

GUIA TÉCNICO • EDIÇÃO OUTUBRO 2026

Como proteger a refrigeração

Segurança e contingência dos supervisórios.
Como proteger o acesso, atualizar os equipamentos
e recuperar a operação com segurança.

PARA TI, MANUTENÇÃO E GESTÃO DA OPERAÇÃO

Rafael Cocchiaro

Head of Tech | Digital Tech

15 de outubro de 2026 • Versão 2.0

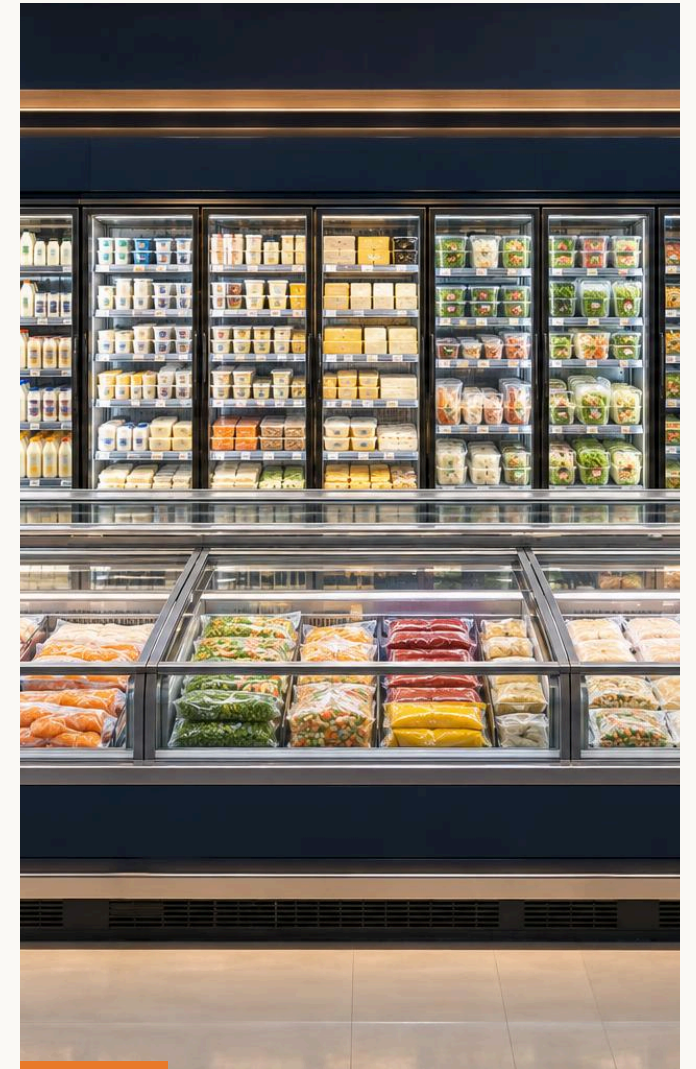


RESUMO EXECUTIVO • LEITURA RÁPIDA

O que vocês precisam garantir em cada loja

Estas são as prioridades para decidir e cobrar a execução.
As próximas páginas detalham modelos, versões e procedimentos.

- 01 **Proteger o acesso remoto**
Retirem as interfaces de administração da internet pública e usem VPN ou rede protegida.
Alinhem a mudança com a Estech para preservar as leituras.
- 02 **Atualizar ou substituir**
Confirmem modelo e firmware: atualizem Danfoss 800A e XWEB PRO conforme o fabricante.
Para equipamentos sem suporte, como XWEB EVO, aprovem a migração.
- 03 **Ter backup que já foi restaurado**
Guardem cópias da configuração fora do equipamento e da loja.
Testem a restauração de verdade e registrem o resultado e o tempo de recuperação.
- 04 **Definir responsável e frequência**
Adotem revisão a cada 3, 6 ou 12 meses, conforme criticidade e capacidade.
Alertas críticos e mudanças relevantes exigem ação fora do calendário.
- 05 **Preparar a resposta ao incidente**
Protejam os produtos, isolem o acesso remoto e acionem TI, integrador e Estech.
Antes da reconexão, reconstruam e validem o equipamento conforme o fabricante.



NAVEGAÇÃO

Sumário

Escolham um tema para ir diretamente à página.
O botão Sumário, no rodapé, traz vocês de volta.

02	Resumo executivo	➤	04	O alerta e a prioridade	➤
05	Modelos AK-SM 800A	➤	06	Faixas de firmware vulneráveis	➤
07	Modelos antigos e substituição	➤	08	Onde buscar a atualização	➤
09	XWEB EVO e PRO: versões e suporte	➤	10	Acesso remoto protegido	➤
11	Mudança sem perder leitura	➤	12	O que incluir no backup	➤
13	Onde guardar as cópias	➤	14	Como testar a restauração	➤
15	Revisões a cada 3, 6 ou 12 meses	➤	16	Responsáveis e evidências	➤
17	Primeira resposta ao incidente	➤	18	Reconstrução do zero	➤
19	Critérios para voltar à operação	➤	20	Fontes e contato	➤



01 • ENTENDER O RISCO

Retirem o acesso aberto à internet

O CERT-FR relatou comprometimentos de supervisórios de refrigeração. A primeira medida é impedir acesso público às interfaces de administração.

01 Famílias citadas no alerta

Danfoss AK-SM e AK-SC, além de Copeland/Dixell XWEB.
O alerta foi publicado em 12/10/2026 e ampliado em 13/10/2026.

02 Proteção permanente

Use VPN, uma conexão privada protegida, ou outra rede protegida.
Filtro por IP serve só como medida temporária, até a VPN ficar pronta.

03 Se houver comprometimento

Isolem o acesso e planejem a recuperação de fábrica com o integrador.
Um reset sozinho não corrige uma falha de segurança.



02 • IDENTIFICAR O EQUIPAMENTO

AK-SM 800A: confirmam cada modelo

A família 800A inclui os modelos abaixo.
A letra A faz parte do modelo e muda a orientação de atualização.

MODELO	FAIXA COM FALHAS PUBLICADAS ¹	AÇÃO
AK-SM 820A	Anterior a 4.3.1	Atualizar pela página oficial
AK-SM 850A	Anterior a 4.3.1	Atualizar pela página oficial
AK-SM 880A	Anterior a 4.3.1	Atualizar pela página oficial

¹ Nos boletins consultados, os limites são comuns à série 8xxA.
As falhas específicas e seus limites estão na próxima página.
Incluem versões especiais, como a de retrofit TP78 (rede antiga de controladores), conforme o código na etiqueta.



03 • CONFERIR A VERSÃO

Quais firmwares estão vulneráveis?

Os limites abaixo valem para AK-SM 820A, 850A e 880A.
 “Anterior a” inclui todas as versões abaixo do número indicado.

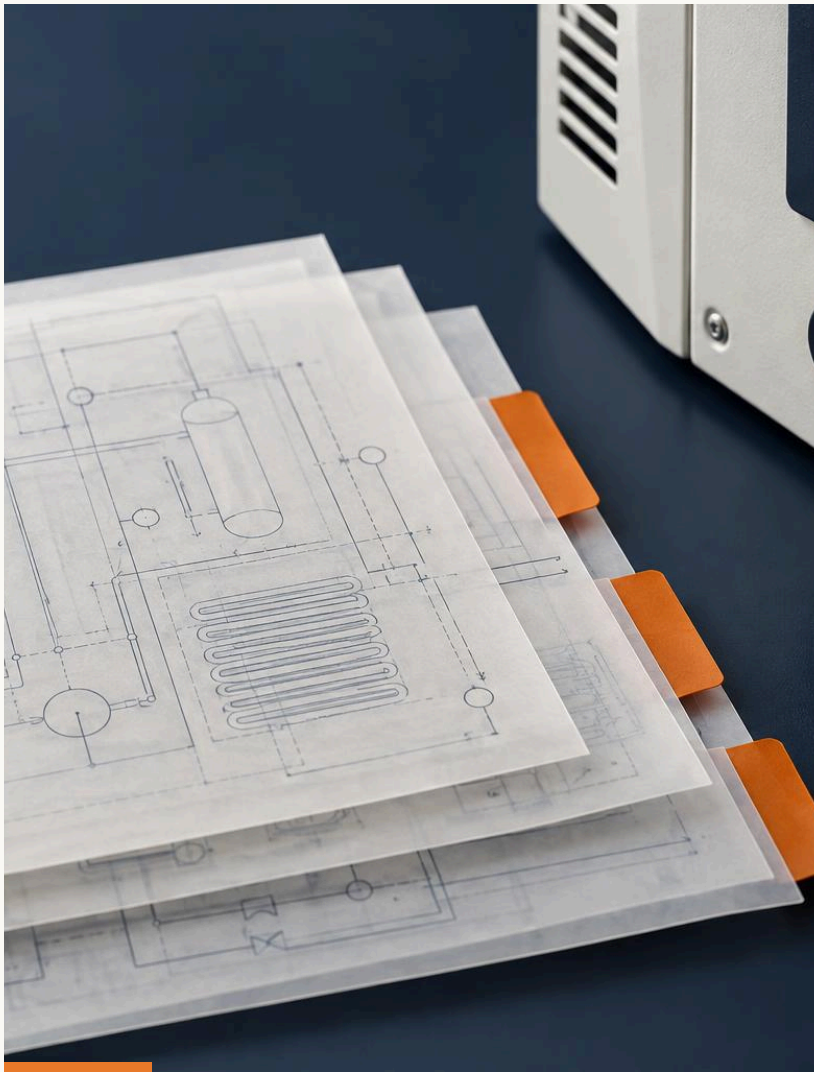
FIRMWARE AFETADO	FALHAS PUBLICADAS (CVE) ¹	PRIMEIRA CORREÇÃO
Anterior a 3.3	2023-25913, 2023-25914 e 2023-25915	3.3
Anterior a 4.2	2025-41450	4.2
Anterior a 4.3.1	2025-41451 e 2025-41452	4.3.1

As faixas se sobrepõem.

A versão 4.2 ainda é afetada pelas falhas corrigidas em 4.3.1.
 Atualizem para a versão atual compatível, seguindo a sequência do fabricante; o mínimo histórico não é uma recomendação para parar de atualizar.

¹ CVE é o identificador público de uma falha.
 Esta matriz reúne os boletins AK-SM 800A consultados em 15/10/2026; não identifica qual falha foi usada em cada incidente.

Fontes: DSA-2023-08-01 ↗ · DSA-2025-03-01 ↗ · DSA-2025-08-01 ↗



04 • TRATAR EQUIPAMENTOS ANTIGOS

Sem correção disponível, planejem a substituição

Não apliquem o firmware do 800A em um modelo antigo.
A Danfoss informa encerramento de serviço para as famílias legadas abaixo.

MODELO / FAMÍLIA	FIRMWARE DE SEGURANÇA	ENCAMINHAMENTO
AK-SM 820, 850 e 880 Família 800, sem A	Sem versão corretiva indicada nas fontes consultadas	Isolar e migrar
AK-SC 255 e AK-SC 355	Sem versão corretiva indicada nas fontes consultadas	Isolar e substituir
AK-SM 350 e AK-SM 720	Famílias com serviço encerrado	Avaliar migração com a Danfoss

O CERT-FR não detalha modelos nem firmwares da série AK-SC.
Não é possível declarar uma versão “segura” dessa série com base no alerta.
Para legados, confirmem a situação pelo código do produto com o suporte Danfoss.
A lista acima não equivale a uma lista de CVEs por modelo.



05 • ATUALIZAR COM CONTROLE

Baixem somente da fonte oficial

Para AK-SM 820A, 850A e 880A, usem a página Danfoss da série 800A. Em 15/10/2026, ela lista o pacote 5.3.x e o sistema Danux 4.14.017.194.

01 AK-SM 800A: software e sistema operacional

Abrir downloads oficiais Danfoss ↗.

Leiam as instruções, os pré-requisitos e a compatibilidade antes de instalar.

02 AK-SM antigo / AK-SC: suporte e migração

Falar com a Danfoss ↗.

Informem modelo, código, versão e fotos da etiqueta.

Não usem arquivos de fóruns ou de outro modelo.

03 Copeland / Dixell XWEB: trilha própria

Abrir System Software Updates ↗.

Selecione a família exata e confirmem a correção com o fabricante; não extrapolem a matriz AK para XWEB.

Firmware é o software interno do equipamento.

Danux é o sistema operacional do 800A.

Registrem as duas versões e sigam a ordem de instalação exigida nas notas do pacote.

Danfoss · downloads e instruções ↗



06 • COPELAND / DIXELL XWEB

XWEB EVO e PRO: confirmam versões e suporte

O alerta oficial também inclui Copeland/Dixell XWEB.
O CERT-FR não separa EVO e PRO nem informa versões; os detalhes abaixo vêm da Copeland.

FAMÍLIA E MODELOS	FIRMWARE / SUPORTE	ORIENTAÇÃO
XWEB 300D PRO XWEB 500D PRO XWEB 500B PRO	Falhas publicadas em versões até 1.12.1, inclusive.	Atualizar para 1.13.0 ou versão posterior compatível. A versão 1.13 trata as falhas identificadas no boletim de fevereiro/2026.
XWEB 300D EVO XWEB 500D EVO XWEB 500 EVO	Sem versão segura indicada no alerta. Suporte de software encerrado em 16/03/2026.	Manter isolado da internet pública e planejar migração para PRO. Arquivos antigos não comprovam correção de segurança.
XWEB 3000 EVO XWEB 5000 EVO	Mesma condição de fim de suporte da família EVO.	Isolar e substituir por solução com suporte. O firmware PRO não se aplica ao EVO.

PRO: atenção à sequência. Na atualização manual, versões até 1.2.1 exigem passar pela 1.3.0 antes da 1.13.0. Confirmam o procedimento do modelo, façam backup e validem a restauração com o integrador.

Downloads oficiais: selecionem a família e o modelo exatos ↗

Fontes: CERT-FR ↗ · Copeland: modelos e versões ↗ · PRO 1.13 ↗ · EVO: fim do suporte ↗ · Sequência de atualização ↗



07 • PROTEGER A CONEXÃO

Acesso remoto por VPN ou rede protegida

A TI deve separar a rede de refrigeração e liberar somente os acessos necessários. A administração do roteador e do modem exige o mesmo cuidado.

- 01 **Conexão permanente**
Use VPN ou rede protegida, contas individuais e autenticação adicional quando disponível. Separem a refrigeração do Wi-Fi e dos computadores da loja.
- 02 **Medida emergencial**
Se precisarem de filtro por IP até concluir a VPN, limitem origens, portas e prazo. Registrem quem aprovou e a data de migração.
- 03 **Origens do NEO 360**
Peçam à Estech a lista de origens antes de fechar o acesso. Assim as leituras continuam chegando depois da mudança.

Desativem serviços sem uso e troquem senhas de fábrica.
HTTPS, a conexão web criptografada, protege a comunicação, mas não substitui atualização e restrição de acesso.



08 • PLANEJAR A MUDANÇA

Fechem o acesso sem perder o monitoramento

TI, integrador e Estech devem combinar a mudança e verificar o resultado antes de encerrar a manutenção.

01 Antes da janela

Registrem modelo, firmware e conexão atual.

Façam backup, definam como voltar à configuração anterior e mantenham um técnico local disponível.

02 Durante a execução

Criem o caminho protegido e testem as integrações.

No 800A, confirmem que o nível de segurança está em Strict (rigoroso), que exige HTTPS e controle de sessão.

03 Antes de dar o aceite

Confirmem que a interface não está aberta ao público e que as leituras, os alarmes e a comunicação com o NEO 360 continuam funcionando.

Se o monitoramento ficar interrompido, a gerência deve executar rondas locais de temperatura na frequência aprovada pela qualidade.

Registrem início, fim e responsável pela interrupção.

Danfoss · modo Strict e integrações ↗



09 • PREPARAR A RECUPERAÇÃO

O backup precisa permitir reconstruir a configuração

Exportem a configuração de cada supervisório antes de atualizar e sempre que alterarem parâmetros relevantes.

01 Parâmetros da operação

Incluem temperaturas programadas (setpoints), horários e limites de degelo, alarmes, agendas, sensores e vínculos com os controladores.

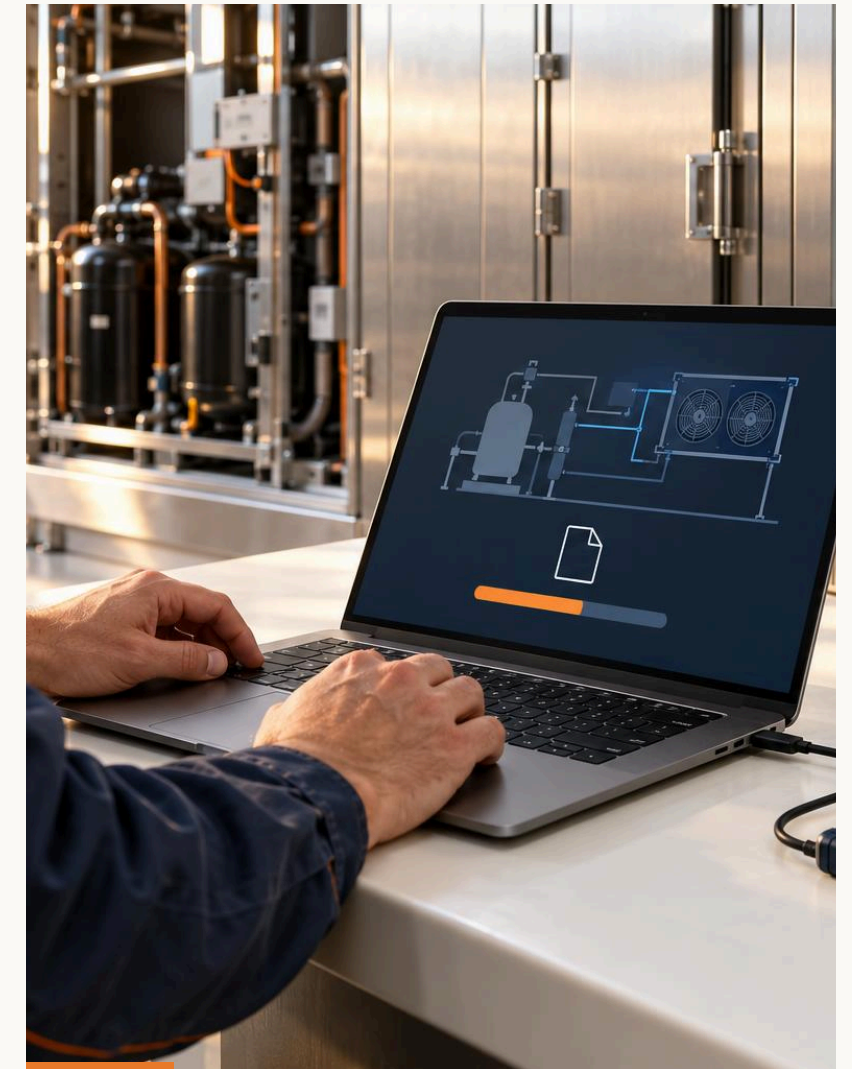
02 Arquivos e dependências

Guardem a exportação original, arquivos de dispositivos, licenças quando aplicáveis, versões, manual e instaladores oficiais necessários à recuperação.

03 Identificação e instruções

Registrem loja, modelo, número de série, data, autor e procedimento de restauração. Mantenham senhas e chaves em cofre de credenciais separado.

Confirmem no manual o que a exportação inclui.
A cópia do supervisório pode não conter a configuração de cada controlador de campo.
Salvem essas configurações separadamente quando necessário.



10 • GUARDAR COM SEGURANÇA

Mantenham cópias fora do equipamento e da loja

A Estech recomenda a regra 3-2-1 como referência: três cópias no total, em dois meios de armazenamento, com uma cópia fora do local.

01 Proteção contra alteração

Mantenham ao menos uma cópia desconectada ou protegida contra modificação.
Opcional: usem criptografia, isto é, proteção que exige uma chave para leitura.

02 Acesso controlado

Restrinjam o acesso à TI e aos responsáveis autorizados.
Guardem as chaves em cofre separado, com acesso de emergência testado.

03 Histórico de versões

Preservem a configuração atual aprovada e versões anteriores.
Depois de um incidente, escolham uma cópia anterior à alteração indevida e verifiquem seu conteúdo.

Definam prazo de retenção e confirmem se as cópias abrem.

Uma cópia guardada somente no notebook do integrador ou no próprio supervisor deixa a recuperação dependente de um único ponto.



11 • PROVAR QUE FUNCIONA

Façam uma restauração de verdade

Um arquivo exportado não comprova que a recuperação funciona.
O teste precisa carregar a cópia em um ambiente compatível e validar o resultado.

01 Preparar o teste

Use equipamento de reserva compatível ou ambiente homologado pelo fabricante.
Se só houver a unidade em operação, reservem uma janela supervisionada e um plano de retorno.

02 Restaurar e conferir

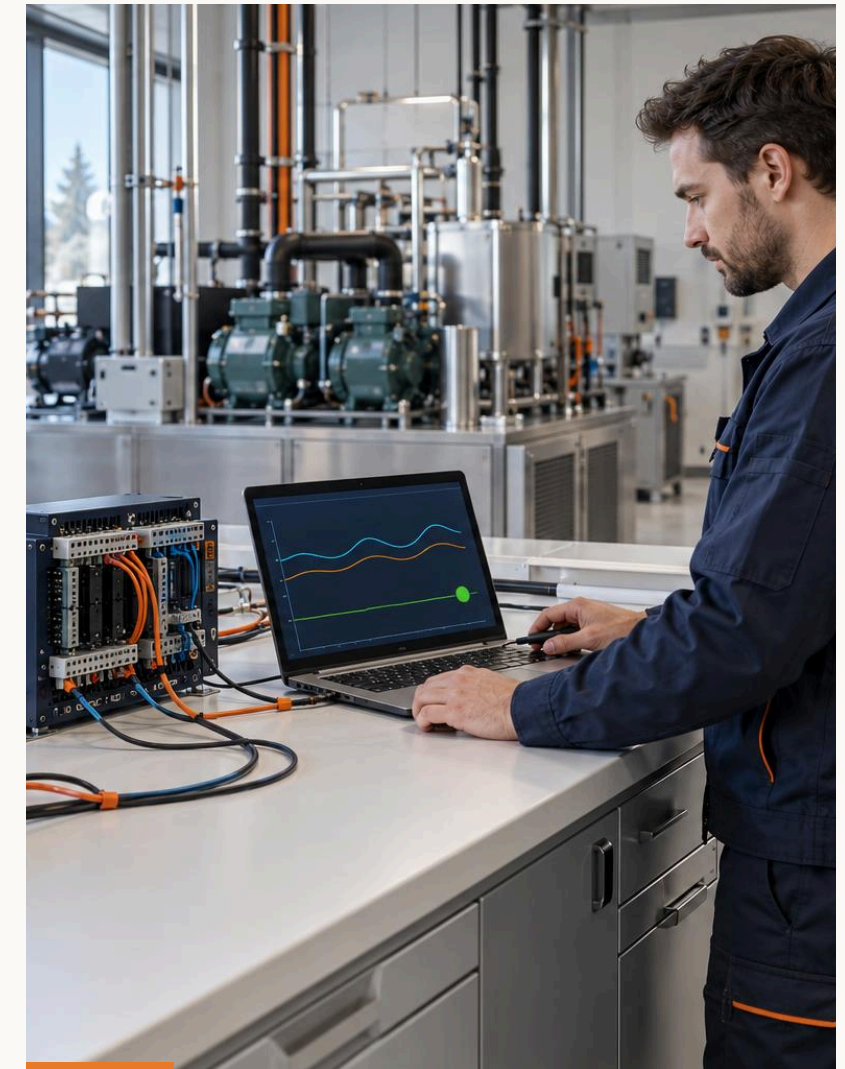
Restauram a configuração e comparem sensores, horários, alarmes, acessos e parâmetros.
Verifiquem também a comunicação com os controladores e o NEO 360.

03 Registrar e corrigir

Anotem arquivo e versão usados, duração, divergências e responsáveis.
Se falhar, corrijam o processo e repitam até obter o aceite.

Simulador ajuda a preparar, mas não substitui sozinho o teste no equipamento quando a recuperação depende de interfaces físicas.

O ensaio não deve acionar degelo ou alterar a refrigeração de uma loja em funcionamento.



12 • DEFINIR A FREQUÊNCIA

Escolham um ciclo de 3, 6 ou 12 meses

As frequências abaixo são recomendações da Estech.

A decisão deve considerar criticidade, capacidade da equipe e tempo aceitável de recuperação.

3 meses

Operação crítica

Muitas lojas, maior impacto de parada ou equipamentos antigos.
Revisão completa e teste real de restauração a cada ciclo.

6 meses

Rotina recomendada

Estrutura intermediária.
Revisão completa e teste real de restauração semestral, com responsáveis definidos.

12 meses

Capacidade limitada

Limite proposto para operação de menor criticidade, com risco aceito pela gestão e teste real anual.

Não esperem o próximo ciclo para tratar um alerta crítico.

Atualizem o backup em cada revisão e após mudanças aprovadas.
Reavaliem acesso e recuperação ao trocar equipamento, integrador, rede ou firmware.
Apliquem correções conforme os boletins e a compatibilidade, sem esperar o calendário.



13 • DAR RESPONSABILIDADE

Cada loja precisa de um responsável e evidências

A gestão aprova o ciclo e a prioridade.

A TI coordena a rotina e registra o que foi verificado com o integrador e a operação.

RESPONSÁVEL	ENTREGA QUE PRECISA FICAR REGISTRADA
Gestão da operação	Criticidade, frequência, orçamento, prazo e aceite dos riscos pendentes.
TI de vocês	Inventário, regras de acesso, contas, local das cópias e próxima revisão.
Integrador / fabricante	Compatibilidade, atualização, exportação e teste real de restauração.
Gerência / qualidade	Contatos, proteção dos produtos e validação da operação local.
Estech	Conferência da integração e do retorno das leituras no NEO 360, conforme escopo combinado.

Ficha por loja: ativo e série · firmware e Danux · responsável e substituto · localização do backup · último restore e duração · falhas pendentes · prazo · evidência de aceite · próxima revisão.



14 • RESPONDER AO INCIDENTE

Protejam os produtos e isolem o acesso remoto

Degelos fora de horário, alterações sem autorização ou aquecimento simultâneo exigem verificação imediata.

Não esperem a confirmação de um ataque.

01 Gerência e qualidade: agir imediatamente

Confirmam temperaturas com medição local, mantenham portas fechadas e sigam o plano de proteção ou transferência dos produtos. Registrem horários.

02 TI e integrador: conter a entrada

Isolem o caminho de acesso remoto identificado.

Não desliguem rack, controladores ou cabos sem identificar a função, pois isso pode afetar o controle da refrigeração.

03 Equipe responsável: acionar e preservar

Acionem TI, integrador e Estech.

Preservem registros de acesso e fotos antes do reset, se isso não atrasar a proteção da operação.

Os sinais também podem ter causas operacionais.

A equipe deve investigar sem presumir a origem.

Na interrupção da leitura remota, mantenham a verificação local de temperatura.



15 • RECUPERAR DO ZERO

Reconstruam o equipamento antes de reconectar

Após comprometimento, o integrador deve executar a recuperação de fábrica prevista pelo fabricante,
com o equipamento isolado e a operação protegida.

1. **Preservar e preparar.** Guardem evidências e confirmem cópia confiável, versões, licenças e recursos para recuperação.
2. **Restaurar de fábrica.** Executem o reset e a reinstalação oficial quando prevista.
"Formatar" não é um procedimento universal: sigam o método do modelo.
3. **Corrigir e reconfigurar.** Instalem os pacotes oficiais na ordem do fabricante, troquem credenciais e carreguem uma configuração anterior ao incidente, já conferida.
4. **Validar isolado.** Confiram parâmetros, contas, comunicação e funções locais.
Apliquem os critérios de aceite da próxima página.
5. **Reconectar protegido.** Usem VPN ou rede protegida e acompanhem a operação com a Estech e a gerência.

Se não houver firmware com suporte, um reset deixa o equipamento exposto à mesma falha.
Mantenham o isolamento e aprovelem a substituição.
Não restaurem uma configuração suspeita sem revisão.



16 • DAR O ACEITE

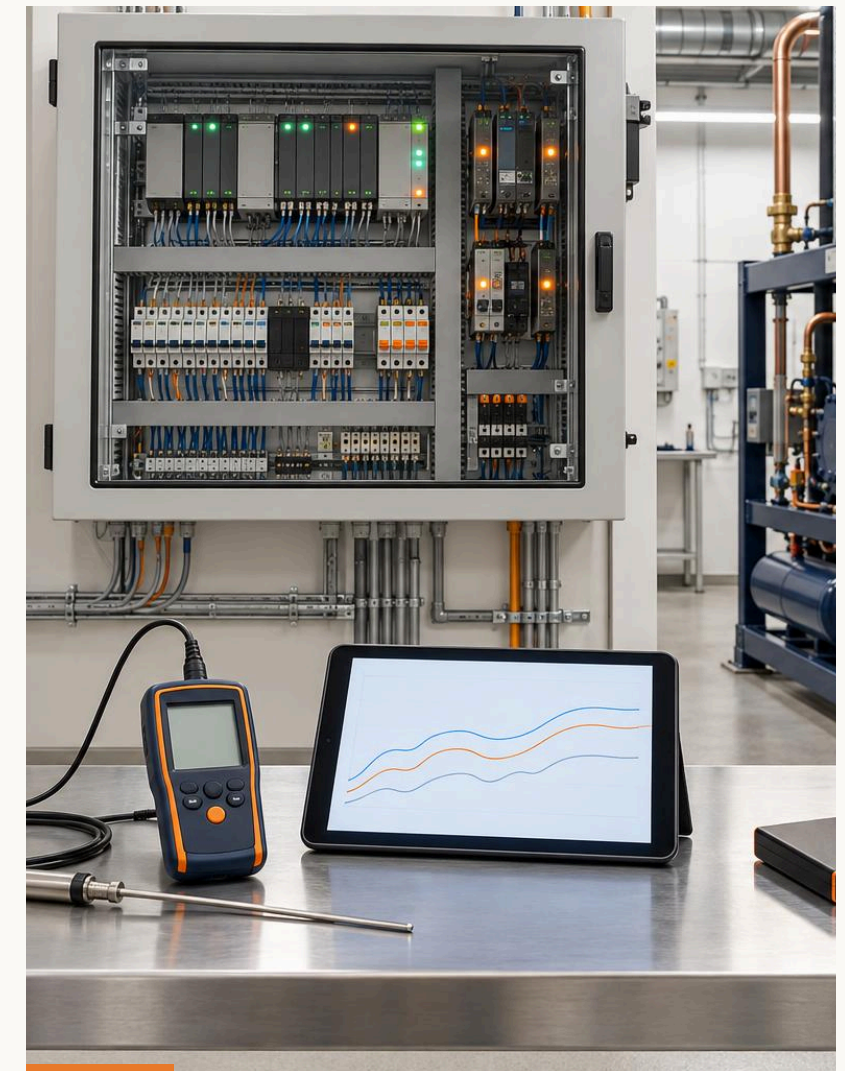
Só encerrem depois de verificar a operação

TI, integrador e gerência devem registrar o aceite.

Combinem com a Estech a verificação do retorno do monitoramento.

- 🌐 Modelo e versões documentados, com correções aplicáveis ou isolamento aprovado para substituição.
- 🌐 Interface sem acesso público; caminho protegido e acessos autorizados conferidos.
- 🌐 Contas revisadas e senhas trocadas após o incidente, incluindo roteador e acesso remoto.
- 🌐 Temperaturas programadas, degelos e alarmes comparados com a configuração aprovada.
- 🌐 Leituras e comunicação no NEO 360 conferidas; teste seguro de alarme combinado com a operação.
- 🌐 Novo backup protegido, teste de restauração registrado e próxima revisão agendada.

Definam antes da intervenção o tempo máximo aceitável sem supervisorio e o tempo máximo sem leitura. Meçam a recuperação e estabeleçam o período de acompanhamento conforme a criticidade da loja.



REFERÊNCIAS • CONTATO

Fontes para consulta e próximos passos

Comecem pelo inventário de cada loja.

Priorizem exposição à internet, equipamentos sem suporte e ausência de cópia testada.

- 01 CERT-FR · alerta CERTFR-2026-ALE-012 ↗
- 02 Danfoss · boletins DSA de segurança ↗
- 03 Danfoss · software e Danux do AK-SM 800A ↗
- 04 Danfoss · fim de serviço de modelos antigos ↗
- 05 Copeland / Dixell · atualizações XWEB ↗
- 06 Copeland · modelos e versões afetadas ↗
- 07 Copeland · fim do suporte da família EVO ↗

SUPORTE ESTECH / JORNADA NEO

help@neoestech.com

Para incidentes, acionem também os contatos de emergência já acordados com a operação de vocês.

Rafael Cocchiaro | Head of Tech | Digital Tech

