

Onde e como opera um centro de dados

Seleção do local, análise de riscos e operações fiáveis: os fundamentos que determinam a resiliência real de uma instalação crítica



Introdução

Um centro de dados pode ter o melhor design técnico do mercado e, ainda assim, falhar sistematicamente se estiver localizado no sítio errado ou se as suas operações não estiverem à altura da sua infraestrutura. A localização e a qualidade das operações são duas variáveis que as equipas técnicas tendem a dar como resolvidas, quando, na realidade, são as que mais frequentemente determinam a resiliência real de uma instalação crítica.

Este e-book aborda estas duas dimensões numa perspetiva operacional. A primeira parte analisa os critérios de seleção do local e o mapa de riscos que todos os profissionais devem conhecer antes de decidir onde construir ou onde alojar os seus sistemas. A segunda parte aborda o modelo de operações fiáveis: o ciclo de vida do centro de dados, a estrutura organizativa, os procedimentos e as ferramentas de gestão que transformam uma infraestrutura numa operação fiável.

O que vai encontrar neste e-book

NESTE E-BOOK

Os 8 fatores-chave de seleção do local

- Taxonomia completa de desastres naturais e antropogénicos
- Como ler um índice de risco
- Ciclo de vida do centro de dados e janelas de renovação
- Estrutura organizativa das operações
- SOP, MOP e EOP: os três tipos de procedimento
- ITIL, CMMS, DCIM e BAS: as ferramentas de gestão
- Documentação mínima obrigatória
- Programa de formação por perfil

01

CAPÍTULO

A localização do centro de dados

A decisão mais permanente

De todas as decisões tomadas ao longo do ciclo de vida de um centro de dados, a escolha da localização é provavelmente a mais difícil de reverter. Um sistema de arrefecimento pode ser modernizado e uma UPS pode ser substituída, mas mudar a localização física de um centro de dados é uma operação tão complexa que, na prática, equivale a construir um novo.

Por isso, a análise do local deve ser exaustiva, sistemática e documentada antes de qualquer decisão de investimento. Existem oito fatores principais a avaliar.

1.1 Os oito fatores de seleção do local

Fator	O que avaliar	Risco se for ignorado
Acesso à energia elétrica	Fiabilidade do fornecedor, redundância de circuitos e rotas de alimentação independentes a partir de subestações distintas	Dependência de uma única fonte; sem alternativa perante um corte prolongado
Acesso a telecomunicações	Disponibilidade de vários operadores e rotas físicas de fibra diversificadas	Ponto único de falha na conectividade; sem alternativa perante um corte de fibra
Propriedades adjacentes	Instalações industriais, militares, químicas ou de alto risco nas imediações	Exposição a incêndios, explosões ou contaminação de fontes externas

Fator	O que avaliar	Risco se for ignorado
Estabilidade sísmica e do subsolo	Tipo de solo, atividade sísmica histórica, proximidade de falhas geológicas	Danos estruturais em caso de sismo; colapso da infraestrutura do edifício
Leito de cheia	Histórico de inundações, cota do terreno, proximidade de rios ou da costa	Inundação catastrófica sem possibilidade de resposta operacional
Qualidade do ar	Concentração de partículas, gases industriais, atividade vulcânica ou urbana próxima	Contaminação acelerada do hardware; corrosão prematura de circuitos
Acesso à água	Disponibilidade para sistemas de arrefecimento (chillers, torres) e extinção de incêndios	Limitação nas tecnologias de arrefecimento; risco em caso de incêndio
Acesso a transportes	Pelo menos duas vias de acesso independentes a partir de uma via principal	Impossibilidade de acesso do pessoal ou de equipamentos numa emergência

■ 1.2 O acesso à energia: o fator mais crítico

Dos oito fatores, o acesso a energia elétrica de qualidade é o que mais condiciona a viabilidade do projeto. A avaliação deve ir além de confirmar que existe fornecimento elétrico na zona: deve analisar a fiabilidade histórica do fornecedor, a possibilidade de alimentar o local a partir de duas subestações diferentes através de rotas fisicamente separadas e a disponibilidade de média ou alta tensão que permita reduzir a dependência de transformações intermédias.

Redundância da alimentação elétrica

ESSENCIAL

A melhor prática é dispor de duas alimentações a partir de subestações elétricas diferentes, com rotas físicas completamente separadas (incluindo canalizações subterrâneas distintas). Um local alimentado a partir de dois pontos da mesma subestação não tem redundância real: uma falha na subestação afeta ambas as alimentações em simultâneo.

2

A reter

subestações distintas, com rotas físicas separadas: a única forma de ter redundância elétrica real.

02CAPÍTULO

O Mapa de risco

Conhecer para antecipar

A seleção do local não pode ser feita sem uma análise sistemática dos riscos associados à localização. Estes riscos dividem-se em duas grandes categorias: desastres naturais e desastres antropogénicos (causados pela atividade humana). Ambas as categorias podem atuar de forma independente ou encadeada, e ambas têm o potencial de comprometer definitivamente a operação de um centro de dados.

■ 2.1 Taxonomia de desastres naturais

Categoria	Tipos	Impacto típico no centro de dados
Desastres geológicos	Sismos, erupções vulcânicas, deslizamentos de terras	Danos estruturais no edifício, corte de serviços, contaminação por cinzas vulcânicas
Desastres hidrológicos	Inundações, tsunamis, erupções límnicas	Inundação das instalações, corte de acessos, danos irreversíveis nos equipamentos
Desastres climáticos	Furacões, tornados, ondas de calor, secas, tempestades severas	Corte de energia prolongado, danos físicos no edifício, falha dos sistemas de arrefecimento
Incêndios naturais	Incêndios florestais, descargas atmosféricas	Danos estruturais, contaminação por fumo, corte de acessos
Meteorologia espacial	Tempestades geomagnéticas solares	Interferências eletromagnéticas, danos em sistemas elétricos não protegidos

■ 2.2 Desastres antropogénicos: a ameaça que se constrói perto

Os desastres antropogénicos são especialmente relevantes porque muitos deles são identificáveis e evitáveis na fase de seleção do local. Um centro de dados situado junto a uma instalação química industrial, no cone de aproximação de um aeroporto ou a menos de 100 metros de uma autoestrada com elevada densidade de tráfego de mercadorias perigosas está a assumir riscos que nenhum sistema de redundância interno consegue compensar.

Os perigos antropogénicos dividem-se em dois grupos:

- **Perigos sociológicos:** terrorismo, crime organizado, distúrbios civis, conflitos armados. Determinam os requisitos de segurança física e o nível de exposição pública do local.
- **Perigos tecnológicos:** instalações industriais de alto risco, bases militares, armazenamento de materiais perigosos, rotas de transporte de substâncias inflamáveis ou explosivas, proximidade de pistas de aviação.

O risco das adjacências

ATENÇÃO

Um caso real documentado no manual mostra um centro de dados com vários riscos simultâneos num raio reduzido: autoestrada a menos de 100 metros, zona industrial de alto risco, cone de aproximação de uma pista de aviação e armazenamento de munições de uma base da força aérea. Nenhum destes riscos é visível numa análise exclusivamente técnica do edifício. Só uma análise geográfica e de adjacências os revela.

■ 2.3 Índices de risco como ferramenta de decisão

Existem índices de risco públicos que quantificam de forma sistemática a exposição de cada território a desastres naturais e antropogénicos. O índice INFORM (Index for Risk Management), desenvolvido pela ONU e pela União Europeia, é um dos mais completos e está disponível publicamente.

Estes índices permitem comparar localizações potenciais de forma objetiva e documentar a decisão do local com critérios rastreáveis. Para um centro de dados de missão crítica, a consulta de índices de risco não é opcional: faz parte do processo de due diligence do projeto.

Os desastres naturais encadeiam-se

ESSENCIAL

Uma característica frequentemente subestimada é que os desastres naturais podem encadear-se: um sismo pode provocar um tsunami; uma seca pode causar incêndios florestais que, por sua vez, degradam a qualidade do ar. A análise de riscos deve considerar estes cenários compostos, e não apenas os eventos individuais.

<100 m

A reter

de uma autoestrada com mercadorias perigosas: um risco que nenhuma redundância interna consegue compensar.

03 CAPÍTULO

O ciclo de vida do centro de dados

Planear para décadas, renovar a cada poucos anos

Um centro de dados estratégico é concebido para operar entre 20 e 30 anos. Nesse período, os sistemas de cablagem duram entre 15 e 25 anos, mas os servidores e os sistemas de armazenamento são renovados a cada 3 a 5 anos. Esta assimetria é fundamental para perceber como deve ser gerido um centro de dados ao longo do tempo.

3.1 Vida útil por camada de infraestrutura

Camada	Vida útil típica	Implicação operacional
Centro de dados estratégico (edifício e infraestrutura)	20 – 30 anos	As decisões de design têm um impacto de décadas. Os erros de localização ou de capacidade são muito dispendiosos de corrigir
Sistema de cablagem estruturada	15 – 25 anos	Deve ser planeado para suportar várias gerações de equipamentos de TI. A capacidade da cablagem deve antecipar densidades futuras
Servidores e sistemas de armazenamento	3 – 5 anos	O ciclo de renovação de TI é contínuo. A infraestrutura deve conseguir absorver alterações de densidade e configuração sem obras de grande dimensão
Computadores de secretária	3 – 5 anos	Impacto direto limitado na infraestrutura do centro de dados
Portáteis	2 – 3 anos	Impacto direto limitado na infraestrutura do centro de dados

3.2 O ciclo de renovação a cada 5 anos

Aproximadamente a cada 5 anos, um centro de dados bem gerido deve passar por um ciclo de revisão e renovação que pode incluir desde a atualização de equipamentos de TI até à substituição de sistemas de infraestrutura (UPS, CRAC/CRAH, quadros elétricos). Aproximadamente a cada 15 anos, pode ser necessária uma renovação profunda que implique substituições significativas de sistemas e, possivelmente, uma atualização da arquitetura.

Este ciclo de vida tem uma implicação direta no planeamento orçamental: um centro de dados sem um plano de renovação documentado está a acumular dívida técnica que, em algum momento, se materializará numa falha ou numa obsolescência que compromete a capacidade de crescer.

As fases do ciclo de vida

ESSENCIAL

~90%

da vida de um centro de dados decorre em operação

1

Planeamento

2

Design

3

Construção

4

Comissionamento (commissioning)

5

Operação contínua

- Renovação de TI a cada 3-5 anos
- Renovação profunda a cada 15 anos

04CAPÍTULO

Operações fiáveis

O triângulo que sustenta a disponibilidade

As operações de um centro de dados assentam em três pilares interdependentes: as pessoas, os procedimentos e a documentação. A gestão integra e supervisiona estes três elementos. Nenhum deles consegue compensar as deficiências dos outros dois: uma equipa excelente sem procedimentos gera inconsistências; procedimentos perfeitos sem pessoal com formação não passam de letra morta.

4.1 Estrutura organizativa das operações

A organização das operações de um centro de dados estrutura-se em dois ramos principais, sob a direção de IT Operations:

Ramo	Função	Subáreas
Facility Management	Gestão da infraestrutura física do centro de dados	Engineering (edifício, elétrica, mecânica) + Maintenance (edifício, elétrica, mecânica)
IT Management	Gestão dos sistemas de informação e telecomunicações	IT Infrastructure (Telco/Networking, Computing/Storage, Disaster Recovery) + Technical Support (Call Center)

Além disso, existem funções de apoio que estão fora da cadeia de comando direta, mas que são imprescindíveis para as operações: o CISO (responsável pela cibersegurança), a equipa de Segurança Física e a equipa de Saúde e Segurança no Trabalho. Estas funções devem estar formalmente integradas nos processos operacionais, e não ser tratadas como entidades independentes.

■ 4.2 Os três tipos de procedimento: SOP, MOP e EOP

Um dos conceitos mais importantes na gestão das operações de um centro de dados é a distinção entre os três tipos de procedimentos. Confundi-los ou utilizá-los de forma indistinta é um dos erros mais frequentes em equipas de operações sem formação formal.

Tipo	Nome completo	Finalidade	Quando se utiliza
SOP	Standard Operating Procedure (Procedimento Operacional Padrão)	Define uma rotina recorrente e processos críticos. Pode ser funcional ou administrativo	Operações de rotina: rondas de inspeção, abertura/fecho da sala, receção de equipamentos, gestão de visitantes
MOP	Method of Procedure (Método de Procedimento)	Procedimento detalhado, passo a passo, para uma intervenção específica. Mais detalhado do que o SOP	Intervenções técnicas planeadas: substituição de UPS, manutenção de CRAC, alteração da configuração elétrica
EOP	Emergency Operating Procedure (Procedimento de Operação de Emergência)	Procedimento para um modo de falha potencial ou conhecido	Emergências: falha de UPS, ativação do sistema de extinção de incêndios, corte de energia não planeado, ativação do EPO

Um EOP que não se pratica não funciona

ATENÇÃO

Um EOP é inútil se o pessoal não o tiver praticado antes de a emergência acontecer. Os EOP devem incluir simulacros periódicos (drills) com toda a equipa operacional, incluindo cenários de falha de UPS, incêndio na sala e ativação accidental do EPO. A frequência recomendada é de, pelo menos, uma vez por ano por cenário.

■ 4.3 Ferramentas de gestão operacional

As operações de um centro de dados moderno exigem ferramentas específicas para gerir o fluxo de trabalho dos procedimentos, o acompanhamento dos ativos e o controlo dos sistemas de infraestrutura. Existem quatro categorias principais:

Ferramenta	Nome completo	Função principal
ITIL	Information Technology Infrastructure Library	Referencial de boas práticas para a gestão de alterações de ativos, o nível de serviço e o registo de incidentes, com as suas causas e consequências
CMMS	Computerized Maintenance Management System	Programação, atribuição e acompanhamento de todas as atividades de manutenção das instalações. Calcula KPI de gestão da manutenção (MTBF, MTTR)
DCIM	Data Center Infrastructure Management	Maximiza a utilização eficiente das capacidades de energia, arrefecimento e espaço. Proporciona visibilidade em tempo real de toda a infraestrutura do centro de dados

Ferramenta	Nome completo	Função principal
BAS	Building Automation System	Software que permite controlar os sistemas do edifício de forma automatizada (AVAC, iluminação, acessos, segurança)
DMS	Document Management System	Armazenamento, recuperação e fluxo de aprovação de toda a documentação do centro de dados

DCIM: a ferramenta que vê tudo

ESSENCIAL

O DCIM é a ferramenta com maior impacto operacional num centro de dados moderno. Integra dados de energia, arrefecimento, espaço e ativos numa única plataforma, permitindo tomar decisões informadas sobre capacidade, eficiência e planeamento. Um centro de dados sem DCIM opera parcialmente às cegas: consegue gerir os sistemas individualmente, mas não tem visibilidade sobre o comportamento integrado da infraestrutura.



A reter
simulacro por ano, no mínimo, por cada cenário de emergência.

05 CAPÍTULO

Documentação e formação

A memória institucional do centro de dados

A documentação de um centro de dados não é um requisito burocrático: é a memória institucional que permite que as operações sejam consistentes, auditáveis e transferíveis. Um centro de dados que opera sem documentação atualizada corre o risco permanente de o conhecimento crítico residir exclusivamente nas pessoas, e não nos sistemas.

5.1 Documentação mínima obrigatória

O sistema documental de um centro de dados deve manter um registo atualizado dos seguintes elementos:

- **Desenhos as-built:** plantas atualizadas que refletem o estado real da instalação, e não o projeto original.
- **Base de dados de ativos:** inventário completo de todos os equipamentos, com as suas características técnicas, datas de instalação e garantias.
- **Âmbito do trabalho de manutenção preventiva:** descrição detalhada de todas as tarefas de manutenção planeadas.
- **Programa de manutenção:** calendário de todas as intervenções preventivas, com atribuição de responsáveis.
- **Normas de trabalho em instalações críticas:** regras de segurança e procedimentos específicos para trabalhar em ambientes energizados ou de alta disponibilidade.

- **Programa de segurança:** políticas e procedimentos de segurança física e cibersegurança.
- **Lista de verificação de comissionamento:** checklist de arranque para cada sistema.
- **Procedimentos e processos:** biblioteca completa de SOP, MOP e EOP.
- **Relatórios:** registos históricos de incidentes, manutenções e auditorias.

O documento mais perigoso

ATENÇÃO

O desenho as-built desatualizado é um dos documentos mais perigosos num centro de dados. Quando o pessoal intervém num sistema com base numa planta que não reflete a realidade, o risco de erro é máximo. Manter os desenhos as-built atualizados após cada alteração não é opcional: é uma obrigação operacional.

5.2 Programa de formação por perfil

A formação do pessoal deve ser diferenciada consoante o perfil e as responsabilidades de cada função. O manual distingue dois níveis principais:

Perfil	Conteúdos de formação
Técnicos e engenheiros de campo	• Fundamentos e boas práticas • Teoria de funcionamento dos principais equipamentos e sistemas • Módulos de formação para SOP e MOP • Simulacros para EOP • Exames por nível de formação
Gestores e supervisores (adicionalmente)	• Data Center Management • Data Center Energy Efficiency • Data Center Operations • Data Center Design Awareness • Formação contínua e participação em conferências do setor

A formação não é um evento pontual no momento da integração: é um processo contínuo. As alterações na infraestrutura, a incorporação de novos sistemas, as atualizações normativas e as lições aprendidas com incidentes devem traduzir-se em atualizações dos programas de formação.

Conclusão

A resiliência começa antes de instalar o primeiro rack

Um centro de dados resiliente não se constrói apenas com tecnologia redundante. Constrói-se escolhendo o local certo, conhecendo os riscos do meio envolvente, estabelecendo operações estruturadas e documentando cada decisão. Estas são as disciplinas que as equipas técnicas mais frequentemente subestimam e que mais frequentemente determinam o resultado real.

A localização é permanente. As operações são contínuas. A documentação é cumulativa. Nenhuma das três pode ser improvisada no momento da emergência: têm de estar implementadas muito antes de ocorrer qualquer evento não planeado.

ESSENCIAL

Os cinco princípios de um centro de dados bem localizado e bem operado

1. A seleção do local exige a análise de oito fatores físicos e um mapa de riscos naturais e antropogénicos. Uma localização com vários riscos simultâneos não pode ser compensada pela redundância interna.
2. Os desastres naturais encadeiam-se. A análise de riscos deve contemplar cenários compostos, e não apenas eventos individuais.
3. SOP, MOP e EOP são três documentos distintos com finalidades distintas. Confundi-los é um risco operacional.
4. Um EOP que não se pratica não funciona. Os simulacros são obrigatórios, não opcionais.
5. Os desenhos as-built desatualizados são tão perigosos como um sistema sem redundância. A documentação deve refletir o estado real, e não o projeto original.