

TESTES INTEGRADOS DE SISTEMAS EM DATA CENTERS: CENÁRIOS, METODOLOGIA E CRITÉRIOS DE ACEITE

Entenda como planejar e executar testes integrados de sistemas em Data Centers, com cenários, instrumentação, critérios de aceite, evidências e retestes.

SUMÁRIO

1. O QUE SÃO TESTES INTEGRADOS DE SISTEMAS EM DATA CENTERS?	5
2. IST, SAT, TESTE FUNCIONAL E TESTE DE DESEMPENHO	6
2.1. SAT	6
2.2. TESTE FUNCIONAL POR SISTEMA	6
2.3. TESTE INTEGRADO DE SISTEMAS	6
2.4. TESTE DE DESEMPENHO	6
3. FUNDAMENTAÇÃO TÉCNICA E NORMATIVA	6
4. QUAL É O OBJETIVO DO IST?	7
5. O IST DEVE SER ORIENTADO POR REQUISITOS E RISCOS	8
6. PRÉ-REQUISITOS PARA INICIAR OS TESTES INTEGRADOS	8
6.1. REQUISITOS E DOCUMENTAÇÃO ATUALIZADOS	8
6.2. SISTEMAS INDIVIDUAIS CONCLUÍDOS	8
6.3. PENDÊNCIAS CLASSIFICADAS	9
6.4. CONFIGURAÇÃO CONTROLADA	9
6.5. INSTRUMENTAÇÃO E OBSERVABILIDADE DISPONÍVEIS	9
6.6. EQUIPE E RESPONSABILIDADES DEFINIDAS	9
7. GOVERNANÇA E AUTORIDADE DURANTE O IST	9
8. COMO ESTRUTURAR UMA MATRIZ DE CENÁRIOS	10
9. FAMÍLIAS DE CENÁRIOS PARA DATA CENTERS	10
9.1. OPERAÇÃO NORMAL	10
9.2. MANUTENÇÃO PLANEJADA	10
9.3. FALHA DE FONTE OU COMPONENTE	10
9.4. ESTADO DEGRADADO	10
9.5. FALHAS DE COMUNICAÇÃO E AUTOMAÇÃO	11
9.6. INCÊNDIO E SEGURANÇA	11
9.7. CONDIÇÕES AMBIENTAIS	11
9.8. RECUPERAÇÃO E RETORNO AO ESTADO NORMAL	11
10. COMO ESCREVER UM SCRIPT DE TESTE INTEGRADO	12
10.1. IDENTIFICAÇÃO E OBJETIVO	12
10.2. REFERÊNCIAS	12
10.3. CONFIGURAÇÃO INICIAL	12
10.4. PRÉ-CONDIÇÕES E GATE	12
10.5. PASSOS DE EXECUÇÃO	12
10.6. CRITÉRIOS DE ABORTAGEM	12

10.7. PLANO DE RESTAURAÇÃO	12
10.8. CRITÉRIOS DE ACEITE	13
11. SEGURANÇA DURANTE A EXECUÇÃO	13
12. INSTRUMENTAÇÃO, SINCRONIZAÇÃO E EVIDÊNCIAS	13
12.1. INSTRUMENTOS POSSÍVEIS	13
12.2. SINCRONIZAÇÃO DE TEMPO	13
12.3. TAXA DE AMOSTRAGEM	13
12.4. EVIDÊNCIA MÍNIMA	14
13. EXECUÇÃO PASSO A PASSO	14
13.1. 1. REUNIÃO DE PRONTIDÃO	14
13.2. 2. REGISTRO DO BASELINE	14
13.3. 3. APLICAÇÃO DO ESTÍMULO	14
13.4. 4. OBSERVAÇÃO DA RESPOSTA	14
13.5. 5. PERMANÊNCIA EM CONDIÇÃO REPRESENTATIVA	14
13.6. 6. RESTAURAÇÃO	14
13.7. 7. VERIFICAÇÃO PÓS-TESTE	14
13.8. 8. DEBRIEFING IMEDIATO	15
14. CRITÉRIOS DE ACEITE DO IST	15
14.1. CRITÉRIOS FUNCIONAIS	15
14.2. CRITÉRIOS TEMPORAIS	15
14.3. CRITÉRIOS DE CAPACIDADE	15
14.4. CRITÉRIOS DE OBSERVABILIDADE	15
14.5. CRITÉRIOS OPERACIONAIS	15
14.6. CRITÉRIOS DE RESTAURAÇÃO	15
15. GESTÃO DE ISSUES, FALHAS E RETESTES	15
15.1. CLASSIFICAÇÃO POR CRITICIDADE	15
15.2. RETESTE	16
16. VERIFICAÇÃO POR DISCIPLINA	16
16.1. SISTEMA ELÉTRICO	16
16.2. CLIMATIZAÇÃO	16
16.3. AUTOMAÇÃO E SUPERVISÃO	16
16.4. TELECOMUNICAÇÕES E REDE	16
16.5. INCÊNDIO E SEGURANÇA	16
17. TESTES INTEGRADOS EM DATA CENTERS EXISTENTES	17
18. ENTREGÁVEIS DOS TESTES INTEGRADOS	17

19. ERROS COMUNS	17
19.1. TRATAR O IST COMO DEMONSTRAÇÃO	17
19.2. COMEÇAR ANTES DA PRONTIDÃO	17
19.3. TESTAR SOMENTE ENERGIA	17
19.4. USAR SCRIPTS GENÉRICOS	17
19.5. IGNORAR O ESTADO DEGRADADO	18
19.6. NÃO TESTAR A RESTAURAÇÃO	18
19.7. REGISTRAR APENAS O RESULTADO FINAL	18
19.8. ALTERAR LÓGICA DURANTE O TESTE SEM CONTROLE	18
19.9. ACEITAR INTERVENÇÃO MANUAL NÃO PREVISTA	18
19.10. EXCLUIR A OPERAÇÃO	18
20. CHECKLIST EXECUTIVO	18
21. CONCLUSÃO	18

Os testes integrados de sistemas em Data Centers verificam se a infraestrutura crítica responde de forma coordenada quando ocorre uma mudança de estado, uma manutenção planejada, uma falha, uma condição degradada ou uma emergência. O objetivo não é apenas confirmar que cada equipamento funciona isoladamente, mas demonstrar que energia, climatização, automação, telecomunicações, segurança, incêndio, controles e operação preservam conjuntamente a função crítica dentro dos limites definidos.

Essa distinção é essencial. Um UPS pode ter sido aprovado no teste funcional; um grupo gerador pode ter concluído sua partida; um chiller pode ter atingido a capacidade nominal; o BMS pode ter recebido os pontos previstos. Ainda assim, a infraestrutura pode falhar quando esses sistemas precisam atuar em sequência. É justamente nessa fronteira entre sistemas que surgem atrasos de comando, intertravamentos inconsistentes, alarmes ambíguos, dependências ocultas, falhas de comunicação, prioridades incorretas e dificuldades de retorno ao estado normal.

O artigo geral sobre [comissionamento de Data Center](#) explica o processo completo, os níveis de verificação e os gates do empreendimento. Este conteúdo possui uma intenção mais específica: aprofundar como estruturar, executar, registrar e aceitar o **Integrated Systems Testing – IST**, frequentemente associado ao nível final dos programas de comissionamento.

1. O QUE SÃO TESTES INTEGRADOS DE SISTEMAS EM DATA CENTERS?

O teste integrado de sistemas é uma verificação orientada a cenários. Ele provoca ou simula eventos previamente definidos e observa se os sistemas envolvidos respondem de acordo com os requisitos do proprietário, a base de projeto, as sequências de operação, as lógicas de controle, os procedimentos aprovados e os critérios de desempenho.

Em vez de perguntar apenas “o equipamento funcionou?”, o IST procura responder:

Um cenário de perda de alimentação da concessionária, por exemplo, pode envolver detecção da condição, atuação de proteções, sustentação por UPS e baterias, partida de grupos geradores, transferência de cargas, priorização de sistemas auxiliares, continuidade da climatização, atualização dos supervisórios, geração de alarmes, atuação da equipe e posterior retorno à condição normal.

O resultado não pode ser reduzido a “não houve desligamento”. O teste precisa demonstrar que a resposta completa foi coerente com os requisitos e que não surgiram condições ocultas capazes de comprometer a operação futura.

2. IST, SAT, TESTE FUNCIONAL E TESTE DE DESEMPENHO

A terminologia deve ser definida no plano de comissionamento e no contrato, pois diferentes organizações utilizam nomenclaturas próprias. Ainda assim, algumas distinções são fundamentais.

2.1. SAT

O Site Acceptance Test verifica a aceitação em campo de um equipamento, pacote ou sistema após instalação. Pode incluir inspeção, energização, configuração, funcionamento local, comunicação e desempenho específico.

2.2. TESTE FUNCIONAL POR SISTEMA

Verifica funções, sequências, intertravamentos e desempenho de um sistema ou disciplina. Um teste funcional de UPS, por exemplo, pode avaliar transferência para baterias, bypass, alarmes, autonomia ou compartilhamento de carga.

2.3. TESTE INTEGRADO DE SISTEMAS

Avalia a interação entre sistemas durante um evento comum. A perda de uma fonte elétrica, por exemplo, pode exigir resposta coordenada de UPS, geradores, quadros, automação, BMS, EPMS, climatização e equipe operacional.

2.4. TESTE DE DESEMPENHO

Demonstra se a instalação ou sistema atinge parâmetros garantidos em condições definidas. A ABNT NBR IEC 62337 estabelece que os procedimentos, condições de partida, instrumentação, métodos de medição, tolerâncias, duração, avaliação e relatórios precisam ser previamente acordados.

O IST pode incluir verificações de desempenho, mas sua característica principal é a avaliação das interfaces e da resposta conjunta.

3. FUNDAMENTAÇÃO TÉCNICA E NORMATIVA

A ABNT NBR ISO/IEC 22237-1 estabelece que a operação, a gestão, os processos e os indicadores devem ser considerados desde o projeto. A norma também orienta que processos, papéis e responsabilidades sejam definidos antes do início da operação, e que a equipe operacional seja instruída sobre a infraestrutura e treinada durante os testes de aceitação.

A mesma norma determina que a verificação de aceitação e o comissionamento sejam realizados antes da entrega do Data Center para operação. Seus conceitos de disponibilidade, confiabilidade e resiliência reforçam que uma instalação não deve ser avaliada apenas pela existência de componentes redundantes, mas por sua capacidade de desempenhar a função pretendida e resistir a falhas.

A ABNT NBR IEC 62337, embora tenha origem em sistemas elétricos, instrumentação e controle de processos industriais, fornece princípios diretamente aplicáveis à governança do comissionamento: fases e marcos definidos, planejamento de testes, documentação, responsabilidades, listas de pendências, procedimentos detalhados, registros operacionais, condições de prontidão, avaliação formal e aceitação pelo proprietário.

O Tier Standard: Operational Sustainability do Uptime Institute inclui o teste operacional de sistemas integrados como comportamento pré-operacional relevante para instalações de maior criticidade. O mesmo padrão destaca que comissionamento, treinamento, procedimentos, manutenção e gestão são necessários para que a infraestrutura realize o potencial de desempenho de sua topologia.

Normas específicas continuam aplicáveis às disciplinas. A ABNT NBR 17207 estabelece critérios ambientais para ambientes de TIC e Data Centers; a ABNT ISO/IEC TS 22237-5 trata da disponibilidade e dos múltiplos caminhos da infraestrutura de telecomunicações; e a ABNT NBR 17240 estabelece requisitos próprios para sistemas de detecção e alarme de incêndio. O IST deve integrar interfaces sem substituir ensaios legais, aceitações regulatórias ou responsabilidades técnicas específicas.

4. QUAL É O OBJETIVO DO IST?

O objetivo do IST deve ser definido a partir dos requisitos do empreendimento. Em termos gerais, o processo procura demonstrar:

1. **continuidade da função crítica** durante os cenários previstos; 2. **resposta coordenada** dos sistemas e interfaces; 3. **atuação correta das proteções e intertravamentos**; 4. **capacidade remanescente suficiente** em estados degradados; 5. **manutenção das condições ambientais** requeridas pela carga de TIC; 6. **detecção e comunicação dos eventos** por BMS, EPMS, DCIM e demais plataformas; 7. **compreensão operacional do estado da instalação**; 8. **estabilidade durante o período de observação**; 9. **recuperação e retorno seguro** ao estado normal; 10. **rastreabilidade do resultado**, com dados e evidências verificáveis.

O objetivo não deve ser provar que “tudo funciona ao mesmo tempo”, mas confirmar cenários selecionados com base nos riscos, requisitos, arquitetura e modos de falha

relevantes.

5. O IST DEVE SER ORIENTADO POR REQUISITOS E RISCOS

Scripts genéricos produzem testes genéricos. A matriz de cenários precisa derivar dos documentos que definem o empreendimento, incluindo:

A análise deve identificar quais eventos podem comprometer a função crítica, quais interfaces participam da resposta e quais evidências demonstram o resultado.

Uma matriz de rastreabilidade permite relacionar:

requisito risco cenário estímulo resposta esperada variável medida critério de aceite evidência responsável pela aprovação.

Essa estrutura reduz lacunas e evita que o teste seja definido apenas com base na experiência informal dos participantes.

6. PRÉ-REQUISITOS PARA INICIAR OS TESTES INTEGRADOS

O IST não deve ser utilizado para descobrir pendências básicas de instalação. Antes de autorizar os cenários, convém realizar uma revisão formal de prontidão.

6.1. REQUISITOS E DOCUMENTAÇÃO ATUALIZADOS

Os documentos devem representar a instalação real. Diagramas desatualizados, lógicas alteradas em campo, etiquetas divergentes e sequências não revisadas comprometem a segurança e a validade do teste.

A base mínima inclui:

6.2. SISTEMAS INDIVIDUAIS CONCLUÍDOS

Os componentes e sistemas envolvidos devem ter concluído os testes anteriores previstos no plano. Dependendo da metodologia, isso inclui FAT, recebimento, inspeção, pré-funcionamento, partida, SAT e testes funcionais.

Iniciar o IST com sistemas básicos ainda instáveis gera resultados inconclusivos e aumenta o risco de dano.

6.3. PENDÊNCIAS CLASSIFICADAS

A punch list deve ser revisada por criticidade. Pendências que possam alterar a resposta do cenário, impedir observabilidade, comprometer segurança ou exigir intervenção improvisada devem ser encerradas antes do teste.

Pendências aceitas temporariamente precisam estar documentadas, acompanhadas de análise de impacto e aprovação da autoridade designada.

6.4. CONFIGURAÇÃO CONTROLADA

O estado inicial dos sistemas deve ser conhecido e registrado. Isso inclui:

Sem controle de configuração, o resultado não pode ser reproduzido ou comparado.

6.5. INSTRUMENTAÇÃO E OBSERVABILIDADE DISPONÍVEIS

Os sistemas precisam registrar o que ocorreu. BMS, EPMS, DCIM e plataformas específicas devem estar operacionais, com tendências configuradas, históricos disponíveis e relógios sincronizados.

Quando os instrumentos permanentes não forem suficientes, devem ser utilizados instrumentos temporários adequados e calibrados.

6.6. EQUIPE E RESPONSABILIDADES DEFINIDAS

O teste deve possuir uma estrutura de comando clara. Todos os participantes precisam saber quem:

7. GOVERNANÇA E AUTORIDADE DURANTE O IST

Testes integrados envolvem múltiplas organizações: proprietário, operação, agente de comissionamento, projetistas, construtores, integradores, fornecedores, equipe de TI, segurança, incêndio e especialistas de sistemas.

Uma matriz RACI deve definir responsabilidades por atividade e cenário. Em termos gerais:

A autoridade de abortagem deve ser explícita. Qualquer participante designado deve poder interromper o teste quando houver risco a pessoas, equipamentos, carga crítica ou integridade da instalação.

8. COMO ESTRUTURAR UMA MATRIZ DE CENÁRIOS

A matriz de IST deve organizar os eventos de forma compreensível e rastreável. Cada linha pode conter:

A matriz deve ser revisada pelas disciplinas envolvidas. Um cenário aparentemente elétrico pode exigir participação mecânica, de automação, telecomunicações e operação.

9. FAMÍLIAS DE CENÁRIOS PARA DATA CENTERS

9.1. OPERAÇÃO NORMAL

Verifica condições estáveis e transições previstas sem falha, como:

Esses cenários confirmam se a instalação consegue executar as rotinas necessárias sem gerar degradações inesperadas.

9.2. MANUTENÇÃO PLANEJADA

Avalia a retirada controlada de um componente ou caminho para manutenção. Deve verificar:

O artigo sobre [manutenção concorrente em Data Centers](#) aprofunda os critérios específicos dessa condição.

9.3. FALHA DE FONTE OU COMPONENTE

Pode incluir perda de:

O cenário deve respeitar as limitações dos fabricantes e evitar métodos destrutivos não previstos. Quando a falha real não puder ser aplicada com segurança, pode ser utilizada simulação autorizada, desde que sua representatividade seja demonstrada.

9.4. ESTADO DEGRADADO

O teste deve observar o comportamento da instalação após a perda de redundância, mesmo que a carga permaneça atendida.

É necessário verificar:

9.5. FALHAS DE COMUNICAÇÃO E AUTOMAÇÃO

A infraestrutura física pode permanecer disponível enquanto a supervisão perde visibilidade ou os controladores deixam de coordenar as sequências.

Cenários relevantes incluem:

O teste deve confirmar que a falha de monitoramento não provoca comandos indevidos e que a equipe consegue identificar a condição real.

9.6. INCÊNDIO E SEGURANÇA

As interfaces de incêndio podem envolver detecção, alarme, supressão, desligamento ou manutenção de equipamentos, controle de acesso, liberação de portas, elevadores, climatização, dampers, energia e comunicação.

Cada cenário precisa respeitar a ABNT NBR 17240, o projeto aprovado, as exigências das autoridades competentes e as responsabilidades dos profissionais habilitados.

O IST não substitui o comissionamento próprio do sistema de incêndio. Ele verifica as interfaces necessárias para a resposta integrada do Data Center.

9.7. CONDIÇÕES AMBIENTAIS

Podem ser avaliadas perda de unidade de resfriamento, falha de bomba, indisponibilidade de circuito, mudança de vazão, perda de contenção, variação de setpoint ou falha de sensor.

As medições devem observar, conforme aplicável:

A NBR 17207 estabelece que os parâmetros ambientais devem ser assegurados nas condições de projeto e que a análise deve considerar carga térmica, variações, redundância e confiabilidade.

9.8. RECUPERAÇÃO E RETORNO AO ESTADO NORMAL

O cenário não termina quando a carga permanece energizada. É necessário testar:

Muitas falhas aparecem durante a restauração, e não no evento inicial.

10. COMO ESCREVER UM SCRIPT DE TESTE INTEGRADO

O script precisa ser executável, auditável e seguro. Ele deve conter pelo menos os elementos a seguir.

10.1. IDENTIFICAÇÃO E OBJETIVO

Indicar código, título, sistemas participantes, requisito associado, risco avaliado e resultado que se pretende demonstrar.

10.2. REFERÊNCIAS

Relacionar diagramas, sequências, manuais, estudos, procedimentos, matriz de causa e efeito e documentos normativos utilizados.

10.3. CONFIGURAÇÃO INICIAL

Descrever o estado necessário para iniciar o cenário, incluindo equipamentos ativos, reservas, posições, setpoints, cargas, modos de controle, alarmes e indisponibilidades.

10.4. PRÉ-CONDIÇÕES E GATE

Definir condições que precisam ser confirmadas antes do início:

10.5. PASSOS DE EXECUÇÃO

Cada passo deve indicar:

A redação precisa evitar comandos vagos como “simular falha”. Deve ser especificado o método autorizado e o ponto exato de atuação.

10.6. CRITÉRIOS DE ABORTAGEM

Devem ser definidos limites objetivos para interromper o teste, como:

10.7. PLANO DE RESTAURAÇÃO

O script deve estabelecer como retornar à condição segura, inclusive em caso de falha do próprio teste. O plano deve considerar ações manuais, responsáveis, comunicação, equipamentos de apoio e condições para reinício.

10.8. CRITÉRIOS DE ACEITE

Cada resposta esperada deve possuir condição mensurável ou verificável.
“Funcionamento normal” não é critério suficiente.

11. SEGURANÇA DURANTE A EXECUÇÃO

O IST pode envolver energia elétrica, combustíveis, baterias, sistemas pressurizados, equipamentos rotativos, altas temperaturas, água, agentes de supressão, alarmes e alterações temporárias de redundância.

O planejamento deve integrar:

Nenhum objetivo de comissionamento justifica uma intervenção insegura. Quando a falha real não puder ser provocada de forma controlada, deve-se utilizar método alternativo tecnicamente fundamentado.

12. INSTRUMENTAÇÃO, SINCRONIZAÇÃO E EVIDÊNCIAS

A qualidade do resultado depende da qualidade da medição. O IST precisa capturar não apenas o estado final, mas a sequência temporal do evento.

12.1. INSTRUMENTOS POSSÍVEIS

12.2. SINCRONIZAÇÃO DE TEMPO

Relógios divergentes impedem a reconstrução do evento. Antes dos testes, deve ser verificado o sincronismo entre instrumentos, BMS, EPMS, DCIM, PLCs, sistemas de segurança, câmeras e registros manuais.

Quando não houver sincronização automática, deve ser estabelecido um método de correlação.

12.3. TAXA DE AMOSTRAGEM

A frequência de registro deve ser compatível com a velocidade do fenômeno. Um intervalo adequado para tendências térmicas pode ser insuficiente para capturar transferências elétricas, atuação de proteções ou transientes.

12.4. EVIDÊNCIA MÍNIMA

Para cada cenário, convém reunir:

13. EXECUÇÃO PASSO A PASSO

13.1. 1. REUNIÃO DE PRONTIDÃO

A equipe revisa objetivo, riscos, configuração, responsabilidades, critérios de abortagem e restauração. Qualquer dúvida crítica impede o início.

13.2. 2. REGISTRO DO BASELINE

Antes do estímulo, são registrados estados, cargas, temperaturas, pressões, alarmes e equipamentos em serviço. Esse baseline permite comparar o comportamento posterior.

13.3. 3. APLICAÇÃO DO ESTÍMULO

O evento é provocado ou simulado conforme o método aprovado. A execução deve seguir estritamente o script.

13.4. 4. OBSERVAÇÃO DA RESPOSTA

Cada disciplina acompanha suas variáveis e confirma eventos esperados. Intervenções não previstas devem ser registradas.

13.5. 5. PERMANÊNCIA EM CONDIÇÃO REPRESENTATIVA

Quando aplicável, o estado degradado deve ser mantido por tempo suficiente para demonstrar estabilidade, capacidade e condições ambientais.

13.6. 6. RESTAURAÇÃO

A equipe executa a sequência de retorno e confirma a recomposição dos sistemas, alarmes e redundâncias.

13.7. 7. VERIFICAÇÃO PÓS-TESTE

São revisados estados finais, condições anormais, alarmes latentes, mudanças temporárias, ferramentas e bloqueios.

13.8. 8. DEBRIEFING IMEDIATO

Os participantes registram observações enquanto o evento ainda está recente. Resultados preliminares, desvios e ações são consolidados.

14. CRITÉRIOS DE ACEITE DO IST

Os critérios precisam ser estabelecidos antes da execução. Eles podem ser organizados em categorias.

14.1. CRITÉRIOS FUNCIONAIS

14.2. CRITÉRIOS TEMPORAIS

14.3. CRITÉRIOS DE CAPACIDADE

14.4. CRITÉRIOS DE OBSERVABILIDADE

14.5. CRITÉRIOS OPERACIONAIS

14.6. CRITÉRIOS DE RESTAURAÇÃO

Um cenário pode manter a carga energizada e ainda ser reprovado se apresentar sobrecarga, perda de monitoramento, resposta térmica inadequada, alarmes incorretos, atuação manual não prevista ou impossibilidade de restauração segura.

15. GESTÃO DE ISSUES, FALHAS E RETESTES

Toda divergência entre resultado esperado e observado deve gerar registro. A issue precisa conter:

Não se deve apagar o histórico de falhas após a correção. A rastreabilidade demonstra como a instalação evoluiu e evita que problemas semelhantes reapareçam.

15.1. CLASSIFICAÇÃO POR CRITICIDADE

Uma classificação prática pode considerar:

A classificação deve ser definida pelo empreendimento.

15.2. RETESTE

O reteste deve verificar a correção sem perder a visão sistêmica. Em alguns casos, repetir apenas o passo afetado é suficiente. Em outros, a alteração pode impactar interfaces e exigir repetição do cenário completo ou de uma família de cenários.

16. VERIFICAÇÃO POR DISCIPLINA

16.1. SISTEMA ELÉTRICO

Cenários podem envolver fontes, transformadores, quadros, UPS, baterias, geradores, ATS, STS, PDUs, distribuição A/B, proteções e EPMS.

Devem ser observados:

16.2. CLIMATIZAÇÃO

O teste deve considerar a resposta coordenada de chillers, bombas, torres, CRAHs, CRACs, CDUs, válvulas, controles, contenção e sensores.

Devem ser verificados:

16.3. AUTOMAÇÃO E SUPERVISÃO

BMS, EPMS, PLCs e DCIM devem registrar e apresentar a condição correta. O teste precisa verificar alarmes, prioridades, timestamps, estados, comandos, permissivos, tendências e falhas de comunicação.

16.4. TELECOMUNICAÇÕES E REDE

A ABNT ISO/IEC TS 22237-5 estabelece múltiplos caminhos físicos para classes superiores de disponibilidade e destaca a necessidade de redundância nos equipamentos ativos. O IST deve avaliar caminhos, reconvergência, perda de enlace, comunicação de controle e impacto sobre sistemas supervisórios.

16.5. INCÊNDIO E SEGURANÇA

Interfaces devem ser verificadas conforme projeto e normas aplicáveis. Isso pode incluir detecção, alarme, liberação de acessos, atuação de dampers, climatização, desligamentos autorizados, supressão e comunicação.

17. TESTES INTEGRADOS EM DATA CENTERS EXISTENTES

Em instalações em operação, o risco é maior porque a carga real está presente. O escopo deve ser adaptado com base em análise de risco e criticidade.

Podem ser utilizadas abordagens como:

O artigo sobre [recomissionamento após expansão ou modernização](#) detalha a necessidade de redefinir o baseline após alterações.

Nenhuma limitação deve ser ocultada. O relatório precisa indicar quais cenários foram testados, simulados, inferidos ou não executados.

18. ENTREGÁVEIS DOS TESTES INTEGRADOS

Um programa completo pode produzir:

O relatório executivo deve traduzir os resultados técnicos em condições de decisão: aprovado, aprovado com restrições, reteste requerido ou não aprovado.

19. ERROS COMUNS

19.1. TRATAR O IST COMO DEMONSTRAÇÃO

Uma apresentação ensaiada, sem critérios prévios e sem registro de dados, não comprova desempenho.

19.2. COMEÇAR ANTES DA PRONTIDÃO

Testes integrados não devem compensar pendências de instalação, lógica ou documentação.

19.3. TESTAR SOMENTE ENERGIA

A continuidade elétrica não garante climatização, controle, comunicação, segurança ou recuperação.

19.4. USAR SCRIPTS GENÉRICOS

O cenário precisa refletir a arquitetura e os requisitos reais do empreendimento.

19.5. IGNORAR O ESTADO DEGRADADO

A perda de redundância pode ser operacionalmente crítica mesmo sem desligamento imediato.

19.6. NÃO TESTAR A RESTAURAÇÃO

O retorno ao estado normal pode introduzir novas falhas e precisa fazer parte do cenário.

19.7. REGISTRAR APENAS O RESULTADO FINAL

A sequência temporal e as condições intermediárias são essenciais para avaliação.

19.8. ALTERAR LÓGICA DURANTE O TESTE SEM CONTROLE

Qualquer modificação deve ser registrada, analisada e submetida a reteste.

19.9. ACEITAR INTERVENÇÃO MANUAL NÃO PREVISTA

Ação corretiva improvisada durante o cenário pode mascarar uma falha de projeto ou automação.

19.10. EXCLUIR A OPERAÇÃO

A equipe que receberá o ativo precisa participar da preparação, execução, debriefing e atualização dos procedimentos.

20. CHECKLIST EXECUTIVO

Antes do IST, confirme:

Durante o teste, confirme:

Após o teste, confirme:

21. CONCLUSÃO

Testes integrados de sistemas em Data Centers são a etapa em que a infraestrutura deixa de ser avaliada como conjunto de equipamentos independentes e passa a ser verificada como sistema crítico. Seu valor está em revelar falhas de interface, dependências ocultas, tempos inadequados, alarmes inconsistentes, limitações de capacidade e dificuldades de recuperação antes que essas condições provoquem indisponibilidade real.

Um IST tecnicamente robusto exige requisitos rastreáveis, sistemas previamente testados, configuração controlada, cenários orientados a risco, scripts detalhados, instrumentação adequada, sincronização temporal, critérios de abortagem, procedimentos de restauração, gestão de issues e aceite formal.

A A3A Engenharia atua no planejamento, revisão, acompanhamento e documentação de testes integrados em Data Centers, conectando requisitos, projeto, execução, operação e critérios de aceite para produzir evidências independentes sobre a prontidão da infraestrutura crítica.

[1] ABNT. [ABNT NBR ISO/IEC 22237-1:2023 – Tecnologia da informação – Instalações e infraestruturas de data center – Parte 1: Conceitos gerais.](#)

[2] ABNT. [ABNT NBR IEC 62337:2020 – Comissionamento de sistemas elétricos, de instrumentação e de controle de processos industriais – Fases e marcos específicos.](#)

[3] UPTIME INSTITUTE. [Data Center Site Infrastructure Tier Standard: Operational Sustainability.](#)

[4] UPTIME INSTITUTE. [Data Center Site Infrastructure Tier Standard: Topology.](#)

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

[6] ABNT. ABNT NBR 17207:2025 – Sistemas de ventilação e climatização em ambientes de tecnologia da informação, de comunicação e de Data Center.

[7] ABNT. ABNT ISO/IEC TS 22237-5:2024 – Tecnologia da informação – Instalações e infraestruturas de Data Center – Parte 5: Infraestrutura de cabeamento de telecomunicações.

[8] ABNT. ABNT NBR 17240 – Sistemas de detecção e alarme de incêndio – Projeto, instalação, comissionamento e manutenção de sistemas de detecção e alarme de incêndio – Requisitos.

O que é um teste integrado de sistemas em Data Center? É um teste orientado a cenários que verifica se diferentes sistemas e interfaces respondem de forma coordenada a condições normais, degradadas, de falha, manutenção ou emergência, preservando a função crítica e produzindo evidências rastreáveis. **IST é o mesmo que teste funcional?** Não. O teste funcional verifica um sistema ou disciplina. O IST avalia a interação entre energia, climatização, automação, telecomunicações, segurança, incêndio e operação durante um evento comum. **O IST corresponde sempre ao nível L5?** Em muitos programas

de comissionamento, sim. Entretanto, a numeração L1–L5 não é universal e deve ser definida no plano e no contrato. O conteúdo técnico do teste é mais importante que o rótulo. **Quais são os pré-requisitos para iniciar o IST?** Requisitos e documentos atualizados, sistemas individuais testados, pendências críticas encerradas, configuração controlada, instrumentos calibrados, supervisórios operacionais, equipe definida, critérios de aceite e plano de restauração aprovados. **É obrigatório provocar falhas reais?** Não em todos os casos. Quando a falha real não puder ser provocada com segurança ou sem risco desproporcional, pode ser utilizada simulação autorizada, desde que sua representatividade e limitações sejam demonstradas. **Quais sistemas devem participar dos testes integrados?** Depende do cenário. Podem participar energia, UPS, baterias, geradores, climatização, automação, BMS, EPMS, DCIM, telecomunicações, rede, incêndio, controle de acesso, segurança e a própria equipe operacional. **Como definir os critérios de aceite?** Os critérios devem derivar dos requisitos e incluir respostas funcionais, tempos, capacidade remanescente, condições ambientais, alarmes, registros, atuação da equipe, estabilidade e retorno ao estado normal. **Manter a carga energizada significa que o teste foi aprovado?** Não. O cenário pode ser reprovado por sobrecarga, perda de monitoramento, atuação manual não prevista, resposta térmica inadequada, alarmes incorretos, instabilidade ou impossibilidade de restauração segura. **A operação precisa participar do IST?** Sim. A equipe operacional deve revisar os cenários, acompanhar ou executar manobras, interpretar alarmes, participar da restauração e incorporar os resultados aos SOPs, MOPs e EOPs. **Quais documentos são entregues após o IST?** Plano e matriz de cenários, scripts, registros de execução, dados brutos, tendências, relatórios, lista de issues, evidências de retestes, matriz de atendimento, riscos residuais e aceite formal do proprietário.

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.