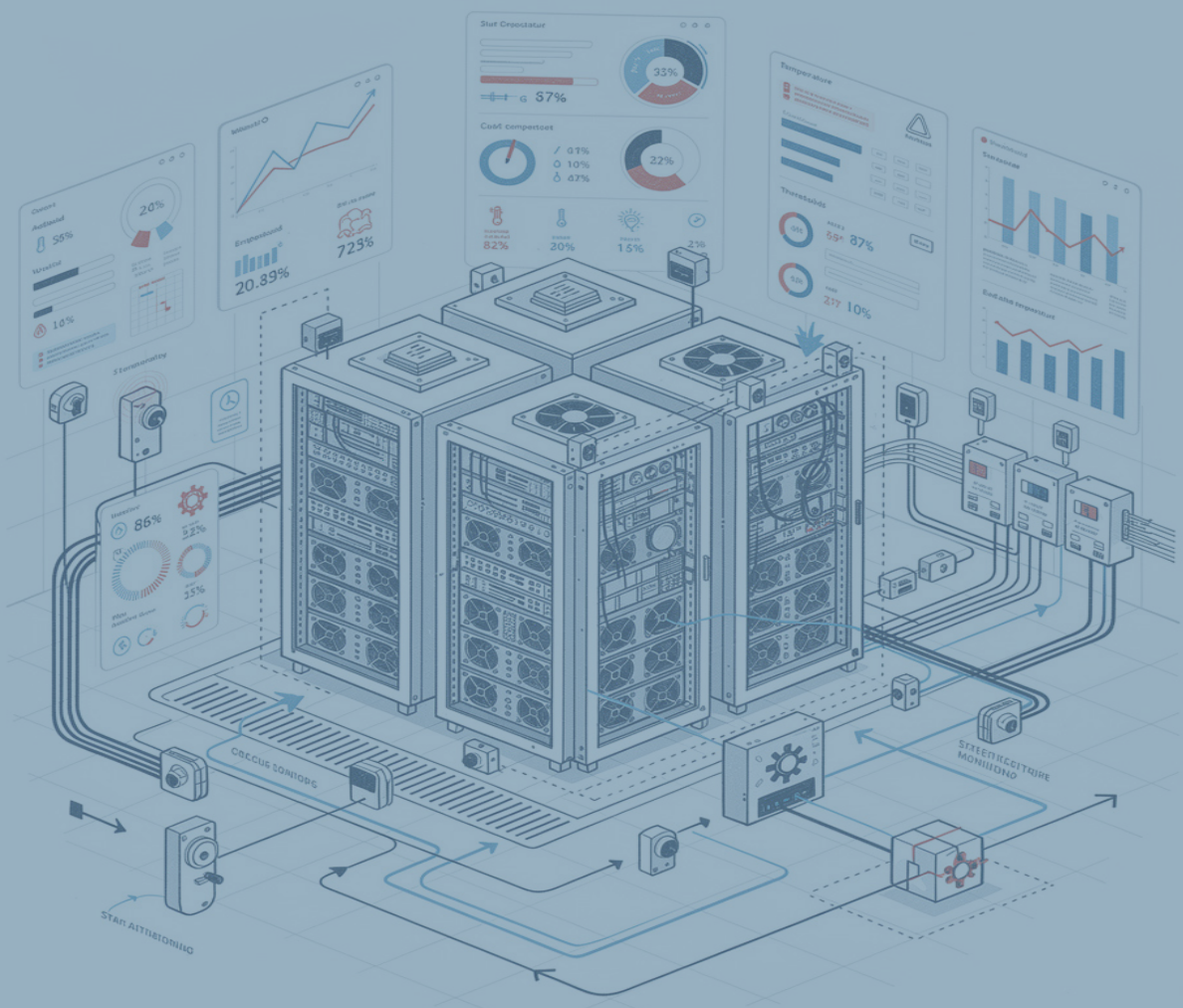
Bjumper

Umbrales y alarmas en el Data Center

Guía técnica de monitorización y gestión de alarmas



Introducción

Un data center opera como un organismo complejo en el que temperatura, energía, humedad y conectividad están permanentemente interrelacionadas. Cuando cualquiera de estas variables sale de rango, la cadena de fallos puede ser rápida e irreversible: desde la degradación silenciosa de componentes hasta la pérdida total de servicio.

Los umbrales de alarma son la primera línea de defensa operativa. Definen el límite entre el funcionamiento normal y la situación que requiere intervención. Configurarlos correctamente marca la diferencia entre una alerta que llega a tiempo y el apagado de un servidor que nadie vio venir.

Contexto económico

Según datos de Uptime Institute, el coste medio de una interrupción no planificada en un data center supera los 9.000 EUR por minuto. La correcta configuración de umbrales y alarmas es, con diferencia, la inversión con mayor retorno en operaciones críticas.

Esta guía cubre tres grandes dominios de monitorización:

- Ambiental: temperatura, humedad y presión diferencial.
- Eléctrico: UPS, PDU, calidad de corriente y eficiencia energética.
- Gestión de alarmas: conceptos clave, niveles, escalado al NOC, fatiga y automatización.

Marco normativo de referencia

Toda decisión sobre umbrales debe apoyarse en estándares reconocidos. Los tres que más condicionan la operativa diaria son:

- ASHRAE TC 9.9 (5.a ed., 2021): parámetros térmicos y de humedad para equipos de proceso de datos.
- Uptime Institute Tier Standard: clasifica la resiliencia y condiciona el rigor de los runbooks.
- ISA-18.2: filosofía de gestión de alarmas para sistemas de control industrial, aplicable al BMS y DCiM.
- ITIL 4: marco de gestión de servicios TI. Define los conceptos de evento, alarma e incidente y su ciclo de vida operativo.

Conceptos clave: métricas, eventos, alarmas e inicidentes

Antes de configurar cualquier umbral es imprescindible hablar el mismo idioma. La industria utiliza términos que se confunden con frecuencia pero que tienen significados precisos y diferenciados. Su correcta distinción es la base de una arquitectura de monitorización coherente.

Jerarquía de conceptos operativos

Concepto	Definición	Quién lo gestiona
Métrica	Medida continua de un parámetro físico o lógico. No implica ninguna acción	DCiM / EMS (automático)
Evento	Cambio de estado detectado por el sistema. Puede ser informativo o requerir acción	EMS / DCiM (automático)
Alarma	Evento que supera un umbral definido y genera notificación activa. Requiere acuse de recibo	Operador NOC
Incidente	Alarma que no se resuelve en el tiempo definido o que provoca impacto en el servicio. Gestionado con ticket ITSM	Equipo técnico + NOC

Métricas: qué se mide y con qué frecuencia

Una métrica es el dato bruto recogido de sensores, dispositivos o APIs. Por sí sola no indica si hay problema: es el umbral quien convierte una métrica en un evento relevante. Las métricas se clasifican según su naturaleza:

- **Métricas ambientales**: temperatura de entrada/salida de rack, humedad relativa, punto de rocío, presión diferencial, caudal de aire, detección de agua
- **Métricas eléctricas**: tensión AC/DC, corriente por fase, potencia activa (W) y aparente (kVA), factor de potencia, THD, energía acumulada (kWh), autonomía de batería UPS.
- **Métricas de eficiencia**: PUE, WUE (Water Usage Effectiveness), CUE (Carbón Usage Effectiveness).

La frecuencia de muestreo es clave. Los sensores de temperatura suelen muestrear cada 30-60 segundos, los de corriente eléctrica pueden hacerlo cada 5-10 segundos en instalaciones críticas.

Eventos: la materia prima del NOC

Un evento es cualquier cambio de estado que el sistema detecta y registra. No todos los eventos son alarmas: la mayor parte son información almacenada para análisis histórico. Los tipos de eventos son:

- **Informativo:** el sistema registra el cambio sin notificar a nadie. Por ejemplo, temperatura que sube de 22 C a 23 C dentro del rango normal.
- **Advertencia**: el parámetro se acerca a un umbral. Se notifica al operador de turno para seguimiento.
- **Critico**: el parámetro supera el umbral definido. Requiere acuse de recibo y acción en tiempo definido.

La gestión de eventos en el NOC se apoya en herramientas de correlación que agrupan múltiples eventos relacionados en un único incidente. Si cinco racks del mismo pasillo frío superan simultáneamente el umbral de temperatura, el sistema debe generar un único incidente, no cinco alarmas independientes.

Alarmas: de la señal a la acción

Una alarma es un evento que cruza un umbral y requiere intervención humana. Su efectividad depende de que sea accionable: debe decirle al operador que ocurrió, donde y que tiene que hacer. Los atributos de una alarma bien diseñada son:

- **Identificación**: nombre del dispositivo, ubicación física (sala, fila, rack, posición) y parámetro afectado.
- **Valor actual vs. umbral**: el operador debe ver de inmediato cuanto se ha superado el límite.
- **Severidad:** clasificada de forma inequívoca (Informativo / Advertencia / Critico / Emergencia).
- **Runbook asociado**: enlace directo al procedimiento de actuación.
- **Tiempo de vida**: desde cuando esta activa la alarma y si ha sido reconocida.

Incidentes y severidades

Un incidente es una alarma que no se resuelve en el tiempo estipulado o que tiene impacto en la disponibilidad del servicio. Su gestión se formaliza mediante un ticket en el sistema ITSM con propietario, SLA de resolución y trazabilidad completa. La clasificación de severidad combina dos dimensiones: el impacto y la urgencia.

Severidad	Nombre	Impacto	Urgencia	Resp. (min)	Resolución
SEV 1 / P1	Crítico	Servicio critico caído. Impacto inmediato en negocio	Máxima	< 5	< 1 h
SEV 2 / P2	Alto	Degradación significativa. Funcionalidad reducida	Alta	< 15	< 4 h
SEV 3 / P3	Medio	Impacto limitado. Workaround disponible	Media	< 30	< 8 h
SEV 4 / P4	Bajo	Sin impacto operativo inmediato. Mejora o prevención	Baja	< 120	< 5 días
SEV 5 / P5	Informativo	Registro sin acción requerida.	Ninguna	____	____

Incidentes y severidades

No todas las alarmas deben llegar al NOC. El filtrado previo es esencial para evitar la fatiga operativa. Llegan al NOC todos los eventos de nivel advertencia o superior que no han podido resolverse automáticamente.

Dominio ambiental

- Temperatura de entrada de rack > 28 C (Advertencia) o > 32 C (Critico).
- Humedad relativa fuera del rango 30-70 % HR.
- Fallo de sensor de temperatura o humedad (pérdida de señal).
- Detección de agua en cualquier punto del suelo técnico o bajo unidades CRAC/CRAH.
- Presión diferencial de pasillo frio < 8 Pa (posible rotura de contención).
- Fallo de CRAC/CRAH o alarma de alta temperatura interna de unidad de climatización.

Dominio eléctrico

- UPS en modo batería (fallo de alimentación de red).
- Autonomía de batería UPS < 10 minutos.
- Carga de UPS > 85 % de la capacidad nominal.
- Tensión fuera de rango +/- 10 % del nominal.
- Desequilibrio de fases > 15 % en cualquier PDU.
- Circuito de PDU > 90 % de la capacidad nominal (riesgo de disparo de diferencial).
- Fallo de generador o incapacidad de arranque en test.

Dominio TI / Hardware

- Servidor en estado de throttling térmico (la CPU reduce frecuencia por temperatura excesiva).
- Servidor apagado por protección térmica (acción iDRAC/iLO).
- Pérdida de conectividad de red con equipos de monitorización.
- Fallo de ventiladores internos de servidor (alarma de hardware vía IPMI/ Redfish).

Regla práctica de escalado al NOC

Todo evento de tipo critico o emergencia debe llegar al NOC sin excepción. Los eventos de advertencia solo llegan al NOC si superan el tiempo de persistencia (dwell) configurado sin resolverse automáticamente, o si se producen en horario sin personal de guardia en sala.

Umbrales de temperatura

La temperatura es la variable más monitorizada en cualquier sala de servidores. Su gestión incorrecta genera dos problemas igualmente costosos: el sobrecalentamiento y el sobre enfriamiento, que desperdicia entre el 30 y el 40 % de la energía de refrigeración.

Estándar ASHRAE TC 9.9: rangos recomendados y admisibles

ASHRAE distingue entre el rango recomendado, óptimo para la vida útil del equipo, y el rango admisible dentro del cual el fabricante garantiza funcionamiento, aunque el desgaste aumenta.

Clase	Rango recomendado (C)	Rango admisible (C)	Aplicación típica
A1	18 - 27	15 - 32	Servidores enterprise y almacenamiento critico
A2	18 - 27	10 - 35	Servidores de volumen, workstations
A3	18 - 27	5 - 40	PCs, equipos de laboratorio
A4	18 - 27	5 - 45	Equipos industriales, máxima flexibilidad
H1 (HPC / IA)	18 - 22	15 - 25	Sistemas IA, GPU clusters, HPC

La medición se toma siempre en la entrada de aire del servidor (inlet). Monitorizar solo el ambiente general puede enmascarar puntos calientes en racks concretos que superen el límite recomendado en 8-10 C.

Configuración práctica de alarmas de temperatura

La configuración de alarmas en tres niveles, advertencia, crítico y emergencia, permite escalar la respuesta de forma progresiva sin saturar al equipo operativo.

Nivel	Umbral entrada rack (C)	Acción requerida	Tiempo de respuesta
Normal (OK)	18 - 26	Ninguna	____
Advertencia	26 - 28	Revisar estado del sistema de refrigeración	< 30 min
Critico	28 - 32	Intervención inmediata. Activar CRAC redundante	< 10 min
Emergencia	> 32 / < 15	Shutdown controlado. Escalar al NOC como SEV 1	< 5 min

Colocación de sensores: dónde medir

ASHRAE recomienda un mínimo de 6 sensores por rack: parte superior, media e inferior tanto en la parte delantera como en la trasera. En la práctica, muchos operadores parten de 3 puntos por rack (frente, alto/medio/bajo) y añaden cobertura adicional en los extremos de cada fila, que son los puntos más propensos a la recirculación de aire caliente.

Regla de colocación

Evitar situar sensores en zonas de corriente directa, frente a rejillas de CRAC, cerca de puertas frecuentes o expuestos a luz solar directa. Estas posiciones generan lecturas erróneas que disparan falsas alarmas.

Umbrales de humedad y punto de rocío

La humedad relativa (HR) controla dos riesgos opuestos: si es demasiado baja favorece las descargas electrostáticas (ESD); si es demasiado alta provoca condensación sobre circuitos y superficies metálicas.

Rangos de referencia ASHRAE

Parámetro	Rango recomendado	Rango admisible (A1/A2)	Riesgo fuera de rango
Humedad relativa	50 - 60 % HR	8 - 80 % HR	ESD (<30 %) / Condensación (>70 %)
Punto de rocío	-9 C a 15 C	-12 C a 17 C	Condensación sobre componentes
Velocidad de cambio	< 5 C / 20 h	____	Choque térmico en componentes

Configuración umbrales de alarma de humedad

Nivel	Humedad relativa	Acción
Normal	40 - 60 % HR	Ninguna
Advertencia baja	30 - 40 % HR	Verificar humidificador. Evaluar riesgo ESD
Advertencia alta	60 - 70 % HR	Verificar deshumidificador y carga de enfriamiento
Critico bajo	< 30 % HR	Activar humidificación de emergencia
Critico alto	> 70 % HR	Inspección física. Riesgo de condensación

Configuración umbrales de alarma de humedad

La humedad relativa es una medida relativa a la temperatura: el mismo contenido de vapor en el aire da lecturas de HR muy distintas si la temperatura cambia. El punto de rocío, en cambio, es absoluto: indica directamente la temperatura a la que el vapor se condensa. Este valor es el que realmente predice el riesgo de condensación cuando el aire frío de los pasillos fríos entra en contacto con superficies metálicas más calientes.

La ratio de despliegue estándar es un sensor de humedad por cada cinco racks, dado que la humedad varía con menos rapidez que la temperatura dentro de la sala.

Presión diferencial y flujo de aire

En instalaciones con pasillos fríos/calientes y contenedores de pasillos, la presión diferencial (ΔP) entre el pasillo frío y el espacio general de la sala es el indicador que mejor refleja la eficiencia de la distribución de aire. Una caída de ΔP indica filtración, el aire frío se escapa por rendijas o baldosas mal posicionadas, que degrada directamente la temperatura de entrada de los servidores.

Configuración umbrales de alarma de humedad

Situación	delta P típica (Pa)	Indicación
Optimo (pasillo contenido)	12 - 25 Pa	Distribución correcta, sin fugas significativas
Advertencia	< 10 Pa	Posibles fugas en sellos o baldosas. Inspeccionar
Critico	< 5 Pa	Fallo en contención. Riesgo de recirculación caliente
Sobrepresión	> 35 Pa	Revisar velocidad de fans/ CRAH

Sensores de flujo de aire

Los sensores de flujo de aire se instalan en los puntos de suministro de aire frío y en los retornos de aire caliente para calcular la distribución volumétrica. Una anomalía en el flujo, combinada con un incremento de temperatura en la entrada de rack, confirma un problema de contención antes de que los servidores entren en protección térmica.

Tiempo de reacción en fallo de HVAC

Según la especificación de ASHRAE TC 9.9, cuando falla el sistema de climatización, la temperatura del pasillo frío puede subir 30 °C en tan solo 5 minutos en instalaciones de alta densidad. El tiempo de ride-through, el margen antes de que los servidores apaguen por protección térmica, es el parámetro crítico que define la urgencia del escalado.

Umbrales de alimentación eléctrica

La cadena de suministro eléctrico es el dominio que más directamente condiciona la disponibilidad. Sus umbrales no solo protegen los equipos, sino que permiten operar de forma eficiente, evitando sobredimensionar la infraestructura.

Monitorización del UPS

La siguiente tabla recoge los umbrales operativos de referencia para instalaciones genéricas. Son valores de gestión recomendados, independientes del fabricante. Los umbrales específicos .

Métrica UPS	Normal	Advertencia	Critico
Tensión salida (V AC)	220 - 230 V	210 - 219 V / 231 - 240 V	< 210 V o > 240 V
Carga (%)	0 - 75 %	75 - 85 %	> 85 %
Carga batería (%)	90 - 100 %	50 - 90 %	< 50 %
Autonomía batería	> 15 min	5 - 15 min	< 5 min
Temperatura bateria (C)	20 - 25 C	25 - 30 C	> 30 C / < 15 C

Monitorización de PDUs inteligentes

Las PDUs inteligentes (iPDU) son el punto de medición más granular de la cadena eléctrica. Permiten configurar umbrales a nivel de circuito (infeed), fase e incluso outlet individual. Los valores de la tabla siguiente son umbrales operativos genéricos de referencia. Las métricas que deben monitorizarse son:

Métrica PDU	Normal	Advertencia	Critico
Corriente por fase (A)	< 80 % del nominal	80 - 90 % del nominal	> 90 % del nominal
Balance de fases (%)	< 10 %	10 - 20 %	> 20 %
Tensión de entrada (V)	220 - 230 V	210 - 219 V	< 210 V o > 240 V
Factor de potencia	0,95 - 1,0	0,85 - 0,95	< 0,85
THD (Distorsión armonica %)	< 5 %	5 - 10 %	> 10 %

El superamiento del 80 % de la capacidad de un circuito es la señal de advertencia estándar en la industria porque garantiza margen para picos transitorios y evita el disparo del interruptor automático, que genera una interrupción inmediata e incontrolada.

Detección de agua y fugas

El agua es uno de los riesgos más subestimados en el data center. Las fugas en sistemas de refrigeración por agua pueden provocar cortocircuitos y danos irreversibles en cuestión de minutos.

Tipos de sensores y su colocación

- Sensores de punto: detectan presencia de agua en una ubicación concreta. Se instalan en los puntos más bajos del suelo técnico, bajo las unidades de climatización y cerca de bandejas de condensación.
- Cables de detección lineal: cubren grandes superficies de forma continua. Ideales para perímetros de sala y pasillos bajo suelo técnico. Un único cable puede cubrir decenas de metros.

Protocolo de respuesta

La detección de agua no tiene niveles intermedios: cualquier señal positiva es un evento critico (SEV 1) que requiere notificación inmediata en todos los canales y apertura automática de ticket con el protocolo de actuación adjunto.

Protocolo de respuesta ante fuga

1. Identificar la fuente (visual o por posición del sensor activado).
2. Cortar el suministro de agua al circuito afectado si es posible.
3. Evaluar si hay equipos en riesgo inmediato.
4. Nunca apagar equipos por proximidad al agua sin confirmar contacto real.

KPIs de gestión de alarmas

La madurez del sistema de alarmas se mide con indicadores concretos. Los más utilizados en el sector son:

KPI	Definición	Objetivo recomendado
MTTD	Mean Time to Detect: tiempo medio de detección del evento	< 2 min
MTTA	Mean Time to Acknowledge: tiempo hasta acuse de recibo de alarma crítica	< 5 min
MTTR	Mean Time to Resolve: tiempo medio de resolución de incidente	< 60 min (SEV 1
Ratio alarmas falsas	Porcentaje de alarmas que no corresponden a eventos reales	< 5 %
Alarmas por turno (8 h)	Número de alarmas activas por turno de operación	< 30 por turno

Arquitectura de gestión de alarmas y NOC

Disponer de sensores bien configurados no es suficiente si la arquitectura de alarmas no está diseñada para que la información correcta llegue a la persona correcta en el momento correcto. Una mala gestión de alarmas lleva a la fatiga operativa: el equipo empieza a ignorar notificaciones porque hay demasiadas o demasiado poco significativas.

Niveles de severidad y codificación de color

Nivel	Color	Definición operativa	Tiempo de respuesta
Informativo	Azul	Evento registrado sin impacto operativo. Sin notificación activa	——
Advertencia	Amarillo	Parámetro acercándose al limite. Requiere revisión programada.	< 30 min
Critico	Naranja	Parámetro fuera de rango operativo seguro. Intervención necesaria.	< 10 min
Emergencia	Rojo	Riesgo inminente de perdida de servicio o dano fisico.	< 5 min

Protocolo de escalado al NOC

El escalado automático garantiza que ninguna alarma crítica quede sin respuesta. La lógica típica de escalado funciona en tres etapas:

- **Nivel 1** (0-5 min): notificación al operador de guardia por email y SMS. Si no hay acuse de recibo en 5 minutos, escala automáticamente.
- **Nivel 2** (5-10 min): notificación al responsable técnico de turno y apertura automática de ticket ITSM con datos del evento y runbook de actuación.
- **Nivel 3** (> 10 min sin resolución): notificación al responsable de instalaciones o dirección técnica. En eventos de emergencia, el escalado a nivel 3 es inmediato.

Mantenimiento y ventanas de supresión

Durante trabajos planificados, los sistemas DCiM permiten activar el modo mantenimiento para suprimir alarmas en dispositivos concretos sin desactivar la monitorización global. Esto evita el ruido durante ventanas de mantenimiento y el riesgo de pasar por alto eventos reales en el resto de la infraestructura.

Protocolo de escalado al NOC

La fatiga de alarmas ocurre cuando el volumen de notificaciones supera la capacidad de procesamiento del equipo operativo. El resultado es que las alertas empiezan a ignorarse, incluyendo las críticas con consecuencias graves para la disponibilidad.
Las causas más habituales son:

- Umbrales demasiado estrechos, generando alarmas por fluctuaciones normales.
- Ausencia de tiempo de persistencia (dwell), disparando eventos puntuales sin relevancia real.
- Sin duplicación: múltiples sensores alertando del mismo evento de forma independiente.
- Alarmas informativas enviadas por los mismos canales que las críticas.

Regla del sector: más de 1 alarma por minuto durante un turno normal de operación indica que la arquitectura de alarmas necesita revisión.

Integración DCIM / BMS / ITSM

- **DCIM**: consolida datos ambientales y de potencia, aplica la lógica de umbrales y genera alarmas normalizadas.
- **BMS:** gestiona sistemas mecánicos (HVAC, grupos de presión, detección de incendios) y comparte datos con el DCiM.
- **ITSM**: recibe alarmas del DCiM y genera tickets con propietario, runbook y SLA de resolución.

Arquitectura de monitorización: niveles de despliegue

La arquitectura de monitorización no es única: cada instalación requiere un modelo adaptado a su tamaño, criticidad y recursos. Existen tres modelos de referencia que escalan progresivamente.

Modelo autónomo (sala única)

Adecuado para instalaciones pequeñas, menos de 20 racks, o salas de telecomunicaciones remotas sin personal permanente. Un controlador local recoge los datos de sensores de temperatura, humedad y corriente, y envía alertas por email o SMS. No hay integración con plataformas de mayor nivel.

- Ventajas: coste bajo, despliegue rápido, sin dependencia de sistemas centrales.
- Limitaciones: sin correlación de eventos, sin trazabilidad histórica profunda, sin integración con ITSM.

Modelo de red (múltiples salas o edificios)

Los gateways locales normalizan y reenvían la telemetría a una plataforma central. Este modelo permite visibilidad unificada, correlación de alarmas entre ubicaciones y QA/QC (control de calidad de los datos recibidos) centralizado.

- Ventajas: visión consolidada, deduplicación de alarmas, reporting centralizado.
- Limitaciones: requiere conectividad estable entre sites y mayor complejidad de configuración.

Modelo integrado completo

La plataforma DCiM se integra con el BMS del edificio y con el ITSM corporativo. Las alarmas generan tickets automáticamente con el runbook incluido, los cuadros de mando muestran estado en tiempo real a operadores, responsables de instalaciones y dirección, y los informes periódicos documentan las desviaciones frente a los SLAs acordados.

- Ventajas: máxima trazabilidad, respuesta automatizada, soporte a auditorías.
- Limitaciones: mayor inversión inicial, requiere integración de datos entre sistemas heterogéneos.

Buenas prácticas operativas

Calibración y mantenimiento de sensores

Un sensor descalibrado es peor que no tener sensor: genera falsa confianza. Los sensores de temperatura y humedad deben calibrarse al menos una vez al año o cuando los datos muestren desviaciones sistemáticas respecto a medidas de referencia. Los sensores de corriente requieren verificación semestral en instalaciones críticas.

Revisión periódica de umbrales

Los umbrales configurados en la puesta en marcha pueden volverse inadecuados a medida que cambia la carga del data center. La revisión trimestral de umbrales y la validación semestral mediante ejercicios de simulación son practicas recomendadas por Uptime Institute.

Runbooks operativos

Sin runbook, la respuesta depende del conocimiento individual de quien esté de guardia, lo que introduce variabilidad y alarga el tiempo de resolución. Este es uno de los factores que alimenta la fatiga operativa descrita en el capítulo 10.3: si cada incidente se gestiona de forma diferente, el equipo dedica más tiempo a decidir qué hacer que a hacerlo. Un catálogo de runbooks bien mantenido es el antídoto más eficaz.

KPIs de gestión de alarmas

Los indicadores clave de rendimiento para la gestión de alarmas (MTTD, MTTA, MTTR, ratio de falsas alarmas y alarmas por turno) están definidos y tabulados en el capítulo 10.5, junto con los objetivos recomendados para cada uno. Se recomienda consultar ese apartado como referencia operativa central.

Fuentes y referencias:

- ASHRAE TC 9.9: Thermal Guidelines for Data Processing Environments, 5.a ed. (2021). ashrae.org
- Uptime Institute: Global Data Center Survey 2024. journal.uptimeinstitute.com
- MFE-IS: Data Center Environmental Monitoring: An In-Depth Guide. mfe-is.com
- INOC: 5 Key Processes for Network Operations Centers. inoc.com envigilance.com: ASHRAE TC 9.9 - Data Center Thermal Guide (2026).
- U.S. Department of Energy: Data Center Metering and Resource Guide. datacenters.lbl.gov