GUÍA TÉCNICA • EDICIÓN OCTUBRE 2026

Cómo proteger su refrigeración

Seguridad y contingencia de los sistemas de supervisión. Cómo proteger el acceso, actualizar los equipos y recuperar la operación con seguridad.

PARA TI, MANTENIMIENTO Y GESTIÓN DE LA OPERACIÓN



Rafael Cocchiaro

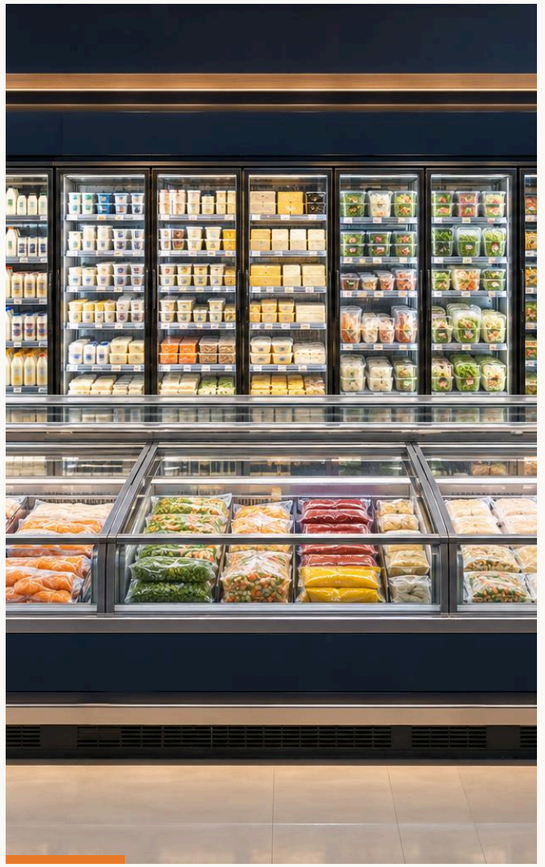
Head of Tech | Digital Tech

15 de octubre de 2026 · Versión 2.0

RESUMEN EJECUTIVO • LECTURA RÁPIDA

Lo que ustedes deben garantizar en cada tienda

Estas son las prioridades para decidir y exigir la ejecución.
Las páginas siguientes detallan modelos, versiones y procedimientos.



01 **Proteger el acceso remoto**

Retiren las interfaces de administración de internet pública y usen VPN o red protegida.
Coordinen el cambio con Estech para preservar las lecturas.

02 **Actualizar o sustituir**

Verifiquen modelo y firmware: actualicen Danfoss 800A y XWEB PRO según el fabricante.
Para equipos sin soporte, como XWEB EVO, aprueben la migración.

03 **Tener un backup ya restaurado**

Guarden copias de la configuración fuera del equipo y de la tienda.
Prueben la restauración de verdad y registren el resultado y el tiempo de recuperación.

04 **Definir responsable y frecuencia**

Adopten una revisión cada 3, 6 o 12 meses, según criticidad y capacidad.
Las alertas críticas y los cambios relevantes exigen acción fuera del calendario.

05 **Preparar la respuesta al incidente**

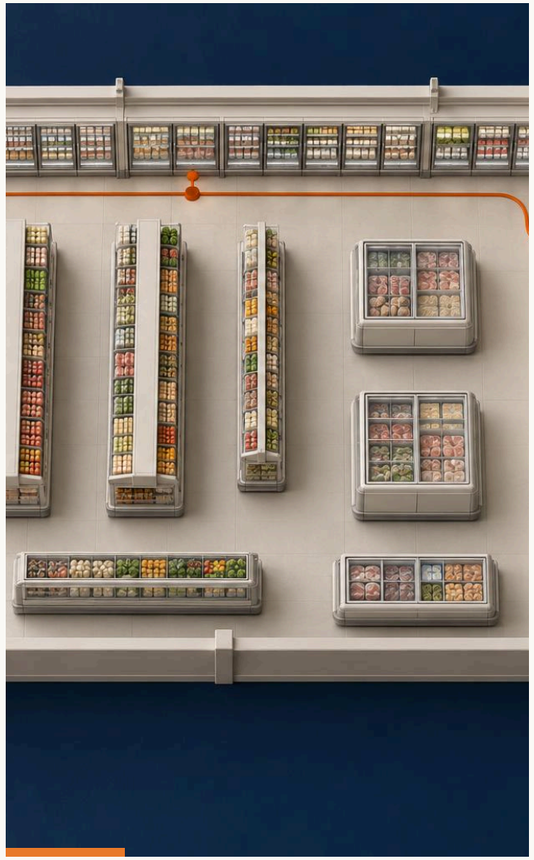
Protejan los productos, aíslen el acceso remoto y avisen a TI, al integrador y a Estech.
Antes de reconectar, reconstruyan y validen el equipo según el fabricante.

NAVEGACIÓN

Índice

Elijan un tema para ir directamente a la página.
El botón Índice, en el pie de página, los trae de vuelta.

02 Resumen ejecutivo
04 La alerta y la prioridad
05 Modelos AK-SM 800A
06 Rangos de firmware vulnerables
07 Modelos antiguos y sustitución
08 Dónde obtener la actualización
09 XWEB EVO y PRO: versiones y soporte
10 Acceso remoto protegido
11 Cambio sin perder lecturas
12 Qué incluir en el backup
13 Dónde guardar las copias
14 Cómo probar la restauración
15 Revisiones cada 3, 6 o 12 meses
16 Responsables y evidencias
17 Primera respuesta al incidente
18 Reconstrucción desde cero
19 Criterios para volver a operar
20 Fuentes y contacto



01 • ENTENDER EL RIESGO

Eliminen el acceso abierto a internet

El CERT-FR reportó intrusiones en sistemas de supervisión de refrigeración.
La primera medida es impedir el acceso público a las interfaces de administración.

01 **Familias citadas en la alerta**

Danfoss AK-SM y AK-SC, además de Copeland/Dixell XWEB.
La alerta se publicó el 12/10/2026 y se amplió el 13/10/2026.

02 **Protección permanente**

Usen VPN, una conexión privada protegida, u otra red protegida.
El filtrado por IP sirve solo como medida temporal, hasta que la VPN esté lista.

03 **Si hay una intrusión**

Aíslen el acceso y planifiquen la recuperación de fábrica con el integrador.
Un restablecimiento por sí solo no corrige una falla de seguridad.



CERT-FR · CERTFR-2026-ALE-012 ↗

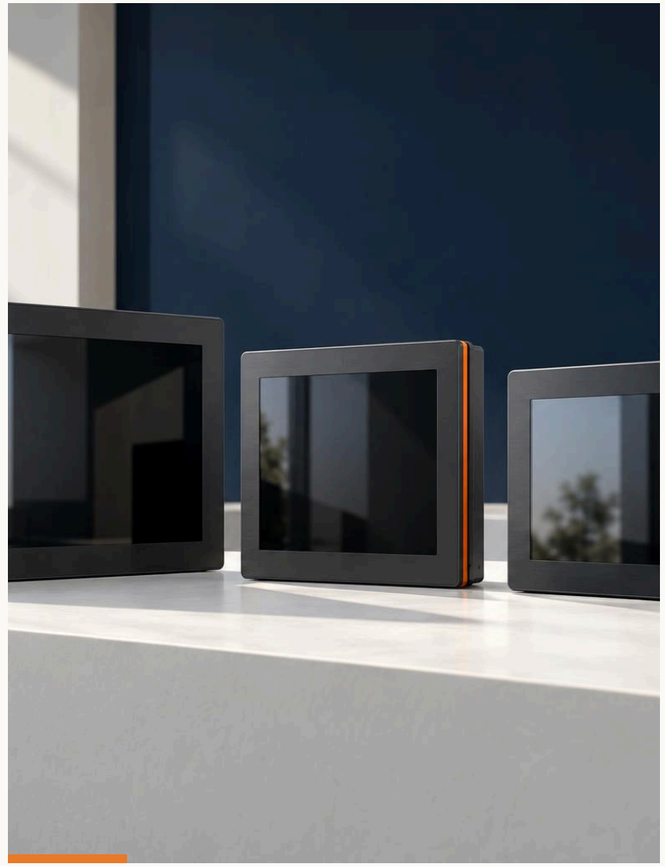
02 • IDENTIFICAR EL EQUIPO

AK-SM 800A: verifiquen cada modelo

La familia 800A incluye los modelos siguientes.
La letra A forma parte del modelo y cambia la guía de actualización.

MODELO	RANGO CON FALLAS PUBLICADAS[1]	ACCIÓN
AK-SM 820A	Anterior a 4.3.1	Actualizar en la página oficial
AK-SM 850A	Anterior a 4.3.1	Actualizar en la página oficial
AK-SM 880A	Anterior a 4.3.1	Actualizar en la página oficial

[1] En los boletines consultados, los límites son comunes a la serie 8xxA.
Las fallas específicas y sus límites están en la página siguiente.
Incluyan versiones especiales, como la de retrofit TP78 (red antigua de controladores), según el código de la etiqueta.



Catálogo Danfoss ↗ · Boletines de seguridad ↗

03 • VERIFICAR LA VERSIÓN

¿Qué firmwares son vulnerables?

Los límites siguientes valen para AK-SM 820A, 850A y 880A.
“Anterior a” incluye todas las versiones por debajo del número indicado.

FIRMWARE AFECTADO	FALLAS PUBLICADAS (CVE)[1]	PRIMERA CORRECCIÓN
Anterior a 3.3	2023-25913, 2023-25914 y 2023-25915	3.3
Anterior a 4.2	2025-41450	4.2
Anterior a 4.3.1	2025-41451 y 2025-41452	4.3.1

Los rangos se superponen.
La versión 4.2 todavía está afectada por las fallas corregidas en 4.3.1.
Actualicen a la versión actual compatible, siguiendo la secuencia del fabricante; el mínimo histórico no es una recomendación para dejar de actualizar.



[1] CVE es el identificador público de una falla.
Esta matriz reúne los boletines AK-SM 800A consultados el 15/10/2026; no identifica qué falla se usó en cada incidente.

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

04 • TRATAR EQUIPOS ANTIGUOS

Sin corrección disponible, planifiquen la sustitución

No apliquen el firmware del 800A en un modelo antiguo.
Danfoss informa el fin de servicio de las familias heredadas siguientes.

MODELO / FAMILIA	FIRMWARE DE SEGURIDAD	ACCIÓN
AK-SM 820, 850 y 880 Familia 800, sin A	Sin versión correctiva en las fuentes consultadas	Aislar y migrar
AK-SC 255 y AK-SC 355	Sin versión correctiva en las fuentes consultadas	Aislar y sustituir
AK-SM 350 y AK-SM 720	Familias con servicio finalizado	Evaluar migración con Danfoss

El CERT-FR no detalla modelos ni firmwares de la serie AK-SC.
No es posible declarar una versión “segura” de esa serie con base en la alerta.
Para equipos heredados, confirmen la situación con el soporte de Danfoss por el código del producto.
La lista anterior no equivale a una lista de CVE por modelo.



Danfoss · fin de servicio ↗ · CERT-FR ↗

05 • ACTUALIZAR CON CONTROL

Descarguen solo de la fuente oficial

Para AK-SM 820A, 850A y 880A, usen la página de Danfoss de la serie 800A.
Al 15/10/2026, lista el paquete 5.3.x y el sistema Danux 4.14.017.194.

01 **AK-SM 800A: software y sistema operativo**

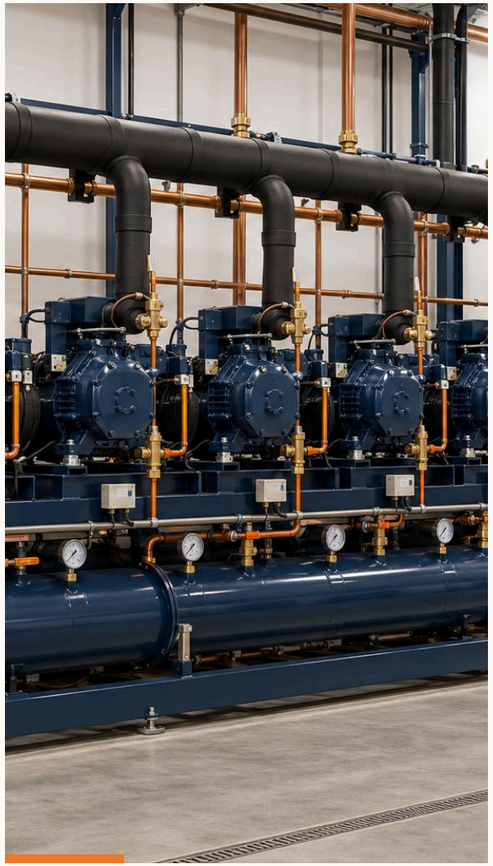
Abrir descargas oficiales de Danfoss ↗.
Lean las instrucciones, los requisitos previos y la compatibilidad antes de instalar.

02 **AK-SM antiguo / AK-SC: soporte y migración**

Contactar a Danfoss ↗.
Indiquen modelo, código, versión y fotos de la etiqueta.
No usen archivos de foros ni de otro modelo.

03 **Copeland / Dixell XWEB: ruta propia**

Abrir System Software Updates ↗.
Seleccionen la familia exacta y confirmen la corrección con el fabricante; no extrapolen la matriz AK a XWEB.



El firmware es el software interno del equipo.
Danux es el sistema operativo del 800A.
Registren ambas versiones y sigan el orden de instalación exigido en las notas del paquete.

Danfoss · descargas e instrucciones ↗

06 • COPELAND / DIXELL XWEB

XWEB EVO y PRO: revisen versiones y soporte

La alerta oficial también incluye Copeland/Dixell XWEB.
El CERT-FR no separa EVO y PRO ni informa versiones; los detalles siguientes vienen de Copeland.

FAMILIA Y MODELOS	FIRMWARE / SOPORTE	ORIENTACIÓN
XWEB 300D PRO **XWEB 500D PRO** **XWEB 500B PRO**	Fallas publicadas en versiones **hasta la 1.12.1, inclusive.**	Actualizar a **1.13.0** o versión posterior compatible. La versión 1.13 corrige las fallas del boletín de febrero/2026.
XWEB 300D EVO **XWEB 500D EVO** **XWEB 500 EVO**	Sin versión segura indicada en la alerta. Soporte de software finalizado el **16/03/2026**.	Mantener aislado de internet pública y planificar migración a PRO. Archivos antiguos no prueban corrección de seguridad.
XWEB 3000 EVO **XWEB 5000 EVO**	Misma condición de fin de soporte que la familia EVO.	Aislar y sustituir por una solución con soporte. El firmware PRO no se aplica al EVO.



PRO: atención a la secuencia. En la actualización manual, las versiones hasta la 1.2.1 exigen pasar por la 1.3.0 antes de la 1.13.0.
Verifiquen el procedimiento del modelo, hagan backup y validen la restauración con el integrador.

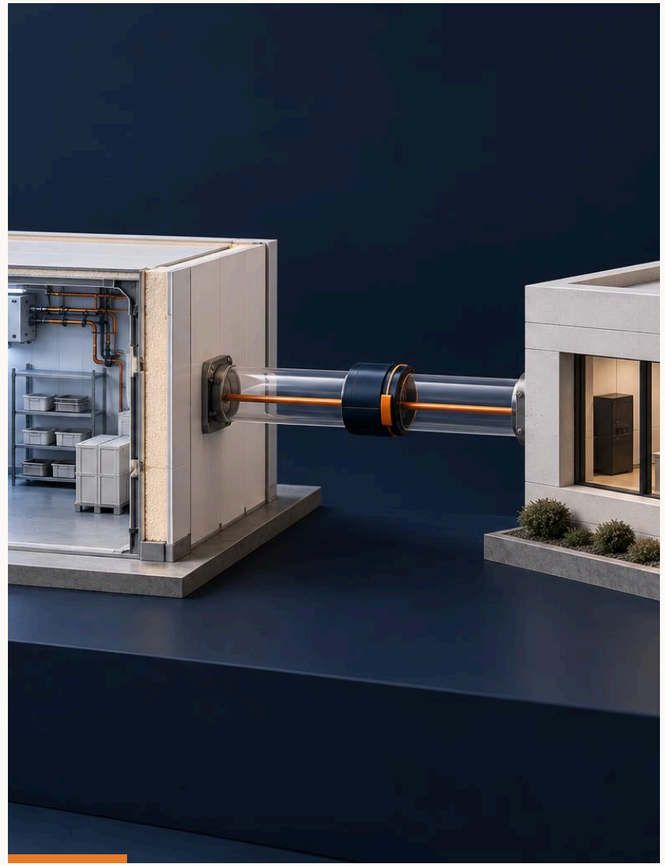
Descargas oficiales: seleccionen la familia y el modelo exactos ↗

Fuentes: CERT-FR ↗ · Copeland: modelos y versiones ↗ · PRO 1.13 ↗ · EVO: fin del soporte ↗ · Secuencia de actualización ↗

07 • PROTEGER LA CONEXIÓN

Acceso remoto por VPN o red protegida

TI debe separar la red de refrigeración y habilitar solo los accesos necesarios.
La administración del router y del módem exige el mismo cuidado.



01 **Conexión permanente**

Usen VPN o red protegida, cuentas individuales y autenticación adicional si está disponible.
Separen la refrigeración del Wi-Fi y de las computadoras de la tienda.

02 **Medida de emergencia**

Si necesitan filtrado por IP hasta concluir la VPN, limiten orígenes, puertos y plazo.
Registren quién lo aprobó y la fecha de migración.

03 **Orígenes del NEO 360**

Pidan a Estech la lista de orígenes antes de cerrar el acceso.
Así las lecturas siguen llegando después del cambio.

Desactiven los servicios sin uso y cambien las contraseñas de fábrica.
HTTPS, la conexión web cifrada, protege la comunicación, pero no sustituye la actualización ni la restricción de acceso.

CERT-FR · VPN y filtrado de emergencia ↗ · Orígenes del NEO 360: pidan la lista a Estech.

08 • PLANIFICAR EL CAMBIO

Cierren el acceso sin perder el monitoreo

TI, integrador y Estech deben coordinar el cambio y verificar el resultado antes de cerrar el mantenimiento.



01 **Antes de la ventana**

Registren modelo, firmware y conexión actual.
Hagan backup, definan cómo volver a la configuración anterior y mantengan un técnico local disponible.

02 **Durante la ejecución**

Creen el camino protegido y prueben las integraciones.
En el 800A, confirmen que el nivel de seguridad esté en Strict (estricto), que exige HTTPS y control de sesión.

03 **Antes de dar la aceptación**

Confirmen que la interfaz no esté abierta al público y que lecturas, alarmas y comunicación con el NEO 360 sigan funcionando.

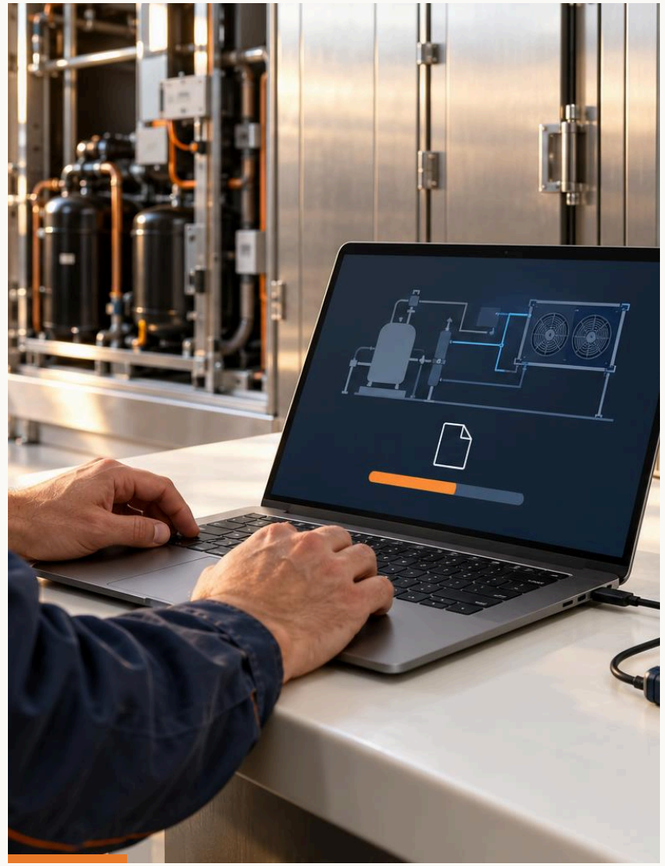
> Si el monitoreo se interrumpe, la gerencia debe hacer rondas locales de temperatura con la frecuencia aprobada por calidad. Registren inicio, fin y responsable de la interrupción.

Danfoss · modo Strict e integraciones ↗

09 • PREPARAR LA RECUPERACIÓN

El backup debe permitir reconstruir la configuración

Exporten la configuración de cada supervisor antes de actualizar y siempre que modifiquen parámetros relevantes.



01 **Parámetros de la operación**

Incluyan temperaturas programadas (setpoints), horarios y límites de desescarche, alarmas, agendas, sensores y vínculos con los controladores.

02 **Archivos y dependencias**

Guarden la exportación original, archivos de dispositivos, licencias cuando correspondan, versiones, manual e instaladores oficiales necesarios para la recuperación.

03 **Identificación e instrucciones**

Registren tienda, modelo, número de serie, fecha, autor y procedimiento de restauración.
Mantengan contraseñas y claves en una bóveda de credenciales separada.

Confirmen en el manual qué incluye la exportación.
La copia del supervisor puede no contener la configuración de cada controlador de campo.
Guarden esas configuraciones por separado cuando sea necesario.

10 • GUARDAR CON SEGURIDAD

Mantengan copias fuera del equipo y de la tienda

Estech recomienda la regla 3-2-1 como referencia:
tres copias en total, en dos medios de almacenamiento, con una copia fuera del sitio.

01 **Protección contra alteraciones**

Mantengan al menos una copia desconectada o protegida contra modificaciones.
Opcional: usen cifrado, es decir, una protección que exige una clave para leer.

02 **Acceso controlado**

Restrinjan el acceso a TI y a los responsables autorizados.
Guarden las claves en una bóveda separada, con acceso de emergencia probado.

03 **Historial de versiones**

Conserven la configuración actual aprobada y las versiones anteriores.
Tras un incidente, elijan una copia anterior a la alteración indebida y verifiquen su contenido.



Definan un plazo de retención y comprueben que las copias abran.
Una copia guardada solo en la laptop del integrador o en el propio supervisor deja la recuperación en un único punto.

11 • PROBAR QUE FUNCIONA

Hagan una restauración de verdad

Un archivo exportado no prueba que la recuperación funcione.
La prueba debe cargar la copia en un entorno compatible y validar el resultado.

01 **Preparar la prueba**

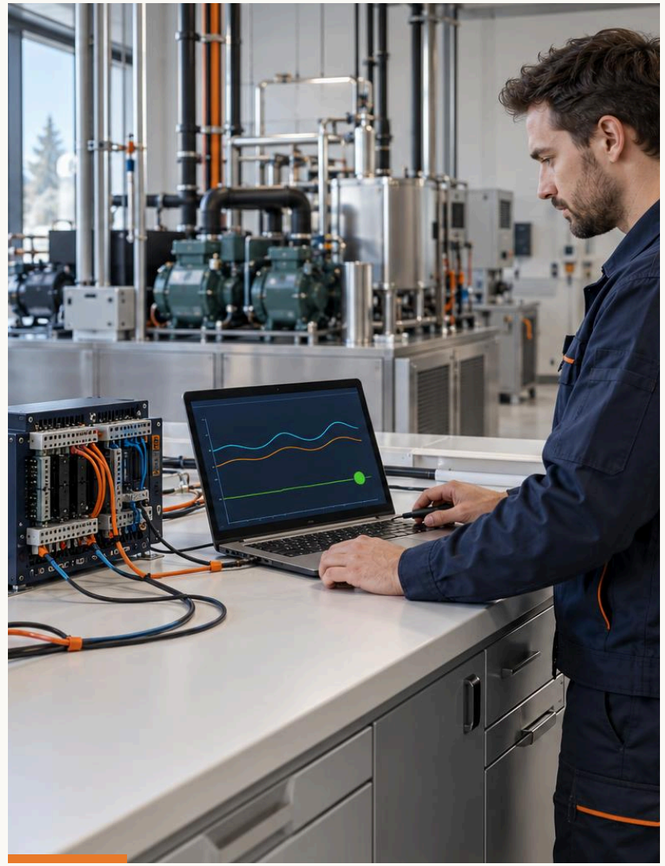
Usen un equipo de reserva compatible o un entorno homologado por el fabricante.
Si solo existe la unidad en operación, reserven una ventana supervisada y un plan de reversión.

02 **Restaurar y verificar**

Restauren la configuración y comparen sensores, horarios, alarmas, accesos y parámetros.
Verifiquen también la comunicación con los controladores y el NEO 360.

03 **Registrar y corregir**

Anoten archivo y versión usados, duración, divergencias y responsables.
Si falla, corrijan el proceso y repitan hasta obtener la aceptación.



Un simulador ayuda a preparar, pero no sustituye la prueba en el equipo si la recuperación depende de interfaces físicas.
El ensayo no debe activar desescarches ni alterar la refrigeración de una tienda en funcionamiento.

12 • DEFINIR LA FRECUENCIA

Elijan un ciclo de 3, 6 o 12 meses

Las frecuencias siguientes son recomendaciones de Estech.
La decisión debe considerar criticidad, capacidad del equipo y tiempo aceptable de recuperación.

3 meses

Operación crítica

Muchas tiendas, mayor impacto de una parada o equipos antiguos.
Revisión completa y prueba real de restauración en cada ciclo.

6 meses

Rutina recomendada

Estructura intermedia.
Revisión completa y prueba real de restauración semestral, con responsables definidos.

12 meses

Capacidad limitada

Límite propuesto para operaciones de menor criticidad, con riesgo aceptado por la gestión y prueba real anual.



No esperen al próximo ciclo para atender una alerta crítica.
Actualicen el backup en cada revisión y tras cambios aprobados.
Reevalúen acceso y recuperación al cambiar de equipo, integrador, red o firmware.
Apliquen correcciones según los boletines y la compatibilidad, sin esperar el calendario.

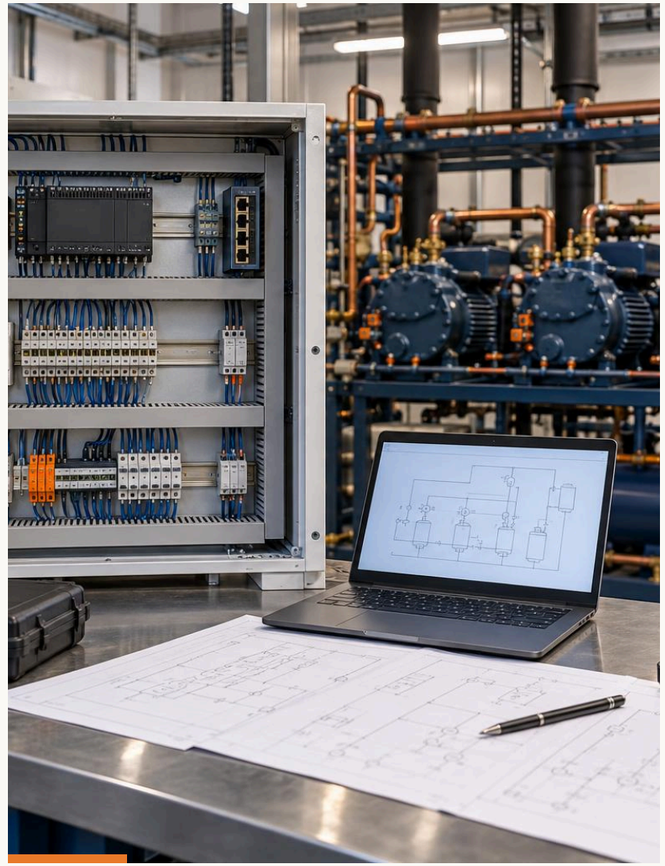
13 • ASIGNAR RESPONSABILIDADES

Cada tienda necesita un responsable y evidencias

La gestión aprueba el ciclo y la prioridad.
TI coordina la rutina y registra lo verificado con el integrador y la operación.

RESPONSABLE	ENTREGABLE QUE DEBE QUEDAR REGISTRADO
Gestión operativa	Criticidad, frecuencia, presupuesto, plazo y aceptación de riesgos pendientes.
Su equipo de TI	Inventario, reglas de acceso, cuentas, ubicación de copias y próxima revisión.
Integrador / fabricante	Compatibilidad, actualización, exportación y prueba real de restauración.
Gerencia / calidad	Contactos, protección de productos y validación de la operación local.
Estech	Verificación de la integración y las lecturas en el NEO 360, según alcance acordado.

Ficha por tienda: activo y serie · firmware y Danux · responsable y suplente · ubicación del backup · último restore y duración · fallas pendientes · plazo · evidencia de aceptación · próxima revisión.



14 • RESPONDER AL INCIDENTE

Protejan los productos y aíslen el acceso remoto

Desescarches fuera de horario, cambios no autorizados o calentamiento simultáneo exigen verificación inmediata.
No esperen la confirmación de un ataque.



01 **Gerencia y calidad: actuar de inmediato**

Verifiquen temperaturas con medición local, mantengan las puertas cerradas y sigan el plan de protección o traslado de los productos.
Registren los horarios.

02 **TI e integrador: contener la entrada**

Aíslen la vía de acceso remoto identificada.
No apaguen ni desconecten rack, controladores o cables sin identificar su función: puede afectar el control de la refrigeración.

03 **Equipo responsable: avisar y preservar**

Avisen a TI, al integrador y a Estech.
Preserven registros de acceso y fotos antes del restablecimiento, si eso no retrasa la protección de la operación.

> Las señales también pueden tener causas operativas.
> El equipo debe investigar sin presumir el origen.
> Si se interrumpe la lectura remota, mantengan la verificación local de temperatura.

CERT-FR · contención y recuperación ↗

15 • RECUPERAR DESDE CERO

Reconstruyan el equipo antes de reconectar

Tras una intrusión, el integrador debe ejecutar la recuperación de fábrica prevista por el fabricante, con el equipo aislado y la operación protegida.

1. **Preservar y preparar.** Guarden evidencias y confirmen una copia confiable, versiones, licencias y recursos para la recuperación.
2. **Restaurar de fábrica.** Ejecuten el restablecimiento y la reinstalación oficial cuando esté prevista. “Formatear” no es un procedimiento universal: sigan el método del modelo.
3. **Corregir y reconfigurar.** Instalen los paquetes oficiales en el orden del fabricante, cambien las credenciales y carguen una configuración anterior al incidente, ya verificada.
4. **Validar en aislamiento.** Verifiquen parámetros, cuentas, comunicación y funciones locales. Apliquen los criterios de aceptación de la página siguiente.
5. **Reconectar de forma protegida.** Usen VPN o red protegida y acompañen la operación con Estech y la gerencia.

> Si no hay firmware con soporte, un restablecimiento deja el equipo expuesto a la misma falla.
> Mantengan el aislamiento y aprueben la sustitución.
> No restauren una configuración sospechosa sin revisión.



CERT-FR · Reset Factory y riesgo de nueva intrusión ↗

16 • DAR LA ACEPTACIÓN

Solo cierren después de verificar la operación

TI, integrador y gerencia deben registrar la aceptación.
Acuerden con Estech la verificación del retorno del monitoreo.

- Modelo y versiones documentados, con correcciones aplicables o aislamiento aprobado para sustitución.
- Interfaz sin acceso público; camino protegido y accesos autorizados verificados.
- Cuentas revisadas y contraseñas cambiadas tras el incidente, incluidos router y acceso remoto.
- Temperaturas programadas, desescarches y alarmas comparados con la configuración aprobada.
- Lecturas y comunicación en el NEO 360 verificadas; prueba segura de alarma acordada con la operación.
- Nuevo backup protegido, prueba de restauración registrada y próxima revisión programada.

> Definan antes de la intervención el tiempo máximo aceptable sin supervisor y el tiempo máximo sin lectura.
> Midan la recuperación y establezcan el período de seguimiento según la criticidad de la tienda.

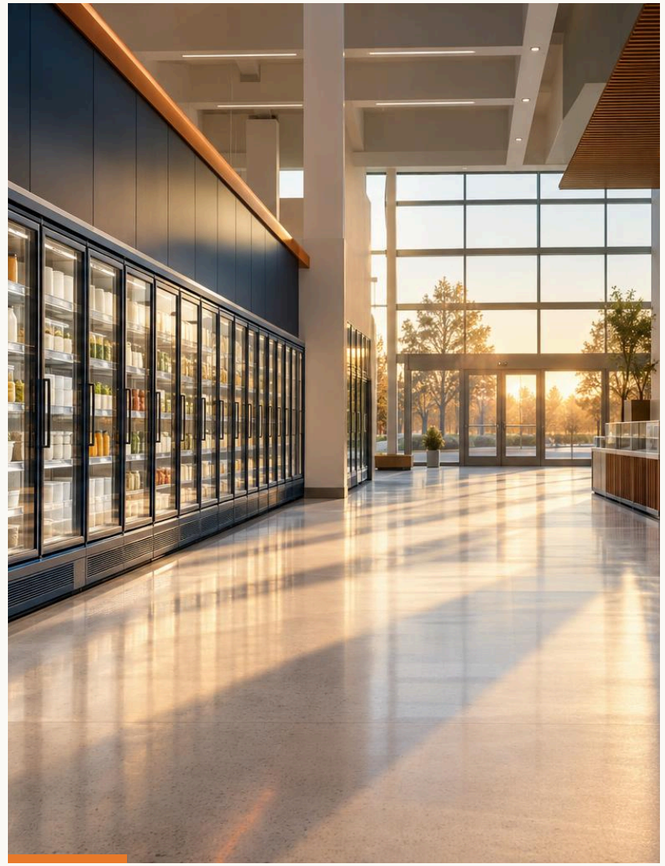


REFERENCIAS • CONTACTO

Fuentes de consulta y próximos pasos

Empiecen por el inventario de cada tienda.
Prioricen la exposición a internet, los equipos sin soporte y la falta de una copia probada.

01 CERT-FR · alerta CERTFR-2026-ALE-012 ↗
02 Danfoss · boletines de seguridad DSA ↗
03 Danfoss · software y Danux del AK-SM 800A ↗
04 Danfoss · fin de servicio de modelos antiguos ↗
05 Copeland / Dixell · actualizaciones XWEB ↗
06 Copeland · modelos y versiones afectados ↗
07 Copeland · fin del soporte de la familia EVO ↗



SOPORTE ESTECH / JORNADA NEO

help@neoestech.com

Ante incidentes, avisen también a los contactos de emergencia ya acordados con su operación.

Rafael Cocchiaro | Head of Tech | Digital Tech