

TIPOS DE CONTROLE DE ACESSO

O que é Controle de Acesso Biométrico? O controle de acesso é um conjunto de tecnologias e processos que têm como finalidade permitir ou restringir a entrada e saída de pessoas ou veículos em uma determinada área. A tecnologia de controle de acesso biométrico touchless, ou sem contato, representa uma evolução significativa em sistemas de autenticação e segurança. Esse tipo de tecnologia utiliza a captura de dados biométricos, como reconhecimento facial ou leitura de impressões digitais, sem a necessidade de tocar fisicamente em um dispositivo. O controle de acesso é um dos principais pilares da segurança física, sendo essencial em ambientes [...]

SUMÁRIO

0.1. O QUE É CONTROLE DE ACESSO BIOMÉTRICO?	3
1. TIPOS DE SISTEMAS DE CONTROLE DE ACESSO	3
1.0.1. 1 Controle de Acesso Físico	3
1.0.2. 2 Controle de Acesso Eletrônico	4
1.0.3. 3 Controle de Acesso Biométrico	4
1.0.4. 4 Controle de Acesso por Senhas e Códigos	4
2. TECNOLOGIAS UTILIZADAS NO CONTROLE DE ACESSO	5
2.0.1. 1 Cartões de Proximidade (RFID)	5
2.0.2. 2 Biometria	5
2.0.2.1. RECONHECIMENTO FACIAL	6
2.0.2.2. IMPRESSÕES DIGITAIS	6
2.0.2.3. PRINCIPAIS CARACTERÍSTICAS:	7
2.0.3. 3 Códigos e Senhas	7
2.0.4. 4 Terminais de Controle de Acesso	8
2.0.5. 5 Controle de Acesso via Smartphone	8
3. BOAS PRÁTICAS NA IMPLEMENTAÇÃO DE SISTEMAS DE CONTROLE DE ACESSO	8
3.0.1. 1 Análise de Riscos	8
3.0.2. 2 Integração com Outros Sistemas de Segurança	9
3.0.3. 3 Definição de Políticas de Acesso	9
3.0.4. 4 Manutenção Preventiva e Atualizações	10
4. CONTROLE DE ACESSO E LGPD	10
4.0.1. 1 Coleta e Tratamento de Dados Pessoais	10
4.0.2. 2 Armazenamento e Proteção de Dados	11
4.0.3. 3 Direitos dos Titulares dos Dados	11
4.0.4. 4 Responsabilidade em Caso de Incidentes	12
5. TENDÊNCIAS E FUTURO DO CONTROLE DE ACESSO	12
5.0.1. 1 Integração com a Internet das Coisas (IoT)	12
5.0.2. 2 Controle de Acesso Baseado em Nuvem	13
5.0.3. 3 Uso de Inteligência Artificial e Machine Learning	13
5.0.4. 4 Autenticação Sem Contato e Mobile	14
5.0.5. 5 Blockchain para Controle de Acesso	14
6. CONCLUSÃO	14

0.1. O QUE É CONTROLE DE ACESSO BIOMÉTRICO?

O controle de acesso é um conjunto de tecnologias e processos que têm como finalidade **permitir ou restringir** a entrada e saída de pessoas ou veículos em uma determinada área.

A tecnologia de controle de acesso biométrico **touchless, ou sem contato**, representa uma evolução significativa em sistemas de autenticação e segurança. Esse tipo de tecnologia utiliza a captura de dados biométricos, como reconhecimento facial ou leitura de impressões digitais, sem a necessidade de tocar fisicamente em um dispositivo.

O controle de acesso é um dos principais pilares da segurança física, sendo essencial em ambientes corporativos e industriais.

[elementor-template id="24446"]

1. TIPOS DE SISTEMAS DE CONTROLE DE ACESSO

Os sistemas de controle de acesso podem ser classificados em várias categorias, dependendo da tecnologia empregada e do tipo de ambiente que protegem. Cada sistema é projetado para atender a necessidades específicas de segurança, escalabilidade e flexibilidade.

A seguir, estão os principais tipos de sistemas utilizados:

1.0.1. 1 Controle de Acesso Físico

Este é o tipo mais comum e básico de controle de acesso. Ele envolve barreiras físicas que impedem ou permitem o acesso a uma área. Geralmente, são usados em conjunto com sistemas de verificação, como cartões de proximidade ou biometria, para liberar portas, portões, cancelas ou catracas.

Exemplos de controle de acesso físico:

- **Catracas e torniquetes:** Comuns em entradas de prédios comerciais ou industriais, controlam o fluxo de pessoas de maneira ordenada.
- **Portas controladas eletronicamente:** Podem ser abertas por meio de cartões de proximidade, teclados numéricos ou sistemas biométricos.
- **Cancelas:** Instaladas em entradas de estacionamentos para controlar o acesso de veículos

1.0.2. 2 Controle de Acesso Eletrônico

Esse tipo de sistema usa **dispositivos eletrônicos e software** para controlar o acesso em locais maiores, onde o gerenciamento manual seria ineficiente. Ele pode ser integrado com câmeras de CFTV e outros subsistemas para garantir monitoramento contínuo e, em alguns casos, ações automatizadas.

Exemplos:

- **Sistemas baseados em RFID:** Usam a tecnologia de identificação por rádio frequência para autorizar acessos de forma rápida e sem contato físico.
- **Controle de acesso em rede:** Permite a gestão centralizada de diversos pontos de acesso espalhados por um grande campus ou edifício.

1.0.3. 3 Controle de Acesso Biométrico

Sistemas biométricos identificam indivíduos com base em características físicas únicas, como impressões digitais, reconhecimento facial ou leitura de íris. Esses sistemas são altamente seguros e minimizam fraudes associadas à troca de credenciais.

Principais características:

- **Impressão digital:** Ainda uma das formas mais usadas, por ser rápida e de fácil implementação.
- **Reconhecimento facial:** Cada vez mais popular devido ao avanço dos algoritmos de inteligência artificial e sua capacidade de operação mesmo em ambientes com pouca iluminação.
- **Leitura de íris:** Proporciona um nível ainda mais alto de segurança, usado em locais de alta sensibilidade, como instalações governamentais ou militares.

1.0.4. 4 Controle de Acesso por Senhas e Códigos

Embora esteja se tornando menos popular devido a questões de segurança, o controle de acesso por senhas ainda é amplamente utilizado em ambientes menores ou onde há uma necessidade menor de proteção.

Vantagens:

- Simplicidade de instalação e uso.
- Menor custo em comparação com outros sistemas.

Desvantagens:

- Vulnerabilidade a fraudes ou compartilhamento de senhas.
- Segurança inferior em relação a sistemas biométricos ou RFID.

2. TECNOLOGIAS UTILIZADAS NO CONTROLE DE ACESSO

A escolha da tecnologia adequada é fundamental para garantir a eficiência e a segurança de um sistema de controle de acesso. As tecnologias disponíveis variam em complexidade, custo e nível de segurança.

A seguir seguem as principais tecnologias usadas nos sistemas de controle de acesso.

2.0.1. 1 Cartões de Proximidade (RFID)

Os cartões de proximidade, baseados na tecnologia RFID (Radio-Frequency Identification), são amplamente utilizados em ambientes corporativos, industriais e comerciais por sua praticidade e flexibilidade. Eles funcionam sem a necessidade de contato direto com o leitor, o que acelera o processo de entrada e saída.

Principais características:

- **Facilidade de uso:** O usuário só precisa aproximar o cartão do leitor, sem inserir ou passar por leitores tradicionais.
- **Segurança moderada:** Apesar de práticos, os cartões RFID podem ser clonados se não forem adotadas tecnologias adicionais de criptografia e autenticação.
- **Aplicações típicas:** Controle de entrada em escritórios, estacionamentos, acesso a salas de servidores ou áreas restritas.

2.0.2. 2 Biometria

A biometria está entre as tecnologias mais seguras para controle de acesso, pois usa características físicas únicas dos indivíduos, como impressões digitais, reconhecimento facial, leitura de íris, ou até padrões de voz. Devido à sua precisão, é ideal para áreas que exigem alto nível de segurança.

A tecnologia de **controle de acesso biométrico touchless**, ou sem contato, representa uma evolução significativa em sistemas de autenticação e segurança. Esse tipo de tecnologia utiliza a captura de dados biométricos, como **reconhecimento facial** ou **leitura de impressões digitais**, sem a necessidade de tocar fisicamente em um dispositivo.

2.0.2.1. RECONHECIMENTO FACIAL

No caso do [reconhecimento facial](#), as câmeras analisam e mapeiam os traços do rosto, como a distância entre os olhos, formato do nariz e outras características faciais únicas. Essa informação é então comparada com os dados armazenados em banco de dados para conceder ou negar o acesso.

2.0.2.2. IMPRESSÕES DIGITAIS

O sistema de **leitura biométrica touchless** também pode incluir sensores que escaneiam impressões digitais à distância, utilizando luzes infravermelhas para mapear as digitais sem contato direto.

O **MorphoWave** é um sistema avançado de controle de acesso biométrico desenvolvido pela IDEMIA, que utiliza tecnologia de leitura de impressões digitais em movimento e de forma totalmente **touchless** (sem contato). Este sistema inovador é projetado para capturar e reconhecer as impressões digitais com alta precisão, apenas passando a mão através do sensor, sem a necessidade de tocar fisicamente em qualquer superfície.

A tecnologia empregada pelo MorphoWave envolve o uso de **imagens tridimensionais** para capturar as impressões digitais. O dispositivo escaneia todos os quatro dedos de uma mão em movimento, usando sensores ópticos que realizam uma captura em 3D das digitais, enquanto o usuário movimenta a mão por cima do leitor. Esse processo ocorre de forma instantânea, permitindo um fluxo contínuo de pessoas sem atrasos ou a necessidade de parar para interação com o dispositivo. O sensor é capaz de coletar até 4.000 imagens de alta resolução em menos de um segundo.

2.0.2.3. PRINCIPAIS CARACTERÍSTICAS:

- **Captura de impressão digital 3D em movimento:** Utiliza tecnologia avançada para mapear as digitais em três dimensões, proporcionando maior precisão na comparação biométrica.
- **Alta velocidade e eficiência:** O MorphoWave oferece leitura em menos de um segundo, o que o torna ideal para ambientes de alto tráfego, como edifícios corporativos, aeroportos e áreas industriais.
- **Segurança e conveniência:** Ao não exigir contato físico, minimiza riscos de contaminação e desgaste do equipamento. Além disso, a precisão da tecnologia garante um nível elevado de segurança, pois realiza comparações em tempo real com bases de dados previamente cadastradas.
- **Integração com sistemas existentes:** O MorphoWave pode ser integrado a diversas plataformas de controle de acesso, facilitando sua adoção em diferentes setores.

Vantagens:

- **Intransponível:** É praticamente impossível replicar ou compartilhar características biométricas.
- **Confiabilidade:** Oferece alta taxa de precisão, minimizando falsos positivos ou negativos.
- **Aplicações:** Uso em bancos, instituições governamentais, laboratórios de alta segurança, data centers, entre outros.

2.0.3. 3 Códigos e Senhas

Apesar de ser uma tecnologia mais simples e de segurança inferior, os sistemas baseados em senhas ou códigos ainda são amplamente utilizados em pequenas empresas ou ambientes com menor risco. Eles oferecem uma solução barata e de fácil implementação, mas carecem da robustez necessária para locais que exigem alto nível de proteção.

Principais usos:

- **Portas internas:** Acesso a salas ou escritórios de baixa sensibilidade.
- **Pequenos negócios:** Usado como camada de segurança básica em áreas que não precisam de proteção crítica.

2.0.4. 4 Terminais de Controle de Acesso

Os terminais são os dispositivos que conectam o usuário ao sistema de controle de acesso. Eles podem integrar diversas tecnologias em um único ponto, oferecendo flexibilidade e segurança em diferentes níveis. Alguns terminais combinam RFID com biometria, ou até mesmo reconhecimento facial com senhas numéricas, aumentando as camadas de autenticação.

Exemplos de terminais:

- **Leitores multifatoriais:** Usam mais de uma tecnologia para autenticar o acesso, como cartões e biometria juntos.
- **Totens e quiosques:** Frequentemente usados em prédios corporativos ou grandes eventos, facilitam o controle de visitantes e colaboradores.

2.0.5. 5 Controle de Acesso via Smartphone

Com a crescente digitalização, muitos sistemas de controle de acesso agora integram smartphones como uma solução prática e segura. O usuário pode usar um aplicativo dedicado ou tecnologia NFC (Near Field Communication) para acessar áreas restritas.

Vantagens:

- **Mobilidade:** Permite que os usuários usem seus próprios dispositivos, eliminando a necessidade de cartões ou senhas.
- **Segurança avançada:** Smartphones modernos oferecem criptografia robusta, biometria integrada e autenticação multifator.

3. BOAS PRÁTICAS NA IMPLEMENTAÇÃO DE SISTEMAS DE CONTROLE DE ACESSO

A implementação de um sistema de controle de acesso requer conhecimento e expertise para definir a tecnologia correta. Existem práticas recomendadas que garantem que o sistema funcione com eficiência e ofereça a proteção necessária ao ambiente. Abaixo estão as principais boas práticas a serem seguidas:

3.0.1. 1 Análise de Riscos

Antes da implementação de qualquer sistema de controle de acesso, é fundamental realizar uma análise detalhada dos riscos associados ao ambiente. Isso inclui a identificação das áreas mais vulneráveis, os ativos mais críticos e a definição do nível de segurança necessário para cada um deles.

Principais passos na análise de riscos:

- **Mapeamento de áreas sensíveis:** Identificar os pontos que necessitam de um controle de acesso mais rigoroso, como salas de servidores, cofres ou áreas de produção.
- **Avaliação de fluxos de pessoas:** Compreender como e quando as pessoas acessam determinadas áreas ajuda a definir o melhor sistema e horários de maior necessidade de segurança.
- **Identificação de possíveis ameaças:** Desde fraudes internas até invasões externas, todas as ameaças devem ser consideradas na escolha do sistema.

3.0.2. 2 Integração com Outros Sistemas de Segurança

Um sistema de controle de acesso não deve atuar de forma isolada. A integração com outros subsistemas de segurança, como **câmeras de CFTV, alarmes e sensores de intrusão**, cria um ambiente mais seguro e garante respostas rápidas em caso de violação.

Benefícios da integração:

- **Monitoramento em tempo real:** Integrar o controle de acesso ao CFTV permite a visualização instantânea de quem está acessando determinadas áreas.
- **Automatização de respostas:** Caso uma violação de segurança seja detectada, o sistema pode ativar outros mecanismos automaticamente, como bloquear portas ou acionar alarmes.
- **Registro centralizado:** Os eventos registrados por diferentes sistemas podem ser armazenados em uma única base de dados, facilitando a auditoria e a investigação de incidentes.

3.0.3. 3 Definição de Políticas de Acesso

Estabelecer políticas claras para o controle de acesso é essencial para garantir que as regras sejam seguidas de maneira uniforme em toda a organização. Isso inclui a definição de quem pode acessar determinadas áreas, em que horários, e sob quais circunstâncias.

Pontos importantes nas políticas de acesso:

- **Acesso por níveis hierárquicos:** Definir níveis de autorização com base nas funções e responsabilidades dos funcionários, garantindo que apenas as pessoas certas tenham acesso às áreas mais sensíveis.
- **Revisão periódica de autorizações:** Verificar regularmente as permissões de acesso para garantir que não haja colaboradores com acesso indevido a determinadas áreas.
- **Autenticação multifator:** Para áreas críticas, é recomendado o uso de mais de um fator de autenticação, como um cartão RFID combinado com uma senha ou biometria.

3.0.4. 4 Manutenção Preventiva e Atualizações

A manutenção preventiva dos sistemas de controle de acesso é fundamental para evitar falhas que comprometam a segurança. Da mesma forma, é importante manter os softwares de controle atualizados para se proteger contra vulnerabilidades e melhorar a eficiência do sistema.

Boas práticas de manutenção:

- **Inspeções regulares:** Verificar periodicamente o funcionamento de leitores, catracas e fechaduras eletrônicas.
- **Atualização de firmware e software:** Garantir que os dispositivos e o software de controle estejam sempre com a versão mais recente para prevenir falhas de segurança.
- **Monitoramento de logs:** Acompanhar os registros de eventos pode identificar comportamentos anômalos ou tentativas de violação antes que um problema maior ocorra.

4. CONTROLE DE ACESSO E LGPD

Com a implementação da Lei Geral de Proteção de Dados (LGPD), as empresas que utilizam sistemas de controle de acesso precisam garantir que estão em conformidade com as normas de proteção de dados pessoais. A LGPD estabelece regras sobre a coleta, o tratamento e o armazenamento de dados, e isso inclui informações coletadas por sistemas de controle de acesso, como biometria e dados de identificação.

4.0.1. 1 Coleta e Tratamento de Dados Pessoais

Os sistemas de controle de acesso frequentemente coletam dados pessoais sensíveis, como impressões digitais, imagens faciais ou até dados de localização de funcionários. A LGPD exige que o tratamento desses dados seja realizado com transparência e apenas com o consentimento do titular, exceto em casos onde o tratamento seja necessário para o cumprimento de obrigações legais ou contratuais.

Boas práticas para conformidade:

- **Consentimento informado:** Os indivíduos cujos dados estão sendo coletados devem ser informados sobre o propósito e a forma de utilização dessas informações, e o consentimento deve ser claro e explícito.
- **Finalidade específica:** Os dados devem ser coletados com uma finalidade específica, e seu uso deve se limitar a essa finalidade. Por exemplo, dados biométricos coletados para controle de acesso não devem ser utilizados para outros fins sem a devida autorização.
- **Minimização de dados:** Apenas os dados estritamente necessários devem ser coletados. Isso reduz o risco de vazamento e facilita o gerenciamento das informações.

4.0.2. 2 Armazenamento e Proteção de Dados

Além da coleta, a LGPD também impõe obrigações rigorosas sobre como os dados devem ser armazenados e protegidos. A empresa deve garantir que todos os dados pessoais estejam protegidos contra acessos não autorizados, alterações ou perda.

Medidas de segurança recomendadas:

- **Criptografia de dados:** Informações sensíveis, como dados biométricos, devem ser criptografadas tanto no armazenamento quanto durante a transmissão.
- **Controle de acesso aos dados:** Apenas indivíduos autorizados devem ter acesso às informações coletadas. Isso pode ser feito através de autenticação multifatorial e registros de auditoria.
- **Tempo de retenção:** Os dados não devem ser mantidos por mais tempo do que o necessário para a finalidade original. Após esse período, eles devem ser devidamente descartados ou anonimizados.

4.0.3. 3 Direitos dos Titulares dos Dados

A LGPD também garante uma série de direitos aos titulares dos dados, incluindo o direito de acessar, corrigir ou excluir seus dados. As empresas devem estar preparadas para atender essas solicitações em conformidade com os prazos estabelecidos pela lei.

Direitos previstos:

- **Acesso aos dados:** O titular tem o direito de solicitar uma cópia dos dados que foram coletados sobre ele.
- **Correção de dados:** Se houver erros nos dados coletados, o titular pode solicitar sua correção.
- **Exclusão de dados:** O titular pode solicitar a exclusão de seus dados, exceto quando a retenção for necessária para cumprimento de obrigações legais ou contratuais.

4.0.4. 4 Responsabilidade em Caso de Incidentes

Em caso de vazamento ou violação de dados, a empresa responsável pelo controle de acesso pode ser penalizada se não tiver tomado as devidas precauções para proteger as informações. Além das multas, que podem chegar a 2% do faturamento da empresa, o incidente pode prejudicar seriamente a reputação da organização.

Medidas preventivas:

- **Plano de resposta a incidentes:** Ter um plano claro para lidar com incidentes de segurança, incluindo a notificação de autoridades e dos titulares dos dados em caso de violação.
- **Auditorias regulares:** Realizar auditorias periódicas nos sistemas de controle de acesso para garantir que as políticas de proteção de dados estejam sendo seguidas adequadamente.

5. TENDÊNCIAS E FUTURO DO CONTROLE DE ACESSO

Com a rápida evolução da tecnologia, os sistemas de controle de acesso estão passando por transformações significativas. Novas tendências e inovações estão sendo incorporadas para melhorar a eficiência, a segurança e a flexibilidade desses sistemas, oferecendo soluções mais inteligentes e conectadas. A seguir, destacamos as principais tendências para o futuro do controle de acesso.

5.0.1. 1 Integração com a Internet das Coisas (IoT)

A Internet das Coisas (IoT) está mudando a forma como dispositivos se comunicam, e o controle de acesso não é exceção. Com a IoT, os dispositivos de controle de acesso podem ser conectados e gerenciados remotamente, permitindo maior flexibilidade e controle em tempo real. Essa tecnologia também facilita a integração com outros dispositivos inteligentes, criando um ecossistema de segurança mais eficiente.

Exemplos de aplicação:

- **Trancas inteligentes:** Integradas com dispositivos IoT, essas trancas podem ser monitoradas e controladas remotamente via smartphones ou outros dispositivos conectados.
- **Monitoramento preditivo:** Sensores IoT podem ser utilizados para prever falhas nos sistemas de controle de acesso, reduzindo o tempo de inatividade e aumentando a segurança.

5.0.2. 2 Controle de Acesso Baseado em Nuvem

A adoção de sistemas de controle de acesso baseados em nuvem está em ascensão, principalmente devido à sua flexibilidade, escalabilidade e facilidade de gerenciamento. Com o gerenciamento em nuvem, as empresas podem controlar e monitorar acessos em diferentes locais de forma centralizada e em tempo real, sem a necessidade de infraestrutura local robusta.

Vantagens do controle de acesso em nuvem:

- **Gerenciamento remoto:** Permite que os administradores controlem os acessos de qualquer lugar, usando dispositivos conectados à internet.
- **Escalabilidade:** Fácil de expandir à medida que a empresa cresce, sem a necessidade de investimentos em hardware adicional.
- **Atualizações automáticas:** Com os sistemas baseados em nuvem, as atualizações de segurança e funcionalidades são implementadas automaticamente, reduzindo o risco de vulnerabilidades.

5.0.3. 3 Uso de Inteligência Artificial e Machine Learning

A inteligência artificial (IA) e o machine learning estão sendo cada vez mais aplicados para aprimorar a segurança dos sistemas de controle de acesso. Essas tecnologias podem ser usadas para detectar padrões comportamentais e identificar anomalias, melhorando a precisão na autenticação e aumentando a segurança do sistema.

Exemplos de uso de IA e machine learning:

- **Autenticação adaptativa:** O sistema pode aprender os padrões de comportamento dos usuários e adaptar os requisitos de autenticação de acordo com o nível de risco percebido.
- **Deteção de fraudes:** IA pode analisar grandes volumes de dados para identificar tentativas de violação ou comportamentos suspeitos, acionando medidas de segurança preventivas.

5.0.4. 4 Autenticação Sem Contato e Mobile

O avanço da tecnologia sem contato e a crescente adoção de smartphones estão impulsionando a popularidade da autenticação sem contato em sistemas de controle de acesso. Soluções baseadas em smartphones, como NFC (Near Field Communication) e Bluetooth, permitem que os usuários desbloqueiem portas ou acessem áreas restritas sem a necessidade de cartões físicos.

Benefícios da autenticação sem contato:

- **Praticidade:** Os usuários podem utilizar seus próprios dispositivos móveis para acessar áreas restritas, eliminando a necessidade de carregar cartões ou chaves.
- **Segurança avançada:** Soluções móveis podem ser combinadas com autenticação multifator, incluindo biometria e reconhecimento facial, aumentando a segurança.

5.0.5. 5 Blockchain para Controle de Acesso

Embora ainda esteja em estágio inicial, o uso de blockchain no controle de acesso está ganhando atenção. A tecnologia de blockchain oferece uma maneira segura e descentralizada de gerenciar autenticações e permissões de acesso, garantindo que os registros de acesso sejam imutáveis e protegidos contra fraudes.

Aplicações potenciais:

- **Autenticação descentralizada:** O blockchain pode ser usado para autenticar usuários sem depender de um servidor central, tornando o sistema menos vulnerável a ataques cibernéticos.
- **Registro imutável de acessos:** Todas as transações e eventos de acesso podem ser armazenados de forma permanente em uma cadeia de blocos, garantindo transparência e auditoria confiável.

6. CONCLUSÃO

O controle de acesso evolui constantemente para atender às crescentes demandas por segurança e eficiência. Com tecnologias como IoT, nuvem, inteligência artificial e blockchain, as soluções de controle de acesso estão se tornando cada vez mais conectadas, automatizadas e inteligentes.

Empresas que investem em sistemas de controle de acesso modernos garantem não apenas a proteção de seus ativos, mas também a conformidade com regulamentações como a LGPD.

Para garantir a implementação eficaz dessas tecnologias, é essencial contar com uma empresa de engenharia especializada, capaz de projetar, instalar e manter sistemas robustos e integrados de controle de acesso.

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.