

DCIM, BMS E EPMS EM DATA CENTERS: DIFERENÇAS, INTEGRAÇÃO E ARQUITETURA

Entenda as diferenças entre DCIM, BMS e EPMS em Data Centers: funções, arquitetura, protocolos, alarmes, integração, cibersegurança e comissionamento.

SUMÁRIO

1. POR QUE DCIM, BMS E EPMS NÃO SÃO SINÔNIMOS?	4
2. O QUE É BMS EM UM DATA CENTER?	5
3. O QUE É EPMS EM UM DATA CENTER?	6
4. O QUE É DCIM EM UM DATA CENTER?	6
5. QUAL SISTEMA DEVE SER A FONTE DA VERDADE?	7
6. ARQUITETURA EM CAMADAS PARA INTEGRAÇÃO	7
6.1. 1. CAMPO E EQUIPAMENTOS	7
6.2. 2. CONTROLE LOCAL E SUPERVISÃO ESPECIALIZADA	7
6.3. 3. INTEGRAÇÃO E NORMALIZAÇÃO	8
6.4. 4. DCIM E OPERAÇÃO	8
6.5. 5. ANALYTICS E SISTEMAS CORPORATIVOS	8
7. PROTOCOLOS E INTERFACES MAIS COMUNS	8
7.1. BACNET	8
7.2. MODBUS	8
7.3. SNMP	9
7.4. OPC UA	9
7.5. REDFISH	9
7.6. APIS REST, WEBHOOKS E MENSAGERIA	9
8. MODELO DE DADOS E IDENTIFICAÇÃO DOS ATIVOS	9
9. ALARMES: ONDE GERAR, ONDE CONSOLIDAR E ONDE AGIR?	10
10. CORRELAÇÃO ENTRE ENERGIA, CLIMATIZAÇÃO E TIC	10
11. TEMPO, RESOLUÇÃO E QUALIDADE DOS DADOS	11
12. PUE, WUE, CER E OUTROS INDICADORES	11
13. PLANEJAMENTO DE CAPACIDADE	11
14. CONTROLE: O DCIM DEVE COMANDAR EQUIPAMENTOS?	12
15. CIBERSEGURANÇA DA INTEGRAÇÃO	12
16. DISPONIBILIDADE DOS PRÓPRIOS SISTEMAS DE MONITORAMENTO	12
17. COMO INTEGRAR UM DATA CENTER EXISTENTE	12
17.1. 1. INVENTARIAR PLATAFORMAS E DISPOSITIVOS	13
17.2. 2. DEFINIR CASOS DE USO	13
17.3. 3. DEFINIR FONTES PROPRIETÁRIAS	13
17.4. 4. MAPEAR PONTOS E ATIVOS	13
17.5. 5. PROJETAR A ARQUITETURA DE REDE E SEGURANÇA	13
17.6. 6. IMPLANTAR POR DOMÍNIO OU ZONA	13

17.7. 7. COMMISSIONAR E DOCUMENTAR	13
18. COMMISSIONAMENTO DE DCIM, BMS E EPMS	13
19. ERROS COMUNS EM PROJETOS DE INTEGRAÇÃO	14
19.1. COMPRAR O SOFTWARE ANTES DE DEFINIR OS CASOS DE USO	14
19.2. DUPLICAR COLETA EM VÁRIOS SISTEMAS	14
19.3. CONFUNDIR DASHBOARD COM FONTE DA VERDADE	14
19.4. NÃO PADRONIZAR NOMES E IDENTIFICADORES	14
19.5. CENTRALIZAR CONTROLES CRÍTICOS NO DCIM	14
19.6. IGNORAR RESOLUÇÃO E RETENÇÃO	14
19.7. NÃO PROJETAR CIBERSEGURANÇA OT	15
19.8. NÃO TRATAR MUDANÇA E ATUALIZAÇÃO	15
19.9. COMMISSIONAR SOMENTE EM CONDIÇÃO NORMAL	15
20. MATRIZ DE DECISÃO PARA O PROJETO	15
21. ENTREGÁVEIS RECOMENDADOS	15
22. CONCLUSÃO	16

Data Centers produzem milhares de pontos de informação sobre energia, climatização, ambiente, ativos de TIC, capacidade, alarmes e manutenção. O desafio não é apenas coletar esses dados, mas definir qual sistema é responsável por cada função, como os dados serão integrados e qual plataforma será considerada a fonte confiável para cada tipo de informação.

Nesse contexto, três siglas aparecem com frequência: **BMS**, **EPMS** e **DCIM**. Elas não representam o mesmo sistema. Um BMS supervisiona e controla principalmente a infraestrutura predial e mecânica. Um EPMS aprofunda a observabilidade da distribuição elétrica. Um DCIM relaciona infraestrutura física, ativos de TIC, capacidade, energia, ambiente e processos operacionais.

A sobreposição entre produtos pode confundir a especificação. Algumas plataformas comerciais incorporam recursos das três categorias, enquanto outras atuam somente em uma camada. Por isso, a arquitetura deve ser definida por responsabilidades, dados, interfaces e estados de falha, e não apenas pelo nome do software.

Este artigo apresenta as diferenças entre DCIM, BMS e EPMS, explica como integrar essas plataformas e estabelece critérios para projeto, implantação, comissionamento e operação em Data Centers.

1. POR QUE DCIM, BMS E EPMS NÃO SÃO SINÔNIMOS?

Os três sistemas podem exibir temperaturas, potência, estados e alarmes. Essa semelhança na interface não significa que tenham a mesma finalidade.

O **BMS – Building Management System** atua próximo aos sistemas prediais e de climatização. Ele recebe sinais de sensores, controladores, equipamentos HVAC, bombas, válvulas, ventiladores e outros componentes, permitindo supervisão, sequenciamento, controle e alarmes.

O **EPMS – Electrical Power Monitoring System** é especializado na infraestrutura elétrica. Ele coleta medições de medidores, relés, UPS, painéis, unidades de distribuição, barramentos e circuitos, oferecendo análise histórica, eventos, qualidade de energia e suporte à investigação de falhas.

O **DCIM – Data Center Infrastructure Management** relaciona o mundo de Facilities ao mundo de TIC. Ele organiza ativos, racks, circuitos, conexões, energia, ambiente, capacidade, dependências, mudanças, documentação e indicadores operacionais.

Critério	BMS	EPMS	DCIM
Foco principal	Sistemas prediais, mecânicos e ambientais	Distribuição e qualidade da energia elétrica	Infraestrutura do Data Center, ativos e capacidade
Objetos típicos	CRAC, CRAH, chillers, bombas, válvulas, sensores, dampers	Medidores, relés, UPS, QGBT, PDU, RPP, barramentos e circuitos	Sites, salas, racks, ativos, portas, circuitos, capacidade e dependências
Função predominante	Supervisão e controle	Monitoramento elétrico e análise	Correlação, inventário, planejamento e governança operacional
Resolução necessária	Compatível com controle e supervisão predial	Pode exigir eventos e dados elétricos de alta resolução	Normalmente orientada a estado, tendência, capacidade e workflow
Fonte da verdade típica	Estado e comandos dos sistemas prediais	Grandezas e eventos elétricos	Inventário, topologia, ocupação, capacidade e relações entre ativos
Usuários principais	Operação predial e HVAC	Engenharia elétrica e operação de energia	Operação de Data Center, Facilities, TIC, capacidade e gestão

A arquitetura madura não tenta transformar uma única plataforma em proprietária de tudo. Ela define responsabilidades e integra os dados necessários para que cada sistema execute sua função.

2. O QUE É BMS EM UM DATA CENTER?

O BMS, também chamado de BAS em alguns contextos, é a plataforma de automação e supervisão predial. Em um Data Center, sua criticidade aumenta porque a disponibilidade dos equipamentos de TIC depende diretamente das condições de climatização, circulação de fluidos, ventilação, umidade e pressurização.

O BMS pode supervisionar e controlar:

A **ABNT NBR 17207:2025** estabelece critérios ambientais para ambientes de TIC e reforça que temperatura, umidade, ponto de orvalho e vazão de remoção de calor são parâmetros fundamentais. Esses pontos normalmente são medidos e controlados pela infraestrutura de automação predial.

O BMS deve manter os laços de controle locais mesmo quando a integração com sistemas superiores estiver indisponível. Uma falha de comunicação com o DCIM não pode impedir o controle de temperatura, a alternância de bombas ou a atuação de uma sequência de contingência.

Sistemas de detecção e alarme de incêndio, controle de acesso e outras funções de segurança podem enviar estados ao BMS ou ao DCIM, mas suas funções críticas devem

permanecer em plataformas dedicadas, conforme a engenharia e os requisitos aplicáveis.

3. O QUE É EPMS EM UM DATA CENTER?

O EPMS é a plataforma de monitoramento do sistema de energia elétrica. Sua função não é apenas mostrar a potência instantânea, mas registrar o comportamento da cadeia elétrica e apoiar a análise de disponibilidade, capacidade, eficiência e causa raiz.

Um EPMS pode integrar dados de:

As capacidades típicas incluem:

O EPMS possui profundidade elétrica que um BMS genérico normalmente não oferece. Um BMS pode receber um alarme de disjuntor aberto, mas o EPMS pode correlacionar grandezas, sequência temporal, eventos de proteção e qualidade de energia associados à ocorrência.

As funções de proteção permanecem nos relés, disjuntores e controladores locais. O EPMS observa, registra, analisa e, quando previsto no projeto, pode encaminhar comandos supervisionados. Ele não substitui a proteção elétrica independente.

4. O QUE É DCIM EM UM DATA CENTER?

DCIM é uma camada de gestão da infraestrutura física do Data Center. Seu objetivo é conectar informações de Facilities, energia, ambiente e TIC para apoiar operação, capacidade, expansão, mudança e governança.

Uma solução DCIM pode incluir:

A solução de **Data Center Infrastructure Management da A3A Engenharia** trata o DCIM como uma camada de governança técnica, integrando inventário, documentação, monitoramento e capacidade. O DCIM não deve duplicar indiscriminadamente dados que já possuem uma fonte proprietária confiável. Em vez disso, deve referenciar, consumir e contextualizar essas informações.

Por exemplo, o valor instantâneo de potência pode vir do EPMS, o estado de uma válvula pode vir do BMS e a relação entre aquele circuito, o rack e os serviços de TIC pode pertencer ao DCIM.

5. QUAL SISTEMA DEVE SER A FONTE DA VERDADE?

A expressão **source of truth** precisa ser aplicada por domínio. Não é realista declarar que uma única plataforma será a fonte da verdade de todos os dados do Data Center.

Uma divisão funcional possível é:

Domínio de informação	Fonte proprietária recomendada
Temperatura, umidade, válvulas, bombas e estados HVAC	BMS ou controlador local
Medições elétricas, qualidade de energia e eventos de proteção	EPMS e dispositivos elétricos
Ativos, racks, posição, portas, circuitos lógicos e capacidade	DCIM ou plataforma de inventário
Configuração de servidores e hardware	Ferramentas de gestão de TIC, Redfish ou plataformas de fabricante
Endereçamento, VLANs, VRFs e redes	IPAM/DCIM ou source of truth de rede
Incidentes, mudanças e ordens de serviço	ITSM, EAM/CMMS ou workflow corporativo
Indicadores consolidados	Camada analítica com rastreabilidade das fontes

O **NetBox**, por exemplo, pode funcionar como source of truth para redes, IPAM, racks, dispositivos, conexões e circuitos. Ele não substitui um EPMS de alta resolução nem um BMS responsável por controle mecânico. A integração deve respeitar essas fronteiras.

6. ARQUITETURA EM CAMADAS PARA INTEGRAÇÃO

Uma arquitetura integrada pode ser organizada em cinco camadas.

6.1. 1. CAMPO E EQUIPAMENTOS

Inclui sensores, medidores, relés, controladores, UPS, PDUs, CRACs, chillers, bombas, válvulas, servidores, switches e demais dispositivos que produzem dados ou executam comandos.

6.2. 2. CONTROLE LOCAL E SUPERVISÃO ESPECIALIZADA

Nesta camada ficam controladores HVAC, PLCs, BMS, EPMS, sistemas de monitoramento de baterias, plataformas de fabricantes e outros sistemas responsáveis por operação especializada.

6.3. 3. INTEGRAÇÃO E NORMALIZAÇÃO

Gateways, conectores, APIs, coletores, brokers e serviços de integração convertem protocolos, normalizam unidades, associam identificadores e aplicam regras de qualidade de dados.

6.4. 4. DCIM E OPERAÇÃO

O DCIM relaciona dados ao inventário físico e lógico, à topologia, à capacidade e aos processos. Ele permite responder não apenas que um alarme ocorreu, mas quais racks, circuitos, ativos, clientes ou serviços podem ser afetados.

6.5. 5. ANALYTICS E SISTEMAS CORPORATIVOS

Dados consolidados podem alimentar ferramentas de BI, sustentabilidade, gestão de ativos, ITSM, manutenção, planejamento financeiro e relatórios executivos.

A integração não precisa obrigatoriamente seguir uma pirâmide rígida. Em alguns projetos, o DCIM coleta diretamente SNMP de PDUs e UPS. Em outros, recebe os pontos normalizados pelo BMS ou EPMS. A decisão deve considerar responsabilidade, desempenho, licenciamento, disponibilidade e risco de duplicação.

7. PROTOCOLOS E INTERFACES MAIS COMUNS

A integração entre DCIM, BMS e EPMS raramente utiliza um único protocolo.

7.1. BACNET

O BACnet é um padrão de comunicação para automação e controle predial. É comum em chillers, controladores, unidades HVAC e BMS. Sua estrutura de objetos facilita a representação de pontos, estados, alarmes, agendas e comandos.

7.2. MODBUS

O Modbus é amplamente utilizado em medidores, UPS, relés, geradores, controladores e equipamentos mecânicos. Pode operar em redes seriais ou TCP/IP. A simplicidade facilita a integração, mas o significado dos registradores, escalas e unidades precisa ser documentado pelo fabricante.

7.3. SNMP

O SNMP é frequente em equipamentos de TIC, UPS, PDUs inteligentes, sensores de rack e dispositivos de rede. A qualidade da integração depende das MIBs, traps, polling, identificação dos objetos e tratamento das versões de segurança.

7.4. OPC UA

O OPC UA oferece modelos de informação, serviços e mecanismos de comunicação para interoperabilidade entre sistemas industriais e empresariais. Pode ser útil quando o projeto exige semântica mais estruturada, descoberta de objetos e integração entre múltiplas plataformas OT.

7.5. REDFISH

O Redfish utiliza interfaces RESTful e modelos padronizados para gestão de servidores, sistemas e equipamentos de Data Center. Ele pode fornecer inventário, saúde, energia, temperatura e operações de gerenciamento fora de banda, conforme o suporte do fabricante.

7.6. APIS REST, WEBHOOKS E MENSAGERIA

APIs permitem integrar DCIM, ITSM, inventário, analytics e sistemas corporativos. Webhooks e brokers de mensagens reduzem a dependência de polling para eventos. A especificação deve definir autenticação, versionamento, limites de chamadas, tratamento de falhas e reconciliação de dados.

O protocolo resolve apenas o transporte. A interoperabilidade real exige semântica: nome do ponto, equipamento, unidade, escala, qualidade, timestamp, estado, criticidade e relação com o ativo correspondente.

8. MODELO DE DADOS E IDENTIFICAÇÃO DOS ATIVOS

A integração falha quando sistemas diferentes usam nomes incompatíveis para o mesmo objeto. Um medidor pode aparecer no EPMS como MDB1_MTR_04, no BMS como QGBT-M04 e no DCIM como MED-DC01-004.

O projeto deve estabelecer:

O DCIM pode manter a relação entre os identificadores, mas não deve alterar automaticamente a nomenclatura dos sistemas especializados sem governança. Uma camada de mapeamento evita que atualizações de um fornecedor quebrem todas as

integrações.

9. ALARMES: ONDE GERAR, ONDE CONSOLIDAR E ONDE AGIR?

Alarmes devem ser gerados o mais próximo possível da condição que precisam detectar. Um controlador HVAC deve reconhecer perda de vazão; um relé deve registrar uma atuação elétrica; uma UPS deve informar bypass ou falha interna.

A plataforma superior pode normalizar e correlacionar esses eventos. O fluxo pode seguir esta lógica:

1. o dispositivo identifica a condição; 2. o BMS ou EPMS registra o alarme especializado; 3. a integração transmite estado, severidade, timestamp e contexto; 4. o DCIM relaciona o alarme aos racks, ativos e capacidades afetadas; 5. o ITSM cria ou atualiza o incidente e atribui responsabilidades; 6. a equipe executa o procedimento operacional e registra a resolução.

A simples repetição do mesmo alarme em quatro telas cria ruído. É necessário definir qual plataforma reconhece, silencia, encerra e audita cada evento.

O modelo de alarmes deve incluir:

10. CORRELAÇÃO ENTRE ENERGIA, CLIMATIZAÇÃO E TIC

O principal valor da integração aparece quando os dados deixam de ser isolados.

Considere a abertura inesperada de um disjuntor que alimenta uma PDU. O EPMS registra a mudança de estado, grandezas elétricas e sequência do evento. O BMS pode identificar redução de carga térmica ou alteração no comportamento da climatização. O DCIM relaciona a PDU aos circuitos, racks e ativos alimentados. O ITSM registra o incidente e a equipe avalia o impacto nos serviços.

Em outro exemplo, uma CRAH perde capacidade. O BMS detecta falha do ventilador ou perda de vazão. Sensores mostram aumento de temperatura na entrada dos racks. O DCIM identifica os ativos naquela zona, a carga elétrica associada e a margem disponível para redistribuição. A operação pode decidir entre reduzir carga, migrar serviços ou acionar capacidade redundante.

Essa correlação depende de topologia atualizada. Sem relação entre pontos, circuitos, equipamentos e racks, a integração produz dashboards, mas não produz decisão operacional confiável.

11. TEMPO, RESOLUÇÃO E QUALIDADE DOS DADOS

Nem todos os dados possuem a mesma necessidade de atualização.

Eventos de proteção e qualidade de energia podem exigir registros de alta resolução no dispositivo ou EPMS. Temperaturas e pressões podem ser coletadas em intervalos compatíveis com a dinâmica térmica. Inventário e capacidade mudam em ritmos menores, normalmente por processos de mudança.

O projeto deve definir:

NTP pode atender grande parte da supervisão. Aplicações que exigem correlação temporal mais rigorosa podem demandar arquiteturas específicas de sincronização. O critério deve partir da análise dos eventos que precisam ser reconstruídos.

12. PUE, WUE, CER E OUTROS INDICADORES

A integração pode apoiar indicadores de eficiência, mas o software não corrige uma fronteira de medição mal definida.

A ABNT NBR 17207 referencia:

Para calcular indicadores confiáveis, devem ser definidos:

O EPMS fornece grande parte das medições elétricas. O BMS pode fornecer água, temperaturas, vazões e estados mecânicos. O DCIM ou a camada analítica consolida os dados dentro das fronteiras acordadas.

13. PLANEJAMENTO DE CAPACIDADE

O DCIM deve transformar medições e inventário em capacidade utilizável. A capacidade de um rack não é apenas espaço em unidades de altura.

A análise pode considerar:

Dados do EPMS mostram utilização elétrica. Dados do BMS demonstram comportamento térmico. O DCIM relaciona essas medições à topologia e às reservas. Assim, uma instalação pode ter espaço físico livre, mas não possuir capacidade elétrica ou térmica suficiente para um novo rack.

14. CONTROLE: O DCIM DEVE COMANDAR EQUIPAMENTOS?

A resposta depende da arquitetura e da análise de risco. Em muitos projetos, o DCIM opera como camada de observação, correlação e workflow, enquanto os comandos permanecem no BMS, EPMS, controladores ou plataformas dos fabricantes.

Quando comandos são permitidos a partir de uma camada superior, devem existir:

Automação sem governança pode transformar uma integração de monitoramento em uma nova causa comum de falha. O projeto deve privilegiar controle local resiliente e integração superior com autoridade limitada e auditável.

15. CIBERSEGURANÇA DA INTEGRAÇÃO

BMS e EPMS fazem parte do ambiente de tecnologia operacional. Sua integração com DCIM, nuvem, sistemas corporativos e acesso remoto aumenta a superfície de ataque.

A arquitetura deve considerar:

A **NIST SP 800-82 Rev. 3** trata sistemas de automação predial e monitoramento ambiental como tecnologia operacional e recomenda que segurança seja compatibilizada com requisitos de desempenho, confiabilidade e segurança física.

Protocolos legados não devem ser expostos diretamente a redes não confiáveis. Quando não há suporte nativo a autenticação e criptografia, a proteção precisa ser implementada pela arquitetura de rede, gateways e controles compensatórios.

16. DISPONIBILIDADE DOS PRÓPRIOS SISTEMAS DE MONITORAMENTO

Uma plataforma que monitora infraestrutura crítica também precisa de arquitetura de disponibilidade.

Devem ser avaliados:

A perda do DCIM não pode eliminar controles locais. A perda do BMS central não deve interromper laços autônomos essenciais. A perda do EPMS não pode desabilitar a proteção elétrica. Essa independência precisa ser comprovada em testes.

17. COMO INTEGRAR UM DATA CENTER EXISTENTE

A implantação deve começar por diagnóstico, não pela instalação imediata de conectores.

17.1. 1. INVENTARIAR PLATAFORMAS E DISPOSITIVOS

Identificar BMS, EPMS, sistemas de fabricantes, versões, protocolos, licenças, servidores, redes, pontos disponíveis e responsáveis.

17.2. 2. DEFINIR CASOS DE USO

Exemplos: gestão de capacidade, alarmes consolidados, PUE, investigação elétrica, mapa térmico, workflow de mudanças, relatórios de clientes ou operação multisite.

17.3. 3. DEFINIR FONTES PROPRIETÁRIAS

Cada dado deve possuir origem, responsável, frequência, unidade e regra de atualização.

17.4. 4. MAPEAR PONTOS E ATIVOS

Relacionar tags, registradores, OIDs, objetos BACnet, endpoints de API e recursos Redfish aos ativos e localizações do DCIM.

17.5. 5. PROJETAR A ARQUITETURA DE REDE E SEGURANÇA

Definir segmentos, firewalls, gateways, certificados, contas técnicas, acesso remoto e registro de eventos.

17.6. 6. IMPLANTAR POR DOMÍNIO OU ZONA

Um piloto controlado permite validar nomenclatura, qualidade, alarmes e desempenho antes de escalar.

17.7. 7. COMMISSIONAR E DOCUMENTAR

As integrações precisam ser testadas ponto a ponto, funcionalmente e em estados de falha.

O serviço de **Diagnóstico e Modernização de Data Centers e CPDs** pode organizar essa linha de base antes da implantação, identificando lacunas de inventário, monitoramento, redes, capacidade e documentação.

18. COMISSONAMENTO DE DCIM, BMS E EPMS

O aceite não deve se limitar à confirmação de que as telas estão recebendo valores.

O plano de comissionamento pode incluir:

O comissionamento deve utilizar uma matriz de pontos que identifique origem, destino, transformação, unidade, criticidade, alarme, comando e evidência de teste.

O artigo sobre **Comissionamento de Data Center: testes, níveis e critérios de aceite** apresenta a progressão entre inspeção, testes funcionais e testes integrados. Para DCIM, BMS e EPMS, essa progressão precisa incluir tanto a infraestrutura física quanto a cadeia de dados.

19. ERROS COMUNS EM PROJETOS DE INTEGRAÇÃO

19.1. COMPRAR O SOFTWARE ANTES DE DEFINIR OS CASOS DE USO

A plataforma pode ser implantada sem resolver problemas operacionais reais.

19.2. DUPLICAR COLETA EM VÁRIOS SISTEMAS

Três plataformas consultando diretamente o mesmo dispositivo aumentam carga, complexidade e divergência de dados.

19.3. CONFUNDIR DASHBOARD COM FONTE DA VERDADE

Uma tela consolidada pode exibir dados sem possuir autoridade sobre sua origem, qualidade ou atualização.

19.4. NÃO PADRONIZAR NOMES E IDENTIFICADORES

Sem um modelo de dados, a integração depende de associações manuais e frágeis.

19.5. CENTRALIZAR CONTROLES CRÍTICOS NO DCIM

A indisponibilidade da camada superior pode comprometer funções que deveriam permanecer locais.

19.6. IGNORAR RESOLUÇÃO E RETENÇÃO

Dados agregados podem ser insuficientes para investigar eventos elétricos rápidos ou reconstruir uma sequência de falha.

19.7. NÃO PROJETAR CIBERSEGURANÇA OT

Conectar BMS e EPMS diretamente à rede corporativa ou à internet cria riscos desnecessários.

19.8. NÃO TRATAR MUDANÇA E ATUALIZAÇÃO

Substituições de medidores, racks, controladores e firmware podem quebrar tags, APIs e dashboards.

19.9. COMMISSIONAR SOMENTE EM CONDIÇÃO NORMAL

Falhas de rede, servidor, gateway, energia e comunicação precisam ser testadas.

20. MATRIZ DE DECISÃO PARA O PROJETO

Necessidade predominante	Sistema principal	Integrações recomendadas
Controle de climatização e hidráulica	BMS	DCIM, analytics e ITSM
Qualidade de energia e causa raiz elétrica	EPMS	DCIM, BMS e manutenção
Inventário, rack, capacidade e mudança	DCIM	EPMS, BMS, IPAM e ITSM
Source of truth de rede e conectividade	NetBox/IPAM/DCIM	Monitoramento, automação e ITSM
Indicadores de energia e sustentabilidade	EPMS + BMS + analytics/DCIM	Medição fiscal, TIC e relatórios corporativos
Alarmes consolidados e impacto nos serviços	DCIM ou plataforma de eventos	BMS, EPMS, TIC e ITSM
Controle especializado de equipamento	Controlador ou plataforma do fabricante	BMS/EPMS para supervisão e DCIM para contexto

A escolha não é entre DCIM, BMS ou EPMS. Em Data Centers com infraestrutura crítica, os três podem ser necessários, desde que suas funções sejam complementares e suas fronteiras estejam documentadas.

21. ENTREGÁVEIS RECOMENDADOS

Um projeto de integração pode produzir:

22. CONCLUSÃO

BMS, EPMS e DCIM possuem áreas de sobreposição, mas resolvem problemas diferentes. O BMS mantém a infraestrutura predial e mecânica sob controle. O EPMS oferece profundidade sobre a cadeia elétrica. O DCIM relaciona ativos, capacidade, energia, ambiente e processos de operação.

A integração eficaz exige mais do que protocolos compatíveis. Ela depende de fonte proprietária por domínio, modelo de dados, identificação consistente, qualidade temporal, filosofia de alarmes, segurança OT, disponibilidade e comissionamento.

Quando essas bases são definidas, o Data Center deixa de operar com telas e bancos isolados e passa a utilizar uma arquitetura de informação capaz de apoiar disponibilidade, capacidade, eficiência, manutenção e tomada de decisão.

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 17207:2025 – Sistemas de ventilação e climatização em ambientes de tecnologia da informação, de comunicação e de data center. Rio de Janeiro: ABNT, 2025. Disponível no [catálogo da ABNT](#).

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC TS 22237-7:2018 – Information technology – Data centre facilities and infrastructures – Part 7: Management and operational information. Geneva: ISO, 2018. Disponível na [página oficial da ISO](#).

[3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security. Gaithersburg: NIST, 2023. Disponível na [página oficial do NIST](#).

[4] BACNET INTERNATIONAL. About BACnet: global data communications standard for building automation and control networks. Kennesaw: BACnet International. Disponível no [site oficial do BACnet International](#).

[5] MODBUS ORGANIZATION. Modbus Application Protocol Specification V1.1b3 and implementation guides. Boxborough: Modbus Organization. Disponível no [site oficial da Modbus Organization](#).

[6] OPC FOUNDATION. OPC Unified Architecture – Part 1: Overview and Concepts. Scottsdale: OPC Foundation. Disponível na [referência oficial da OPC Foundation](#).

[7] DMTF. Redfish Data Model Specification. Portland: Distributed Management Task Force. Disponível no [documento oficial do DMTF](#).

[8] EATON. Electrical Power Monitoring System software — EPMS. Dublin: Eaton. Disponível na [página oficial da Eaton](#).

[9] SCHNEIDER ELECTRIC. Selecting a Building Management System (BMS) for Sites with a Data Center or IT Room. Rueil-Malmaison: Schneider Electric, 2016. Disponível na [biblioteca oficial da Schneider Electric](#).

[10] SCHNEIDER ELECTRIC. How Modern DCIM Supports CIOs in Managing Distributed, AI-Driven IT Environments. Rueil-Malmaison: Schneider Electric, 2026. Disponível na [biblioteca oficial da Schneider Electric](#).

Qual é a diferença entre DCIM e BMS? O BMS supervisiona e controla principalmente sistemas prediais e mecânicos, como climatização, bombas, válvulas e sensores ambientais. O DCIM relaciona esses dados ao inventário de racks, ativos de TIC, circuitos, capacidade, dependências e processos operacionais. **Qual é a diferença entre BMS e EPMS?** O BMS é orientado à automação predial e ao controle de sistemas mecânicos. O EPMS é especializado em monitoramento elétrico, medições, eventos, qualidade de energia e investigação da cadeia de distribuição. **O DCIM substitui o EPMS?** Não necessariamente. O DCIM pode consumir medições do EPMS e relacioná-las a racks, ativos e capacidade, mas normalmente não oferece a mesma profundidade em qualidade de energia, formas de onda, sequência de eventos e análise elétrica. **O DCIM pode controlar equipamentos do Data Center?** Algumas plataformas permitem comandos, mas a autoridade deve ser definida por análise de risco. Laços críticos e intertravamentos devem permanecer nos controladores locais, BMS, relés ou sistemas especializados, com comandos superiores limitados e auditáveis. **Quais protocolos são usados para integrar DCIM, BMS e EPMS?** São comuns BACnet, Modbus, SNMP, OPC UA, Redfish, APIs REST, webhooks e mensageria. A escolha depende dos dispositivos, da resolução necessária, da segurança, do suporte dos fabricantes e do modelo de dados. **Qual sistema deve calcular o PUE?** O cálculo pode ocorrer no DCIM, EPMS ou plataforma analítica, desde que a fronteira de medição, os medidores de entrada e de TIC, os períodos, a qualidade dos dados e a fórmula estejam documentados. O EPMS normalmente fornece as medições elétricas. **O NetBox é um DCIM?** O NetBox oferece recursos de DCIM e IPAM para sites, racks, dispositivos, conexões, circuitos e redes. Ele pode atuar como source of truth de infraestrutura, mas não substitui automaticamente BMS, EPMS ou plataformas especializadas de controle e monitoramento. **Como evitar alarmes duplicados em várias plataformas?** É necessário definir onde o alarme nasce, qual sistema o reconhece, como ele é normalizado, qual plataforma consolida o impacto e como o incidente é encerrado. Severidade, timestamp, estado e responsabilidade devem ser consistentes. **Como proteger a integração entre BMS, EPMS e DCIM?** A arquitetura deve segmentar redes OT e TI,

controlar fluxos por firewall, utilizar gateways ou DMZ, aplicar menor privilégio, autenticação forte, logs, hardening, backups e acesso remoto temporário e auditado. **O que deve ser testado no comissionamento?** Devem ser validados pontos, unidades, escalas, timestamps, alarmes, comandos, intertravamentos, perda de comunicação, failover, permissões, retenção, APIs, dashboards, backup, restauração e eventos integrados com carga representativa.

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.