A3A®
Engenharia
de Sistemas

Projeto de Sistema Integrado de Segurança Eletrônica

Service Overview

2026

www.a3aengenharia.com.br

Um **Projeto de Sistema Integrado de Segurança Eletrônica** transforma requisitos de proteção patrimonial, controle operacional e gestão de riscos em uma arquitetura técnica executável, integrada, documentada e preparada para o ciclo de vida da operação. Ele conecta videomonitoramento, controle de acesso, alarmes, sensores, analíticos, rede, servidores, armazenamento, energia, automação e operação de segurança em uma solução coordenada.

Mais do que distribuir câmeras, leitoras, catracas, cancelas ou sensores, o projeto define zonas de segurança, objetivos operacionais, critérios de cobertura, fluxos de acesso, eventos, alarmes, integrações, infraestrutura de rede, retenção de imagens, governança de evidências, permissões, testes, documentação e requisitos para contratação da execução.

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

ESCOPO DO SERVIÇO

O escopo do Projeto de Sistema Integrado de Segurança Eletrônica pode ser ajustado conforme o porte, a criticidade, o nível de integração e a fase do empreendimento, abrangendo desde estudos preliminares até projeto executivo completo, apoio à contratação, fiscalização técnica e validação dos testes integrados.

LEVANTAMENTO TÉCNICO E DIAGNÓSTICO

- Reuniões com stakeholders de segurança patrimonial, TI, facilities, engenharia, operação, compliance e gestão
- Levantamento de necessidades atuais e futuras de segurança eletrônica
- Análise de ameaças, vulnerabilidades, áreas sensíveis, fluxos de circulação e pontos críticos
- Vistoria em campo para avaliação de acessos, perímetros, recepções, salas técnicas, áreas restritas e ambientes operacionais
- Mapeamento de sistemas existentes: CFTV, VMS, controle de acesso, alarmes, interfonia, rede, servidores, automação e SOC
- Identificação de pontos cegos, falhas de cobertura, obsolescência, limitações de integração e riscos de manutenção
- Registro de premissas, restrições, oportunidades de melhoria e critérios técnicos do empreendimento

ESTUDOS DE RISCO, ZONAS E REQUISITOS OPERACIONAIS

- Definição de zonas de segurança, áreas críticas, áreas restritas e áreas públicas ou semipúblicas
- Mapeamento de fluxos de pessoas, veículos, visitantes, terceiros, prestadores e equipes operacionais
- Identificação de eventos críticos, cenários de intrusão, acesso indevido, permanência irregular e falhas operacionais
- Definição de requisitos para detecção, verificação, resposta, registro e preservação de evidências
- Caracterização de operação 8x5, 12x7, 24x7 ou conforme a criticidade do ambiente
- Definição de requisitos de retenção de imagens, logs, eventos, clipes e trilhas de auditoria
- Definição de critérios de privacidade, LGPD, controle de permissões e acesso a dados sensíveis
- Estabelecimento do nível de automação, integração, supervisão e resposta esperado para a operação

ARQUITETURA INTEGRADA DO SISTEMA

O projeto define a arquitetura geral do sistema, tratando os subsistemas de segurança eletrônica como partes de uma operação integrada, e não como equipamentos isolados.

- Integração entre CFTV IP, VMS, controle de acesso, alarmes, sensores, interfonia e automação
- Integração com SOC, BMS, diretórios corporativos, RH, sistemas de visitantes, ERP, ITSM ou plataformas de operação
- Definição de servidores, estações, storage, rede, VLANs, switches, links, energia protegida e infraestrutura associada
- Definição de integrações por API, eventos, metadados, drivers, SDKs, conectores ou protocolos compatíveis
- Desenho de fluxos de operação, resposta, escalonamento, notificação e registro de ocorrências
- Elaboração de arquitetura lógica, física e operacional do sistema integrado
- Compatibilização entre segurança eletrônica, TI, infraestrutura, automação, facilities e operação

PROJETO DE VIDEOMONITORAMENTO IP E VMS

O videomonitoramento deve ser projetado a partir do objetivo operacional de cada cena. Detectar, observar, reconhecer ou identificar pessoas, veículos e eventos exige diferentes níveis de detalhe, posicionamento, iluminação, lente, resolução, compressão e armazenamento.

- Definição dos objetivos de cada câmera: detecção, observação, reconhecimento ou identificação
- Cálculo de densidade de pixels e avaliação de campo de visão, distância, altura e ângulo de instalação
- Especificação de resolução, lente, FPS, compressão, WDR, sensibilidade, infravermelho e iluminação complementar
- Seleção de câmeras fixas, dome, bullet, panorâmicas, PTZ, térmicas, multisensores ou aplicações especiais
- Cobertura de perímetros, acessos, recepções, estacionamentos, áreas críticas, circulação, docas e salas técnicas
- Integração com VMS, mapas, layouts, perfis de usuário, permissões, alarmes e operação de monitoramento

- Definição de gravação contínua, por evento, por agenda, por analítico ou em modelo híbrido
- Definição de retenção, arquivamento, exportação, busca, evidências e documentação de câmeras

PROJETO DE CONTROLE DE ACESSO

O controle de acesso estabelece as regras de entrada, circulação e permanência em áreas controladas, conectando identidade, credencial, localidade, horário, autorização, evento e evidência.

- Definição de portas, catracas, cancelas, torniquetes, elevadores, fechaduras, botoeiras e áreas controladas
- Especificação de leitoras, controladoras, módulos, fontes, sensores, atuadores e dispositivos de liberação
- Autenticação por cartão, QR Code, senha, biometria, credencial móvel, NFC, BLE ou autenticação multifator
- Regras de acesso por usuário, grupo, área, horário, calendário, criticidade e perfil operacional
- Políticas para funcionários, visitantes, terceiros, prestadores, recepção e áreas restritas
- Funções como anti-passback, intertravamento, lockdown, liberação de emergência e mustering quando aplicável
- Integração com VMS para vídeo associado a eventos de acesso
- Integração com RH, diretórios corporativos, sistemas de visitantes, SOC e plataformas de auditoria
- Trilhas de auditoria, relatórios e revisão periódica de acessos concedidos

PROJETO DE ALARMES, INTRUSÃO E SENSORES

Sistemas de alarme e intrusão devem ser projetados com critérios de zona, grau de segurança, classe ambiental, autonomia, comunicação, operação e prevenção de alarmes falsos.

- Definição de zonas de alarme, áreas armadas, perímetros, áreas internas e pontos vulneráveis
- Especificação de sensores de abertura, presença, quebra de vidro, barreiras, botões de pânico e sensores perimetrais
- Definição de lógica de arme/desarme, tempos de entrada e saída, bypass, supervisão e permissões de operação
- Classificação de graus de segurança e classes ambientais conforme risco e aplicação

- Definição de fontes de alimentação, baterias, autonomia, supervisão e comunicação de falhas
- Integração com VMS, câmeras associadas, mapas, controle de acesso e operação de monitoramento
- Critérios para redução de alarmes falsos, validação operacional, testes e aceitação
- Documentação de zonas, sensores, eventos, respostas, manutenção e responsabilidades operacionais

ANALÍTICOS DE VÍDEO E INTELIGÊNCIA ARTIFICIAL

Analíticos de vídeo e recursos de inteligência artificial podem acelerar investigações, automatizar tarefas repetitivas e gerar alertas em tempo real. O projeto deve definir onde esses recursos agregam valor, quais condições de cena são necessárias e como os eventos serão tratados pela operação.

- Detecção de pessoas, veículos, cruzamento de linha, intrusão, permanência indevida e objeto abandonado
- Contagem de pessoas e veículos, aglomeração, direção de deslocamento e comportamento anômalo
- LPR/ANPR, busca por atributos, classificação de objetos e metadados de cena
- Definição de análise em borda, servidor, cloud ou arquitetura híbrida
- Validação de iluminação, enquadramento, obstruções, distância de detecção e qualidade de imagem
- Configuração de zonas, regras, calendários, sensibilidade, tolerâncias e gatilhos de eventos
- Integração com VMS, alarmes, dashboards, SOC, relatórios e fluxos de resposta
- Critérios de redução de falso positivo, manutenção das cenas e revalidação periódica

RECONHECIMENTO FACIAL, BIOMETRIA E CREDENCIAIS SENSÍVEIS

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

- Análise de aplicabilidade em áreas restritas, acessos críticos, recepções, visitantes ou ambientes de alta segurança
- Especificação de terminais faciais, leitores biométricos, painéis de reconhecimento e dispositivos associados
- Definição de liveness, anti-spoofing, autenticação multifator e critérios de confiança
- Integração com controle de acesso, VMS, sistemas corporativos, eventos e relatórios

- Criptografia, segregação de permissões, trilhas de auditoria e proteção dos dados biométricos
- Definição de base legal, consentimento quando aplicável, retenção, exclusão e gestão de templates
- Critérios de uso, operação, auditoria, revisão de acessos e governança LGPD

INFRAESTRUTURA DE REDE, PROCESSAMENTO E ARMAZENAMENTO

Vídeo IP, controle de acesso, alarmes e analíticos dependem de rede, processamento, armazenamento e energia adequados. O projeto deve dimensionar a infraestrutura para transmissão, gravação, busca, exportação e operação contínua.

- Dimensionamento de banda de vídeo, tráfego de eventos, metadados, áudio, controle e integrações
- Definição de VLANs, segmentação, QoS, multicast, unicast, roteamento, uplinks e redundância de rede
- Dimensionamento de PoE, PoE budget, switches, fibras ópticas, links, racks e infraestrutura associada
- Especificação de servidores de gravação, servidores de aplicação, estações de operação e storage
- Definição de RAID, gravação centralizada, gravação local, edge recording, arquivamento e retenção diferenciada
- Avaliação de codecs, H.264, H.265, FPS, GOP, resolução, bitrate e impacto no armazenamento
- Definição de pre-buffer, gravação por evento, criptografia, assinatura, proteção de evidências e backup
- Monitoramento de saúde do sistema, capacidade, disponibilidade, falhas e integridade de gravação

ENERGIA, DISPONIBILIDADE E PROTEÇÃO

Sistemas de segurança eletrônica precisam permanecer disponíveis em cenários de falha parcial, indisponibilidade de energia, falha de rede ou manutenção programada. A disponibilidade deve ser compatível com a criticidade da operação protegida.

- Dimensionamento de alimentação, fontes, nobreaks, baterias e autonomia
- Proteção contra surtos, aterramento, equipotencialização e organização elétrica dos dispositivos
- Redundância de rede, links, servidores, storage e componentes críticos quando aplicável

- Definição de failover, edge recording, contingência e operação degradada
- Monitoramento de falhas de alimentação, comunicação, gravação, dispositivo e servidor
- Critérios de manutenção, acessibilidade, reposição e continuidade operacional
- Documentação de pontos de energia, circuitos, autonomia, responsabilidade e testes de aceitação

CIBERSEGURANÇA, PRIVACIDADE E GOVERNANÇA

Sistemas de segurança eletrônica modernos operam em rede, armazenam dados sensíveis e integram plataformas corporativas. Por isso, o projeto deve contemplar cibersegurança, governança de usuários, proteção de evidências e privacidade desde a concepção.

- Hardening de câmeras, servidores, VMS, controladoras, switches, estações e dispositivos de campo
- Troca de senhas padrão, perfis de acesso, autenticação forte, certificados e criptografia quando aplicável
- Segmentação de rede, controle de acesso administrativo, atualização de firmware e gestão de vulnerabilidades
- Logs, trilhas de auditoria, retenção, exportação controlada de imagens e gestão de evidências
- Políticas de usuários, grupos, permissões, operadores, administradores e terceiros
- Critérios de LGPD para imagens, biometria, visitantes, logs de acesso e dados sensíveis
- Procedimentos para compartilhamento de evidências, cadeia de custódia e relatórios pós-incidente

INTEGRAÇÃO OPERACIONAL, EVENTOS E RESPOSTA

Um sistema integrado deve transformar eventos de segurança em ações operacionais claras. O projeto define quais eventos são relevantes, como são correlacionados, quem recebe o alerta e quais respostas devem ser executadas.

- Definição de eventos críticos, alarmes, severidades, prioridades e critérios de escalonamento
- Correlação entre eventos de acesso físico, vídeo, sensores, alarmes, interfonia e sistemas corporativos
- Pop-up de câmera em evento de acesso, alarme de intrusão associado a mapa e câmera, e abertura de ocorrência
- Notificações para operadores, supervisores, segurança patrimonial, facilities, TI ou SOC

- Registro de ocorrência, evidências, linha do tempo, ações executadas e responsáveis
- Matriz de escalonamento, fluxos de resposta, playbooks operacionais e relatórios pós-evento
- Integração com central de monitoramento, SOC, BMS, ITSM ou plataformas de gestão operacional

ENSAIOS, TESTES, COMISSIONAMENTO E 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 desempenho, integração e operação.

- Testes funcionais por subsistema: câmeras, VMS, controle de acesso, alarmes, sensores, interfonia e analíticos
- Testes integrados de eventos, alarmes, mapas, vídeo associado, notificações, permissões e fluxos de resposta
- Validação de campo de visão, densidade de pixels, iluminação, gravação, busca, exportação e retenção
- Testes de portas, leitoras, catracas, cancelas, biometria, visitantes, lockdown e liberações de emergência
- Testes de autonomia, falhas de comunicação, failover, edge recording e recuperação de operação
- Simulações operacionais, cenários de incidente, avaliação de tempos de resposta e critérios de aceite
- Registro de pendências, correções, relatórios de teste, documentação final e aceite técnico

ETAPAS

1. DIAGNÓSTICO E LEVANTAMENTO DE REQUISITOS

A etapa inicial consolida objetivos, restrições, criticidade, sistemas existentes, vulnerabilidades, fluxos de circulação, áreas sensíveis, infraestrutura disponível e expectativas de integração.

2. ESTUDO PRELIMINAR E DIRETRIZES TÉCNICAS

Com base no diagnóstico, são avaliadas alternativas de arquitetura, tecnologias, cobertura, controle, armazenamento, rede, energia, integração, operação e riscos. Essa fase define a direção técnica antes do detalhamento.

3. PROJETO BÁSICO

O projeto básico define a solução, os subsistemas, a arquitetura principal, os pontos de controle, as áreas monitoradas, os critérios de desempenho, os quantitativos preliminares e os requisitos para aprovação e contratação.

4. PROJETO EXECUTIVO

O projeto executivo detalha a implantação com plantas, diagramas, memoriais, detalhes de instalação, listas de materiais, especificações, matriz de eventos, arquitetura de rede, mapa de câmeras, mapa de acessos, 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, testes exigidos 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 e documentação final.

ENTREGÁVEIS

Os entregáveis são definidos conforme o escopo contratado e o nível de maturidade exigido pelo empreendimento. 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 riscos, áreas críticas, zonas de segurança e fluxos operacionais
- Memorial descritivo e memorial técnico
- Plantas de localização de câmeras, campo de visão e áreas monitoradas
- Plantas de controle de acesso, portas, catracas, cancelas, leitoras e áreas controladas
- Plantas de alarmes, sensores, zonas, sirenes, botoeiras e dispositivos de intrusão
- Plantas de infraestrutura associada, rede, racks, servidores, pontos de energia e rotas técnicas
- Diagramas de arquitetura lógica, arquitetura física, rede, servidores e armazenamento
- Diagramas de integração entre VMS, controle de acesso, alarmes, sensores, automação, SOC e sistemas corporativos
- Matriz de eventos, alarmes, severidades, ações, notificações e escalonamentos
- Matriz de permissões, perfis de usuários, operadores, administradores e responsabilidades
- Mapa de cobertura de videomonitoramento e critérios DORI por câmera
- Lista de materiais, quantitativos e especificações técnicas de equipamentos e serviços
- Dimensionamento de rede, banda, PoE, storage, servidores, retenção e energia
- Orçamento estimativo e cronograma físico de referência
- Plano de testes, comissionamento e critérios de aceitação
- Matriz normativa, matriz de responsabilidades e requisitos de contratação
- Requisitos de LGPD, governança de evidências, retenção e trilhas de auditoria
- ART/RRT quando aplicável ao escopo contratado
- Documentação as built, quando incluída no escopo de apoio à implantação

APLICAÇÕES E AMBIENTES

O Projeto de Sistema Integrado de Segurança Eletrônica é aplicável a empreendimentos novos, expansões, retrofits, modernizações tecnológicas, regularizações e ambientes que precisam integrar proteção patrimonial, operação, evidências e resposta a incidentes.

- Edifícios corporativos e condomínios empresariais
- Indústrias, plantas produtivas e ambientes IT/OT
- Centros logísticos, galpões, docas e pátios operacionais
- Data centers, salas críticas e infraestruturas de missão crítica
- Hospitais, laboratórios e ambientes de saúde
- Universidades, escolas, centros de pesquisa e campus
- Instituições financeiras, bancos e ambientes regulados
- Órgãos públicos, centros administrativos e equipamentos urbanos
- Shopping centers, hotéis, centros comerciais e empreendimentos multiusuário
- Portos, aeroportos, terminais, utilities e infraestruturas críticas
- Centros de controle, centrais de monitoramento, SOCs e salas de operação
- Empreendimentos com múltiplas unidades, perímetros extensos ou operação 24x7

CONSIDERAÇÕES DE ENGENHARIA

Executar segurança eletrônica sem projeto é transferir decisões de engenharia, integração e operação para o campo. Essa prática aumenta o risco de pontos cegos, equipamentos mal especificados, rede insuficiente, armazenamento subdimensionado, alarmes excessivos, integrações frágeis, baixa rastreabilidade 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, desempenho e operação. Para a execução, significa menos improviso e mais clareza sobre o que deve ser instalado, integrado, testado e documentado.

COBERTURA, IMAGEM E OBJETIVO OPERACIONAL

Cada câmera deve ter objetivo definido: detectar, observar, reconhecer ou identificar. A escolha de lente, resolução, altura, distância, iluminação e campo de visão deve partir desse objetivo, e não apenas da quantidade de megapixels.

INTEGRAÇÃO ENTRE SUBSISTEMAS

Um sistema integrado precisa que CFTV, controle de acesso, alarmes, sensores, VMS e plataformas corporativas troquem eventos de forma consistente. A integração deve ser definida em projeto, com fluxos, gatilhos, permissões e responsabilidades.

REDE, LATÊNCIA E ARMAZENAMENTO

Vídeo IP exige dimensionamento de rede, links, switches, PoE, VLANs, servidores, storage, retenção, arquivamento e disponibilidade. O projeto deve prever transmissão, gravação, recuperação e exportação de evidências.

CONFIABILIDADE E MANTENABILIDADE

Equipamentos, arquitetura, redundância, fontes de alimentação, bateria, acesso para manutenção e documentação devem ser definidos para reduzir falhas, facilitar reparos e manter a operação ao longo do ciclo de vida.

PRIVACIDADE E PROTEÇÃO DE DADOS

Sistemas com imagem, biometria, reconhecimento facial, visitantes e logs de acesso devem prever governança de dados, retenção, permissões, trilhas de auditoria, exportação controlada e aderência à LGPD.

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 e visão de ciclo de vida do sistema.

ENTENDIMENTO DA OPERAÇÃO

- Compreensão da rotina do empreendimento, fluxos de pessoas, veículos, visitantes e terceiros
- Identificação de áreas críticas, responsabilidades operacionais, eventos relevantes e expectativas de resposta
- Levantamento das necessidades de segurança patrimonial, TI, facilities, automação, compliance e gestão

LEVANTAMENTO TÉCNICO

- Vistorias, análise documental, levantamento de infraestrutura existente e diagnóstico de sistemas instalados
- Mapeamento de acessos, perímetros, salas técnicas, pontos de energia, rede, rotas e áreas monitoradas
- Registro de condições existentes, pontos cegos, falhas de cobertura, limitações e oportunidades de melhoria

ENGENHARIA NORMATIVA

- Aplicação de normas ABNT IEC, boas práticas de segurança eletrônica e requisitos internos do cliente
- Definição de critérios técnicos para videomonitoramento, controle de acesso, alarmes, fontes, ensaios e documentação
- Adaptação dos requisitos normativos ao ambiente real do empreendimento e ao nível de risco identificado

COMPATIBILIZAÇÃO

- Coordenação com arquitetura, elétrica, rede, cabeamento estruturado, infraestrutura seca, climatização e incêndio
- Compatibilização com automação, facilities, segurança patrimonial, TI, SOC e operação
- Tratamento de interferências, definição de rotas executáveis e integração entre subsistemas

PROJETO E ESPECIFICAÇÃO

- Elaboração de plantas, memoriais, diagramas, listas, quantitativos e especificações técnicas
- Definição de matriz de eventos, plano de testes, 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
- Avaliação de testes funcionais, testes integrados, relatórios e tratamento de não conformidades
- Consolidação de documentação final, recomendações de operação, manutenção e melhoria contínua

NORMAS E REFERÊNCIAS TÉCNICAS

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

- ABNT NBR IEC 62676-1-1 - Sistemas de videomonitoramento para uso em aplicações de segurança - Requisitos de sistema - Generalidades
- ABNT NBR IEC 62676-1-2 - Sistemas de videomonitoramento para uso em aplicações de segurança - Requisitos de desempenho para transmissão de vídeo
- ABNT NBR IEC 62642-1 - Sistemas de alarme contra intrusão e roubo - Requisitos do sistema
- ABNT NBR IEC 62642-6 - Sistemas de alarme contra intrusão e roubo - Fontes de alimentação
- ABNT IEC/TS 62642-7 - Sistemas contra intrusão e roubo - Diretrizes de aplicação
- ABNT NBR IEC 60839-11-1 - Sistemas eletrônicos de controle de acesso - Requisitos do sistema e dos componentes
- ABNT NBR IEC 60839-11-2 - Sistemas eletrônicos de controle de acesso - Diretrizes de aplicação
- ABNT NBR 5462 - Confiabilidade e mantenabilidade
- ABNT NBR IEC 60065 - Aparelhos de áudio, vídeo e aparelhos eletrônicos similares - Requisitos de segurança
- LGPD - Lei Geral de Proteção de Dados
- Boas práticas de VMS, rede IP, armazenamento, cibersegurança, analíticos de vídeo, biometria e governança de evidências

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.

© 2026 - A3A Engenharia de Sistemas.

Este documento é de propriedade da A3A Engenharia de Sistemas e seu conteúdo tem caráter exclusivamente informativo. Reservamo-nos o direito de inserir modificações sem aviso prévio.

A3A® Engenharia de Sistemas