A3A®
Engenharia
de Sistemas

Projeto de Controle de Acesso

Service Overview

2026

www.a3aengenharia.com.br

Um **Projeto de Controle de Acesso** transforma requisitos de segurança física, operação, circulação de pessoas, proteção de áreas críticas, governança de credenciais e rastreabilidade em uma solução técnica executável, integrada, documentada e preparada para o ciclo de vida da edificação.

Mais do que especificar leitoras, fechaduras, catracas ou cartões, o projeto define quem pode acessar, onde pode acessar, quando pode acessar, por qual credencial, sob quais regras, com quais níveis de proteção, quais eventos devem ser registrados e como o sistema se integra a vídeo, alarmes, visitantes, elevadores, RH, diretórios corporativos, SOC, rede e sistemas de segurança eletrônica.

ESCOPO DO SERVIÇO

A A3A Engenharia de Sistemas desenvolve projetos de controle de acesso físico com foco em segurança, integração, conformidade normativa, cibersegurança, proteção de dados, previsibilidade de implantação e segurança técnica para tomada de decisão. O resultado é uma base objetiva para contratar, executar, fiscalizar, testar, comissionar, operar e manter o sistema com controle e rastreabilidade.

O escopo de um Projeto de Controle de Acesso pode ser ajustado conforme o porte, a criticidade, o nível de integração, o fluxo de pessoas, o perfil de ocupação e a fase do empreendimento, abrangendo desde estudos preliminares até projeto executivo completo, apoio à contratação, fiscalização técnica, testes integrados e comissionamento.

LEVANTAMENTO TÉCNICO E DIAGNÓSTICO

- Reuniões com segurança patrimonial, TI, facilities, engenharia, operação, compliance, RH e gestão
- Levantamento de áreas controladas, áreas críticas, áreas públicas, semipúblicas e restritas
- Análise de fluxos de funcionários, visitantes, terceiros, prestadores, fornecedores e veículos
- Vistoria em campo para avaliação de portas, catracas, cancelas, torniquetes, elevadores, recepções e acessos de emergência
- Mapeamento de sistemas existentes de controle de acesso, CFTV, alarmes, visitantes, interfonia, rede e automação
- Identificação de falhas, obsolescência, credenciais frágeis, ausência de trilha de auditoria e limitações de integração
- Registro de premissas, restrições, riscos, interferências e oportunidades de melhoria

ESTUDOS DE RISCO, ZONAS E REQUISITOS OPERACIONAIS

- Definição de zonas de segurança, áreas críticas, áreas restritas e áreas de livre circulação
- Classificação de áreas por criticidade, risco, ocupação e necessidade de rastreabilidade
- Mapeamento de fluxos de entrada, saída, circulação interna, permanência e acesso emergencial
- Definição de perfis de usuários, grupos, visitantes, terceiros, prestadores, operadores e administradores
- Identificação de eventos críticos, tentativas de acesso indevido, acesso fora de horário e violações operacionais

- Definição de requisitos de operação 8x5, 12x7, 24x7 ou conforme criticidade do ambiente
- Definição de requisitos de auditoria, logs, retenção, relatórios e rastreabilidade
- Definição de requisitos de integração com SOC, CFTV, alarmes, RH, AD/IAM e sistemas corporativos

ARQUITETURA DO SISTEMA DE CONTROLE DE ACESSO

A arquitetura do sistema deve conectar regras de acesso, dispositivos de campo, servidores, credenciais, integrações, rede, energia e operação em uma solução coerente, escalável e administrável.

- Definição de arquitetura centralizada, distribuída, cloud, on-premises ou híbrida
- Especificação de controladoras, módulos de porta, leitoras, sensores, botoeiras, fechaduras, fontes e dispositivos de campo
- Definição de comunicação entre controladoras, servidores, clientes, estações de operação e dispositivos
- Avaliação de comunicação IP, RS-485, OSDP, Wiegand, APIs ou protocolos compatíveis
- Definição de arquitetura online, offline ou híbrida conforme criticidade e disponibilidade
- Planejamento de redundância de servidores, autonomia local das portas e sincronização de eventos e credenciais
- Integração com VMS, alarmes, visitantes, elevadores, interfonia, SOC e sistemas corporativos
- Definição de perfis administrativos, operadores, gestores descentralizados e trilhas de auditoria

PONTOS DE ACESSO, PORTAS E DISPOSITIVOS CONTROLADOS

O projeto deve tratar cada ponto de acesso conforme sua função operacional, criticidade, tipo de porta, sentido de controle, tecnologia de autenticação, dispositivo de travamento, emergência e integração com outros sistemas.

- Portas simples, portas duplas, portas técnicas, portas de emergência e acessos de serviço
- Controle unidirecional ou bidirecional conforme fluxo e necessidade de rastreabilidade
- Catracas, torniquetes, speedgates, cancelas, portões, docas, garagens e acessos veiculares
- Integração com elevadores, pavimentos, áreas restritas, salas técnicas, data centers e ambientes críticos

- Leitoras, sensores de estado de porta, sensores de estado de fechadura, botoeiras e dispositivos de saída
- Eletroímãs, fechaduras elétricas, fechaduras eletromecânicas, strikes, fechaduras motorizadas e dispositivos de bloqueio
- Liberação de emergência, interface com incêndio, evacuação, fail-safe, fail-secure e operação degradada
- Detalhes de instalação, alimentação, infraestrutura, cabeamento, caixas, suportes e proteção mecânica

CREDENCIAIS, AUTENTICAÇÃO E IDENTIDADE

A política de credenciais define como usuários são identificados, autenticados, autorizados, monitorados e removidos do sistema ao longo do ciclo de vida do acesso.

- Cartões de proximidade, smart cards, QR Code, PIN/senha, credenciais móveis, NFC e BLE
- Biometria, reconhecimento facial e autenticação multifator quando aplicável ao risco do ambiente
- Credenciais permanentes, temporárias, emergenciais, de visitantes, terceiros e prestadores
- Política de emissão, ativação, bloqueio, suspensão, expiração, revogação e substituição de credenciais
- Critérios para perda, roubo, duplicidade, compartilhamento indevido e uso fora de política
- Associação entre identidade, credencial, perfil de acesso, área, horário e evento registrado
- Integração com sistemas de RH, diretórios corporativos, IAM, visitantes e fluxos de aprovação

BIOMETRIA, RECONHECIMENTO FACIAL E DADOS SENSÍVEIS

Quando o projeto contempla biometria ou reconhecimento facial, a solução deve considerar necessidade, proporcionalidade, segurança da informação, proteção de dados pessoais sensíveis e governança operacional.

- Análise de necessidade, proporcionalidade e aplicação em áreas críticas ou acessos de maior risco
- Definição de autenticação biométrica local, centralizada ou combinada com outros fatores

- Especificação de reconhecimento facial, impressão digital, palma, íris ou outras modalidades biométricas quando aplicáveis
- Definição de liveness, anti-spoofing, autenticação multifator e critérios de confiança
- Proteção de templates biométricos, criptografia, segregação de permissões e trilhas de auditoria
- Definição de retenção, exclusão, revisão, transparência para titulares e base legal aplicável
- Integração com políticas corporativas de privacidade, LGPD e segurança da informação

REGRAS DE ACESSO, HORÁRIOS E POLÍTICAS OPERACIONAIS

As regras de acesso traduzem a política de segurança da organização em permissões aplicáveis no sistema. Elas devem ser documentadas, auditáveis e compatíveis com a operação real do empreendimento.

- Definição de access levels, grupos de acesso, perfis por cargo, área, função, unidade ou criticidade
- Horários, calendários, feriados, turnos, janelas de manutenção e regras fora de expediente
- Acessos temporários, recorrentes, emergenciais, condicionais ou dependentes de aprovação
- Dupla autorização, autenticação multifator, segregação de áreas e políticas para áreas restritas
- Revisão periódica de permissões, saneamento de usuários inativos e bloqueio automático por expiração
- Matriz de acesso por usuário, perfil, área, ponto de acesso, horário e condição operacional
- Trilhas de auditoria, relatórios de exceção, alertas e indicadores de governança de acesso

VISITANTES, TERCEIROS E PRESTADORES

Visitantes, terceiros e prestadores exigem políticas específicas, porque normalmente possuem acesso temporário, restrito, condicionado e associado a um responsável interno.

- Pré-cadastro, check-in, check-out, associação com anfitrião e validação na recepção
- Emissão de crachá temporário, QR Code temporário, credencial móvel ou badge provisório
- Definição de validade de acesso, restrição por área, horário, unidade, elevador ou fluxo autorizado

- Aceite de termos, políticas, treinamentos, documentos, autorizações ou requisitos de compliance
- Bloqueio automático após expiração, encerramento da visita ou saída do empreendimento
- Relatórios de visitantes presentes, histórico de visitas, permanência e rastreabilidade por anfitrião
- Integração com recepção, segurança patrimonial, sistemas de visitantes, RH e sistemas corporativos

CONTROLE DE ELEVADORES, GARAGENS E VEÍCULOS

- Integração com elevadores para controle por pavimento, grupo de usuários, horário e área autorizada
- Controle de cancelas, portões, garagens, docas, pátios e áreas veiculares
- Leitores de longo alcance, TAG veicular, QR Code, credencial móvel ou LPR/ANPR quando aplicável
- Regras para funcionários, visitantes, terceiros, prestadores, fornecedores e veículos autorizados
- Associação entre veículo, condutor, credencial, autorização, localidade e horário
- Integração com estacionamento, recepção, controle de visitantes, VMS e segurança patrimonial

INTEGRAÇÃO COM CFTV, VMS, ALARMES E SOC

O controle de acesso ganha valor operacional quando seus eventos são correlacionados com vídeo, alarmes, mapas, notificações, workflows de resposta e evidências para investigação.

- Vídeo associado a eventos de acesso, acesso negado, porta forçada, porta mantida aberta e coação
- Pop-up de câmera em evento crítico e gravação por evento no VMS
- Integração com alarmes técnicos, mapas, Smart Map, central de monitoramento e SOC
- Correlação entre anti-passback, tentativas inválidas, intertravamento, acesso fora de horário e eventos de segurança
- Workflow de resposta, abertura de ocorrência, notificações, escalonamentos e registro de ações do operador
- Exportação de evidências, trilha de auditoria e relatórios pós-incidente
- Integração com CFTV, VMS, intrusão, interfonia, automação predial e sistemas corporativos

INTEGRAÇÃO COM RH, IAM, AD E SISTEMAS CORPORATIVOS

Integrações corporativas reduzem retrabalho, aceleram bloqueios, aumentam rastreabilidade e conectam o controle de acesso físico aos processos de negócio e governança de identidade.

- Sincronização de usuários, admissões, desligamentos, alterações de cargo, unidade, área e vínculo
- Integração com Active Directory, IAM, sistemas de RH, ERP, GRC, ITSM e sistemas de visitantes
- Workflows de aprovação, revisão periódica de acessos e gestão descentralizada por responsáveis de área
- Bloqueio ou alteração automática de permissões em eventos de desligamento, transferência ou mudança de função
- Tratamento de usuários inativos, acessos órfãos, credenciais expiradas e exceções operacionais
- Logs de integração, auditoria, monitoramento de falhas e documentação dos fluxos de dados

INTEROPERABILIDADE, PROTOCOLOS E SISTEMAS ABERTOS

A interoperabilidade deve ser considerada desde o projeto, especialmente em ambientes que exigem integração entre controle de acesso, VMS, dispositivos de campo, sistemas legados, APIs e plataformas corporativas.

- Avaliação de ONVIF Profile A, ONVIF Profile C, ONVIF Profile D e Access Control Service quando aplicáveis
- Integração por APIs, SDKs, conectores, eventos, web services, banco de dados ou middleware
- Avaliação de OSDP, Wiegand, RS-485, IP, protocolos proprietários e protocolos abertos
- Modelagem de pontos de acesso, portas, áreas, estados, decisões de acesso, eventos e notificações
- Redução de dependência de fabricante e definição de requisitos mínimos de compatibilidade
- Documentação das integrações, fluxos de dados, responsabilidades, limitações e critérios de teste
- Testes de interoperabilidade entre dispositivos, controladoras, plataformas e sistemas integrados

INFRAESTRUTURA DE REDE, ENERGIA E CAMPO

O controle de acesso depende de infraestrutura física e lógica adequada para garantir comunicação, alimentação, autonomia, segurança, manutenção e continuidade operacional.

- Definição de switches, VLANs, PoE quando aplicável, endereçamento IP, rede dedicada e segmentação
- Fontes de alimentação, nobreaks, baterias, autonomia e supervisão de falhas de energia
- Cabeamento estruturado, infraestrutura seca, eletrocalhas, eletrodutos, caixas, painéis e rotas de campo
- Proteção contra surtos, aterramento, equipotencialização e interfaces com SPDA quando aplicável
- Infraestrutura para leitoras, controladoras, fechaduras, botoeiras, sensores, catracas e cancelas
- Comportamento em falha de energia, falha de rede, perda de servidor, operação offline e recuperação
- Acessibilidade para manutenção, identificação, documentação e expansão futura

CIBERSEGURANÇA DO CONTROLE DE ACESSO

Sistemas modernos de controle de acesso são ativos conectados. Leitoras IP, controladoras, servidores, APIs, integrações, credenciais móveis e cloud ampliam a superfície de ataque e exigem governança conjunta entre segurança física, TI e cibersegurança.

- Inventário de ativos, software, firmware, versões, integrações e contas administrativas
- Hardening de controladoras, leitoras IP, servidores, estações, APIs e dispositivos de campo
- Senhas fortes, certificados, criptografia, autenticação de dispositivos e comunicação segura
- Segmentação de rede, controle de acesso administrativo, logs, monitoramento e alertas
- Gestão de vulnerabilidades, atualização de firmware, patches, fornecedores e suporte de longo prazo
- Acesso remoto seguro, gestão de contas privilegiadas, trilhas de auditoria e resposta a incidentes
- Integração com políticas corporativas de TI, segurança da informação, privacidade e continuidade operacional

ENSAIOS, TESTES, COMISSIONAMENTO E CRITÉRIOS DE ACEITAÇÃO

O projeto deve estabelecer como o sistema será testado, validado e aceito. Isso evita que a entrega dependa apenas de funcionamento aparente, sem comprovação de regras, integrações, eventos, segurança e operação.

- Testes funcionais por porta, catraca, cancela, elevador, leitora, controladora e dispositivo de saída
- Testes de leitura de credenciais, biometria, QR Code, credencial móvel e autenticação multifator
- Testes de regras de acesso, grupos, horários, feriados, visitantes, terceiros e acessos temporários
- Testes de eventos de porta forçada, porta mantida aberta, acesso negado, coação, anti-passback e intertravamento
- Testes de integração com VMS, alarmes, mapas, SOC, RH, AD/IAM e sistemas corporativos
- Testes de liberação de emergência, falha de comunicação, autonomia, operação offline e recuperação
- Testes de logs, relatórios, permissões administrativas, auditoria, alertas e trilhas de eventos
- Critérios de aprovação, reprovação, pendências, correções, documentação de aceite e operação assistida

ETAPAS

1. DIAGNÓSTICO E LEVANTAMENTO DE REQUISITOS

A etapa inicial consolida características do empreendimento, fluxos de pessoas e veículos, áreas críticas, sistemas existentes, infraestrutura disponível, requisitos de segurança, operação, TI, privacidade, visitantes e integração.

2. ESTUDO PRELIMINAR E DIRETRIZES TÉCNICAS

Com base no diagnóstico, são avaliadas alternativas de arquitetura, tecnologias de credencial, leitores, controladoras, portas, fechaduras, catracas, integração com vídeo, rede, energia, operação e cibersegurança. Essa fase define a direção técnica antes do detalhamento.

3. PROJETO BÁSICO

O projeto básico define a solução, a arquitetura principal, os pontos de acesso, as áreas controladas, os níveis de proteção, as tecnologias de autenticação, as integrações, a infraestrutura, os quantitativos preliminares e os subsídios para aprovação e contratação.

4. PROJETO EXECUTIVO

O projeto executivo detalha a implantação com plantas, diagramas, memoriais, detalhes de instalação, lista de materiais, especificações, matriz de acesso, matriz de eventos, infraestrutura, automação, integração, plano de testes e critérios de aceite.

5. APOIO À CONTRATAÇÃO

Quando contratado, o projeto pode apoiar o processo de aquisição com escopo técnico, termo de referência, equalização de propostas, matriz de responsabilidades, critérios de medição, requisitos mínimos, documentação exigida e respostas técnicas a fornecedores.

6. SUPORTE À IMPLANTAÇÃO E COMISSIONAMENTO

Durante a implantação, a A3A Engenharia de Sistemas pode apoiar esclarecimentos técnicos, validação de materiais, análise de desvios, compatibilização em campo, acompanhamento de testes, análise de relatórios, tratamento de pendências, comissionamento e documentação final.

ENTREGÁVEIS

Os entregáveis são definidos conforme o escopo contratado, a fase do empreendimento e o nível de detalhamento necessário para contratação, execução, fiscalização, testes, comissionamento, operação e manutenção. Em projetos executivos completos, podem incluir:

- Relatório de levantamento técnico e diagnóstico dos sistemas existentes
- Análise de requisitos, premissas, restrições e critérios de projeto
- Matriz de áreas controladas, matriz de riscos e matriz de criticidade
- Matriz de acesso por perfil, área, horário, condição e ponto controlado
- Memorial descritivo e memorial técnico
- Plantas de pontos de controle de acesso
- Plantas de portas, catracas, cancelas, torniquetes, elevadores e áreas controladas
- Plantas de infraestrutura associada, rede, alimentação, painéis, caixas e rotas técnicas
- Diagramas de arquitetura lógica, arquitetura física, rede e comunicação
- Diagramas de integração com VMS, alarmes, visitantes, RH, AD/IAM, SOC e sistemas corporativos
- Detalhes típicos de instalação de leitoras, fechaduras, sensores, botoeiras, fontes, controladoras e dispositivos de saída
- Lista de equipamentos, lista de materiais, quantitativos e especificações técnicas
- Matriz de eventos, alarmes, severidades, ações, notificações e escalonamentos
- Matriz de permissões administrativas, operadores, gestores e responsabilidades
- Requisitos de cibersegurança, hardening, comunicação segura, logs e gestão de contas
- Requisitos de LGPD, biometria, governança de dados, retenção e trilhas de auditoria
- Plano de testes, comissionamento e critérios de aceitação
- Orçamento estimativo e cronograma físico de referência
- Matriz normativa, matriz de responsabilidades e documentação para contratação
- ART/RRT quando aplicável ao escopo contratado
- Documentação as built, quando incluída no escopo de apoio à implantação

APLICAÇÕES E AMBIENTES

O Projeto de Controle de Acesso é aplicável a empreendimentos novos, expansões, retrofits, modernizações tecnológicas, regularizações e ambientes que precisam controlar circulação, proteger áreas críticas, registrar eventos e integrar segurança física à operação.

- Edifícios corporativos e condomínios empresariais
- Indústrias, plantas produtivas, ambientes IT/OT e áreas operacionais
- Data centers, salas técnicas, salas de TI, NOCs, SOCs e ambientes de missão crítica
- Hospitais, clínicas, laboratórios, universidades, escolas e centros de pesquisa
- Centros logísticos, docas, galpões, pátios, garagens e estacionamentos
- Shopping centers, hotéis, centros comerciais e empreendimentos multiusuário
- Órgãos públicos, instituições financeiras, aeroportos, portos, terminais e infraestruturas críticas
- Áreas limpas, salas elétricas, salas de controle, recepções e áreas de visitantes
- Empreendimentos com múltiplas unidades, múltiplas áreas de segurança ou operação 24x7

CONSIDERAÇÕES DE ENGENHARIA

Executar controle de acesso sem projeto é transferir decisões de engenharia, segurança, integração e operação para o campo. Essa prática aumenta o risco de regras inconsistentes, credenciais frágeis, portas mal especificadas, integrações incompletas, ausência de auditoria, vulnerabilidades cibernéticas e dificuldade de manutenção.

O projeto reduz incertezas antes do investimento, organiza a contratação, permite comparar propostas, define critérios de qualidade, evita compras indevidas, reduz aditivos, melhora a fiscalização e estabelece uma base objetiva para o aceite técnico do sistema.

Para o cliente, isso se traduz em maior previsibilidade de prazo, custo, segurança, operação e manutenção. Para a execução, significa menos improviso e mais clareza sobre o que deve ser instalado, integrado, testado e documentado.

QUEM, ONDE E QUANDO

A lógica central do controle de acesso é definir quem pode acessar, onde pode acessar e quando pode acessar. O projeto deve transformar essa regra operacional em arquitetura, dispositivos, credenciais, permissões, eventos e relatórios.

SEGURANÇA FÍSICA E CIBERSEGURANÇA CONVERGENTES

Sistemas modernos de controle de acesso são ativos conectados. Leitoras IP, controladoras, servidores, APIs, integrações e credenciais móveis ampliam a superfície de ataque e exigem governança conjunta entre segurança física, TI e cibersegurança.

CREDENCIAIS E AUTENTICAÇÃO

A escolha entre cartão, senha, QR Code, credencial móvel, biometria ou autenticação multifator deve considerar risco, experiência do usuário, custo, fraude, manutenção, disponibilidade, privacidade e ciclo de vida da credencial.

BIOMETRIA E PROTEÇÃO DE DADOS

Biometria e reconhecimento facial devem ser tratados como recursos de alta criticidade, não apenas como funcionalidades comerciais. O projeto deve considerar LGPD, necessidade, proporcionalidade, segurança dos templates, retenção, transparência e controle de acesso aos dados.

INTEGRAÇÃO COM OPERAÇÃO E EVIDÊNCIAS

Controle de acesso ganha valor quando integrado a vídeo, alarmes, visitantes, SOC, relatórios e workflows de resposta. Eventos de acesso negado, porta forçada, coação ou porta mantida aberta devem gerar ações operacionais claras.

DISPONIBILIDADE E OPERAÇÃO DEGRADADA

O sistema deve prever comportamento em falha de energia, falha de rede, indisponibilidade do servidor, emergência, incêndio, evacuação e perda de comunicação. Portas críticas precisam de lógica definida de fail-safe, fail-secure, autonomia e recuperação.

CONTRATABILIDADE E FISCALIZAÇÃO

O projeto deve permitir que a execução seja contratada com escopo claro, quantitativos rastreáveis, materiais especificados, critérios de medição, testes obrigatórios e aceite técnico objetivo. Isso torna propostas comparáveis e reduz ambiguidades contratuais.

METODOLOGIA

A metodologia da A3A Engenharia de Sistemas combina análise de risco, levantamento técnico, engenharia normativa, compatibilização multidisciplinar, especificação técnica, documentação executiva, integração operacional, cibersegurança e visão de ciclo de vida do sistema de controle de acesso.

ENTENDIMENTO DA OPERAÇÃO

- Compreensão do uso do empreendimento, fluxos de pessoas, fluxos de veículos e áreas críticas
- Identificação de visitantes, terceiros, horários, níveis de segurança, requisitos de auditoria e integração
- Levantamento das necessidades de segurança patrimonial, TI, facilities, compliance, RH e gestão

LEVANTAMENTO TÉCNICO

- Vistorias, análise documental e levantamento de portas, acessos, catracas, cancelas, infraestrutura e rede
- Mapeamento de sistemas legados, integrações existentes, credenciais, regras, usuários e limitações operacionais
- Registro de falhas, riscos, interferências, restrições e oportunidades de melhoria

ENGENHARIA NORMATIVA

- Aplicação da ABNT NBR IEC 60839-11-1 e ABNT NBR IEC 60839-11-2
- Definição de critérios de desempenho, classes ambientais, fonte de alimentação, comunicação, autoproteção e registros
- Aplicação de requisitos de reconhecimento, coação, interfaces de pontos de acesso, visualização, alerta, ensaios e documentação
- Adaptação dos requisitos normativos ao ambiente real do empreendimento e aos requisitos internos do cliente

COMPATIBILIZAÇÃO

- Coordenação com arquitetura, portas, esquadrias, elétrica, rede, cabeamento estruturado e infraestrutura seca
- Compatibilização com incêndio, segurança eletrônica, CFTV, automação, elevadores, TI, facilities e operação

- Tratamento de interferências, definição de soluções executáveis e documentação de interfaces entre disciplinas

PROJETO E ESPECIFICAÇÃO

- Elaboração de plantas, memoriais, diagramas, matriz de acesso, matriz de eventos, listas e quantitativos
- Definição de equipamentos, credenciais, regras, integrações, infraestrutura, requisitos de cibersegurança e critérios de desempenho
- Definição de plano de testes, comissionamento, critérios de aceite e documentação de entrega
- Preparação de base técnica para contratação, execução, fiscalização, operação e manutenção

APOIO À IMPLANTAÇÃO E ENTREGA TÉCNICA

- Suporte a dúvidas técnicas, equalização, fiscalização e análise de desvios
- Validação de materiais, equipamentos, relatórios de teste, integrações e comissionamento
- Tratamento de não conformidades, pendências, ajustes operacionais e documentação final
- Consolidação de recomendações de operação, manutenção, revisão de acessos e melhoria contínua

NORMAS E REFERÊNCIAS TÉCNICAS

O projeto pode ser desenvolvido com base em normas nacionais, referências internacionais, especificações de interoperabilidade e boas práticas aplicáveis ao ambiente, à finalidade do sistema, ao nível de risco e aos requisitos do cliente. Entre as principais referências técnicas estão:

- ABNT NBR IEC 60839-11-1 - Sistemas de segurança eletrônica e alarme - Sistemas eletrônicos de controle de acesso - Requisitos do sistema e dos componentes
- ABNT NBR IEC 60839-11-2 - Sistemas de segurança eletrônica e alarme - Sistemas eletrônicos de controle de acesso - Diretrizes de aplicação
- LGPD - Lei Geral de Proteção de Dados
- Guia do Framework de Privacidade e Segurança da Informação - PPSI
- CIS Controls v8.1
- ONVIF Access Control Service Specification
- ONVIF Profile A
- ONVIF Profile C
- ONVIF Profile D
- Boas práticas de cibersegurança para sistemas de controle de acesso físico
- Boas práticas de segurança física e cibersegurança convergentes
- Normas de instalações elétricas, cabeamento estruturado, incêndio, acessibilidade, segurança do trabalho e requisitos internos do cliente, conforme o ambiente

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