A3A®
Engenharia
de Sistemas

Detecção e Combate a Incêndio em Data Centers: proteção, supressão e

Solution Overview

2026

www.a3aengenharia.com.br

VISÃO GERAL

A proteção contra **incêndio em Data Centers** precisa preservar vidas, limitar a propagação do evento, proteger equipamentos e reduzir o impacto sobre a continuidade operacional. O resultado não depende apenas da escolha de detectores ou agentes extintores, mas da coordenação entre arquitetura, compartimentação, energia, climatização, automação, operação, resposta a emergências e critérios de recuperação.

Salas de TI, áreas elétricas, UPS, baterias, geradores, salas de telecomunicações, depósitos, escritórios e ambientes de apoio apresentam riscos e consequências diferentes. A solução deve considerar a origem provável do evento, a velocidade de detecção necessária, a ocupação, a possibilidade de desligamento, o comportamento do HVAC, a segurança das pessoas, a reposição do agente e o tempo aceitável para retorno à operação.

A abordagem da **A3A Engenharia** integra requisitos do empreendimento, engenharia de segurança contra incêndio e infraestrutura crítica. A solução pode abranger concepção, projeto, revisão independente, compatibilização, especificação, apoio à contratação, acompanhamento da implantação, testes, comissionamento e aceite.

RISCOS E REQUISITOS

O ponto de partida é definir o que precisa ser protegido, quais eventos precisam ser detectados, quais consequências são aceitáveis e como a instalação deve responder. O requisito de disponibilidade não elimina as obrigações de segurança; ele acrescenta a necessidade de planejar a resposta e a recuperação sem criar dependências ocultas.

MAPA DE AMBIENTES E FONTES DE RISCO

O levantamento deve separar os ambientes conforme ocupação, equipamentos, carga de incêndio, ventilação, fontes de ignição, acessos, rotas de fuga e impacto da indisponibilidade. Uma sala de baterias, uma sala de geradores e um white space não devem receber automaticamente a mesma estratégia.

- salas de equipamentos de TI e telecomunicações;
- salas elétricas, UPS, painéis e transformadores;
- ambientes de baterias e armazenamento de energia;
- geradores, combustíveis e áreas externas de apoio;
- plenos, pisos elevados, forros, shafts e caminhos de cabos;
- docas, depósitos, oficinas e áreas administrativas.

REQUISITOS DO PROPRIETÁRIO E CONTINUIDADE

Os requisitos devem registrar prioridades de proteção à vida, limites de dano, disponibilidade, capacidade de isolamento, tempo de recuperação, operação por fases e responsabilidades de resposta. Também devem indicar quais sistemas podem ser desligados automaticamente, quais dependem de confirmação e quais precisam permanecer disponíveis para conduzir a emergência.

INTERFACES COM ENERGIA, HVAC E OPERAÇÃO

Uma lógica de incêndio pode comandar dampers, ventiladores, portas, alarmes, pressurização, desligamentos, transferência de energia, liberação de acessos e sistemas de supervisão. Essas interfaces precisam ser definidas em matriz de causa e efeito, com estados normais, ações automáticas, confirmações, temporizações, permissivos e condições de retorno.

O agente extintor não deve ser escolhido antes da arquitetura de risco.

A solução depende do ambiente, da ocupação, da estanqueidade, da ventilação, dos materiais, da resposta operacional, das exigências legais e da estratégia de continuidade.

A escolha isolada de uma tecnologia pode gerar falsa sensação de proteção.

Integrar os requisitos ao Projeto de Data Center

ARQUITETURA DE PROTEÇÃO

A arquitetura deve combinar medidas passivas, detecção, alarme, controle do evento, combate, evacuação, supervisão e recuperação. A redundância dos sistemas de TI não compensa uma compartimentação inadequada ou uma falha comum que afete simultaneamente as rotas A e B.

COMPARTIMENTAÇÃO E PROPAGAÇÃO

Paredes, portas, selagens, shafts, passagens de cabos e elementos construtivos precisam manter a separação prevista entre áreas. A proteção deve considerar propagação por plenos, dutos, bandejas, pisos elevados, forros e penetrações adicionadas durante expansões ou manutenções.

ZONAS DE DETECÇÃO E COMBATE

O zoneamento deve permitir localizar o evento, aplicar a resposta adequada e limitar indisponibilidades desnecessárias. Os limites das zonas precisam ser coerentes com compartimentos, sistemas de climatização, circuitos elétricos, rotas de acesso, áreas de supressão e responsabilidades operacionais.

MATRIZ DE CAUSA E EFEITO

A matriz relaciona entradas, condições confirmatórias, alarmes, temporizações e comandos. Ela deve cobrir detecção inicial, alarme confirmado, pré-descarga, descarga, aborto, falha, perda de comunicação, acionamento manual, retorno ao estado seguro e comunicação com BMS, DCIM, supervisão predial e sistemas de segurança.

EXPANSÕES E MANUTENÇÃO SEM PERDA DE PROTEÇÃO

Data Centers mudam continuamente. Novos racks, cabos, divisórias, corredores confinados e equipamentos podem alterar fluxo de ar, cobertura, compartimentação e concentração de agentes. O projeto deve prever manutenção, isolamento de zonas, testes e expansão sem deixar áreas críticas desprotegidas ou criar indisponibilidades não planejadas.

Uma proteção crítica precisa ser testável.

Arquiteturas que não permitem simular alarmes, verificar comandos, testar intertravamentos ou isolar zonas de forma controlada tendem a acumular falhas ocultas durante a operação.

Conheça o Owner’s Engineering para Data Centers

DETECÇÃO E SUPRESSÃO

A detecção deve identificar o evento em tempo compatível com o risco e fornecer informação suficiente para uma resposta segura. A supressão deve controlar o incêndio sem introduzir riscos incompatíveis com as pessoas, os equipamentos, a construção ou a continuidade planejada.

DETECÇÃO PRECOCE E CONFIRMAÇÃO

A estratégia pode combinar detectores pontuais, sistemas por aspiração, detecção em plenos, supervisão de painéis e outros meios adequados ao ambiente. Sensibilidade, posicionamento, fluxo de ar, filtragem, alarmes graduais e lógica de confirmação precisam ser definidos para reduzir atrasos e alarmes indevidos.

ALARME, NOTIFICAÇÃO E RESPOSTA HUMANA

Alarmes devem chegar às pessoas responsáveis com identificação da zona, criticidade, estágio do evento e ação esperada. A solução precisa considerar ocupantes, equipe de operação, brigada, centro de controle, acesso de emergência, comunicação interna e procedimentos para investigação segura.

SUPRESSÃO LOCALIZADA OU POR INUNDAÇÃO TOTAL

A seleção pode envolver sistemas automáticos de água, agentes limpos, gases inertes, água nebulizada ou outras tecnologias reconhecidas e aprovadas para o risco. A decisão deve considerar eficácia, segurança, descarga, estanqueidade, impacto térmico, reentrada, reposição, disponibilidade local, manutenção e exigências da autoridade competente.

PISOS ELEVADOS, FORROS E CORREDORES CONFINADOS

Os volumes ocultos e os caminhos de ar precisam ser avaliados como parte do ambiente protegido. A cobertura e a distribuição do agente não devem ser presumidas a partir apenas da área aparente da sala. Barreiras, racks, contenções e vazamentos podem alterar o comportamento esperado.

ESTANQUEIDADE E RETENÇÃO DO AGENTE

Quando a estratégia depende de concentração e tempo de retenção, a integridade do compartimento deve ser verificada. Passagens de cabos, portas, grelhas, dampers e alterações posteriores podem comprometer o desempenho. Ensaios e inspeções precisam ser associados à configuração real da sala.

SISTEMAS AUXILIARES E ALIMENTAÇÃO

Centrais, laços, módulos, fontes, baterias, comunicação, acionadores, supervisões e dispositivos de campo precisam permanecer confiáveis nas condições previstas. A alimentação, a segregação de circuitos, a identificação, a integridade funcional e a supervisão de falhas fazem parte da solução.

Detecção precoce não substitui combate, e combate não substitui detecção.

A proteção depende da sequência completa: identificar, confirmar, comunicar, controlar interfaces, combater, registrar evidências e recuperar a operação.

Consultar a solução geral de prevenção e combate a incêndio

OPERAÇÃO E ACEITE

A proteção só pode ser aceita quando projeto, instalação, lógica, documentação e resposta operacional formam um sistema coerente. A aprovação isolada de equipamentos não demonstra o desempenho integrado do ambiente.

TESTES FUNCIONAIS E INTEGRADOS

Os testes devem verificar detecção, alarmes, falhas, comunicação, temporizações, acionamentos manuais, comandos de HVAC, portas, acessos, supervisão e estados de segurança. Quando aplicável, ensaios específicos de distribuição, estanqueidade e retenção devem compor a evidência de desempenho.

CRITÉRIOS DE LIBERAÇÃO E PENDÊNCIAS

As pendências precisam ser classificadas conforme impacto sobre segurança, cobertura, detecção, combate, evacuação, continuidade e documentação. A liberação pode ser recusada, condicionada ou parcial, desde que as restrições, compensações e responsabilidades estejam formalmente registradas.

DOCUMENTAÇÃO E TREINAMENTO

O dossiê deve reunir projetos aprovados, diagramas, matriz de causa e efeito, memoriais, folhas de dados, certificados, relatórios de testes, configuração final, lista de dispositivos, as built, manuais, planos de manutenção e registros de treinamento. A equipe precisa compreender alarmes, bloqueios, procedimentos de investigação, descarga, evacuação, reentrada e retorno à operação.

INSPEÇÕES, MANUTENÇÃO E GESTÃO DE MUDANÇAS

Alterações em racks, cabos, paredes, portas, contenções, HVAC ou ocupação devem passar por avaliação de impacto. Testes periódicos, inspeções, gestão de bypass, controle de falhas e revisão documental reduzem o risco de a proteção perder eficácia ao longo do ciclo de vida.

REFERÊNCIAS TÉCNICAS APLICÁVEIS

A definição do escopo deve considerar legislação local, instruções técnicas do Corpo de Bombeiros, normas ABNT aplicáveis e referências específicas para instalações críticas. Entre as referências internacionais estão a ISO/IEC 22237-6:2024, relacionada aos sistemas de segurança de Data Centers, e a NFPA 75, voltada à proteção contra incêndio

de equipamentos de tecnologia da informação. A seleção final depende da jurisdição, do contrato e da estratégia de conformidade do empreendimento.

ENTREGÁVEIS TÍPICOS

- levantamento de riscos, ambientes e interfaces;
- requisitos de proteção e critérios de desempenho;
- arquitetura de detecção, alarme e supressão;
- zoneamento e matriz de causa e efeito;
- plantas, diagramas, memoriais e especificações;
- compatibilização com energia, HVAC, automação e segurança;
- critérios de FAT, SAT, testes integrados e aceite;
- matriz de pendências e relatório de conformidade;
- dossiê técnico e recomendações de operação e manutenção.

ESCOPO DE ENGENHARIA CONSULTIVA DA A3A ENGENHARIA

A **A3A Engenharia** pode atuar em novos Data Centers, expansões, retrofit e adequações de instalações existentes. O trabalho pode abranger diagnóstico, definição de requisitos, projeto, revisão independente, compatibilização multidisciplinar, apoio à contratação, acompanhamento de fornecedores, fiscalização técnica, testes, comissionamento e aceite.

A solução pode ser contratada de forma autônoma ou integrada ao programa de Engenharia Integrada para Data Centers, ao Owner's Engineering ou ao processo de modernização e comissionamento.

Valide a proteção contra incêndio como parte do sistema crítico.

A A3A Engenharia pode estruturar requisitos, interfaces, critérios de teste e evidências para novos projetos, ampliações e modernizações de Data Centers.

Solicitar avaliação técnica

RESUMO TÉCNICO

A proteção contra incêndio em Data Centers deve ser definida a partir dos riscos, ambientes, requisitos do proprietário, compartimentação, interfaces e estratégia de continuidade. Detecção precoce, alarme, supressão, HVAC, energia, acessos e supervisão precisam responder de forma coordenada e verificável.

O aceite exige evidências de cobertura, lógica, comunicação, comandos, estanqueidade quando aplicável, documentação e prontidão operacional. A solução deve permanecer testável, expansível e compatível com mudanças de layout, capacidade e tecnologia ao longo do ciclo de vida do Data Center.

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