



UNIVERSIDADE FEDERAL DA BAHIA  
SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI  
COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO

## MEMORIAL DESCRITIVO DO PROJETO DE SISTEMA DE CONTROLE DE ACESSO (SICA)

### PROJETO CIENAM - MÓDULO 3

### ESPECIALIDADE SICA

0	IGOR SÁ	JULHO/16	EMIÇÃO INICIAL
Rev.	Por	Data	Descrição



UNIVERSIDADE FEDERAL DA BAHIA  
SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI  
COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO

## SUMÁRIO

1	INTRODUÇÃO .....	3
2	JUSTIFICATIVA DE PROJETO .....	3
3	IMPLANTAÇÃO.....	3
4	ANÁLISE DE VIABILIDADE TÉCNICA .....	3
4.1	INTRODUÇÃO .....	4
4.2	TOPOLOGIA BÁSICA DO SISTEMA DE CONTROLE DE ACESSO (SICA).....	5
4.3	CONCEITOS BÁSICOS DE CONTROLE DE ACESSO .....	5
4.4	POLÍTICAS DE CONTROLE DE ACESSO .....	9
4.5	TECNOLOGIA DO CONTROLE DE ACESSO .....	10
4.6	SELEÇÃO DA TECNOLOGIA .....	13
4.7	CONCLUSÃO.....	13
5	DADOS GERAIS PARA ELABORAÇÃO DO PROJETO DE SICA .....	14
5.1	OBJETIVOS PRINCIPAIS .....	14
5.2	NORMAS PERTINENTES .....	15
5.3	ESPECIFICAÇÕES GERAIS .....	15
6	EQUIPE DE ELABORAÇÃO DE PROJETO / ORÇAMENTO .....	17



UNIVERSIDADE FEDERAL DA BAHIA  
SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI  
COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO

## 1 INTRODUÇÃO

O presente Memorial tem por objetivo descrever as soluções adotadas na elaboração do **Projeto do Módulo 3 - CIENAM - Universidade Federal da Bahia**, situado no Campus Federação / Ondina, na cidade de Salvador–BA.

O presente documento abrange as atividades de **SICA**.

## 2 JUSTIFICATIVA DE PROJETO

O projeto de Instalações do Sistema de Controle de Acesso do **Módulo 3 - CIENAM** foi elaborado para suprir o referido edificação com sistema adequado e moderno de segurança. Foi executado conforme estabelece a Associação Brasileira de Normas Técnicas (ABNT) e Normas Técnicas Internacionais vigentes, com o objetivo de dar soluções viáveis, seguras e tecnicamente econômicas ao cliente.

## 3 IMPLANTAÇÃO

No caso das instalações pertinentes a este memorial, a área de intervenção compreende:

- Pavimentos: Térreo, 1º Pavimento, 2º Pavimento e 3º Pavimento.

## 4 ANÁLISE DE VIABILIDADE TÉCNICA

Nossa análise se concentrou nas tecnologias de SICA para edifícios comerciais mais utilizadas atualmente no mercado brasileiro, desconsiderando as tecnologias já ultrapassadas, tais como sistemas analógicos. O projeto de Instalações do Sistema de Controle de Acesso do **Módulo 3 – CIENAM** contemplou as necessidades de controle e permissões de acesso de colaboradores e visitantes às dependências das edificações, considerando os acessos às edificações (catracas eletrônicas, cancelas).

O projeto deve contemplar as necessidades de controle e permissões de acesso às dependências da edificação, tratando distintamente as situações internas (informadas pela contratante) e externas, atendendo ao acesso veicular e de pessoas, com o objetivo de se utilizar uma solução de tecnologia viável, segura e tecnicamente econômica, sempre com a preocupação: Topologia da Edificação x Tipo de uso da edificação x Interesses do Cliente x Rendimento Operacional x Custo do sistema x Benefício ao usuário.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

#### 4.1 INTRODUÇÃO

O objetivo principal do sistema é proporcionar segurança através da monitoração do acesso de pessoas às instalações de uma empresa conforme as informações contidas no banco de dados do sistema.

O sistema se propõe a controlar uma rede on-line de equipamentos de acesso, liberando ou bloqueando uma tentativa de acesso com o uso de cartão, senha ou biometria.

Entende-se por "equipamento de acesso" um equipamento eletrônico dotado de bloqueio físico, como, por exemplo:

- Catracas;
- Cancelas;
- Torniquetes;
- Porta com fechadura eletrônica.

Os equipamentos acima descritos são comandados por um ou mais leitores de cartão (Código de barras, Magnético, Proximidade ou Smart Card), de teclado ou biometria.

O procedimento de controle de acesso se dá mediante apresentação de um identificador (cartão, senha ou biometria) em um leitor para a verificação do limite de acesso pelo Sistema e a partir disso, liberar ou não a passagem para o portador do cartão.

A verificação do limite de acesso pode ser realizada nas seguintes condições:

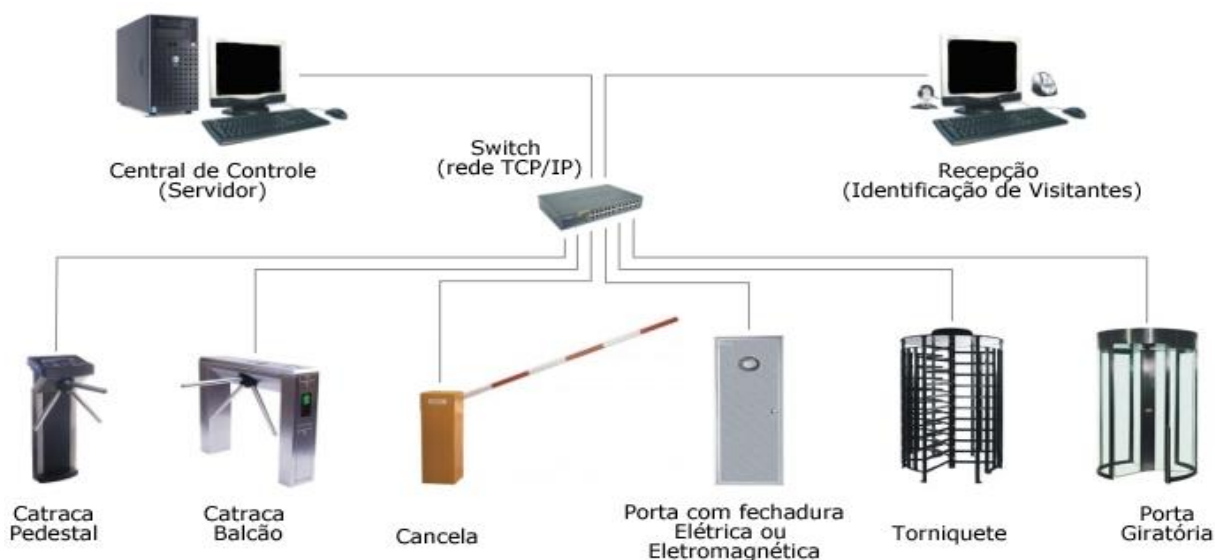
- Existência: se o identificador (cartão, senha ou biometria) já foi cadastrado no sistema;
- Situação: se o identificador está liberado ou bloqueado;
- Validade: se o identificador está dentro do período de validade estipulado;
- Local: se o identificador está sendo utilizado dentro das áreas permitidas para o seu acesso;
- Horário: se o acesso está sendo realizado dentro dos horários permitidos;
- Senha: acesso condicionado à verificação de um código de acesso que deve ser digitado pelo usuário.

As verificações acima são realizadas independentemente se o sistema estiver on-line ou off-line. A principal diferença entre um sistema de controle de acesso on-line e um sistema off-line está na forma de verificar a autorização de acesso de um usuário. Num sistema on-line, este processo é efetuado em um servidor onde estão contidos todos os identificadores cadastrados e os parâmetros que estabelecem as condições de acessos associados a cada identificador. O critério de decisão de um sistema de acesso off-line é baseado em listas que são carregadas nas memórias das controladoras.



UNIVERSIDADE FEDERAL DA BAHIA  
SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI  
COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPPO

#### 4.2 TOPOLOGIA BÁSICA DO SISTEMA DE CONTROLE DE ACESSO (SICA)



Os sistemas de controle de acesso são indispensáveis nas empresas, condomínios residenciais e condomínios comerciais, onde seu sucesso também depende do bom treinamento de seus operadores.

#### 4.3 CONCEITOS BÁSICOS DE CONTROLE DE ACESSO

Esta seção define alguns conceitos básicos sobre controle de acesso, visando substanciar o leitor no assunto.

##### 4.3.1 Autenticação, Autorização e Auditoria

O termo controle de acesso pode ser definido em cima da divisão em três subcampos distintos, que agem em conjunto: autenticação, autorização e auditoria, conhecidos como os “três As”.

Autenticação trata de identificar o usuário a acessar o sistema. Autorização trata do que esse usuário poderá realizar (está autorizado a fazer) no sistema. Auditoria mantém os registros necessários das ações do usuário.

##### 4.3.2 Autenticação

Autenticação refere-se ao processo de fornecer ao sistema informações que identifiquem com um grau de certeza suficiente (para os fins do sistema em questão) o usuário que está requisitando o acesso aos recursos computacionais. Em termos gerais, é o processo de provar ao sistema que o usuário é realmente quem diz ser, e não alguém se passando por ele. O processo de autenticação pode ser realizado ao sistema de três maneiras principais:

- Autenticação utilizando algo que você sabe: é o método mais comum, em que o usuário autentica-se ao sistema fornecendo-lhe alguma informação que (assume-se) só é de conhecimento do usuário: uma senha de acesso, por exemplo. É o mecanismo mais comum de autenticação, e por isso mesmo o mais fácil e mais sujeito a abusos. A principal vulnerabilidade deste tipo de autenticação é que se outra pessoa descobrir ou adivinhar o segredo de acesso, poderá facilmente utilizar o sistema passando-se pelo usuário legítimo.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

Por isso, o segredo deve ser protegido (ficando apenas armazenado na memória do usuário de preferência, ao invés de anotado em algum lugar). Isso levanta o fino balanço entre senhas fáceis de serem decoradas e adivinhadas, ou senhas difíceis de serem adivinhadas, mas também difíceis de serem decoradas, fomentando que sejam registradas fora da memória do usuário;

- Autenticação utilizando algo que você possui: é o segundo método mais comum, em que o usuário autentica-se através da apresentação de algum token ou objeto que esteja em sua posse (uma chave para uma fechadura, um arquivo no seu sistema ou um cartão de crédito são exemplos desse tipo de autenticação, que recentemente vem ganhando força na forma de smartcards). A principal vulnerabilidade desse tipo de autenticação é parecida com a anterior, ainda que mais difícil de acontecer: se o usuário perder o objeto de autenticação, ou for roubado, será possível autenticar-se no sistema. Em geral, quanto mais móvel (leve, prático) for o objeto de autenticação, mais fácil será de ser extraviado;
- Autenticação utilizando algo que você é: esse é o tipo menos comum de autenticação, baseado na apresentação em alguma propriedade fundamental e integrante de uma pessoa para a autenticação. A biometria é extensivamente utilizada neste caso, para autenticação utilizando características únicas de indivíduos, como padrões de íris, impressão digital, impressão baseada na mão, padrões de voz ou de escrita (assinaturas são consideradas como biometria também). A autenticação por técnicas biométricas possui uma série de variações e detalhes específicos, mas em geral funcionam da seguinte maneira:
  - a) As informações biométricas são capturadas do usuário do sistema: por exemplo, é realizada uma análise da retina do indivíduo para autenticação por padrões da íris;
  - b) Os dados biométricos são extraídos da colheita realizada: em geral, são utilizadas técnicas de sumários digitais para resumir a massa de dados em sequências de tamanho físico. Uma característica destes sumários é que eles são função exclusiva dos dados de entrada, não sendo possível recuperá-los a partir do sumário final;
  - c) O sumário biométrico calculado é comparado com um sumário já armazenado no sistema para aquele usuário. Se forem iguais, a autenticação é realizada com sucesso.

Apesar da atenção em cima de tecnologias biométricas de autenticação, elas têm uma vulnerabilidade básica: biométricos são identificadores únicos, mas não são segredos. Ou seja, é perfeitamente possível um atacante conseguir retirar um sumário da impressão digital de um usuário de forma ilícita, e utilizá-lo para se autenticar ao sistema.

Como se pode ver, utilizar um único tipo de autenticação costuma ser insuficiente, já que os três tipos têm vulnerabilidades individuais. Para controle de acesso, o mais efetivo é utilizar pelo menos duas das três técnicas de autenticação em conjunto. Por exemplo, aliar a identificação biométrica ou a posse de um cartão de acesso ao fornecimento de uma senha individual.

A autenticação é o primeiro passo para o controle de acesso. Depois de identificar unicamente o indivíduo que estará utilizando o sistema, é necessário avaliar a extensão da autorização do indivíduo naquele sistema.

#### 4.3.3 Autorização

O processo de autorização rege exatamente que operações e sob que recursos computacionais o usuário poderá executar no sistema. Para que sejam efetivadas quaisquer avaliações de autorização, é necessário ter passado pela etapa de autenticação.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

No processo de autorização é que vem à tona toda a complexidade e riqueza dos modelos de controle de acesso e das políticas que permitem implementar. Os principais modelos de autorização serão definidos e detalhados adiante, em seção própria.

#### 4.3.4 Auditoria

Um aspecto muitas vezes ignorado de sistemas de controle de acesso é o aspecto de auditoria: manter registro das principais transações executadas pelo sistema. A ideia é prover uma “trilha” que permita reconstruir operações relevantes do usuário no sistema.

A definição de “relevante” é dependente das particularidades de cada sistema. Por exemplo, podem-se registrar os horários em que o usuário entrou e saiu do sistema (“logon” e “logoff”), ou os detalhes de cada operação realizada pelo usuário durante a sua sessão de trabalho.

#### 4.3.5 Sujeito, Objeto, Operações e Permissões

Define-se Sujeito (subject) como sendo a representação do usuário dentro do sistema. Pode-se entender o conceito de sujeito como o de um processo no sistema aliado a um conjunto de credenciais de acesso que associam aquele processo a um usuário da base do sistema. Em geral, as regras de autorização são expressas utilizando-se o identificador do usuário (seu login ou identificação única no sistema). No momento da autenticação, as credenciais de acesso são geradas para aquela sessão do usuário. A partir daí, qualquer execução de processo ou rotina dentro do sistema é encarada como um subject, já que alia as credenciais de acesso do usuário com um processo que o representa no sistema.

O objeto (object) representa o recurso computacional cujo acesso é controlado. Ele pode ser, na prática, qualquer estrutura de dados ou abstração fornecida pelo sistema, incluindo: arquivos, área de memória, um dispositivo externo (mouse ou monitor), um socket, uma conta bancária, um processo, e assim por diante.

Operações são realizadas pelos sujeitos do sistema sob seus objetos. As operações podem ter vários níveis de abstração, incluindo operações comuns como leitura, escrita, remoção até operações mais complexas e dependentes da natureza de cada sistema, como operações de débito e crédito em um sistema bancário, por exemplo.

#### 4.3.6 Modelos de controle de acesso: DAC e MAC

Modelos de controle de acesso ou, rigorosamente, modelos de autorização de acesso, definem características primitivas de um determinado conjunto de regras de autorização a serem utilizadas. Essas características influenciam os limites da semântica de autorização que pode ser expressa no modelo e consequentemente a sua implementação. Os principais modelos de controle de acesso hoje são DAC (Discretionary Access Control), MAC (Mandatory Access Control) e RBAC (Role-Based Access Control).

Dentro de um determinado modelo de controle de acesso podem existir diferentes políticas de controle de acesso ou, rigorosamente, políticas de autorização de acesso (declaração sucinta das propriedades de proteção que um sistema ou uma classe genérica de sistemas precisa possuir). Seus pontos-chave em geral cabem em uma única página, e é o documento que expressa os objetivos da proteção e pode ser a base para uma análise matemática formal.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

#### 4.3.7 DAC: Discretionary Access Control

DAC é baseado na noção de que usuários individuais são “donos” de objetos e, portanto, têm controle (descrição) total em quem deve ter permissões para acessar o objeto. Um usuário transforma-se em dono do objeto ao criá-lo. O princípio básico de DAC é posse do objeto pelo usuário que o criou.

Atualmente, o DAC é o modelo mais popular de controle de acesso, pela sua utilização em grande escala em sistemas operacionais comerciais. Todas as variantes do UNIX, o Netware e a série Windows NT, 2000 e XP utilizam o modelo DAC como seu modelo básico de controle de acesso. Estes sistemas operacionais utilizam extensamente a técnica de listas de controle de acesso para conceber e implementar as suas checagens de autorização, dispondo também do conceito de grupos de usuários para facilitar na administração e concessão de permissões.

O modelo DAC possui uma fraqueza inerente: o fato de que informação pode ser copiada de um objeto para outro, de modo que acesso a uma cópia é possível mesmo que o dono do objeto original não tenha provido acesso ao original. Usuários que possuem acesso ao objeto original podem inadvertidamente permitir a realização de cópias não autorizadas, ao executar um programa “cavalo de tróia” que faça a cópia dos dados do objeto sem a explícita autorização ou cooperação do usuário.

Essa fraqueza do modelo DAC tornou-o insuficiente para sistemas militares, em que a informação precisava ter um alto nível de controle e ser resistente a ataque por cavalos de tróia, fomentando a criação do modelo MAC.

#### 4.3.8 MAC: Mandatory Access Control

Enquanto o ponto-chave do DAC é o fato de que os usuários são considerados donos do objeto e, portanto responsáveis pelas suas permissões de acesso, o modelo mandatório prevê que usuários individuais não têm escolha em relação a que permissões de acesso eles possuem ou a que objetos podem acessar.

Neste modelo, os usuários individuais não são considerados donos dos objetos e não podem definir suas permissões; isso é realizado pelos administradores do sistema. O modelo MAC é conhecido, a tal ponto de ser às vezes confundido pela sua utilização em políticas de acesso multinível, em que se deseja controlar o fluxo de informações em um sistema. Em geral, objetiva-se garantir que a informação só flua em um determinado sentido: por exemplo, de níveis mais baixos de confidencialidade para níveis maiores de confidencialidade (nunca de níveis mais altos para níveis mais baixos).

O fluxo de informações dentro destes sistemas deve seguir regras claras para garantir a sua confidencialidade. Esse fluxo e as regras de acesso impostas sobre ele costumam ser expressos utilizando lattices, de tal modo que MAC é em certos contextos conhecido como LBAC (Lattice-Based Access Control).

#### 4.3.9 DAC e MAC na atualidade

Tanto os modelos DAC e MAC são utilizados atualmente; o DAC em maior escala, estando presente em diversos sistemas operacionais comerciais como o UNIX, Windows e Netware. Apesar da sua popularidade, eles apresentam problemas próprios que estão possibilitando o crescimento de outro modelo de acesso, o RBAC a crescer, visando resolver estas questões.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

O MAC, apesar de ser reconhecido genericamente como mais controlável e potencialmente mais seguro que o DAC, não tem obtido grande uso fora dos circuitos militares. Isso se deve principalmente pela dificuldade em adaptar fluxos de negócio e hierarquia comerciais ao modelo formal e estritamente hierarquizado imposto por políticas como Bell-Lapadula e Biba, que são as mais amplamente implementadas. Isso faz com que não seja prático implantá-lo em sistemas que não sejam militares, pelo custo de administração e de overhead que seria gerado.

O DAC, por sua vez, goza de grande popularidade no mundo comercial, mas tem em seu maior problema a questão da dificuldade no gerenciamento das permissões. Sistemas operacionais modernos de rede possuem milhares de usuários e potencialmente milhões de arquivos espalhados pelos seus sistemas. O gerenciamento das permissões de cada um destes objetos em uma escala como esta não é um problema simples de se resolver, já que cada objeto possui sua própria informação de acesso individual.

#### **4.4 POLÍTICAS DE CONTROLE DE ACESSO**

##### **4.4.1 Conceitos e Definições**

Uma política de segurança é elaborada considerando-se o ambiente em que se está trabalhando, para que os critérios estabelecidos estejam de acordo com as práticas internas da empresa e com as práticas de segurança atualmente adotadas, a fim de buscar uma conformidade maior com critérios atualizados e reconhecidos em todo o mundo.

O principal propósito de uma política de segurança é informar aos usuários, à equipe e aos gerentes as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos.

##### **4.4.2 Políticas Discrecionárias e Mandatórias**

Num controle de acesso discrecionário (DAC), as políticas restringem o acesso a objetos baseado na identidade dos usuários ou grupos nos quais pertencem.

No Controle de Acesso Mandatório (MAC), políticas garantem o controle de acesso baseando-se na classificação dos usuários e objetos do sistema. Para cada objeto e usuário do sistema é atribuído um nível de segurança. O nível de segurança associado ao objeto reflete o nível de importância da informação contida no objeto, classificando o objeto quanto ao dano potencial que um acesso não autorizado traria.

##### **4.4.3 Políticas Baseadas em Perfis**

Perfis fornecem um grupo semântico de usuários em comum, pertencendo geralmente a uma posição dentro de uma organização tal como: gerente de departamento, gerente de projeto e analista. Especificar políticas organizacionais, por exemplo, para um grupo de gerentes, permite que, caso exista um novo gerente, não necessite redefinir os deveres e direitos para este novo usuário. Usam-se perfis como um meio para agrupar políticas relacionadas a uma posição particular, por exemplo, criando um perfil de gerente; logo todos os gerentes podem ser atribuídos ou removidos desta posição sem mudar as políticas. Definiram-se também relacionamentos entre perfis no que diz respeito ao uso dos objetos compartilhados ou na estrutura organizacional.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

#### **4.5 TECNOLOGIA DO CONTROLE DE ACESSO**

Os sistemas de reconhecimento biométrico são utilizados quase sempre visando à garantia da segurança. Atualmente, existem várias estratégias biométricas de autenticação de usuários que já estão sendo utilizadas em aplicações comerciais. De forma a tornar os sistemas mais aceitáveis e utilizáveis, deve-se tanto buscar as soluções de menor custo, de maior confiabilidade e de maior simplicidade no que se refere a seus procedimentos de utilização. Assim, esta análise mostrará as características da biometria e suas variantes, buscando apresentar seus pontos positivos e negativos, para a melhoria nos sistemas de segurança especificamente no controle de acesso.

Uma visão geral sobre os sistemas biométricos é apresentada como tecnologia baseada em medida dos seres vivos, ou seja, é a identificação de um indivíduo através de suas características físicas e comportamentais e seus principais aspectos de segurança.

##### **4.5.1 Cartões de Proximidade**

Entre os produtos de segurança eletrônica oferecido para o Sistema de Controle de Acesso estão os crachás de identificação por proximidade, que utilizam a tecnologia de identificação por radiofrequência (RFID). Estes crachás contêm um chip e uma antena. A identificação destes é transmitida para os leitores através de radiofrequência. A identificação de usuários é rápida e segura; não há contato do crachá com o leitor e a manutenção é baixíssima. Além de crachás, também existem cartões e chaveiros de proximidade.

Em complemento a esta tecnologia e solução de controle de acesso, temos os leitores de proximidade, que são usados nos ambientes controlados e são responsáveis por fazer a leitura na face oposta à do controlador de acesso.

Os diversos modelos de cartão de proximidade funcionam integrados com os seguintes sistemas:

- Controlador de acessos de pessoas em fechadura eletrônica, fechadura eletromagnética, trava elétrica, portão automático, cancela de veículos e catracas;
- Leitores de cartão de proximidade;
- Software de controle de acesso para segurança de pessoas e veículos;
- Sistema de controle de portaria para monitoramento de acessos.

##### **4.5.2 Biometria**

A natureza desenvolveu diversos mecanismos biométricos para o reconhecimento entre os seres vivos, por meios sensoriais combinados com registros em memória, os quais são hoje considerados pela ciência como habilidades de alta sofisticação que servem hoje como parâmetro de referência de crescentes pesquisas e desenvolvimento de cunho tecnológico na área de biometria.

O simples ato de identificar indivíduos diferentes, algo que até mesmo crianças são capazes de realizar, e a capacidade de afirmar que uma determinada pessoa é ou não quem afirma ser são algo que as modernas tecnologias só foram capazes de reproduzir de modo minimamente satisfatório na história recente, pois só então os dispositivos informáticos atingiram o necessário grau de processamento, armazenamento e segurança para tanto.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

Não é tarefa simples para um poderoso computador reconhecer um indivíduo, pois seu software deverá ser minuciosamente instruído a reconhecer quais elementos e parâmetros físicos e comportamentais produzem efeitos distintivos entre seres humanos, bem como o equipamento informático que deve dispor de dispositivos eletrônicos que façam a medição adequada destas características biológicas. O desafio final, talvez o maior, para estes aparatos de recepção de dados biométricos é a capacidade de resistir às deliberadas tentativas humanas de enganar estes equipamentos. A capacidade de identificação segura de um determinado sujeito é denominada como autenticidade. Existem diversos meios de autenticação, sendo o mais conhecido e ainda utilizado a assinatura autógrafa, em que, de próprio punho, o indivíduo posta sinal identificador exclusivo seu. Este meio, na verdade, também é um método de natureza biométrica, que pode ser realizado de forma manual ou automático.

#### 4.5.3 Tipos de Tecnologias Biométricas

- a) Fisiológicas ou estáticas: Essas características são traços fisiológicos, originários da carga genética do indivíduo, e essencialmente variam pouco (ou nada) ao longo do tempo. As principais características estáticas são a aparência facial, o padrão da íris, a geometria das mãos e as impressões digitais. Outras características estáticas também são utilizadas em menor grau ou estão em estágios iniciais de pesquisa, como a impressão palmar, o DNA, o formato das orelhas, o padrão vascular da retina, o odor do corpo, o padrão da arcada dentária e o padrão de calor do corpo ou de partes dele.
- b) Comportamentais ou dinâmicas: São características aprendidas ou desenvolvidas ao longo da utilização constante, e que podem variar fortemente ao longo do tempo. Além disso, podem ser facilmente alteradas pela vontade ou estado do usuário. Assim, até mesmo duas amostras consecutivas podem mudar bastante. As principais características dinâmicas utilizadas são o padrão de voz e a dinâmica da assinatura. Outras características dinâmicas também são utilizadas em menor grau ou estão em estágios iniciais de pesquisa, como dinâmica de digitação, modo de andar, movimento labial, som da assinatura, vídeo da assinatura e imagens mentais.

#### 4.5.4 Tecnologia de Reconhecimento da Voz

A autenticação por meio da voz tem sido uma área de pesquisa bastante ativa desde os anos 70. Atualmente, os sistemas podem ser divididos em classes, de acordo com o protocolo estabelecido.

#### 4.5.5 Tecnologia de Reconhecimento Facial

A aparência da face é uma característica biométrica particularmente convincente, pois é usado rotineiramente como primeiro método de reconhecimento entre pessoas. Por sua naturalidade, é a mais aceitável das biometrias. Devido a esta natureza amigável para o usuário, o reconhecimento de face surge como uma ferramenta poderosa, a despeito da existência de métodos mais confiáveis de identificação de pessoas, como impressão digital e íris.

#### 4.5.6 Tecnologia da Impressão Digital

É uma das formas de reconhecimento biométrico de menor custo, junto com o reconhecimento pela voz. Talvez seja por esse motivo que se constitui, atualmente, na técnica mais utilizada.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPPO**

#### 4.5.7 Tecnologia da Geometria da Mão

Esta técnica já é utilizada desde a década de 70. Considera-se que é baixíssima a probabilidade de que existam pessoas com a geometria da mão idêntica e que o formato da mão, a partir de uma determinada idade, não sofre alterações. Neste tipo de técnica realiza-se uma análise tridimensional do comprimento e largura da mão para que seja possível a identificação de um indivíduo. Após o reconhecimento de voz e da impressão digital, a geometria da mão é a técnica mais utilizada. Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai destas medidas um identificador matemático único na criação do modelo.

#### 4.5.8 Tecnologia da Assinatura

Nesta forma de reconhecimento biométrico, o usuário pode ter de repetir diversas vezes a sua assinatura para que o sistema possa obter um padrão médio, possibilitando o reconhecimento posterior. Este fato se constitui em um fator de inconveniência desta forma de reconhecimento biométrico. Existe outra forma de reconhecimento através da assinatura que se constitui na dinâmica da assinatura. Nesse método, o equipamento utilizado é a caneta óptica.

A assinatura pode ser off-line ou estática, aquela impostada em documentos de papel, escrita por meio convencional e posteriormente adquirida por meio de uma câmara ou scanner. Pode ser ainda on-line ou dinâmica, aquela efetuada num dispositivo eletrônico preparado para capturar, com alto grau de resolução, as características dinâmicas temporais da assinatura, como a trajetória da caneta, a pressão, direção e elevação do traço.

#### 4.5.9 Tecnologia da Retina

Pode-se dizer que é forma biométrica mais segura, ou seja, a que apresenta mais dificuldades para o acesso de um usuário não autorizado. Mesmo que uma pessoa tenha doenças graves como glaucoma, ainda assim é possível sua correta identificação. Isso é possível porque o padrão e veias da retina é a característica com maior garantia de singularidade. Não existem casos relatados de falsa rejeição ou fraudes através deste método de reconhecimento biométrico.

Justamente por este aspecto da segurança na identificação é que a análise de retina tem sido uma alternativa de grande interesse no mercado. Os analisadores de retina medem o padrão de vasos sanguíneos, usando um laser de baixa intensidade e uma câmara. O custo para a implantação deste método é alto, além do que para a captura da imagem da retina, o usuário deve olhar fixamente para um ponto infravermelho por cerca de 5 segundos, sem piscar. Algumas pessoas temem que tal operação possa causar danos à vista. Este aspecto representa uma inconveniência desta técnica.

#### 4.5.10 Tecnologia da Íris

A íris é o anel colorido que circunda a pupila do olho. Ela possui um padrão único que permite a identificação de um indivíduo. Também é uma técnica bastante segura e apresenta menor exigência na captura de imagens do que a técnica da retina. A captura da imagem é feita através de uma câmara preto e branco e a identificação da pessoa é realizada através de um scanner que realiza o mapeamento da íris. A pessoa olha a uma distância aproximada de 30cm por alguns segundos. Mesmo que esteja usando lentes de contato, o sistema realiza a identificação com segurança.

A ideia do valor da íris como fonte de informação biométrica confiável, única para cada indivíduo, veio à tona em 1965. A íris contém um rico padrão composto de fibras colágenas, rugas, sulcos, estrias, veias, sardas, fendas, buracos e cores. Embora a tecnologia biométrica de reconhecimento pelo padrão da íris seja relativamente nova, ela tem se mostrado bastante precisa e estável. Dentre poucos sistemas descritos na literatura, o mais conhecido é o IrisCode.



UNIVERSIDADE FEDERAL DA BAHIA  
SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI  
COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPPO

#### 4.6 SELEÇÃO DA TECNOLOGIA

Selecionar uma tecnologia, biométrica ou não, adequada para uma dada aplicação específica é um processo que envolve muitos fatores. A precisão é um fator importante, mas de maneira alguma é o fator mais importante. De uma maneira simplificada, fatores de seleção são extraídos dos requisitos da aplicação.

- **Avaliação de tecnologia:** A avaliação consiste em duas fases, uma fase de treinamento e uma fase de competição. A avaliação de tecnologia permite obter estimativas das taxas de erro dos comparadores. O ponto fraco desta avaliação é que apenas módulos de comparação são avaliados contra bancos de dados, sem controle do ambiente de registro;
- **Avaliação de cenário:** O objetivo da avaliação de cenário é determinar o desempenho geral do sistema numa aplicação prototipada ou simulada. Este tipo de avaliação ocorre em uma instalação especial, um ambiente de teste que simula um ambiente de produção. O ponto fraco desta avaliação fim-a-fim é que os dispositivos não são realmente atacados, o que leva a valores irreais;
- **Avaliação operacional:** O objetivo da avaliação operacional é determinar o desempenho do sistema biométrico como um todo, inserido num ambiente específico de aplicação, atuando sobre uma população-alvo específica, que dependem de características.

#### 4.7 CONCLUSÃO

A tecnologia de Controle de Acesso nas suas diversas formas (cartões de proximidade, impressão digital, face, íris, retina, entre outras) tem se mostrado eficiente no aspecto segurança. A utilização isolada de cada uma dessas técnicas não garante uma segurança absoluta. O conjunto de técnicas a ser escolhido dependerá do grau de segurança que se pretende alcançar. Uma área de pesquisa a ser mais bem explorada está relacionada ao estudo dos níveis de segurança que podem ser obtidos, considerando-se a utilização conjunta de duas ou três técnicas de reconhecimento de forma simultânea.

A identificação da tecnologia para controle da entrada de serviço para pessoas pode ser feita pela comparação do grau (alto, médio ou baixo) com que cada tecnologia satisfaz as propriedades desejáveis de características; embora resumida, ela permite obter um panorama geral dessas tecnologias.

Dentre as características biométricas apresentadas, a impressão digital e a íris são as mais estáveis ao longo do tempo. A íris pode fornecer a maior precisão, embora a impressão digital seja a mais utilizada. A tecnologia baseada no formato da mão já tem seu nicho de mercado bastante consolidado. As tecnologias de face e assinatura possuem a aceitação do usuário e são de fácil coleta. A aplicação de uma determinada tecnologia biométrica depende fortemente dos requisitos do domínio da aplicação. Nenhuma tecnologia pode superar todas as outras em todos os ambientes de operação. Assim, cada uma das tecnologias é potencialmente utilizável em seu nicho apropriado, ou seja, não existe tecnologia ótima.

Como nosso cliente pertence ao setor público, com controle de acesso diversificado para colaboradores e visitantes, a tecnologia de cartões de proximidade melhor se enquadra no custo x benefício. Aliado a esta tecnologia, onde utilizaremos os cartões de funcionários e de visitantes para o Sistema de Controle de Acesso, também utilizaremos nas catracas e salas de rede a tecnologia biométrica de impressão digital; com isso, teremos um sistema seguro, porém não tão oneroso.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

## **5 DADOS GERAIS PARA ELABORAÇÃO DO PROJETO DE SICA**

O PROJETO DE CONTROLE DE ACESSO (SICA) deverá ser elaborado por especialista da área de segurança e prever todas as infraestruturas de tubulações e pontos a serem atendidos (catracas eletrônicas, cancelas, etc.).

Este projeto deve contemplar as necessidades de controle e permissões de acesso às dependências da edificação, tratando distintamente as situações internas (informadas pela contratante) e externas, atendendo ao acesso veicular e de pessoas.

Todas as informações de acesso deverão ser armazenadas e possibilitar exportação em meio de arquivos de formato pré-estabelecido pela contratante. Deverá haver perfeita compatibilidade e integração com a rede local de dados e elétrica.

O projeto de distribuição dos pontos de Controle de Acesso (SICA) deverá ser elaborado de acordo com o projeto de arquitetura, com a locação e a quantidade necessária para garantir a total segurança de acesso à edificação, cobrindo sempre as entradas e pontos de acesso, e todas as áreas e salas que requeiram maiores cuidados com sua segurança.

Deverão ser analisadas as interferências com os demais projetos e solicitados elementos que porventura não estejam contemplados nos projetos complementares, principalmente nos projetos de arquitetura: shafts visitáveis em todos os pavimentos, sala para Racks de segurança (salas de telecomunicações ou de segurança), local para monitoramento de SICA, servidores, etc.

Todos os equipamentos e materiais utilizados nos projetos deverão ser de boa qualidade, contendo na especificação todos os elementos e dados completos, obedecendo às normas técnicas vigentes.

### **5.1 OBJETIVOS PRINCIPAIS**

- Atender à referida edificação com um sistema de Controle de Acesso que permita a máxima segurança de acesso desta edificação, bem como fornecer um sistema tecnologicamente atualizado e de última geração, permitindo ampliações futuras, e que atenda ao balanço financeiro custo x benefício, para o referido posto e área de atuação desta edificação;
- Infraestrutura física com capacidade de crescimento de 50% nos próximos anos;
- Atender aos usuários da edificação dentro das normas técnicas, utilizando-se de criatividade e bom senso;
- Manter sempre a relação custo x benefício do sistema, com facilidade de instalação e operação.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

## 5.2 NORMAS PERTINENTES

Os projetos foram elaborados em consonância com a legislação vigente sendo empregados os seguintes conjuntos de normas técnicas:

NBR 14565: Procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada.

EIA/TIA-568-B: Commercial Building Telecommunications Cabling Standard;

EIA/TIA 568-B.1: General Requirements;

EIA/TIA 568-B.2: Balanced Twisted Pair Cabling Components;

EIA/TIA 568-B.3: Optical Fiber Cabling Components Standard.

EIA/TIA 569-A: Commercial Building Standard for Telecommunication Pathways and Spaces;

EIA/TIA 606-A: Administration Standard for Telecommunications Infrastructure of Commercial Building;

EIA/TIA-607: Grounding and Bonding Requirements for Telecommunications In Commercial Buildings;

EIA/TIA TSB-67: Transmission Performance Specifications for Field Testing of Unshielded Twisted Pair Cabling Systems;

NBR ISO/IEC 17799:2001, Tecnologia da Informação – Código de Prática para Gestão da Segurança da Segurança da Informação.

## 5.3 ESPECIFICAÇÕES GERAIS

Os requisitos considerados no desenvolvimento do projeto do sistema de Controle de Acesso são aqueles estabelecidos pelas normas Técnicas vigentes, considerando para as instalações de Rede IP todas as normas técnicas para o sistema de Cabeamento Estruturado – CATEGORIA 6.

As instalações de SICA deverão ser realizadas seguindo os padrões definidos pelas normas citadas, utilizando-se dos materiais de instalação especificados e acessórios como curvas, suportes, terminações e outros que sejam adequados, não sendo aceitos componentes improvisados.

Os cabos de instalações físicas deverão ser protegidos fisicamente em toda sua extensão, utilizando-se de um ou mais materiais de instalação, não devendo em nenhuma circunstância serem instalados expostos.

Todos os materiais de instalação deverão ser firmemente fixados às estruturas de suporte, formando conjuntos mecânicos rígidos e livres de deslocamento pela simples operação.

Todas as curvas a serem utilizadas não deverão em hipótese alguma ter ângulo inferior a 90°.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

Todas as instalações de SICA deverão ser feitas com no mínimo 20cm de distância de reatores, motores, cabos condutores de eletricidade (exceto em se tratando de condutos metálicos devidamente separados, onde essa separação física garante a isolação eletromagnética desejável) e demais equipamentos, materiais ou instalações que possam gerar indução eletromagnética, o que afetaria o desempenho da transferência de imagem.

O circuito elétrico que alimenta os equipamentos ativos do sistema de SICA (Rack's, Servidores, Monitores, etc.) deve ser dedicado.

Os serviços de instalação do sistema de SICA consistem basicamente das seguintes atividades:

- Instalar eletrocalhas e/ou bandejas metálicas e acessórios;
- Instalar eletrodutos e acessórios necessários;
- Instalar caixas de passagem e/ou caixas de tomadas;
- Instalar Racks;
- Instalar equipamentos;
- Fazer a passagem dos cabos lógicos;
- Recompôr todas as partes danificadas (alvenaria, gesso ou qualquer material existente);
- Fazer a pintura das partes afetadas;
- Retirar o entulho proveniente da obra;
- Efetuar testes da instalação executada;
- Efetuar treinamento técnico do sistema ao pessoal de segurança indicado pela Edificação;
- Fazer limpeza nos locais afetados pelos serviços.

Na correta administração futura deste sistema, deve-se atentar para a identificação destas instalações com códigos e cores. Estes códigos visam a um melhor gerenciamento do sistema de cabeamento estruturado a ser implantado, proporcionando as seguintes vantagens:

- Facilidade de manutenção do cabeamento;
- Facilidade na manipulação dos patch cords nos Racks;
- Facilidade na configuração da rede;
- Identificação rápida e segura de problemas físicos nos cabos;
- Agilidade nas expansões.



**UNIVERSIDADE FEDERAL DA BAHIA**  
**SUPERINTENDÊNCIA DE MEIO AMBIENTE E INFRAESTRUTURA – SUMAI**  
**COORDENAÇÃO DE PLANEJAMENTO, PROJETOS E OBRAS – CPPO**

## **6 EQUIPE DE ELABORAÇÃO DE PROJETO / ORÇAMENTO**

Coordenação de Planejamento, Projetos e Obras / SUMAI

- Arq. Márcia Elizabeth Pinheiro (CAU A21359-4) – Coordenadora de Planejamento, Projetos e Obras
- Arq. Rosana De Leo (CAU A18234-6) – Chefe do Núcleo de Planejamento e Projetos
- Arq. Clara Soledade (CAU A85603-7) – Responsável Técnica do Anteprojeto de Arquitetura

Elaboração do Projeto do Sistema de Controle de Acesso

- Eng. José Carlos da Rocha (RNP 050093923-3) – Coordenador de Contrato
- Eng. Mayrthon Júnior (RNP 060191712-0) – Responsável Técnico do Projeto Executivo de SICA
- Eng. Igor Sá (RNP 061038361-2)