

Especificación técnica y operativa (MVP) — Servicio operado de cadena de frío

Documento para: Área técnica (Ingeniero electrónico) y equipo fundador

Fecha: 29-Mar-2026 | Versión: 2.0 (profesional)

Propósito: definir con precisión qué debe construirse y cómo debe operar el sistema para que podamos prestar un servicio serio desde el día 1 en Colombia. Prioridades: confiabilidad, offline-first, gestión de incidentes con evidencia, reportes auditables y operación replicable por sede. Este documento evita que el proyecto se convierta en “solo monitoreo”.

Resumen ejecutivo (1 página)

- **Qué vendemos:** control operativo con evidencia (incidente → acción confirmada → escalamiento → cierre con evidencia → reporte mensual).
- **Qué NO vendemos:** sensores como producto principal; la tecnología es un medio.
- **Entregable técnico mínimo:** sensor offline-first + panel + bitácora de incidentes + reporte mensual de incidentes + modo sin nuestros sensores.
- **Entregable operativo mínimo:** protocolo de incidentes, matriz de responsabilidades y escalamiento por turnos.
- **Pruebas Go/No-Go:** sin offline, sin incidentes, sin cierre con acción y sin reporte mensual no se instala en un banco de sangre.

1) Alcance del MVP (fase 1) y límites

- **Variables:** temperatura (obligatorio). Puerta (opcional si ya está estable).
- **Frecuencia:** 1–5 minutos configurable (default: 1 minuto en salud).
- **Capacidad inicial:** 1 sede, 2–4 equipos críticos (primer despliegue).
- **No metas en fase 1:** humedad/pH/corriente, analítica avanzada, dashboards complejos, integraciones enterprise profundas.

2) Vista general del sistema (arquitectura)

- **Dispositivo:** lectura + timestamp + buffer local + envío (store & forward).
- **Backend:** API + base de datos + motor de alarmas/incidentes + registro de auditoría.
- **Panel:** sedes/equipos, gráficas, incidentes, cierre, exportación y reportes.
- **Canales de alerta:** WhatsApp/email/SMS (según disponibilidad) con registro de envío.

3) Requisitos del dispositivo (sensor) — no negociables

- **Offline-first:** debe registrar y almacenar lecturas sin internet. Buffer mínimo 48 horas (ideal 7 días).
- **Sincronización:** al reconectar, subir backlog en orden, sin duplicados, con control de integridad.
- **Timestamps:** sincronización de hora (NTP) al conectarse y control de drift.
- **Identificación:** device_id visible y mapeo obligatorio a un equipo (asset).
- **Robustez:** watchdog/reinicio seguro, logs básicos, telemetría de “última conexión”.
- **Seguridad básica:** autenticación del dispositivo contra el backend (token/clave).

4) Alarmas (diseño para evitar fatiga de alarmas)

- Configuración **por equipo:** rango permitido (min/max) + retardo (p. ej., fuera de rango ≥ 5 min) + severidad.
- Separar **evento** (pico breve) de **incidente** (salida sostenida).
- Registrar excursiones en gráfico y asociarlas a incidentes cuando aplique.

5) Incidentes (núcleo del producto) — modelo mínimo

- **Creación automática:** incident_id, site_id, asset_id, start_time, detected_time, severity, status=ABIERTO.
- **Notificación trazable:** lista de contactos por sede + registro de envío (a quién/cuándo).
- **Cierre obligatorio:** acción tomada (texto), causa (PUERTA/ENERGÍA/FALLA EQUIPO/MANIPULACIÓN/DESCONOCIDO), cerrador, hora de cierre.
- **Escalamiento:** si no hay acción confirmada en X minutos → notificar nivel 2 y nivel 3; registrar cada escalamiento.
- **Auditoría:** registro de cambios (quién cambia rangos, quién cierra incidentes).

6) Panel mínimo vendible (pantallas obligatorias)

- **Sedes:** lista y estado (OK/alarma/sensor caído).
- **Equipos:** nombre, rango, último dato, última conexión.
- **Gráfica:** histórico + excursiones destacadas.
- **Incidentes:** lista abiertos/cerrados, detalle, trazabilidad, botón “Cerrar” con campos obligatorios.
- **Exportaciones:** CSV/Excel de lecturas e incidentes.
- **Reportes:** reporte mensual de incidentes descargable.

7) Reportes (lo que cierra ventas y evita discusión de precio)

- **Reporte mensual de incidentes (obligatorio):** incidentes por equipo; tiempos (detección→notificación→acción/cierre); % cerrados con acción; incidentes sin respuesta; reincidencias (Top 5); recomendaciones.
- **Reporte de temperatura:** curvas + excursiones (secundario).

8) Modo B (operar sin nuestros sensores) — requisito estratégico

- Permitir crear incidentes desde fuentes externas (CSV/Excel o webhook/API simple).
- El motor de incidentes/cierre/reportes debe operar aunque la medición sea de un tercero.
- Esto permite vender a clientes grandes que “ya tienen monitoreo”.

9) Seguridad y confiabilidad (mínimo viable)

- Usuarios y roles: administrador (proveedor) y cliente (ver y cerrar incidentes).
- Backups diarios de base de datos.
- Registro de auditoría: cambios en rangos y cierres de incidentes.
- Monitoreo de ‘sensor desconectado’ (último seen).

10) Pruebas Go/No-Go (antes de instalar en un banco de sangre)

- **Offline:** internet caído 6 horas → no se pierde historial → sincroniza al volver.
- **Incidente:** fuera de rango ≥ 10 min → se crea incidente automático.
- **Cierre:** no se puede cerrar sin acción tomada + causa → queda auditado.
- **Reporte:** se genera reporte mensual de incidentes (PDF/Excel).
- **Estabilidad:** 7 días sin reinicios manuales.
- **Integridad:** timestamps coherentes, sin duplicados en reconexión.

11) Playbook de instalación en sitio (primer despliegue)

- Arranque con 2–4 equipos críticos (no más). Etiquetar asset_id y tomar foto de referencia.
- Definir conectividad (WiFi o SIM). Verificar señal y última conexión.
- Configurar rangos y retardo por equipo. Probar alarma, creación y cierre de incidente en sitio.
- Cargar contactos y escalamiento (responsable/suplente/calidad).
- Entregar al cliente hoja de responsabilidades: la acción física inmediata es del cliente.

12) Interfaz técnica-operativa (lo que debe quedar alineado con operación)

- La plataforma debe permitir registrar el 'cierre' del incidente con campos obligatorios. Sin cierre, no hay evidencia.
- Debe existir un flujo de escalamiento (automático o semi-automático) que quede registrado.
- El reporte mensual debe poder generarse sin intervención manual excesiva (exportación/plantilla).

13) Números técnicos para fijar precios y no quebrarnos

- Costo real del dispositivo (hoy) y costo estimado en producción (100/500/1000 unidades).
- Costo mensual por punto: SIM/datos, hosting, soporte, tasa de fallas/reposiciones.
- Tiempo estándar de instalación por equipo y por sede (para costear visitas).

14) Roadmap recomendado (45 días) con entregables

- **Semana 1:** dispositivo offline + envío + BD + gráfica.
- **Semana 2:** motor de alarmas con retardo + eventos.
- **Semana 3:** incidentes automáticos + UI de incidentes.
- **Semana 4:** cierre con acción + escalamiento + exportación.
- **Semana 5–6:** reporte mensual + pruebas de estrés + hardening + Modo B.

15) Límites y no negociables (para mantener el enfoque)

- No múltiples variables en fase 1.
- No '24/7 físico' desde el producto: visitas físicas son add-on comercial.
- No depender de internet para registrar.
- No lanzar sin bitácora de incidentes + cierre con acción + reporte mensual.