WHITEPAPER

SEGURANÇA FÍSICA EM DATA CENTERS: ZONAS, CONTROLE DE ACESSO, CFTV E PERÍMETRO

Entenda como projetar a segurança física de Data Centers: zonas, perímetro, controle de acesso, CFTV, biometria, integração, LGPD e comissionamento.

A3A® Engenharia de Sistemas

SUMÁRIO

A **segurança física em Data Centers** protege pessoas, infraestrutura, equipamentos, mídias e continuidade operacional contra acessos não autorizados, intrusão, sabotagem, furto, intervenção indevida e falhas de controle. Em uma instalação crítica, instalar câmeras e leitores não é suficiente: é necessário organizar o ambiente em zonas, controlar fluxos, relacionar permissões às atividades e garantir que cada evento relevante possa ser detectado, verificado, respondido e investigado.

O projeto deve começar pela análise de risco e pela criticidade dos ativos. A arquitetura resultante combina medidas construtivas, barreiras físicas, controle de acesso, videomonitoramento, detecção de intrusão, comunicação, procedimentos operacionais, integração entre plataformas e testes de desempenho. A solução comercial de Segurança Física para Data Centers atende à contratação e implantação; este artigo apresenta os critérios técnicos para especificar, integrar e aceitar esses sistemas.

1. POR QUE A SEGURANÇA FÍSICA DE UM DATA CENTER É DIFERENTE?

Um Data Center reúne ativos de alto valor, infraestrutura elétrica e mecânica crítica, redes de telecomunicações, informações sensíveis e serviços cuja indisponibilidade pode afetar toda a organização. Ao mesmo tempo, recebe funcionários, fornecedores, clientes, equipes de manutenção, entregas e intervenções programadas. Essa combinação cria riscos externos e internos que não são resolvidos por uma única barreira.

A segurança deve considerar pelo menos quatro dimensões:

A arquitetura precisa continuar funcional em condições degradadas. Falha de rede, perda de comunicação com o servidor, indisponibilidade de uma controladora, falta de energia, manutenção de uma porta ou defeito em uma câmera não podem transformar automaticamente uma área crítica em espaço sem controle.

1.1. SEGURANÇA FÍSICA E CIBERSEGURANÇA SÃO INTERDEPENDENTES

Câmeras IP, controladoras, leitores, sensores, servidores, VMS e plataformas de gestão são sistemas conectados. Uma vulnerabilidade digital pode desabilitar uma função física, apagar evidências ou conceder privilégios indevidos. No sentido inverso, o acesso físico a racks, switches, consoles e meios de armazenamento pode contornar controles lógicos.

Por isso, a segurança física deve participar da arquitetura de redes, da gestão de identidades, da segmentação, do hardening, da sincronização de tempo, da continuidade e do gerenciamento de mudanças. A integração com o DCIM, BMS e EPMS deve fornecer contexto sem criar dependências que impeçam a atuação local dos sistemas de segurança.

2. A ESTRATÉGIA DEVE SER BASEADA EM RISCO

O projeto começa com a identificação de ativos, ameaças, vulnerabilidades, impactos e controles existentes. O objetivo não é prever apenas invasões externas. Credenciais mantidas após o encerramento de contratos, acompanhamento indevido, compartilhamento de cartões, portas em bypass, circulação de prestadores, retirada de equipamentos e intervenção em sistemas redundantes também são riscos físicos relevantes.

2.1. ATIVOS E CONSEQUÊNCIAS

O levantamento deve identificar o que precisa ser protegido e qual seria a consequência de perda, manipulação ou indisponibilidade. Entre os ativos estão:

A criticidade não depende apenas do valor patrimonial. Uma porta de acesso à sala elétrica pode ter impacto operacional superior ao de uma área com equipamentos mais caros, porque uma ação incorreta pode afetar múltiplas cargas.

2.2. AMEAÇAS EXTERNAS E INTERNAS

O modelo de ameaça deve considerar intrusão, vandalismo, sabotagem, furto, acesso fraudulento, uso indevido de credenciais, engenharia social, falhas de escolta, intervenção não autorizada, retirada de ativos e danos provocados por veículos ou obras próximas. Também devem ser avaliadas ameaças naturais e ambientais que alterem a operação do perímetro ou dos acessos.

A ameaça interna não pressupõe intenção maliciosa. Erros de operação, manutenção fora da janela aprovada, acesso a área incompatível com a atividade e falta de segregação de funções podem produzir consequências equivalentes às de um ataque deliberado.

2.3. REQUISITOS DE PROTEÇÃO E TEMPO DE RESPOSTA

Cada cenário deve ser associado a uma resposta esperada. Detectar um evento sem possuir equipe, procedimento, comunicação ou tempo adequado para intervir não constitui proteção completa. A arquitetura deve relacionar:

3. DEFESA EM PROFUNDIDADE: PREVENIR, DISSUADIR, DETECTAR, ATRASAR E RESPONDER

A segurança por camadas evita que uma única falha conceda acesso direto ao ativo crítico. As funções são complementares:

Duas portas controladas não representam necessariamente duas camadas independentes. Se ambas dependem da mesma fonte, controladora, rede, base de identidade ou procedimento de contingência, uma falha comum pode comprometer as duas.

4. COMO ORGANIZAR AS ZONAS DE SEGURANÇA

As zonas devem refletir criticidade, função, fluxo e necessidade de acesso. O número e o nome das zonas podem variar, mas a progressão deve ser compreensível e auditável.

Zona	Exemplo de espaço	Controle predominante	Objetivo
Contexto externo	vias, vizinhança e aproximação	análise de risco, iluminação e observação	identificar ameaças antes de alcançarem o imóvel
Perímetro	limites, portões, estacionamento e guarita	barreiras, detecção, CFTV e controle veicular	controlar aproximação e entrada no sítio
Área de recepção	recepção, espera e áreas administrativas	identificação, credenciamento e separação de fluxos	impedir circulação livre de visitantes
Circulação técnica	corredores, docas e áreas de apoio	autorização por perfil, vídeo e supervisão	controlar deslocamento até áreas críticas
Área crítica	white space, MMR, salas elétricas e mecânicas	autenticação reforçada, registro e restrição temporal	limitar acesso a atividades justificadas
Microzona	cage, rack, gabinete, cofre de mídia	autorização específica e evidência individualizada	proteger ativos ou clientes determinados

Arquitetura física orientada ao risco

Zonas, transições e barreiras precisam ser definidas pela criticidade dos ativos, pelos fluxos autorizados e pelo tempo de resposta. A independência entre camadas deve ser verificada também em falhas de energia, comunicação e controladoras.

Conheça a solução de Segurança Física para Data Centers

4.1. TRANSIÇÕES ENTRE ZONAS

Cada transição precisa ter uma razão. A passagem deve definir quem pode atravessar, em quais condições, durante qual período e com quais registros. Quanto maior a criticidade, maior deve ser a independência entre autenticação, barreira, verificação e supervisão.

Uma credencial que abre o portão não deveria, por consequência, conceder acesso ao white space. Da mesma forma, autorização para manutenção de climatização não implica acesso a racks de clientes ou à sala de telecomunicações.

4.2. ZONAS DE CLIENTES E COLOCATION

Ambientes de colocation exigem segregação adicional. Clientes podem compartilhar corredores e infraestrutura, mas não devem acessar cages, racks, registros ou imagens de terceiros. A arquitetura deve separar permissões, visualizações, relatórios e responsabilidades operacionais.

Em operações com cages, a proteção do edifício não substitui a proteção do espaço contratado. É necessário definir fronteiras de responsabilidade entre operador e cliente, inclusive para portas, fechaduras, CFTV, alarmes, retenção de evidências e tratamento de incidentes.

5. SEGURANÇA PERIMETRAL DO DATA CENTER

O perímetro estabelece a primeira oportunidade de detectar, avaliar e controlar uma aproximação. A solução pode combinar limites físicos, iluminação, controle de vegetação, portões, barreiras veiculares, guaritas, sensores, radares, câmeras convencionais ou térmicas e análise de vídeo.

A seleção depende do contexto. Um campus isolado, um Data Center urbano, um CPD dentro de edifício corporativo e um Edge Data Center não apresentam as mesmas ameaças nem o mesmo espaço para atraso e resposta.

5.1. BARREIRAS FÍSICAS E CIRCULAÇÃO DE VEÍCULOS

Muros, cercas, portões e barreiras devem conduzir pessoas e veículos aos pontos controlados, evitando passagens improvisadas. O projeto deve avaliar resistência, visibilidade, drenagem, topografia, áreas de ocultação, proximidade de vias e possibilidade de impacto veicular.

O controle veicular deve separar acesso cotidiano, entregas, manutenção, emergência e áreas de carga. A autorização de um motorista não significa autorização automática para a carga, acompanhantes ou acesso às áreas internas.

5.2. ILUMINAÇÃO E QUALIDADE DA IMAGEM

A iluminação deve apoiar observação humana, CFTV e segurança de circulação sem criar ofuscamento, sombras profundas ou reflexos que prejudiquem a identificação. O desempenho precisa ser verificado em diferentes horários e condições meteorológicas.

Iluminadores infravermelhos, câmeras térmicas e recursos de ampla faixa dinâmica podem complementar a iluminação, mas não corrigem posicionamento inadequado, oclusão ou ausência de objetivo operacional.

5.3. DETECÇÃO DE INTRUSÃO

Sensores perimetrais devem ser selecionados conforme ambiente, vegetação, clima, animais, tráfego e geometria. A taxa de alarmes improdutivos é um requisito de desempenho: um sistema que alarma continuamente tende a perder credibilidade operacional.

A integração com CFTV deve levar o operador diretamente às imagens e informações relevantes, preservando o evento original, o horário, a localização e as ações tomadas. A Proteção Perimetral deve ser tratada como sistema de detecção e resposta, não como coleção de sensores.

6. CONTROLE DE ACESSO FÍSICO

O controle de acesso administra identidades, credenciais, regras, horários, zonas e eventos. O sistema precisa refletir a política de segurança, e não apenas substituir chaves mecânicas por cartões.

6.1. IDENTIDADE, FUNÇÃO E MENOR PRIVILÉGIO

As permissões devem ser concedidas conforme função, vínculo, site, atividade e período. O princípio de menor privilégio limita o acesso ao necessário. A segregação de funções reduz o risco de uma única pessoa executar e ocultar uma intervenção crítica.

A autorização precisa possuir responsável, justificativa e prazo. Perfis permanentes genéricos e credenciais compartilhadas prejudicam a rastreabilidade e dificultam a revogação.

6.2. CICLO DE VIDA DAS CREDENCIAIS

Admissão, mudança de função, afastamento, troca de fornecedor, perda de credencial e encerramento de contrato devem gerar eventos formais no sistema. Sempre que possível, permissões temporárias devem expirar automaticamente.

Revisões periódicas identificam acessos acumulados, perfis incompatíveis e credenciais sem uso. O processo precisa incluir contas administrativas, credenciais de emergência e chaves mecânicas mantidas como contingência.

6.3. VISITANTES E PRESTADORES

O visitante deve possuir patrocinador, finalidade, janela de acesso, áreas permitidas e regra de acompanhamento. A identificação na recepção não substitui a autorização para entrar em áreas técnicas.

Prestadores devem ser vinculados a contrato, ordem de serviço, mudança aprovada ou atividade planejada. A permissão precisa ser compatível com o escopo e expirar ao fim da janela. Em atividades críticas, pode ser exigida dupla autorização ou presença de responsável local.

6.4. MANTRAP, INTERTRAVAMENTO E ANTI-TAILGATING

A mantrap é uma câmara com portas intertravadas destinada a controlar a passagem individual e reduzir acompanhamento indevido. Ela deve ser especificada a partir do fluxo, da ocupação, das condições de emergência, da acessibilidade e do modo degradado.

Intertravamento não deve impedir evacuação nem conflitar com a segurança contra incêndio. O projeto precisa definir claramente o comportamento em alarme, falta de energia, falha de comunicação, acionamento de emergência e manutenção.

Antipassback, contagem de ocupação, sensores de presença e análise de vídeo podem apoiar a detecção de passagem indevida. Nenhum desses recursos elimina a necessidade de procedimentos e supervisão.

6.5. FAIL-SAFE, FAIL-SECURE E LIBERAÇÃO DE EMERGÊNCIA

A escolha entre destravar ou permanecer travado em uma falha depende da porta, da rota de fuga, da ocupação, do risco e dos requisitos aplicáveis. Não existe uma regra única para todas as portas do Data Center.

A decisão deve ser documentada na matriz de causa e efeito e testada com os sistemas de incêndio, energia, supervisão e comunicação. A vida e a evacuação segura têm prioridade sobre a proteção patrimonial.

6.6. COMUNICAÇÃO ENTRE LEITORES E CONTROLADORAS

A interface entre leitores, controladoras e servidores também precisa de proteção. Protocolos supervisionados e com canal seguro, como OSDP quando compatível com os equipamentos, reduzem limitações de interfaces legadas e melhoram a monitoração de comunicação.

A especificação deve abranger modo offline, armazenamento local de eventos, atualização de listas, sincronismo, chaves criptográficas, gestão de firmware e recuperação após retorno da rede.

7. BIOMETRIA E PROTEÇÃO DE DADOS PESSOAIS

Biometria pode reforçar a autenticação, mas envolve dados pessoais sensíveis. A decisão deve considerar finalidade, necessidade, proporcionalidade, base legal, transparência, segurança, retenção, compartilhamento e descarte.

A biometria não deve ser escolhida apenas porque o equipamento está disponível. O projeto precisa avaliar:

Reconhecimento facial e identificação biométrica não são equivalentes a simples registro de imagem. O tratamento exige governança específica. O sistema deve coletar apenas os dados necessários e limitar seu uso à finalidade definida.

8. CFTV PARA DATA CENTERS

O Videomonitoramento deve ser projetado por objetivos. Cada câmera precisa responder a uma necessidade: detectar aproximação, observar comportamento, reconhecer uma pessoa conhecida, identificar detalhes, registrar uma transação ou acompanhar uma intervenção.

8.1. COBERTURA ORIENTADA AO RISCO

Áreas normalmente avaliadas incluem:

O interior de áreas sensíveis deve respeitar finalidade, privacidade e regras contratuais. Uma câmera não deve registrar telas, teclados ou espaços de terceiros sem necessidade claramente definida.

8.2. CAMPO DE VISÃO, ILUMINAÇÃO E OCLUSÃO

A quantidade de câmeras não comprova cobertura. O projeto deve verificar distância, ângulo, altura, lente, densidade de imagem, iluminação, contraste, movimento, oclusão, reflexos e posição provável das pessoas.

O ensaio precisa reproduzir o objetivo operacional. Uma imagem que parece nítida em uma visão geral pode não permitir verificar uma credencial, acompanhar a retirada de um equipamento ou associar uma pessoa a uma porta específica.

8.3. GRAVAÇÃO, RETENÇÃO E DISPONIBILIDADE

A retenção deve derivar de risco, investigação, requisitos contratuais e proteção de dados. Armazenar indefinidamente aumenta custo e exposição sem necessariamente melhorar segurança.

A arquitetura deve considerar falha de câmera, rede, storage, servidor, energia e sincronismo. Gravação na borda pode complementar o VMS, mas precisa ser reconciliada após a recuperação. Alarmes de perda de vídeo, desfoque, obstrução, alteração de cena e falha de gravação devem possuir responsáveis e procedimentos.

8.4. SINCRONIZAÇÃO E CADEIA DE EVIDÊNCIAS

Eventos de acesso, vídeo, intrusão e sistemas prediais precisam compartilhar referência de tempo confiável. Diferenças de relógio prejudicam correlação e investigação.

A exportação de evidências deve registrar origem, intervalo, operador, formato, integridade e cadeia de custódia. O acesso às imagens e aos registros precisa ser controlado e auditável.

8.5. INTEROPERABILIDADE E ANALÍTICOS

Perfis ONVIF podem apoiar interoperabilidade entre dispositivos e clientes. Para vídeo, Profile T é mais adequado às funções modernas de streaming; Profile M trata metadados e eventos de analíticos. Em controle de acesso, Profiles A, C e D cobrem diferentes funções de configuração, sistema e periféricos.

A conformidade declarada deve ser verificada por modelo e função. “Compatível com ONVIF” não significa que todos os recursos de dois produtos serão interoperáveis.

Analíticos podem apoiar detecção de permanência, cruzamento de linha, objeto abandonado, presença em área restrita e correlação com acesso. Devem ser testados no cenário real, com metas de desempenho e tratamento de alarmes improdutivos.

9. INTRUSÃO, PORTAS E GABINETES

Sensores de abertura, porta forçada, porta mantida aberta, vibração, movimento e contato de gabinete complementam controle de acesso e CFTV. A relevância depende da zona e do ativo.

Portas críticas devem possuir supervisão do estado real. Um comando de abertura não comprova fechamento, travamento ou ausência de obstrução. Da mesma forma, uma credencial válida não comprova que somente uma pessoa atravessou.

Racks, cages e gabinetes podem formar microzonas. O controle individualizado é útil quando existem múltiplos clientes, equipes distintas, equipamentos especialmente críticos ou necessidade de vincular acesso físico a uma ordem de serviço.

10. SALA-COFRE E SALA SEGURA

Sala-cofre e sala segura são alternativas construtivas para elevar proteção física e ambiental de um espaço. Elas podem integrar resistência a intrusão, fogo, água, fumaça e outros riscos, conforme especificação e certificação aplicáveis.

Entretanto, uma sala-cofre não substitui a estratégia completa. A porta ainda depende de identidade, autorização, emergência, manutenção e registro; os acessos de cabos, dutos e tubulações precisam preservar a proteção; e a operação continua exigindo CFTV, procedimentos e resposta.

A escolha deve comparar risco, estrutura existente, interfaces, capacidade de expansão, peso, estanqueidade, rotas, prazo, certificação, manutenção e custo de ciclo de vida. Em muitos projetos, compartimentação e controles convencionais bem especificados são mais adequados do que adotar uma sala-cofre sem análise integrada.

11. INTEGRAÇÃO ENTRE ACESSO, VÍDEO, INTRUSÃO E OPERAÇÃO

A integração deve reduzir o tempo entre evento e decisão. Exemplos incluem abrir automaticamente as câmeras associadas a uma porta forçada, correlacionar uma tentativa negada com vídeo, vincular acesso de prestador à ordem de serviço e confirmar se uma área foi evacuada.

11.1. VMS, PSIM E PLATAFORMA UNIFICADA

O VMS administra vídeo, gravação, eventos e investigação. Uma plataforma unificada pode acrescentar controle de acesso e outras funções. Um PSIM tende a orquestrar eventos e procedimentos de múltiplos sistemas.

A escolha deve considerar escala, operadores, integrações, redundância, licenciamento, evidência, cibersegurança e dependência do fornecedor. Centralizar a interface não significa centralizar todos os pontos de falha.

11.2. MATRIZ DE EVENTOS E RESPOSTAS

Cada evento relevante precisa possuir:

Alarmes sem prioridade, contexto ou procedimento aumentam carga operacional e podem ocultar eventos críticos.

Integração precisa reduzir o tempo de resposta

Correlacionar acesso, vídeo, intrusão e procedimentos só agrega valor quando cada evento possui prioridade, contexto, autoridade definida, responsável e evidência de tratamento. A integração não deve eliminar a autonomia das funções locais essenciais.

Veja o Projeto de Segurança Eletrônica Integrada

11.3. INTEGRAÇÃO COM INCÊNDIO E EMERGÊNCIA

O controle de acesso deve receber apenas os sinais necessários e executar a sequência aprovada. Liberação de portas, desbloqueios, mensagens, acionamento de câmeras e restrição de áreas devem ser definidos na matriz de causa e efeito da segurança contra incêndio em Data Centers.

Não se deve programar uma integração que impeça evacuação ou introduza dependência de um servidor não classificado para função de segurança da vida.

12. INFRAESTRUTURA DOS SISTEMAS DE SEGURANÇA

A disponibilidade da segurança depende da infraestrutura que a suporta. O projeto deve definir:

O cabeamento do Data Center deve contemplar os sistemas de segurança, evitando caminhos vulneráveis e pontos únicos de falha incompatíveis com a criticidade.

12.1. CIBERSEGURANÇA DOS SISTEMAS FÍSICOS

Câmeras e controladoras devem ser tratadas como ativos de rede. Senhas padrão, serviços desnecessários, firmware desatualizado, acesso remoto sem controle e certificados inválidos comprometem a proteção.

A arquitetura deve incluir inventário, segmentação, autenticação administrativa, criptografia, backup de configuração, logging, gestão de vulnerabilidades, controle de fornecedores e plano de recuperação. Acesso remoto temporário deve possuir autorização, MFA quando aplicável, registro e expiração.

13. OPERAÇÃO E GOVERNANÇA

A segurança física perde eficácia quando permissões, alarmes e exceções não são administrados. A operação precisa ser formal, mensurável e auditável.

13.1. PROCEDIMENTOS OPERACIONAIS

Devem existir procedimentos para credenciamento, visitantes, manutenção, entrega, retirada de ativos, porta em bypass, falha de sistema, emergência, investigação, preservação de evidências e retorno à condição normal.

Os procedimentos devem ser testados. Um documento que nunca foi executado pode conter dependências inexistentes, contatos desatualizados ou ações incompatíveis com a operação.

13.2. GESTÃO DE BYPASS E MANUTENÇÃO

Portas, sensores e câmeras colocados em manutenção reduzem a proteção. Toda indisponibilidade deve possuir autorização, prazo, controle compensatório, comunicação e confirmação de restabelecimento.

O sistema precisa distinguir manutenção planejada de falha não tratada. Bypass permanente ou recorrente deve gerar análise de causa e correção de projeto, não normalização da exceção.

13.3. INDICADORES DE DESEMPENHO

Indicadores úteis incluem disponibilidade de câmeras e leitores, falhas de gravação, portas mantidas abertas, acessos negados, credenciais vencidas, alarmes recorrentes, tempo de reconhecimento, tempo de resposta, duração de bypass e conclusão das revisões de acesso.

Métricas devem apoiar decisões. A redução artificial de alarmes pela desativação de regras não representa melhoria de desempenho.

14. COMISSIONAMENTO E ACEITE DA SEGURANÇA FÍSICA

O comissionamento verifica se o sistema instalado cumpre os requisitos em condições normais, degradadas e de emergência. Testar cada dispositivo isoladamente não comprova o funcionamento da arquitetura.

14.1. REVISÃO DOCUMENTAL E INSPEÇÃO

Antes dos testes funcionais, devem ser verificados desenhos, listas de pontos, identificação, endereçamento, alimentação, rede, licenças, versões, certificados, parâmetros, cobertura, retenção, permissões e matriz de eventos.

A inspeção deve confirmar instalação, acabamento, proteção de cabos, posição de câmeras, sentido de abertura, fechaduras, contatos, botoeiras, fontes, baterias, racks, ventilação e identificação.

14.2. TESTES DE CONTROLE DE ACESSO

Os testes devem abranger concessão e revogação, horários, zonas, credenciais temporárias, acesso negado, porta forçada, porta mantida aberta, antipassback, intertravamento, modo offline, perda de servidor, retorno da comunicação, falta de energia e emergência.

Também devem ser testadas exceções: visitante, prestador, credencial perdida, acesso administrativo, override autorizado e recuperação após falha.

14.3. TESTES DE CFTV

Cada câmera deve ser testada contra seu objetivo operacional. Devem ser verificados campo de visão, detalhe, iluminação diurna e noturna, foco, movimento, WDR, oclusão, gravação, reprodução, exportação, retenção, perda de rede, gravação de borda, sincronismo e alarmes de saúde.

O teste deve utilizar cenários representativos, não apenas confirmar que existe imagem.

14.4. TESTES DE INTRUSÃO E PERÍMETRO

Sensores e analíticos devem ser avaliados nas condições reais previstas, incluindo variações ambientais. O aceite precisa registrar detecção, tempo, localização, vídeo associado, apresentação ao operador, reconhecimento, escalonamento e encerramento.

14.5. TESTES INTEGRADOS E MODOS DEGRADADOS

Devem ser simuladas sequências completas entre acesso, vídeo, intrusão, interfonia, incêndio, BMS, DCIM e centro de operação. O teste precisa confirmar que a falha de uma integração não elimina a função local essencial.

Modos degradados incluem perda de rede, servidor, storage, controlador, sincronismo e alimentação. O retorno à condição normal deve preservar eventos, reconciliar dados e não conceder permissões indevidas.

O serviço de Comissionamento e Aceite de Data Centers deve utilizar critérios objetivos, evidências e rastreabilidade das não conformidades.

O aceite precisa testar modos degradados

Perda de rede, servidor, storage, controlador, sincronismo ou alimentação deve ser ensaiada de forma controlada. O sistema precisa preservar funções essenciais, registrar eventos e retornar à condição normal sem criar permissões indevidas ou lacunas de evidência.

Conheça o Comissionamento e Aceite de Data Centers

15. MODERNIZAÇÃO DE AMBIENTES EXISTENTES

Data Centers existentes frequentemente possuem sistemas de gerações e fabricantes diferentes, permissões acumuladas, pontos cegos, retenção insuficiente e integrações frágeis. A modernização deve começar pelo diagnóstico, não pela substituição indiscriminada.

15.1. LEVANTAMENTO DO ESTADO ATUAL

O inventário deve abranger dispositivos, versões, licenças, redes, fontes, autonomia, gravação, storage, integrações, credenciais, perfis, portas, câmeras, sensores e documentação. Também é necessário observar a operação real: bypass, falhas recorrentes, alarmes ignorados e procedimentos informais.

15.2. MIGRAÇÃO POR FASES

A implantação pode ser dividida por perímetro, acessos, áreas críticas, plataformas e integrações. Cada fase deve manter proteção, compatibilidade, evidências e plano de retorno. A migração de credenciais exige saneamento de identidades e permissões, evitando transferir erros do sistema antigo.

O Diagnóstico e Modernização de Data Centers e CPDs ajuda a priorizar riscos, dependências e intervenções sem comprometer a operação.

16. ERROS COMUNS

16.1. COMEÇAR PELA LISTA DE EQUIPAMENTOS

Selecionar câmeras, leitores e sensores antes de definir riscos, zonas e objetivos produz lacunas e excesso de dispositivos sem função clara.

16.2. CONCEDER ACESSO AMPLO POR CONVENIÊNCIA

Perfis genéricos facilitam a operação imediata, mas eliminam menor privilégio, segregação e responsabilização.

16.3. TRATAR BIOMETRIA COMO DECISÃO APENAS TÉCNICA

Biometria envolve dados sensíveis, governança, finalidade, retenção, segurança e alternativas operacionais.

16.4. CONFUNDIR GRAVAÇÃO COM COBERTURA ÚTIL

Ter vídeo armazenado não significa que a cena permite detectar, reconhecer ou investigar o evento necessário.

16.5. INTEGRAR SEM DEFINIR AUTORIDADE

Sistemas podem gerar comandos conflitantes ou dependências circulares quando não se define qual plataforma é autoridade para cada função.

16.6. IGNORAR MODOS DEGRADADOS

A arquitetura pode funcionar em demonstração e falhar justamente durante perda de rede, energia, servidor ou storage.

16.7. NÃO TESTAR A RESPOSTA HUMANA

Alarmes tecnicamente corretos são ineficazes quando o operador não possui contexto, procedimento, comunicação ou tempo para responder.

16.8. MANTER BYPASS SEM CONTROLE

Exceções temporárias tornam-se vulnerabilidades permanentes quando não possuem prazo, controle compensatório e confirmação de restabelecimento.

17. ENTREGÁVEIS RECOMENDADOS

Um projeto ou diagnóstico de segurança física para Data Center pode incluir:

18. CONCLUSÃO

A segurança física de um Data Center deve ser projetada como arquitetura integrada de risco, zonas, identidades, barreiras, detecção, evidência e resposta. O perímetro reduz oportunidades; o controle de acesso limita quem pode entrar e onde; o CFTV verifica e registra; a intrusão antecipa eventos; e a operação transforma alarmes em ações consistentes.

O resultado não é medido pela quantidade de equipamentos, mas pela capacidade de prevenir acesso indevido, detectar violações, atrasar a aproximação aos ativos, manter funções em condições degradadas e produzir evidências confiáveis. Projetar, integrar e comissionar essas camadas é essencial para preservar pessoas, ativos e continuidade operacional.

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 22237-6:2024 — Information technology — Data centre facilities and infrastructures — Part 6: Security systems. Geneva: ISO, 2024.

[2] TELECOMMUNICATIONS INDUSTRY ASSOCIATION. ANSI/TIA-942-C — Telecommunications Infrastructure Standard for Data Centers. Arlington: TIA, 2024.

[3] TELECOMMUNICATIONS INDUSTRY ASSOCIATION. TIA-942-C Data Center Infrastructure Standard: keeping pace with the evolving digital world. Arlington: TIA, 2024.

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62676-4:2025 — Video surveillance systems for use in security applications — Part 4: Application guidelines. Geneva: IEC, 2025.

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-53 Rev. 5, Update 1 — Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.

[7] BICSI. ANSI/BICSI 002-2024 — The Standard for Data Center Design. Tampa: BICSI, 2024.

[8] SECURITY INDUSTRY ASSOCIATION. Open Supervised Device Protocol — OSDP. Silver Spring: SIA.

[9] ONVIF. Profile A — Access control configuration. San Ramon: ONVIF.

[10] ONVIF. Profile M — Metadata and events for analytics applications. San Ramon: ONVIF.

[11] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

[12] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Biometria é tema do segundo volume da série Radar Tecnológico. Brasília, DF: ANPD, 2024.

Qual é a diferença entre segurança física e segurança eletrônica em Data Centers?
Segurança física é o conjunto de medidas construtivas, organizacionais, humanas e tecnológicas que protege o ambiente. Segurança eletrônica é uma parte desse conjunto e

inclui controle de acesso, CFTV, intrusão, interfonia e plataformas de monitoramento.**Quantas zonas de segurança um Data Center deve possuir?** Não existe quantidade universal. As zonas devem resultar da análise de risco, criticidade, fluxos e modelo operacional. O importante é existir progressão de proteção e requisitos claros em cada transição.**Mantrap é obrigatória em todo Data Center?** Não. A necessidade depende do risco, do fluxo, da classificação da área e dos requisitos do empreendimento. Quando adotada, deve respeitar evacuação, acessibilidade, emergência e modos degradados.**Biometria é sempre a melhor credencial para áreas críticas?** Não. Biometria pode reforçar autenticação, mas envolve dados sensíveis, erros de reconhecimento, continuidade e privacidade. A escolha deve ser justificada por risco e acompanhada de alternativa operacional.**CFTV substitui o controle de acesso?** Não. O CFTV observa, verifica e produz evidências, enquanto o controle de acesso administra identidades e permissões. Os sistemas são complementares e devem ser integrados sem perder suas funções locais.**O que deve ser testado no comissionamento da segurança física?** Devem ser testados dispositivos, permissões, alarmes, cobertura de vídeo, gravação, integrações, emergência, falhas de energia e comunicação, modos offline, resposta operacional, evidências e recuperação.**Sala-cofre elimina a necessidade de outros controles?** Não. Ela pode elevar a resistência física e ambiental, mas continua dependendo de controle de acesso, CFTV, interfaces, procedimentos, manutenção, emergência e gestão de evidências.**Como evitar canibalização com a página comercial de segurança física para Data Centers?** A página comercial apresenta a solução e os serviços contratáveis. Este artigo atende à intenção informacional, detalhando critérios de risco, projeto, integração, operação e aceite, com links contextuais para a solução.

- **Guias de segurança eletrônica**
- **Arquitetura e infraestrutura do Data Center**
- **Soluções de proteção física**
- **Projeto, modernização e aceite**

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