WHITEPAPER

# SUSTENTABILIDADE OPERACIONAL EM DATA CENTERS: COMO PRESERVAR A RESILIÊNCIA

Entenda como preservar a resiliência de Data Centers por meio de gestão, manutenção, pessoas, procedimentos, testes e controle de riscos operacionais.

A3A® Engenharia de Sistemas

## SUMÁRIO

A infraestrutura de um Data Center pode ter sido projetada com redundância, manutenção concorrente, caminhos independentes e sistemas de supervisão. Ainda assim, essa resiliência pode ser progressivamente perdida quando a operação acumula manutenções adiadas, procedimentos desatualizados, alarmes permanentes, dependência de pessoas específicas, mudanças sem controle ou estados degradados que deixam de ser temporários.

É esse problema que a **sustentabilidade operacional em Data Centers** procura evitar. O conceito não se limita à eficiência ambiental e não deve ser confundido com Green Data Center. Aqui, sustentabilidade significa preservar ao longo do tempo a capacidade da infraestrutura de entregar disponibilidade, segurança, capacidade e continuidade de acordo com os requisitos para os quais foi concebida.

O Uptime Institute utiliza o conceito de *Operational Sustainability* para alinhar o programa de gestão da instalação à funcionalidade do Tier instalado. A ISO/IEC TS 22237-7 também relaciona os processos operacionais à entrega de resiliência, disponibilidade, gestão de riscos, capacidade, segurança e eficiência. Em ambos os casos, a mensagem central é a mesma: topologia e equipamentos não produzem desempenho de forma automática; eles dependem de pessoas, processos, manutenção, documentação e disciplina operacional.

Este artigo explica como preservar a resiliência de um Data Center durante sua vida útil. O foco está nos fatores que degradam a disponibilidade, nos pilares da sustentabilidade operacional, nos estados temporários, na manutenção, na gestão de mudanças, na competência das equipes, nos fornecedores, nos testes e no método de avaliação necessário para transformar riscos dispersos em um plano de melhoria priorizado.

## 1. O QUE É SUSTENTABILIDADE OPERACIONAL EM DATA CENTERS?

Sustentabilidade operacional é a capacidade de manter, durante todo o ciclo de vida, o nível de desempenho e resiliência esperado da infraestrutura crítica. Ela procura impedir que decisões cotidianas, restrições de orçamento, mudanças, envelhecimento dos ativos ou falhas de governança reduzam silenciosamente a proteção originalmente prevista.

Em termos práticos, o conceito conecta três perguntas: a instalação continua tecnicamente capaz de atender a carga; a organização possui pessoas e processos para utilizar essa capacidade; e os riscos externos e construtivos permanecem controlados. Uma resposta positiva apenas para a primeira pergunta não comprova sustentabilidade operacional.

O Uptime Institute organiza os fatores de sustentabilidade operacional em três grupos: gestão e operação, características da edificação e localização do site. Esses grupos

mostram que o desempenho de longo prazo não depende apenas das rotinas da equipe.

| Dimensão | Exemplos de fatores | Risco quando não controlada |
|---|---|---|
| Gestão e operação | equipe, manutenção, procedimentos, fornecedores, treinamento, mudanças e planejamento | erro operacional, manutenção inadequada, resposta lenta e perda de conhecimento |
| Características da edificação | acessos, compartimentação, áreas técnicas, rotas de manutenção, proteção física e condições construtivas | intervenções inseguras, propagação de eventos e dificuldade de recuperação |
| Localização do site | energia, conectividade, água, clima, logística, riscos naturais, entorno e acesso de equipes | interrupções externas, isolamento do site e contingências insuficientes |

A ISO/IEC TS 22237-7 complementa essa visão ao estabelecer processos de gestão e operação necessários para entregar resiliência, disponibilidade, mitigação de riscos, capacidade, segurança e eficiência. A sustentabilidade operacional pode, portanto, ser entendida como a aplicação contínua desses processos ao Data Center real, considerando sua topologia, sua criticidade e suas limitações.

### 1.1. SUSTENTABILIDADE OPERACIONAL NÃO É SUSTENTABILIDADE AMBIENTAL

Os dois temas se relacionam, mas possuem intenções diferentes. Sustentabilidade ambiental trata principalmente de energia, água, emissões, materiais e impacto ambiental. Sustentabilidade operacional trata da preservação da disponibilidade e da resiliência por meio de gestão, manutenção e controle de riscos.

Uma medida de eficiência só é operacionalmente sustentável quando mantém os limites de segurança e a capacidade de recuperação. Reduzir equipamentos em operação, elevar setpoints ou ampliar faixas pode ser adequado, desde que a mudança seja analisada, testada, monitorada e reversível. O artigo sobre PUE, WUE e CUE em Data Centers aprofunda a medição de eficiência, enquanto o conteúdo sobre Green Data Center aborda a integração entre sustentabilidade ambiental e resiliência.

## 2. COMO A RESILIÊNCIA PROJETADA SE PERDE NA OPERAÇÃO

A arquitetura define capacidades e possibilidades. A operação determina como essas possibilidades serão utilizadas. Um sistema 2N pode perder independência quando uma manutenção coloca os dois caminhos sob uma mesma condição temporária. Uma configuração N+1 pode ficar sem reserva quando o crescimento da carga não é acompanhado. Um grupo gerador pode estar disponível no painel e indisponível na prática por falta de combustível, bateria de partida, ventilação ou manutenção.

Também ocorre o problema inverso: uma equipe pode manter bons resultados durante anos por conhecimento tácito, mesmo com documentos incompletos. Essa situação parece estável, mas cria dependência de pessoas específicas e dificulta expansão, auditoria, treinamento e resposta a eventos incomuns.

A sustentabilidade operacional consiste em alinhar a capacidade técnica da infraestrutura com os comportamentos, recursos e controles usados para operá-la. O Tier Standard: Operational Sustainability, do Uptime Institute, relaciona o desempenho de longo prazo à forma como a instalação é gerenciada. O princípio central é que a topologia instalada precisa ser acompanhada por práticas operacionais compatíveis com sua complexidade e criticidade.

Por isso, a operação deve ser considerada desde o estudo de viabilidade, o OPR, a URS e o Basis of Design. Requisitos como manutenção concorrente, equipe 24 × 7, disponibilidade de peças, tempos de resposta, acesso a diagramas, testes periódicos e capacidade de operar em estados degradados influenciam decisões de projeto e contratação.

## 3. DA ENTREGA DA OBRA À PRONTIDÃO OPERACIONAL

Um Data Center não se torna operacionalmente pronto apenas porque os equipamentos foram instalados e energizados. A transição entre projeto, construção, comissionamento e operação precisa comprovar que a organização consegue assumir o ativo com segurança.

A prontidão operacional deve avaliar quatro condições. A primeira é técnica: sistemas instalados, configurados, testados e aceitos. A segunda é documental: diagramas, listas, manuais, ajustes, lógicas, inventários e registros compatíveis com o campo. A terceira é humana: equipe definida, treinada, autorizada e capaz de executar rotinas e respostas. A quarta é processual: procedimentos, escalonamentos, manutenção, mudanças, incidentes e continuidade em funcionamento.

O processo de handover deve começar antes do final da implantação. A operação precisa participar de revisões de projeto, inspeções, FAT, SAT, testes funcionais e testes integrados. Essa participação reduz a transferência de sistemas que atendem ao projeto, mas são difíceis de manter, manobrar ou recuperar.

A passagem para operação deve incluir, entre outros elementos:

O artigo Comissionamento de Data Center: testes, níveis e critérios de aceite detalha como as verificações de L1 a L5 e os testes integrados podem produzir evidências para essa transição.

**Prontidão operacional precisa começar antes do handover**

Equipe, procedimentos, documentos, sobressalentes e critérios de aceite devem ser desenvolvidos junto com projeto, implantação e comissionamento.

Conheça a Engenharia Integrada para Data Centers

## 4. MODELO OPERACIONAL: QUEM É RESPONSÁVEL PELO QUÊ?

O modelo operacional define como a organização transforma objetivos de negócio em atividades de operação. Ele estabelece papéis, autoridade, cobertura, interfaces, recursos, fornecedores e critérios de decisão.

Não existe um único modelo válido. Um Data Center corporativo pode manter equipe própria e contratar especialistas para manutenções. Um colocation pode possuir operação permanente, centro de controle e fornecedores em regime de prontidão. Um Edge Data Center pode depender de monitoramento remoto e atendimento regional. O modelo precisa corresponder ao risco, à escala, à localização e à capacidade organizacional.

### 4.1. PROPRIETÁRIO, OPERADOR E USUÁRIOS DA INFRAESTRUTURA

O proprietário define os objetivos, aceita riscos e aprova investimentos. O operador controla o estado da instalação, executa ou coordena rotinas e responde a eventos. Os usuários da infraestrutura — áreas de TI, clientes internos, tenants ou unidades de negócio — definem demandas e requisitos de serviço.

Esses papéis podem estar dentro da mesma organização, mas não devem ser confundidos. Quem solicita uma mudança não deve pressupor que possui autoridade para executá-la. Quem mantém um equipamento não deve alterar o estado da instalação sem coordenação com a operação. Quem aprova orçamento precisa compreender o efeito de manutenção adiada e obsolescência sobre o risco.

### 4.2. EQUIPE PRÓPRIA E FORNECEDORES

A terceirização transfere atividades, não a responsabilidade final pela continuidade. Contratos de manutenção precisam definir escopo, disponibilidade, competências, peças, tempos de atendimento, acesso, documentação, evidências e responsabilidades durante intervenções.

O operador deve saber quais ações o fornecedor pode executar autonomamente e quais dependem de autorização. Também precisa verificar se o conhecimento crítico permanece acessível quando um contrato termina ou um profissional é substituído.

### 4.3. RACI E AUTORIDADE OPERACIONAL

Uma matriz RACI ajuda a distinguir quem executa, quem responde pelo resultado, quem precisa ser consultado e quem deve ser informado. Ela é especialmente importante para mudanças, incidentes, manutenções, testes, comunicação de crise e retorno ao estado normal.

Além da RACI, deve existir autoridade explícita para:

O artigo Owner's Engineering em Data Centers: responsabilidades, matriz RACI e limites de atuação mostra como a governança técnica pode proteger os interesses do proprietário durante projeto, implantação, mudanças e aceite.

## 5. ESTADOS OPERACIONAIS DO DATA CENTER

A equipe não deve enxergar a instalação apenas como "normal" ou "em falha". Data Centers passam por diferentes estados, e cada estado altera margens, riscos e ações permitidas.

| Estado | Característica | Controle necessário |
|---|---|---|
| Normal | Sistemas e redundâncias disponíveis conforme o baseline | Rotinas, monitoramento e manutenção planejada |
| Degradado | Capacidade, caminho ou proteção reduzida | Limites, duração máxima, contingência e comunicação |
| Manutenção | Estado temporário criado para intervenção | MOP, hold points, abortagem e reversão |
| Emergência | Condição anormal com ameaça imediata | EOP, segurança, estabilização e escalonamento |
| Recuperação | Retorno controlado após falha ou intervenção | Verificações, sequência, observação e aceite |
| Expansão ou transição | Baseline sendo alterado por fases | Interfaces temporárias, critérios de avanço e atualização documental |

O estado degradado merece atenção especial. Ele pode existir sem interrupção perceptível da carga, mas com menor capacidade de suportar uma segunda falha. Exemplos incluem uma UPS indisponível, um gerador em manutenção, uma unidade de climatização retirada, um caminho de telecomunicações degradado ou uma automação operando em modo manual.

A organização deve definir quem pode declarar o estado degradado, quais serviços precisam ser informados, qual risco é aceitável, por quanto tempo a condição pode permanecer e quais trabalhos ficam suspensos enquanto a proteção estiver reduzida.

## 6. CENTRO DE OPERAÇÃO, TURNOS E PASSAGEM DE SERVIÇO

A continuidade da operação depende de uma visão compartilhada do estado atual. Em ambientes com cobertura contínua, a troca de turno é uma atividade crítica. Ela precisa transferir informações, não apenas presença física.

A passagem deve registrar alarmes ativos, indisponibilidades, manutenções, mudanças em andamento, estados degradados, restrições, pendências, fornecedores no site, condições externas e decisões tomadas. O próximo turno precisa compreender o que mudou, por que mudou e quais ações estão autorizadas.

O log operacional deve permitir reconstruir a sequência de eventos. Registros úteis incluem horário, origem da informação, ativo, estado anterior, ação executada, resultado, responsável e referência ao incidente, ordem de serviço ou procedimento relacionado.

Em operações remotas, os mesmos princípios se aplicam. A equipe precisa garantir disponibilidade de comunicação, acesso contingencial, câmeras, telemetria, contatos locais e critérios claros para deslocamento. Monitoramento remoto não elimina a necessidade de resposta física quando o evento exige inspeção, manobra ou segurança presencial.

## 7. ROTINAS OPERACIONAIS E FREQUÊNCIA DE CONTROLE

Rotinas estruturadas permitem detectar mudanças antes que se transformem em incidentes. A frequência deve ser definida pela criticidade, pelo comportamento do ativo, pela automação disponível e pelos requisitos do fabricante ou da organização.

| Frequência típica | Exemplos de controle |
|---|---|
| Contínua | Alarmes, estado de fontes, carga, temperatura, umidade, pressão, comunicação e segurança |
| Por turno ou diária | Ronda, revisão de eventos, combustível, condições de salas, vazamentos e obstruções |
| Semanal | Tendências, testes autorizados, pendências, capacidade e condições de ativos críticos |
| Mensal | Indicadores, manutenção, alarmes recorrentes, sobressalentes, contratos e riscos |
| Trimestral ou semestral | Exercícios, inspeções aprofundadas, revisão de capacidade e auditorias técnicas |

| Frequência típica | Exemplos de controle |
|---|---|
| Anual | Testes integrados, revisão do programa operacional, orçamento, obsolescência e continuidade |

A rotina não deve produzir apenas formulários preenchidos. Cada verificação precisa possuir limite, critério de aceitação e ação diante de desvio. Registrar uma temperatura sem definir faixa, tendência ou escalonamento gera dado, mas não controle.

Também é necessário revisar a utilidade das rotinas. Verificações que nunca identificam desvios podem estar mal definidas, automatizadas em outra plataforma ou sendo executadas sem análise. Por outro lado, atividades retiradas da rotina precisam ter sua cobertura assegurada por monitoramento ou outro controle equivalente.

## 8. GESTÃO DE ATIVOS E ESTRATÉGIA DE MANUTENÇÃO

Manutenção de Data Center não é simplesmente cumprir periodicidades de fabricante. A estratégia precisa equilibrar desempenho, risco, custo, vida útil e consequência de falha. A ISO 55001:2024 fornece uma estrutura de gestão de ativos voltada a esse equilíbrio entre valor, desempenho, risco e despesas ao longo do ciclo de vida.

O primeiro passo é possuir um inventário confiável. Cada ativo crítico deve ter identificação, localização, fabricante, modelo, número de série, função, sistema, dependências, criticidade, documentação, garantia, plano de manutenção, histórico e condição atual.

### 8.1. CRITICIDADE DO ATIVO

A criticidade não deve ser definida apenas pelo preço do equipamento. Deve considerar consequência sobre pessoas, ambiente, continuidade, capacidade, segurança, conformidade e tempo de recuperação.

Um sensor barato pode ser crítico se sua falha impedir uma sequência automática. Um quadro de grande porte pode possuir caminhos alternativos e ter menor impacto imediato. A análise deve considerar função, redundância, detectabilidade, modos de falha e disponibilidade de contingência.

## 8.2. MANUTENÇÃO PREVENTIVA, PREDITIVA E BASEADA EM CONDIÇÃO

A manutenção preventiva ocorre em intervalos definidos. A preditiva utiliza medições e tendências para identificar degradação. A manutenção baseada em condição aciona intervenção quando parâmetros mostram necessidade. Essas abordagens podem coexistir no mesmo ativo.

Exemplos incluem termografia, análise de óleo, qualidade de energia, resistência interna de baterias, vibração, temperatura, pressão, diferencial de filtros, eficiência, contagem de partidas e tendência de alarmes.

A coleta de dados não substitui diagnóstico. O programa deve definir método, instrumentos, limites, comparação histórica, competência do avaliador e ação diante de desvio.

## 8.3. MANUTENÇÃO CORRETIVA E FALHAS

Mesmo em programas maduros, falhas ocorrerão. A manutenção corretiva deve possuir prioridades, peças, recursos, critérios de isolamento e procedimentos de retorno. A organização precisa distinguir correção definitiva de contenção temporária.

Reparos provisórios devem ter prazo, proprietário, risco registrado e condição de encerramento. Quando se tornam permanentes sem reavaliação, criam dívida técnica e alteram o baseline sem controle.

## 8.4. MANUTENÇÃO ADIADA

Adiar manutenção é uma decisão de risco. A aprovação deve considerar condição do ativo, redundância, probabilidade de falha, impacto, tempo de espera, sobressalentes, contratos e outras intervenções programadas.

O backlog precisa ser visível. Quantidade de ordens abertas, idade, criticidade, reincidência e impacto acumulado são indicadores mais úteis do que apenas o percentual de manutenção concluída.

## 8.5. SOBRESSALENTES E OBSOLESCÊNCIA

Peças críticas devem ser definidas com base no tempo máximo aceitável de reparo, disponibilidade no mercado, logística, vida útil e compatibilidade. Estoque sem controle pode conter itens vencidos, incompatíveis ou armazenados de forma inadequada.

A gestão de obsolescência precisa acompanhar firmware, placas, controladores, baterias, componentes de potência, equipamentos de telecomunicações e sistemas de supervisão. O fim de suporte deve acionar estudo de modernização antes que a substituição se torne emergencial.

**Manutenção altera o estado da instalação**

Uma intervenção segura precisa declarar capacidade remanescente, redundâncias retiradas, critérios de parada, contingências e forma de retorno.

Conheça o Owner's Engineering para Data Centers

## 9. GESTÃO DE MUDANÇAS E INTERVENÇÕES

Qualquer mudança capaz de alterar disponibilidade, capacidade, configuração, segurança ou comportamento da instalação deve passar por controle proporcional ao risco. Isso inclui implantação, manutenção, atualização de firmware, alteração de setpoints, transferência de carga, substituição de ativos, expansão, testes e mudanças em sistemas de automação.

O processo deve começar pela definição do resultado e das dependências. Em seguida, avalia-se o estado temporário, a capacidade remanescente, os riscos, a janela, os recursos, a comunicação, a reversão e os critérios de sucesso.

O artigo sobre MOP, SOP e EOP em Data Centers detalha a estrutura dos procedimentos operacionais. No contexto da operação integrada, o ponto essencial é que o MOP deve estar vinculado a uma mudança aprovada, a uma ordem de trabalho e ao estado real da instalação.

Mudanças simultâneas precisam ser coordenadas. Duas intervenções consideradas seguras isoladamente podem criar risco quando retiram redundâncias diferentes ou dependem do mesmo recurso. Um calendário integrado ajuda a identificar conflitos de energia, climatização, telecomunicações, segurança e pessoal.

Após a execução, deve existir validação técnica, período de observação e atualização do baseline. A mudança só está encerrada quando ativos, diagramas, parâmetros, inventário, procedimentos e pendências representam o novo estado.

## 10. ALARMES, EVENTOS, ANOMALIAS E INCIDENTES

Nem toda indicação é um incidente, mas todo incidente deixa eventos. A operação precisa classificar sinais para evitar tanto a banalização quanto o excesso de escalonamento.

Um evento é uma mudança de estado registrada. Um alarme indica uma condição que requer atenção. Uma anomalia é um comportamento diferente do esperado, ainda que não exista alarme configurado. Um incidente é uma situação que afeta ou ameaça serviço, segurança ou desempenho e exige resposta coordenada.

A matriz de alarmes deve definir prioridade, significado, origem, condição de disparo, atraso, ação inicial, responsável, escalonamento e critério de encerramento. Alarmes sem proprietário tendem a permanecer ativos; alarmes excessivos ocultam os relevantes; alarmes suprimidos sem controle eliminam proteção.

### 10.1. DA DETECÇÃO À ESTABILIZAÇÃO

O tratamento deve seguir uma sequência clara:

1. reconhecer e confirmar o evento; 2. proteger pessoas e áreas; 3. avaliar impacto e tendência; 4. estabilizar a instalação; 5. preservar a continuidade quando seguro; 6. comunicar e escalar; 7. executar recuperação controlada; 8. registrar evidências; 9. analisar causa e ações posteriores.

A primeira leitura pode estar incompleta. Por isso, a equipe deve evitar conclusões prematuras e preservar dados de BMS, EPMS, DCIM, controladores, sistemas de TI, CFTV e registros manuais.

### 10.2. CAUSA RAIZ E APRENDIZADO

A análise não deve parar no componente que falhou. É necessário perguntar por que a falha produziu determinado efeito, por que não foi detectada antes, por que a contingência não atuou ou por que o procedimento não evitou a propagação.

Ações corretivas podem envolver equipamento, projeto, manutenção, treinamento, alarmes, contrato, sobressalentes, procedimento ou governança. A eficácia precisa ser verificada depois da implementação.

## 11. CAPACIDADE E ESTADOS DEGRADADOS

A sustentabilidade operacional depende de conhecer a capacidade disponível não apenas em condição normal, mas também durante manutenção, falha e expansão. Uma arquitetura N+1 pode perder sua reserva quando uma unidade é retirada; um caminho A/B pode permanecer energizado e, ainda assim, operar com distribuição desigual; uma zona térmica pode se aproximar do limite antes que a capacidade global da planta seja consumida.

Por isso, estados degradados precisam ter limites, duração máxima, restrições, contingências e responsáveis definidos. A carga pode continuar atendida, mas a resiliência já ter sido reduzida. Quando esse estado não é formalmente reconhecido, novas mudanças e manutenções podem ser autorizadas sobre premissas incorretas.

A análise detalhada de espaço, energia, climatização, capacidade utilizável e *stranded capacity* pertence ao artigo Gestão de capacidade em Data Centers: espaço, energia e climatização. Neste contexto, capacidade é tratada como um dos controles necessários para preservar a resiliência operacional.

## 12. ENERGIA, ÁGUA E DESEMPENHO OPERACIONAL

Eficiência operacional não significa operar com a menor margem possível. Significa utilizar recursos de forma controlada, medindo efeitos sobre disponibilidade, vida útil e custo total.

Indicadores como PUE, WUE e CUE ajudam a observar energia, água e emissões, mas precisam de fronteiras, períodos e medições consistentes. O artigo PUE, WUE e CUE em Data Centers explica como calcular e interpretar esses indicadores.

A operação deve investigar tendências, não apenas valores médios. Aumento de consumo pode resultar de crescimento de TI, perda de eficiência, filtro obstruído, setpoint inadequado, degradação de equipamento, recarga de baterias ou alteração climática. Sem contexto, o indicador pode levar a uma conclusão errada.

Mudanças de eficiência devem passar por avaliação de risco. Elevar temperatura, ampliar faixas de umidade, ativar modos econômicos, alterar sequências ou reduzir equipamentos em operação pode gerar benefício, mas exige limites, monitoramento, capacidade de reversão e validação.

O framework de desempenho energético para Data Centers de IA desenvolvido por ASHRAE, NEMA e PNNL reforça a integração entre operação, manutenção,

monitoramento, energia e resiliência. Essa relação torna-se ainda mais importante em ambientes de alta densidade e resfriamento líquido.

## 13. MONITORAMENTO E PLATAFORMAS OPERACIONAIS

Ferramentas não substituem processos, mas podem aumentar visibilidade, consistência e rastreabilidade. O valor depende da qualidade dos dados, da integração e da capacidade da equipe de agir.

O BMS acompanha sistemas prediais e sequências de automação. O EPMS concentra grandezas e eventos elétricos. O DCIM relaciona ativos, capacidade, espaço, energia e operação. CMMS ou EAM apoiam manutenção e gestão de ativos. ITSM organiza serviços, mudanças e incidentes.

O artigo DCIM, BMS e EPMS em Data Centers detalha essas diferenças. Na operação, o principal desafio é definir qual sistema é fonte de verdade para cada informação e como os eventos serão correlacionados.

**Dados operacionais precisam orientar decisão**

DCIM, BMS, EPMS, CMMS e ITSM geram valor quando possuem fontes de verdade, qualidade de dados, responsáveis e integração com os processos.

Conheça a solução de Data Center Infrastructure Management — DCIM

### 13.1. QUALIDADE E GOVERNANÇA DOS DADOS

Dados operacionais precisam possuir origem, unidade, horário, qualidade, retenção e proprietário. Sensores sem calibração, timestamps divergentes e pontos duplicados podem comprometer análise de incidentes.

A arquitetura deve prever sincronismo de tempo, controle de acesso, backup, cibersegurança, disponibilidade contingencial e histórico suficiente para tendências. Alterações em telas, alarmes, lógicas e integrações devem passar por gestão de mudanças.

### 13.2. AUTOMAÇÃO E INTERVENÇÃO HUMANA

A automação reduz tarefas repetitivas, mas cria dependência de software, comunicação, sensores e lógica. A equipe precisa compreender o comportamento automático, reconhecer quando ele falha e possuir procedimentos seguros para operação manual.

Modos manuais não devem ser assumidos como equivalentes ao automático. Eles podem remover intertravamentos, temporizações, sequências e proteções. Quando utilizados, precisam de autorização, supervisão e retorno controlado.

## 14. DOCUMENTAÇÃO E FONTE DE VERDADE

A operação depende de documentos que representem a instalação real. Diagramas, plantas, listas de ativos, lógicas, setpoints, manuais, procedimentos e registros precisam estar controlados e acessíveis.

A fonte de verdade não precisa ser um único sistema, mas a governança deve definir onde cada informação oficial reside. O inventário pode estar no DCIM, a manutenção no CMMS, as mudanças no ITSM e os documentos no GED. O importante é que vínculos, responsabilidades e atualizações sejam claros.

Documentos críticos precisam estar disponíveis durante indisponibilidade de sistemas corporativos. Isso pode exigir cópias contingenciais controladas, acesso offline ou repositórios independentes. A solução não deve criar versões paralelas sem rastreabilidade.

Mudanças, incidentes, testes e inspeções devem acionar revisão documental. O estado “as built” não é um evento único ao final da obra; é uma condição que precisa ser mantida durante todo o ciclo de vida.

## 15. CONTINUIDADE OPERACIONAL E RESPOSTA A EMERGÊNCIAS

A operação do Data Center integra-se ao sistema de continuidade da organização, mas não substitui o plano de continuidade de negócios. A infraestrutura precisa possuir procedimentos técnicos para eventos específicos, enquanto a organização decide prioridades, serviços essenciais, comunicação, recuperação e alternativas de negócio.

A ISO 22301 estabelece requisitos para um sistema de gestão de continuidade. Aplicada ao contexto do Data Center, ela ajuda a relacionar análise de impacto, estratégias, planos, exercícios, comunicação e melhoria.

Os EOPs tratam a resposta técnica imediata. Planos de contingência tratam estados alternativos. A recuperação de desastre normalmente envolve serviços de TI, dados, aplicações e sites alternativos. Esses níveis precisam estar conectados.

Exercícios devem incluir cenários plausíveis, como perda prolongada da concessionária, falha de geração, indisponibilidade térmica, vazamento, incêndio, falha de

telecomunicações, acesso restrito ao site, indisponibilidade de fornecedor, evento climático ou falha simultânea durante manutenção.

O exercício não deve buscar apenas confirmar que o plano “funciona”. Ele precisa revelar lacunas em comunicação, autoridade, acesso, tempo, informação, ferramentas, recursos e dependências.

## 16. COMPETÊNCIA, TREINAMENTO E CULTURA OPERACIONAL

A operação segura depende de competência comprovada. Treinamento não se limita à apresentação de equipamentos. Deve incluir arquitetura, estados, riscos, procedimentos, alarmes, comunicação, segurança, contingências e limites de autoridade.

Uma matriz de competência pode relacionar funções, sistemas e níveis de atuação. Um profissional pode estar autorizado a acompanhar um sistema, executar rotina, realizar manobra, aprovar MOP ou liderar resposta a incidente. Essas atribuições não devem ser presumidas apenas pelo cargo.

Métodos de desenvolvimento incluem treinamento em sala, acompanhamento, walkdown, simulação, tabletop, execução supervisionada, exercícios e avaliação prática. Registros precisam mostrar conteúdo, instrutor, data, resultado e validade.

A cultura operacional deve favorecer questionamento e autoridade de parada. Profissionais precisam poder interromper uma atividade quando o campo diverge do documento, quando um alarme inesperado surge ou quando uma proteção é perdida. Continuar para cumprir janela ou prazo não pode prevalecer sobre segurança e controle.

Também é necessário tratar fadiga, carga de trabalho, comunicação e passagem de turno. Muitos erros não resultam de falta de conhecimento técnico, mas de contexto incompleto, pressão, ambiguidade ou excesso de tarefas simultâneas.

## 17. FORNECEDORES, CONTRATOS E NÍVEIS DE SERVIÇO

A operação depende de fabricantes, mantenedores, telecomunicações, combustível, segurança, limpeza, peças e serviços especializados. Cada dependência precisa ter requisitos, contatos, escalonamento e alternativas.

O SLA deve refletir a criticidade. Tempo de atendimento não é o mesmo que tempo de restauração. Um fornecedor pode responder rapidamente e não possuir peça, equipe ou acesso para reparar. Por isso, contratos devem distinguir reconhecimento, mobilização, chegada ao site, diagnóstico, contenção, reparo e recuperação.

O artigo SLA: o que é, como definir e calcular o nível de serviço apresenta essa estrutura de medição.

A gestão de fornecedores deve acompanhar desempenho, documentação, qualificação, segurança, reincidência, pendências e mudanças de equipe. Visitas e intervenções precisam ser registradas e incorporadas ao histórico do ativo.

## 18. INDICADORES DA OPERAÇÃO DE DATA CENTER

Indicadores devem apoiar decisão, não apenas demonstrar atividade. Uma operação pode apresentar grande quantidade de ordens concluídas e continuar acumulando risco crítico.

| Grupo | Exemplos de indicadores |
|---|---|
| Disponibilidade | indisponibilidade, eventos evitados, estados degradados e tempo de recuperação |
| Manutenção | cumprimento por criticidade, backlog, reincidência, falhas pós-manutenção e manutenção adiada |
| Mudanças | sucesso, abortagem, reversão, incidentes associados e atualização documental |
| Alarmes | recorrência, tempo de reconhecimento, alarmes permanentes, suprimidos e sem proprietário |
| Capacidade | utilização, reserva, tendência, saturação local e tempo até expansão |
| Eficiência | PUE, WUE, consumo por sistema, perdas e desvios de desempenho |
| Documentação | documentos vencidos, divergências de campo e tempo de atualização do baseline |
| Pessoas | cobertura de competência, treinamentos, exercícios e dependência de especialistas |
| Fornecedores | SLA, tempo de restauração, disponibilidade de peças e qualidade das evidências |

Indicadores precisam ser segmentados. Uma média de manutenção pode esconder atraso em ativos críticos. Um PUE mensal pode ocultar degradação em determinado sistema. Um bom painel deve permitir chegar da tendência ao ativo, evento ou decisão correspondente.

Metas inadequadas podem incentivar comportamento indesejado. Reduzir número de abortagens, por exemplo, pode pressionar equipes a continuar trabalhos inseguros. O indicador deve avaliar qualidade da decisão, não apenas quantidade.

## 19. AUDITORIAS, TESTES E MELHORIA CONTÍNUA

A operação precisa ser verificada por observação, registros, testes e auditorias. O objetivo não é apenas encontrar não conformidades, mas confirmar se os controles produzem o resultado esperado.

Auditorias podem avaliar campo, documentação, manutenção, alarmes, mudanças, treinamento, capacidade, segurança, contratos e continuidade. Walkdowns ajudam a comparar identificação, acesso, condição física e diagramas.

Testes periódicos devem ser planejados conforme risco. Sistemas de geração, UPS, baterias, transferências, automação, detecção, comunicação e contingências precisam ser exercitados em condições controladas. Testar apenas componentes isolados não comprova o comportamento integrado.

Lições aprendidas devem gerar ações com proprietário, prazo e verificação de eficácia. O mesmo desvio reaparecer indica que a organização registrou o evento, mas não alterou o sistema que o produz.

A melhoria contínua deve considerar mudanças no negócio, carga, tecnologia, clima, legislação, fornecedores e pessoal. Um modelo operacional adequado no início da vida do Data Center pode deixar de ser suficiente após expansão, aumento de densidade ou obsolescência.

**Testes precisam comprovar a resposta integrada**

Equipamentos disponíveis individualmente não garantem que energia, climatização, automação, segurança e procedimentos responderão corretamente em conjunto.

Conheça o Comissionamento e Aceite de Data Centers

## 20. COMO AVALIAR A SUSTENTABILIDADE OPERACIONAL DE UM DATA CENTER

A avaliação deve partir do desempenho esperado da instalação e comparar esse requisito com o estado técnico e gerencial realmente existente. O objetivo não é apenas verificar documentos ou produzir uma nota de maturidade, mas identificar como cada lacuna pode reduzir disponibilidade, segurança, capacidade de manutenção ou recuperação.

O primeiro passo é estabelecer o baseline: topologia instalada, requisitos de disponibilidade, modos de operação, premissas de projeto, cargas críticas, limites de capacidade e critérios de continuidade. Sem essa referência, a equipe pode avaliar se uma prática existe, mas não se ela é suficiente para o nível de resiliência pretendido.

| Etapa | Pergunta principal | Evidências possíveis |
|---|---|---|
| 1. Baseline | Qual desempenho a instalação precisa entregar? | OPR, URS, Basis of Design, diagramas, critérios Tier, SLAs e planos de continuidade |
| 2. Verificação técnica | A infraestrutura continua compatível com o projeto e com a carga atual? | inspeções, testes, histórico, capacidade, condição dos ativos e estados degradados |
| 3. Gestão e operação | Pessoas, processos e fornecedores conseguem preservar essa capacidade? | RACI, escalas, procedimentos, manutenção, treinamento, mudanças e registros |
| 4. Edificação e localização | Existem condições construtivas ou externas que aumentam o risco? | acessos, compartimentação, logística, utilidades, entorno, clima e riscos naturais |
| 5. Priorização | Quais lacunas possuem maior consequência e urgência? | matriz de risco, dependências, recorrência, prazo de correção e contingências |
| 6. Verificação de eficácia | As ações realmente reduziram o risco? | retestes, auditorias, indicadores, exercícios e atualização do baseline |

A coleta deve combinar análise documental, entrevistas, observação das rotinas, *walkdowns*, amostragem de ordens de manutenção, revisão de eventos e testes controlados. Uma política bem redigida não comprova execução; da mesma forma, uma boa prática observada em campo pode depender de conhecimento informal e não ser repetível.

As lacunas precisam ser relacionadas às consequências. Um procedimento vencido pode ser administrativo ou crítico, dependendo do sistema. Uma manutenção atrasada pode ter baixo impacto quando existe redundância comprovada ou representar risco imediato quando afeta um ponto único de falha. A priorização deve considerar probabilidade, impacto, detectabilidade, tempo de exposição, capacidade de contingência e dificuldade de recuperação.

A avaliação de sustentabilidade operacional não substitui uma certificação formal do Uptime Institute nem deve declarar equivalência com suas classificações. Ela pode, entretanto, utilizar os mesmos princípios de alinhamento entre infraestrutura, gestão e risco para estruturar um diagnóstico técnico e um plano de melhoria compatível com os objetivos do proprietário.

## 21. ERROS QUE DEGRADAM A SUSTENTABILIDADE OPERACIONAL

Um erro frequente é confiar na redundância sem controlar estados temporários. A instalação parece protegida em condições normais, mas manutenções e falhas reduzem a margem sem que a organização ajuste suas permissões e prioridades.

Outro erro é transformar rotinas em preenchimento mecânico. Dados são registrados, mas não existem limites, tendências, escalonamentos ou decisões. O resultado é uma grande quantidade de evidências com pouca capacidade de prevenção.

Também é comum manter documentação desatualizada e compensar a divergência com conhecimento individual. Essa prática funciona até que a pessoa não esteja disponível, o sistema seja alterado ou um evento exija resposta fora da rotina.

Manutenção adiada sem avaliação formal, alarmes permanentes, peças sem controle, fornecedores sem SLA verificável e mudanças emergenciais recorrentes são sinais de dívida operacional. Cada item isolado pode parecer administrável, mas o acúmulo reduz a resiliência.

Outro problema é separar completamente facilities e TI. A infraestrutura física e os serviços digitais possuem ritmos e responsabilidades diferentes, porém compartilham dependências. Mudanças, incidentes, capacidade e continuidade precisam de interfaces claras.

Por fim, operar apenas de forma reativa impede aprendizado. Quando toda a equipe está ocupada tratando urgências, não sobra capacidade para revisar causas, atualizar documentos, treinar, testar e modernizar. A governança deve proteger tempo e recursos para prevenção.

## 22. ENTREGÁVEIS DE UMA AVALIAÇÃO DE SUSTENTABILIDADE OPERACIONAL

Uma avaliação estruturada deve produzir evidências que permitam ao proprietário compreender o estado atual, os riscos e a sequência de tratamento. Os entregáveis precisam ser proporcionais à criticidade e à complexidade do site, mas normalmente incluem:

O resultado não deve ser apenas uma lista de pendências. Cada recomendação precisa indicar o risco tratado, o responsável, as dependências, o prazo, a condição de encerramento e a evidência necessária para comprovar que a resiliência foi efetivamente recuperada ou preservada.

## 23. COMO ESTRUTURAR UM PLANO DE MELHORIA OPERACIONAL

A recuperação da sustentabilidade operacional deve ser implantada por risco, e não pela ordem em que as lacunas foram encontradas. O primeiro objetivo é impedir que condições existentes produzam indisponibilidade; o segundo é restaurar o baseline; o terceiro é criar controles capazes de impedir nova degradação.

| Horizonte | Objetivo | Exemplos de ações |
|---|---|---|
| Imediato | controlar exposições críticas | tratar alarmes críticos, recuperar redundâncias, restringir mudanças, revisar EOPs e garantir peças essenciais |
| Curto prazo | restabelecer o baseline | executar manutenção atrasada, corrigir documentos, revisar capacidades, formalizar estados degradados e eliminar reparos provisórios |
| Médio prazo | institucionalizar os controles | implantar RACI, gestão de mudanças, matriz de competências, governança de fornecedores, indicadores e biblioteca de procedimentos |
| Longo prazo | reduzir riscos estruturais | modernizar ativos, corrigir limitações construtivas, ampliar capacidade, diversificar dependências externas e recomissionar sistemas |

Ações de baixo custo e alta criticidade não devem aguardar projetos maiores. Atualizar contatos, definir autoridade de parada, organizar versões de procedimentos ou registrar um estado degradado podem reduzir risco imediatamente. Por outro lado, lacunas que exigem obra, substituição de ativos ou alteração de topologia precisam de engenharia, orçamento, planejamento de fases e controle rigoroso da implantação.

Em instalações existentes, o plano precisa preservar a continuidade durante a própria correção. O artigo Modernização de Data Center sem interromper a operação apresenta os controles necessários para estados temporários, implantação por fases e retorno ao baseline.

O encerramento de uma ação depende de evidência. Uma manutenção concluída precisa demonstrar condição e desempenho; um procedimento atualizado precisa ser treinado e exercitado; uma mudança de topologia precisa ser documentada e testada; uma correção estrutural precisa ter seu efeito verificado. Sem essa validação, o plano registra atividade, mas não comprova redução de risco.

## 24. CONCLUSÃO

Sustentabilidade operacional é a capacidade de preservar, ao longo do tempo, a resiliência que o projeto e a infraestrutura permitem entregar. Ela depende do alinhamento entre topologia, gestão, manutenção, pessoas, características da edificação e riscos da localização.

Um Data Center pode permanecer disponível e, ao mesmo tempo, acumular perda de proteção. Manutenções adiadas, estados degradados, alarmes permanentes, documentos divergentes, mudanças não controladas e dependência de conhecimento informal reduzem progressivamente a capacidade de suportar a próxima falha.

Preservar a resiliência exige conhecer o baseline, verificar o estado real, relacionar lacunas às suas consequências e implantar ações com evidências de eficácia. O objetivo não é produzir mais documentos, mas assegurar que a instalação continue operável, manutenível e recuperável nos cenários previstos para sua criticidade.

A A3A Engenharia atua no diagnóstico, projeto, Owner's Engineering, modernização e comissionamento de Data Centers, apoiando proprietários e operadores na avaliação de riscos operacionais, na recuperação do baseline e na estruturação de planos de melhoria capazes de preservar a continuidade da infraestrutura crítica.

[1] ISO; IEC. ISO/IEC TS 22237-7:2018 — Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information. 2018.

[2] ISO; IEC. ISO/IEC DIS 22237-7 — Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information. Segunda edição em desenvolvimento.

[3] BSI. BS EN 50600-3-1:2026 — Information technology — Data centre facilities and infrastructures — Part 3-1: Management and operational information. 2026.

[4] BICSI. ANSI/BICSI 009-2024 — The Standard for Data Center Operations. 2024.

[5] UPTIME INSTITUTE. Tier Standard: Operational Sustainability.

[6] ISO. ISO 55001:2024 — Asset management — Asset management system — Requirements. 2024.

[7] ISO. ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements. 2019.

[8] ISO. ISO 22301:2019/Amd 1:2024 — Security and resilience — Business continuity management systems — Requirements — Amendment 1: Climate action changes. 2024.

[9] ASHRAE; NEMA; PNNL. AI Data Center Energy Performance Framework — Operations and Maintenance. 2026.

**O que é sustentabilidade operacional em Data Centers?** É a capacidade de preservar ao longo do tempo a resiliência, a disponibilidade e a manutenibilidade previstas para a infraestrutura, por meio de gestão, manutenção, pessoas, processos e controle de riscos.**Sustentabilidade operacional é o mesmo que sustentabilidade ambiental?** Não. A sustentabilidade ambiental trata principalmente de energia, água, emissões e impacto ambiental. A sustentabilidade operacional trata da preservação da disponibilidade e da resiliência da infraestrutura crítica.**Por que um Data Center resiliente pode perder disponibilidade?** Porque redundâncias e capacidades podem ser degradadas por manutenção adiada, mudanças sem controle, alarmes permanentes, documentos desatualizados, obsolescência, estados degradados e falhas de competência ou governança.**Quais são as dimensões da sustentabilidade operacional?** O Uptime Institute relaciona três dimensões principais: gestão e operação, características da edificação e localização do site. Elas precisam ser avaliadas em conjunto com a topologia e os requisitos do Data Center.**O que é um estado degradado?** É uma condição em que a carga continua atendida, mas alguma redundância, capacidade ou proteção foi reduzida. O estado precisa ter limites, duração, restrições, contingências e responsáveis definidos.**Como avaliar a sustentabilidade operacional de um Data Center?** A avaliação deve estabelecer o baseline, verificar o estado técnico, analisar gestão e operação, revisar edificação e localização, relacionar lacunas às consequências e priorizar ações com critérios de eficácia.**Quais evidências devem ser analisadas?** Diagramas, requisitos, inspeções, testes, histórico de eventos, ordens de manutenção, procedimentos, mudanças, treinamentos, contratos, indicadores, estados degradados e registros de capacidade são exemplos relevantes.**Uma avaliação interna substitui a certificação do Uptime Institute?** Não. Uma avaliação técnica pode usar princípios de sustentabilidade operacional para diagnóstico e melhoria, mas não deve declarar equivalência com uma certificação formal do Uptime Institute.

## 24.1. FUNDAMENTOS, PROJETO E GOVERNANÇA

## 24.2. OPERAÇÃO, PROCEDIMENTOS E DESEMPENHO

## 24.3. RESILIÊNCIA, MODERNIZAÇÃO E ACEITE

## 24.4. SOLUÇÕES E SERVIÇOS DE ENGENHARIA

## 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.



A3A® Engenharia de Sistemas