder…

Loja Autorizada | Patrocinado

Saiba Mais