UNIVERSIDADE SÃO FRANCISCO
Engenharia Elétrica

ANTONIO TADEU GALHARDO

SISTEMAS ELETRÔNICOS DE CONTROLE DE ACESSO

Campinas
2011

ANTONIO TADEU GALHARDO – R.A. 004200500031

SISTEMAS ELETRÔNICOS DE CONTROLE DE ACESSO

Monografia apresentada ao Curso de Engenharia Elétrica – Modalidade Telecomunicações da Universidade São Francisco, como requisito Parcial para obtenção do titulo de Bacharel em Engenharia Elétrica.

Orientadora: Prof.ª Débora Meyhofer Ferreira.

Campinas
2011

ANTONIO TADEU GALHARDO

SISTEMAS ELETRÔNICOS DE CONTROLE DE ACESSO

Monografia aprovada pelo Curso de Engenharia Elétrica – Modalidade Telecomunicações da Universidade São Francisco, como requisito para obtenção do titulo de Bacharel em Engenharia Elétrica.

Data de Aprovação: ____ / ____ / ____

Banca Examinadora:

_____

Profª. Debora Meyhofer Ferreira (Orientadora)

Universidade São Francisco

_____

Profº. Dr. Geraldo Peres Caixeta (Examinador)

Universidade São Francisco

_____

Profº. João Hermes Clerici (Examinador)

Universidade São Francisco

Para minha mãe, meu irmão e à memória
do meu pai, Manoel Nelson Galhardo.

AGRADECIMENTOS

Agradeço a Prof.ª Débora Meyhofer Ferreira pela orientação do Trabalho de Conclusão de Curso e pelas aulas das outras disciplinas por ela lecionadas.

A todos os professores e funcionários da Universidade São Francisco que contribuíram direta e indiretamente para minha formação.

A todos os amigos que estudaram comigo na Universidade São Francisco.

Ao Pedro Luiz Moreno (Pedrinho), que me deu a oportunidade de trabalhar em sua empresa (2004 - 2006) e proporcionou a chance para eu aprender muito profissionalmente e também pelo aumento de salário que permitiu que eu ingressasse na Universidade São Francisco.

A empresa Security Link, empresa que trabalhei durante quatro anos, 2006 – 2010, na qual tive oportunidade de aprender muito e fazer grandes amizades, agradeço, em especial, ao Luiz Gonzaga e ao Klebber por me indicarem para trabalhar nesta empresa, ao Katayama que me deu várias oportunidades para aprender e aplicar meus conhecimentos, ao Neto pelas oportunidades, indicações e confiança em meu trabalho, Roberto e Lúcia por sempre estarem dispostos a ajudar e a Naná que é um exemplo de dedicação ao trabalho.

Ao Adalberto Santos, Helder Bertoli e Odair Negreiros da empresa Sigmacon, pela amizade e pela ajuda que recebi neste trabalho no esclarecimento dos conceitos.

Ao meu pai, Manoel N. Galhardo (15/09/1952 – 29/08/2005), por tudo que fez por mim e nesse momento, em especial, por me ensinar os valores e importância da honestidade e do trabalho. A minha mãe, Fátima, com muito amor, por tudo que faz por mim e todos os esforços feitos para permitir que eu chegasse à universidade. Ao meu irmão, Manoel, pela amizade, companheirismo e por estar sempre presente em minha vida.

Agradeço a todos meus amigos, e a todos que de alguma forma contribuíram com este trabalho.

Finalmente, agradeço e peço a Deus que abençoe minha vida, a vida de todos que estão ou estiveram presentes em minha vida e pelos que ainda virão.

RESUMO

Sistemas Eletrônicos de Controle de Acesso permitem ou restringem acesso de pessoas ou veículos a determinadas áreas com ou sem limitação de horários, além de registrar o momento do acesso ou tentativa deste. O individuo cadastrado no sistema (pessoa ou veículo) pode realizar o acesso através da identificação pessoal a qual pode ser através de cartões de proximidade, biometrias ou senhas e em caso de veículos poderá ser realizado através de leitura da placa, controle remoto, TAG ativo ou passivo. Esses sistemas são projetados para atender requisitos de segurança patrimonial e são integrados de forma informatizada através de uma rede ethernet ou serial obedecendo a uma serie de configurações lógicas de softwares, além de trabalhar em conjunto com hardwares de controle que fazem interface elétrica com dispositivos de bloqueio, tais como portas, cancelas, catracas ou portões. Sistemas de controle de acesso têm por finalidade proteger o patrimônio físico e o capital humano, além de prover registros de eventos que podem ser utilizados de forma investigativa e no controle estatístico de movimentações de pessoas ou veículos.

Palavras-chaves: Controle de acesso, identificação pessoal, biometria, proteção, patrimônio físico, capital humano.

ABSTRACT

Electronic Systems Access Control allow or restrict access of people or vehicles to certain areas with or without limitation of time, and record the time of access or attempt this. The registered with this individual (person or vehicle) can make access through the personal identification which can be through proximity cards, biometrics or passwords and if vehicles could be achieved by reading the board, remote control, active TAG or liability. These systems are designed to meet security requirements sheet and are integrated through a computerized network ethernet or serial following a series of logical configurations of software, and hardware work together to control that interface with electrical locking devices such as doors, gates, turnstiles or gates. Access control systems are designed to protect the physical assets and human capital, and provide records of events that can be used in an investigative and statistical control of movements of people or vehicles.

Keywords: access control, personal identification, biometrics, security, physical assets, human capital.

SUMÁRIO

INTRODUÇÃO

Sistemas eletrônicos de segurança são cada vez mais utilizados em residências, empresas, condomínios ou comércios. Presentes em nosso dia a dia os sistemas de câmeras (CFTV) possibilitam o monitoramento em tempo real e gravação de imagens, sistemas de alarmes detectam e notificam intrusões, cercas elétricas agem de forma mais ostensiva, pois há riscos físicos (choque elétrico) ao serem tocadas ou na tentativa de violação das mesmas. Todas estas tecnologias trabalham em conjunto com a ação humana e, em soluções mais complexas, são integradas entre si para assegurar maior proteção ao patrimônio humano e material. Além desta corrente citada anteriormente existem os Sistemas Eletrônicos de Controle de Acesso, o qual será estudado neste trabalho.

Sistemas de controle de acesso têm como objetivo principal o gerenciamento da movimentação de pessoas – funcionários, visitantes, condôminos, prestadores de serviços etc., dependendo do ambiente no qual se aplica – ou veículos dentro de áreas estratégicas das edificações.

Com a implantação de sistemas eletrônicos de controle de acesso, torna-se possível gerenciar o acesso de pessoas previamente cadastradas e identificadas por cartão de proximidade, características biométricas ou senhas às áreas sob supervisão onde seja necessário controle seletivo de entrada ou controle estatístico de movimentação.

Todos os eventos são registrados e armazenados no servidor de controle de acesso. Neste servidor também é feita toda a parametrização do sistema, estas configurações determinam as permissões e restrições dos acessos a determinadas áreas na qual o sistema foi instalado bem como a emissão de relatórios para consultas futuras das operações realizadas.

A finalidade deste trabalho é tratar o tema de forma a abranger todos seus componentes conceituais, físicos e lógicos (software e hardware) e citar um exemplo de aplicação do mesmo através de um projeto teórico de integração de sistema eletrônico de controle de acesso para liberação de pessoas a determinada área de acesso controlado.

A metodologia utilizada neste trabalho foi baseada em bibliografias voltadas para área de segurança corporativa e nos conceitos da *American Society for Industrial Security* (ASIS) para especificação dos equipamentos e dos meios de interligação entre os mesmos e, também, foram utilizados o conhecimento adquiridos durante alguns anos de trabalho no seguimento de integração de sistemas eletrônicos de segurança.

Este trabalho está dividido em 7 capítulos sendo que o Capítulo1 contextualiza o histórico e conceitos de segurança. No Capítulo 2 descreve os objetivos de se utilizar sistemas eletrônicos de controle de acesso. O Capítulo 3 aborda os recursos básicos de forma geral desses sistemas, o Capítulo 4 complementa o anterior, pois, este aborda a arquitetura de um sistema eletrônico de controle de acesso. O Capítulo 5 descreve as principais tecnologias utilizadas para identificação. No Capítulo 6 de forma suscinta cita algumas possíveis aplicações convergindo o tema para o Capitulo 7 que é exemplo de sistema eletrônico de controle de acesso que pode ser instalado em um CPD (centro de processamento de dados). E, finalmente, uma conclusão sobre o tema.

1 SISTEMAS DE CONTROLE DE ACESSO

1.1. Histórico

A partir do século XVI, com sensível aumento da criminalidade e da violência surgiram diferentes seguimentos de organizações policiais contratadas para guardar comércios, mercadorias e propriedades, realizar "rondas noturnas" e recuperar bens roubados ou furtados (MANDARINI, 2005, p.8).

No Brasil desde o período colonial até o final da República velha as milícias evoluíram para serviços orgânicos de instituições públicas e empresas privadas com ênfase na vigilância patrimonial. Em 1930, no Rio de Janeiro, foi instituída a *Guarda Noturna*, modelo de segurança que também foi adotado por outras cidades do Brasil (MANDARINI, 2005, p.9).

Mesmo com o desenvolvimento da segurança pública no Brasil, os serviços de segurança custeados com recursos particulares nunca foram completamente substituídos e sempre estiveram e continuam presentes. Porém as atividades de segurança nos moldes da que hoje existe se estabeleceu de fato, no Brasil, a partir da década de 1960 devido a prática das ações radicais de seqüestros e assaltos a bancos praticados por seguimentos políticos contrários ao regime então vigente. Impossibilitado de prover a segurança necessária o Estado além de incentivar, legislou no sentido de oficializar a *Segurança Não-pública,* autorizadas a atuar somente em agências bancárias, mas somente em 1983 foram estabelecidos os fundamentos e as exigências para a atividade pela Lei nº 7.102 de 20 de junho de 1983 (MANDARINI, 2005, p.9).

Neste contexto histórico as empresas continuaram investindo em segurança privada, a princípio no contingente humano e com a evolução tecnológica se tornou possível incrementar as barreiras físicas com recursos eletroeletrônicos que permitiram um isolamento do funcionário de segurança em relação ao ambiente externo, tornando seu ambiente de trabalho mais seguro e permitindo maior cautela para tomada de decisões, reduzindo a necessidade de confrontos diretos com o intruso garantindo maior integridade física e, muitas vezes, poupando vidas.

Os primeiros recursos eletrônicos utilizados para controle de acesso foram os interfones, instalados nas portarias de empresas e edifícios residenciais e comerciais, desta forma o porteiro seguia a norma de abrir a porta ou portão somente após o individuo se identificar verbalmente, paralelo a isso foi inventada a fechadura eletromecânica, as quais continuam sendo utilizadas, mas a principio eram acionadas por interruptores instalados nos interiores das portarias. Com o avanço das tecnologias de processamento digital de sinais e da informática foram possíveis criar diversas tecnologias em especial as tecnologias de identificação, principalmente as biométricas.

Os sistemas de controle de acesso evoluíram paralelamente com a profissionalização da segurança privada e os procedimentos de segurança corporativa. Um parâmetro possível para vislumbrar essa evolução é em áreas militares, as cancelas são manuais e sua abertura é feita por um soldado, o qual é responsável por identificar a pessoa que deseja entrar e liberar ou não o acesso e muitas vezes não há registro algum dessa ação, além do risco físico para ambos pela vulnerabilidade do possível contato físico.

Porém, mesmo com essas evoluções nos conceitos e na profissionalização da segurança privada, as novas técnicas e os sistemas modernos foram incorporados à Atividade de Segurança no Brasil especialmente a partir da criação do Plano Real, que trouxe a estabilização da moeda nacional (Plano Real criado no governo do Presidente Itamar Franco pelo então Ministro da Fazenda Fernando Henrique Cardoso, que se tornou presidente do Brasil e exerceu a presidência de 1995 - 2002).

Muitos dos produtos eram e muitos continuam sendo importados de fabricantes e distribuidores do Canadá e dos Estados Unidos. Porém com o crescimento do mercado muitas dessas empresas que se dedicavam ao desenvolvimento e produção de tecnologias para segurança eletrônica foram incorporadas a grandes empresas do ramo de produtos elétricos e eletrônicos. Um exemplo disso foi a **Pelco**, empresa norte americana com sede na cidade de Clovis no estado da Califórnia, conhecida por produzir equipamentos de altíssima qualidade para sistemas de circuito fechado de televisão que foi adquirida pela **Schneider Electric** no ano de 2007, que tornaram seus produtos mais competitivos no mercado internacional pela presença da Schneider em 130 países. Outra grande empresa que entrou no mercado foi a **General Eletric (GE)** ao adquirir duas empresas do mercado de sistemas eletrônicos para controle de acesso a **Casi-Rusco** e a **Infographics**. A **Bosch** entrou no mercado em 2003 com uma grande linha de produtos de desenvolvimento próprio.

Porém muitos desses produtos ainda possuem custo elevado devido às altas taxas para importação, porém com a abertura comercial para o mercado asiático surgiram equipamentos com qualidade aceitável e custo reduzido. Desta forma houve um crescimento do setor e surgiram muitas empresas integradoras desses sistemas. Porém, algumas empresas nacionais surgiram para desenvolver sistemas de controle de acesso, utilizando-se dos conceitos e arquiteturas dos sistemas existentes criaram sistemas de fácil operação em português e ofereceram a clientes a possibilidade de customização dos recursos dos softwares, serviço esse que empresas de produtos importados não oferecem.

Atualmente no Brasil boa parte dos sistemas de controle de acesso instalados são de fabricação nacional os quais possuem custos acessíveis, evoluíram de forma a serem competitivos em termos de qualidade com os importados alem de ser flexível a maioria das necessidades de cada

cliente. Mesmo assim algumas empresas multinacionais por possuírem acordos comerciais com outras grandes empresas exigem que o mesmo sistema seja instalado em sua matriz seja instalado em suas filiais.

A estabilidade econômica, a abertura de mercado e a evolução tecnológica, em especial das técnicas para processamento digital de sinais possibilitaram que os sistemas de controle de acesso instalados no Brasil evoluíssem. Dispositivos mecânicos como chaves e fechaduras, por exemplo, dependentes direta e exclusivamente da ação humana para seu controle evoluíram para sistemas biométricos capazes de identificar indivíduos por características físicas na maioria dos casos invisíveis para o olho humano.

Em conjunto com o desenvolvimento das redes comunicação em especial as redes ETHERNET, houve grande evolução no hardware, o que facilitou a integração dos dispositivos entre si e entre computadores o que favoreceu uma melhor interação homem máquina.

Sistemas de controle de acesso estão inseridos em todos os níveis da segurança patrimonial. por isso antes de iniciar o tema deste trabalho é necessário que sejam abordados conceitos de segurança para entender os motivos de controlar acessos.

1.2. Conceitos de Segurança Privada

Segurança pode ser definida como sendo o estado, qualidade, condição daquilo que está seguro ou isento de perigo. (MANDARINI, 2005, p.20).

A atividade de segurança privada não substitui nem concorre com a Segurança Pública apenas a complementa e atua onde a pública não possa operar normalmente, onde apresente deficiência ou onde sua ação não seja conveniente. Assim a Atividade de Segurança deve ser praticada de forma prioritária, mas não exclusiva para esfera privada dos ativos ou pessoas que se busca salvaguardar e, sem constrangimentos, explorar ao máximo a Segurança Pública disponível, sempre que possível, aconselhável ou pertinente. (MANDARINI, 2005, p.20).

A segurança privada visa proteger pessoas e ativos no ambiente que não é pertinente que a segurança pública o faça. No ambiente corporativo exige participação integrada de toda empresa em cada área e imbricada no próprio processo empresarial. Mais do que apenas tentar reduzir a ocorrência de danos isoladamente é necessário também organizar todo o esforço corporativo a ser estabelecido nesse sentido, desta forma é aberta a discussão sobre o custo que eventuais danos poderão ocasionar e os recursos necessários para mitigar as possíveis perdas resultantes, desta forma, os recursos que seriam desembolsados com eventuais perdas, que passarão a ser evitadas, são investidos em ações necessárias para evitá-las. (MANDARINI, 2005, p.21).

Toda organização funciona segundo normas de um caráter geral que orientam suas atividades administrativas e operacionais, da mesma forma as políticas de segurança devem ser estabelecidas com normas expressas e claras formalizadas em documento próprio avaliado, aprovado e apoiado pela alta gestão. Em suma a segurança corporativa trata das ações de segurança a serem tomadas no ambiente das empresas, portanto nesse ambiente há uma preocupação com a segurança das pessoas dos ativos.

Em termos de segurança ativo é todo e qualquer item que possa ser economicamente considerado, ao qual possa ser estimado um valor. Os ativos podem ser tangíveis ou intangíveis, os quais se diferenciam por:

- **Ativos tangíveis:** São os patrimônios produtivos como instalações, maquinas e equipamentos, produtos acabados, matérias primas estocadas, sistemas de informática ou patrimônios financeiros como recursos, aplicações e ações;
- **Ativos intangíveis:** São considerados intangíveis o patrimônio social e institucional, como as pessoas (recursos humanos), meio ambiente, imagem, segredos da empresa, planejamentos, estratégias, dados, conhecimentos, processos, logística, mercado marcas, fornecedores e clientes.

A segurança privada é dividida em níveis, os quais integrados entre si constituem um sistema de segurança, segundo Mandarini (2005, p. 26) esses níveis são:

- **Nível institucional (ou estratégico):** Envolve toda a empresa, porém está mais identificado com a alta administração. Neste nível são elaboradas a filosofia e políticas de segurança e definida a missão do departamento responsável;
- **Nível departamental (ou tático):** Busca a otimização dos recursos. É desenvolvido nos níveis organizacionais intermediários e estabelece os meios necessários para implantação de sistema de segurança integrado. Detalha condições, prazos e responsabilidades.
- **Nível executivo (ou técnico):** Trata da descrição técnica detalhada do sistema integrado, como também de seus equipamentos, manutenção, instalação e equipes de operação e reparos;
- **Nível operacional:** Trata do manual de operações de segurança propriamente dito, descrevendo normas, condutas, procedimentos de rotina ou emergenciais e os seus responsáveis, ou seja, define como as tarefas devem ser cumpridas.

Dentro desses conceitos são utilizados sistemas eletrônicos de segurança com o objetivo de minimizar todos os riscos ao patrimônio da instituição, sejam eles tangíveis ou não. E os sistemas de controle de acesso estão presentes nessa concepção desde o inicio das instituições nos quais as pessoas eram responsáveis diretas por esse controle, seja o porteiro permitindo alguém adentrar a

instituição ou um funcionário que porta a chave de uma área da qual é responsável ou simplesmente por conhecimentos procedimentais sabendo se pode ou não adentrar determinadas áreas.

2 OBJETIVOS DO SISTEMA DE CONTROLE DE ACESSO

Controle de acesso é compreendido pela atividade que resulta no controle de circulação de pessoas ou veículos à determinada instituição através de barreiras físicas que dificultam, retardam e controlam toda movimentação.

Os controles de acesso são geralmente agrupados em três tipos de controle: Físico, Lógico e Administrativo. As empresas necessitam desses três tipos de controles. As políticas de segurança da empresa, através da documentação dos padrões de segurança governam o uso desses controles.

Broderick cita alguns exemplos de cada tipo de controle:

- **Físico**: portas, trancas, guardas, travas de acesso a disquetes, sistemas de travamento por cabos para mesas/paredes, circuito interno de TV, retalhadora de papéis e sistemas de controle de incêndio;
- **Lógico** (Técnico): senhas, permissões para arquivos, listas de controle de acesso, privilégios de contas e sistemas de proteção de energia;
- **Administrativo**: conscientização sobre segurança, revogação de contas de usuários e políticas.

Os controles de acesso podem ser divididos em dois tipos os quais são procedimentais ou propriamente ditos.

Os *controles de acesso procedimentais* são restrições impostas por procedimento através de informações, treinamentos, ou mesmo controlado somente por alguma pessoa (segurança, porteiro, recepcionista), o reconhecimento e controle das pessoas é feito por crachás, credenciais, passes de transito livre, código de cores etc. (BRASILIANO, 2003, p.18)

Os *controles de acesso propriamente ditos* são meios que estabelecem restrições a circulação e/ou acesso. Este tipo de controle é o que nos interessa, pois nele estão contidas, em conjunto com a ação humana, barreiras físicas que restringem acesso a determinadas áreas como cancelas, catracas, portas, portões e torniquetes. Essas barreiras físicas podem ser automatizadas de tal forma utilizando-se recursos de eletrônica, eletromecânica e programas de computadores de forma que a ação humana utilizada para controle das mesmas seja reduzida a um posto de monitoramento, uma vez que a solicitação de acesso é feita com a aproximação do cartão da pessoa que deseja acessar determinada área. (BRASILIANO, 2003, p.19)

O controle de acesso é um ponto extremamente sensível na segurança, pois a exposição do perigo frente a muitas agressões pode aumentar sensivelmente caso a empresa não controle quem está adentrando suas instalações e quando, tendo acesso aos núcleos de informações e ativos corporativos.

O controle de acesso trata prioritariamente a identificação das pessoas, veículos e objetos verificando suas autorizações de entrada e saída nas áreas controladas. Os projetos desses sistemas devem seguir alguns critérios básicos para atender seus objetivos, dentre os quais se destacam:

- **Definir os perímetros de controle:** Os perímetros são espaços internos, as áreas das edificações, incluindo o limite periférico, que podem ter todas suas conexões controladas. Como exemplo pode ser citado salas com as suas portas, as salas são o perímetro de controle e as portas suas conexões controladas. Outro exemplo seria o muro ou alambrado com a portaria de uma empresa, onde toda área murada é o perímetro de controle e a portaria dotada de dispositivos de bloqueio (portões, cancelas e catracas) é a conexão controlada.
- **Definir os critérios de verificação:** São os parâmetros estabelecidos para as pessoas, veículos ou objetos pelos quais o sistema permitirá ou não a entrada ou saída no perímetro de controle. Os critérios de verificação é a forma de identificação do individuo ao sistema de controle de acesso, seja uma senha, cartão ou características biométricas. Os critérios de verificam estão contidos nas tecnologias existentes e são considerados os parâmetros mais importantes no controle de acesso, pois é o que difere os indivíduos no sistema e serão abordados com mais detalhes mais adiante neste trabalho.
- **Registros de todos os eventos decorrentes destas atividades;**
- **Armazenar e disponibilizar os eventos para auditoria.**

Os sistemas de controle de acesso podem ser classificados em manuais, semi automáticos e automáticos a escolha de cada um é feita de acordo com as necessidades e valores disponíveis para investimentos.

- **Sistemas manuais** são controlados direta e exclusivamente pela ação humana (porteiros e recepcionistas), seu funcionamento é operacionalizado pela simples verificação da identidade da pessoa que requer acesso e sua respectiva autorização. O controle é feito visualmente, como por exemplo, a identificação de crachá. Este é o mais simples e vulnerável sistema de controle de acesso, pois como é diretamente operado pelo recurso humano, que tem maior chance de cometer erros, além de enfrentar conflitos com usuários da empresa ou instituição. (BRASILIANO, 2003, p.34)

- **Sistemas Semi Automáticos** integram o recurso humano com a tecnologia. Geralmente esses sistemas selecionam o acesso por meio de um interfone e/ou porteiro eletrônico, supervisionados ou não por circuito interno de televisão, sendo a autorização liberada se as condições de acesso forem preenchidas. Neste caso são estipuladas senhas e contra senha, ou verificação através de câmeras, as empresas que optam por esse tipo de sistema orienta que a pessoa responsável pela liberação do controle de acesso observe crachás, uniforme adesivos que identificam veículos, por exemplo. O erro mais comum é o desleixo na identificação o que torna o sistema completamente burocrático e as pessoas o consideram como mais um "empecilho" da segurança, para atrapalhar a circulação dos usuários; (BRASILIANO, 2003, p.35)
- **Sistemas Automáticos** independem da ação humana para identificar e autorizar o acesso ao interior das instalações. Este é o sistema que será tratado neste trabalho. Todos os eventos são registrados e armazenados no servidor do sistema de controle de acesso, o que é uma grande vantagem, pois não depende da ação humana para que esses registros sejam feitos. Os sistemas automáticos utilizam como meios de identificação para liberação ou restrição do acesso teclados para digitação de senha, cartões de códigos de barras ou proximidade (RFID), TAG (RFID) para identificação de veículos, leitores de características biométricas e bloqueios como cancelas, catracas e portas, essas tecnologias de identificação serão abordadas com mais detalhes em outro tópico deste trabalho. (BRASILIANO, 2003, p.37).

Um sistema projetado com todas essas funcionalidades em conjunto com uma política de segurança clara e funcional irá atender os objetivos dos controles de acessos julgados necessários pela segurança corporativa da empresa.

O diagrama abaixo ilustra os níveis de controle de acesso nas empresas começando pelas portarias até áreas específicas, a partir dela serão citados exemplos de aplicação dos sistemas de

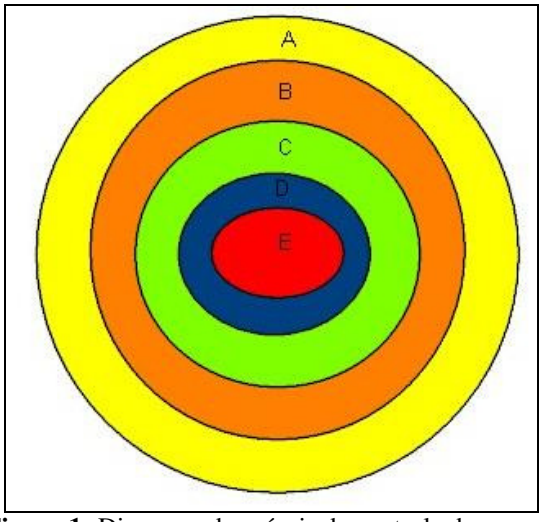

Figura 1: Diagrama dos níveis de controle de acesso.

Cada um dos níveis apresentados no diagrama acima proporciona uma etapa do controle de acesso e podem ser representadas da seguinte forma:

A) A camada *A* pode ser representada pelo local de chegada das pessoas ou veículos, ou seja, as portarias, que mais do que controlar acesso tem a função de orientar e direcionar as pessoas para as áreas desejadas ou para recepção, para que esta o faça. A partir dessa área se começam os controles procedimentais, ou seja, a partir dessa área todas as atividades devem se sujeitar as regras de segurança da instituição. A continuidade do fluxo é uma das principais preocupações por principalmente nos horários entrada e saída de funcionários, por isso os procedimentos nessa área devem ser rápidos e precisos. Normalmente essas áreas utilizam dispositivos de bloqueio como catracas e cancelas para restringir e registrar, principalmente os horários de entradas e de saídas.

B) A camada *B* pode ser representada pela recepção da empresa, pois a partir dessa área há direcionamento para os setores, seja por acesso as escadarias, elevadores ou diretamente aos corredores que levam aos departamentos. Para o caso de visitantes, nesta camada os dados dos mesmos são confirmados e sua chega é comunicada ao responsável pela visita. Nesta área é comum a utilização de catracas como dispositivos de bloqueios.

C) A camada *C* pode ser representada pelo caminho que direciona as pessoas aos departamentos da empresa, os quais podem ser compostos por escadarias, elevadores e corredores. Na maioria dos casos os dispositivos de bloqueio utilizados são portas muitas vezes sem sistema eletrônico de controle para facilitar a integração entre os departamentos;

D) A camada *D* são as áreas internas aos departamentos, dependendo do departamento das políticas da empresa circulação de pessoas nesta área é restrita somente a funcionários deste setor, caso haja algum terceiro este deve estar acompanhado de algum funcionário da área.

E) A camada *E* é representada pelas áreas especificas. Essas áreas são de competência de algum departamento e pode estar contida em um espaço segregado dentro do departamento ou até mesmo em alguma área fora deste. O acesso as áreas especificas muitas vezes é permitido somente a alguns funcionários de determinado departamento, por exemplo, o acesso ao CPD é permitido somente aos funcionários de TI, ou ainda somente ao funcionário de Ti responsável pelos servidores.

A partir disso é possível notar que o controle de acesso fica melhor concebido não só com a utilização de barreiras físicas, mas também com políticas procedimentais que dividem os departamentos e suas responsabilidades individuais em relação ao acesso as suas áreas mais restritas.

3 RECURSOS DOS SISTEMAS DE CONTROLE DE ACESSO

Os sistemas eletrônicos de controle de acesso são implementados através de uma integração entre software e hardware. Todos os parâmetros do sistema são configurados nos software e o hardware fica responsável para fazer a comunicação do meio de identificação utilizado com o software e também para fazer o chaveamento do dispositivo de bloqueio por ele controlado.

Os softwares de gerenciamento de controle de acesso devem possuir basicamente os seguintes recursos:

- Permitir o controle de acesso de pessoas que utilizam o sistema freqüentemente, funcionários de uma empresa por exemplo e visitantes e tratar essas informações de forma independente;
- Permitir configuração zonas, as quais são o conjunto de áreas delimitadas por bloqueios físicos que restringem e controlam o acesso. Pode-se atribuir direito de acesso a todas as áreas de uma zona ou somente a uma ou algumas delas;
- Permitir configuração de tabelas de horários, dias da semana e feriados criadas para que os acessos sejam restritos ou permitidos somente em alguma faixa horária e/ou dias da semana e feriados, associado à zona permite um controle mais rigoroso do acesso;
- Permitir que a associação das tabelas de áreas e horários seja associada para cada pessoa ou grupo de pessoas que terão que obedecer às mesmas políticas de segurança. A associação das tabelas forma um conceito denominado direitos de acesso. As definições dos direitos de acesso são feitas em conjunto entre as gerencias dos diversos departamentos e da gestão de segurança patrimonial, em muitas empresas a gestão de segurança é feita pelo departamento de recursos humanos. Reúne-se a gerencia de todas as áreas, pois o controle de acesso,

muitas vezes, não é aplicado somente pela segurança patrimonial, mas sim também pela segurança do trabalho.

- Armazenar todos os eventos do sistema, tanto os de acessos autorizados quanto os de acessos negados, para possibilitar consultas futuras;
- É possível no cadastro das pessoas inserirem informações de departamento, empresa e categoria;
- Permite emissão de relatórios e importação dos mesmos em diversos formatos, como arquivos texto, planilhas e pdf, por exemplo, para facilitar a análise dos mesmos.
- Monitoramento em tempo real dos eventos de acesso que estejam ocorrendo, esses eventos pode alertar o operador do sistema de que uma pessoa não autorizada está tentando acessar a uma área na qual não tem permissão e também informa ao operador se algum dispositivo de bloqueio permanece aberto por mais tempo que o necessário.

Da mesma forma que os softwares de gerenciamento precisam ter alguns recursos o hardware deve atender alguns requisitos básicos para possibilitar um bom projeto. Desses aspectos básicos se destacam:

- Possuir interface de comunicação serial ou ethernet – as interfaces seriais estão deixando de ser utilizadas por possuir muitas particularidades na sua implementação, como limitações de distância, as interfaces ethernet que utilizam protocolo TCP/IP estão substituindo as seriais pela facilidade de configuração e por muitas vezes permitir o aproveitamento de infraestrutura da rede existente, o que facilita e reduz custos de instalação do sistema;
- Permitir memória interna para armazenamento das listas de cartões e tabelas do sistema para eventual falha de comunicação com o servidor;
- Possuir entrada para conexão de sensores que notificarão o sistema de que houve passagem pelo dispositivo de bloqueio ou mesmo que o dispositivo de bloqueio está aberto por mais tempo do que necessário;
- Entrada para conexão de sinais que indicam emergência como dispositivos de quebra de vidro para liberação do dispositivo de bloqueio;
- Possuir saídas de contato seco, ou seja, relés para que possam ser adaptadas a diferentes dispositivos de bloqueio;
- Possuir entrada para identificadores preferencialmente no protocolo *Wiegand,* o qual funciona com praticamente todos leitores RFID e biométricos.

Integrando os recursos de software e hardware é possível projetar sistemas de controle de acesso Conforme que podem ser instalados em diferentes áreas segregadas entre si por algum dispositivo de bloqueio os quais podem ser portas, cancelas, catracas ou portões.

Na prática esses sistemas são muito utilizados em empresas e condomínios com objetivos distintos.

Em condomínios são utilizados para registro do horário de entrada e saída de condôminos e para controle da entrada de visitantes de forma que essas pessoas devam se identificar na portaria para que o funcionário da portaria verifique com a pessoa que receberá a visita se pode permitir a entrada do visitante.

Em empresas esses sistemas são utilizados também em portarias e recepções com o mesmo objetivo dos condomínios, porém suas principais aplicações são em áreas nas quais se fazem necessários a segurança da informação e de bens, ou seja, os ativos tangíveis e intangíveis.

4 ARQUITETURA DOS SISTEMAS ELETRÔNICOS DE CONTROLE DE ACESSO

Existem muitos fabricantes de software e hardware para sistemas de controle de acesso, dos quais, a grande maioria possibilitam que os sistemas instalados atendam os critérios citados anteriormente, desta forma independente do fabricante escolhido há uma arquitetura básica necessária para implementação do sistema, a qual pode ser representada pela Figura 2.

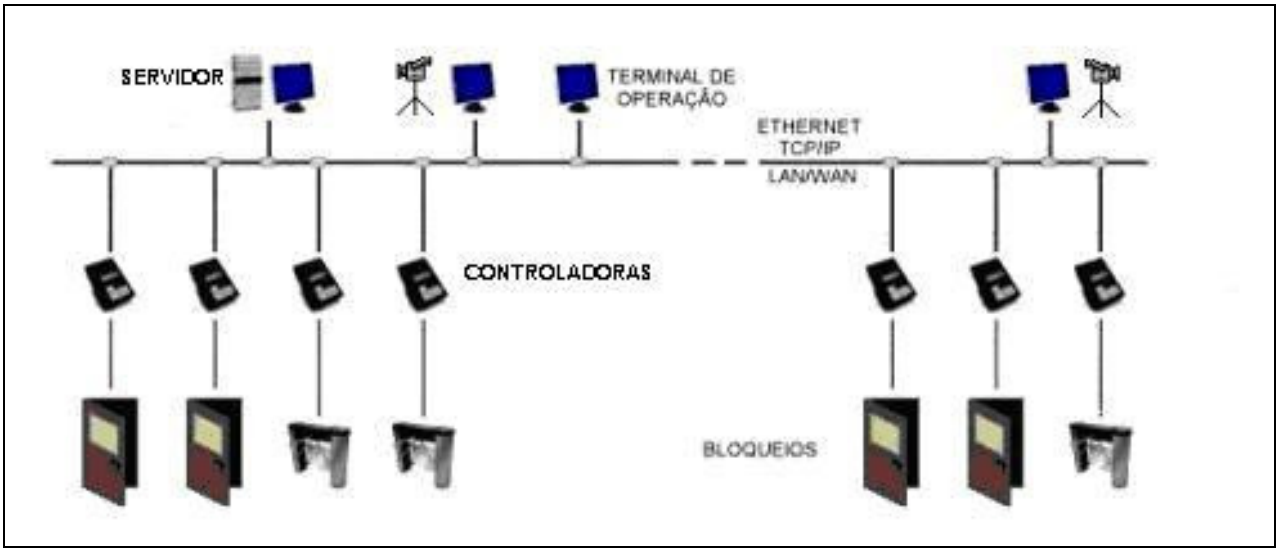

Figura 2: Arquitetura Básica De sistemas de Controle de Acesso.

Note na figura que o sistema é composto por servidor, rede ethernet, terminais de operação, controladoras, bloqueios e identificadores. Todos esses elementos são integrados entre si de forma que a identificação chegue ao servidor e este "responda" se o acesso será ou não permitido. Os próximos tópicos deste capítulo descrevem cada um desses elementos.

4.1. Servidor

O servidor é um computador na qual são instalados banco de dados e o módulo principal do software de gerenciamento do sistema. Neste elemento são armazenas todas as informações como configurações de parâmetros do sistema e de conexão com o banco de dados e serviços instalados no sistema operacional para executar as tarefas de comunicação do software entre os terminais e as controladoras. O servidor do sistema fica em local com acesso físico restrito normalmente no CPD ou na central de segurança.

4.2.Terminal

O terminal é um computador na qual é instalado o aplicativo de operação do software. Neste aplicativo é possível ter acesso a todas as funções de configuração e operação do sistema, porém, todo acesso a essas funções é configurado de acordo com a atribuição de cada operador, alguns tem acesso somente a cadastro de pessoas, outros cadastros de pessoas e emissão de relatórios e outros acesso a todas as funções (administrador do sistema). Mas corriqueiramente a função deste elemento é cadastrar pessoas e emissão de relatórios. Na maioria dos softwares de controle de acesso as licenças dos terminais são compradas de forma unitária, porém na maioria dos casos são adquiridas duas licenças sendo uma na portaria e outra na recepção.

4.3.Câmera tipo Webcam

Utilizada para fotografar a pessoa e/ou documento, essa imagem é associada ao documento da pessoa no banco de dados e facilita muito a identificação física das pessoas.

4.4.Controladora

Este módulo é o responsável pelo gerenciamento do controle de acesso propriamente dito. Recebem do servidor os dados necessários tais como listas de cartões, áreas habilitadas, feriados e outros. Gerencia as solicitações de acesso dos leitores, verifica as restrições e autoriza ou nega o acesso conforme o caso. Todos os eventos detectados nos módulos são informados ao servidor e são armazenados no banco de dados. Possui interfaces para a conexão de leitores de cartões ou identificadores biométricos, saídas de relé para comandar a liberação dos bloqueios e entradas de sinal para confirmação de passagem pelo bloqueio.

4.5.Identificadores

Os identificadores são definidos como a tecnologia utilizada para identificação da pessoa ao sistema. Podem ser utilizados teclados para digitação de senhas, leitores de cartões (RFID ou código de barras), leitores biométricos (identificação de impressões digitais, geometria da mão, reconhecimento facial dentre outros).

4.6.Bloqueios

São as barreiras físicas utilizadas para segregar as áreas controladas das de uso comum, ou seja, é o meio de conexão do individuo (pessoa ou veículo) as áreas de acesso restrito. Vários dispositivos de bloqueio podem ser controlados por sistemas eletrônicos de controle de acesso, pois praticamente todos são chaveados por contato eletromecânico seja por um simples pulso de contato seco ou por chaveamento de um dos fios que alimentam o dispositivo, são exemplos de dispositivos de bloqueios portas, portões, cancelas, catracas dentre outros.

4.7.Meios de Interconexão

É o meio físico que permite a comunicação entre os elementos do sistema. No inicio a comunicação entre o servidor e as placas controladoras eram feita através de comunicação serial, com o avanço tecnológico e também como tendência de mercado a tecnologia de comunicação das placas controladoras convergiram para o padrão ETHERNET com protocolo TCP/IP, ainda assim alguns fabricantes constroem as placas controladoras de forma que funcionem tanto em uma rede TCP/IP quando em rede serial (RS 232 ou RS 485).

As redes seriais para comunicação possuíam diversos empecilhos que algumas vezes inviabilizam a instalação ou ampliação do sistema, pois os cabos utilizados para esse tipo de rede (cabo tipo belden, cabo AFT ou cabo manga) têm custo elevado, além do que a comunicação RS 232 tem limitação de 15 metros, a RS 485 1.200 metros, porém sua utilização era limitada em relação a quantidade de controladoras que podiam ser conectadas na rede, normalmente 32 controladoras. Além de serem extremamente sensíveis a interferências eletromagnéticas. Esses fatores também dificultavam a integração dos sistemas de controle de acesso entre todas as unidades da mesma empresa. Este tipo de rede possui custo elevado pois é uma rede construída para atender de forma dedicada um único sistema, não podendo ser aproveitada para outros fins.

A arquitetura apresentada na Figura 2 mostra a vantagem de utilizar equipamentos que permitem conexão via rede TCP/IP, pois o sistema pode ser operado remotamente e também pode gerenciar dispositivos instalados em localidades diferentes do local onde está instalado o servidor do sistema. O sistema também é muito versátil, pois permite controle e acesso remoto a todos os tipos de bloqueios citados como exemplo neste trabalho.

Outra vantagem da conexão via rede TCP/IP é a possibilidade de utilizar a rede existente. Isso facilita a instalação do projeto e reduzir custos.

É possível observar na Figura 2 que há conexão física entre os componentes do sistema. Essas conexões são feitas por cabos metálicos, sendo que para cada uma delas é utilizado um cabo diferente. Na maioria dos casos para conectar o servidor, terminais e controladoras através de rede ethernet TCP/IP é utilizado cabo UTP categoria 5 na maioria dos casos pois esse cabo permite a transmissão de até 100 Mbps a uma distancia de até 100 metros. Para distâncias superiores são esta conexão é feita através de fibra ótica.

Para conectar os identificadores a controladora é utilizado, por recomendação dos fabricantes, cabo manga blindado 6x26 AWG para distancias de até 15 metros, desta forma conecta-se a malha do cabo ao aterramento para proteger os condutores e conseqüentemente o sinal de interferências eletromagnéticas, dos 6 condutores disponíveis são utilizados somente 5, sendo 2 para alimentação (+12 Vdc e GND), dois para comunicação (data 0 e data 1) e um para sinalização de acesso valido (o led do leitor fica verde e também tem opção de emitir aviso sonoro), um fica de reserva.

A alimentação das controladoras e das fechaduras é de 12 Volts de corrente continua, e utiliza-se cabo paralelo flexível de 0,75 mm. Atualmente existem placas controladoras alimentadas utilizando a tecnologia POE (*Power over Ethernet*). Porém o valor do projeto final fica elevado, pois além da controladora ter valor superior a uma controladora convencional, os demais elementos de rede, os switches, também possuem valor elevado comparados aos de uso comum.

5 TECNOLOGIAS EXISTENTES

Com os conceitos abordados anteriormente, independente da tecnologia utilizada e do fabricante, basicamente todos os sistemas eletrônicos de controle de acesso devem ter por função identificar e permitir ou negar acesso de pessoas, veículos e objetos em uma empresa utilizando critérios pré- configurados de locais e horários, registrando todos os eventos relativos a esta atividade, que visa segurança pela prevenção e proteção dos riscos que podem afetar pessoas, bens e instalações. (BRASILIANO, 2003, p.44).

As funções dos sistemas eletrônicos de controle de acesso são configuradas e gerenciadas por software o qual opera em conjunto com uma placa controladora que faz a interface entre o método de identificação e o software e o dispositivo de bloqueio a ser controlado.Com isso a tecnologia que difere os sistemas eletrônicos de controle de acesso é a forma de coleta da identificação das pessoas ou veículos e os dispositivos de bloqueio utilizados como barreiras físicas.

Este capítulo será divido em duas partes, sendo que a primeira descreve os dispositivos de bloqueio e a segunda as tecnologias de identificação.

5.1.Dispositivos de Bloqueio

Conforme capítulo anterior, dispositivos de bloqueios pode ser definido como sendo as barreiras físicas utilizadas para segregar as áreas controladas das de uso comum. Os dispositivos são escolhidos de acordo com a área que se deseja segredar e em relação ao que se deseja controlar acesso, pessoas ou veículos. Vários dispositivos de bloqueio podem ser controlados por sistemas eletrônicos de controle de acesso, pois praticamente todos ao serem automatizados são acionados por um pulso de contato seco ou pelo chaveamento da alimentação do dispositivo. Os dispositivos de bloqueios mais utilizados em conjunto com sistemas eletrônicos de controle de acesso são as cancelas, catracas, portas, portões e portais, os quais serão abordados a seguir.

5.1.1. Cancelas Automáticas

As cancelas são dispositivos utilizados para controlar locais onde há um grande fluxo de veículos, como portarias de condomínios e empresas, estacionamentos e pedágios, substitui os portões nesses casos, pois libera o fluxo com rapidez. As cancelas são acionadas por um pulso de contato seco, desta forma qualquer hardware de controle de acesso pode ser integrado a cancelas. Devido a vulnerabilidade é aconselhável que se utilize meios de vigilância em conjunto, como sistemas de circuito fechado de televisão, permitindo o monitoramento das imagens em tempo real

e, se necessário, a reprodução dessas imagens para análise futura dos eventos. A Figura 3 abaixo ilustra um diagrama de cancelas em um sistema de controle de acesso.

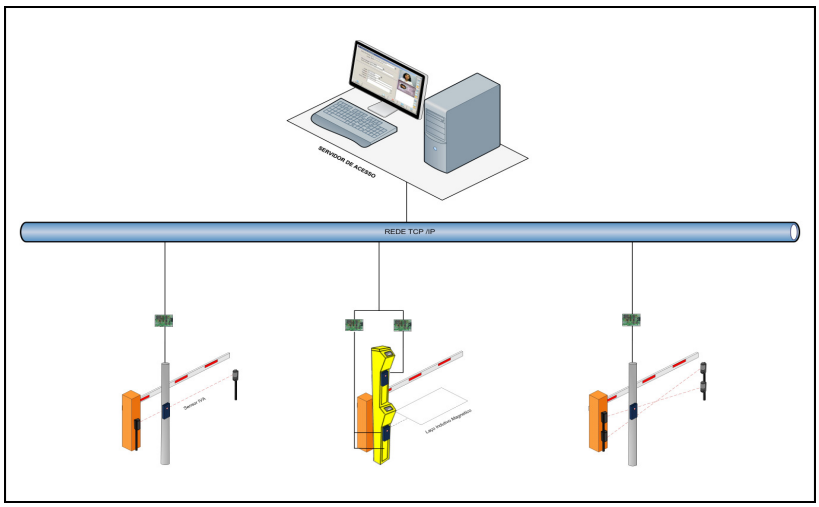

Figura 3: Cancelas em um sistema de controle de acesso.

5.1.2. Catracas Eletrônicas

As catracas são dispositivos eletromecânicos utilizados para controle de passagem de pessoas. São normalmente instaladas em recepções, por não haver necessidade de dividir o ambiente com paredes e portas para restringir a passagem. A vantagem é que por seu controle ser giratório permite que passe uma pessoa por vez evitando que uma pessoa não autorizada aproveite a passagem da pessoa anterior. Normalmente requerem uma atividade anterior como o cadastramento dos visitantes e cadastramento dos funcionários. A Figura 4 ilustra algumas catracas em um sistema de controle de acesso:

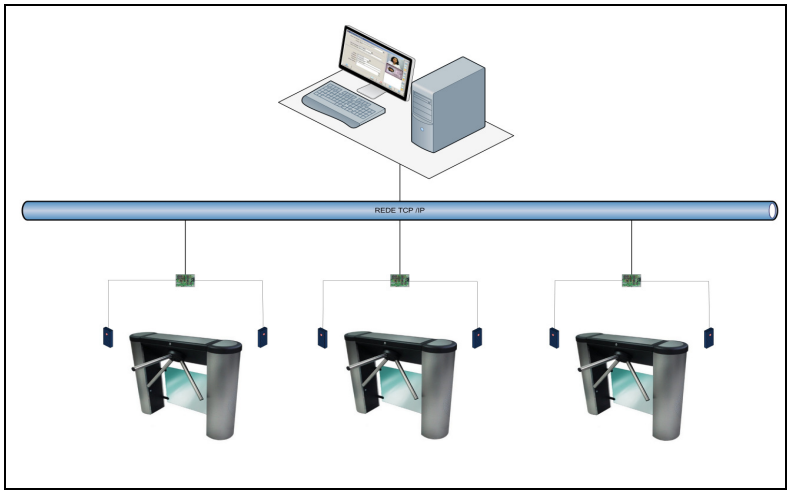

Figura 4: Catracas em um sistema de controle de acesso.

5.1.3. Portas, portões e portais

São muito utilizadas para separar ambientes que necessitem de mais segurança, e será utilizado como exemplo de aplicação neste trabalho. Para que uma porta funcione em um sistema de controle de acesso é instalada uma fechadura eletromagnética para substituir a fechadura existente ou para funcionar em conjunto com a mesma como redundância de segurança. O tipo de porta é projetado de acordo com a área na qual será instalada, os diversos sistemas podem utilizar portas duplas formando uma eclusa na qual uma só pode ser aberta com a outra fechada, as portas também podem ser giratórias para que passe somente uma pessoa por vez e ainda portais com detectores de metais. A Figura 5 mostra o diagrama de duas portas em um sistema de controle acesso.

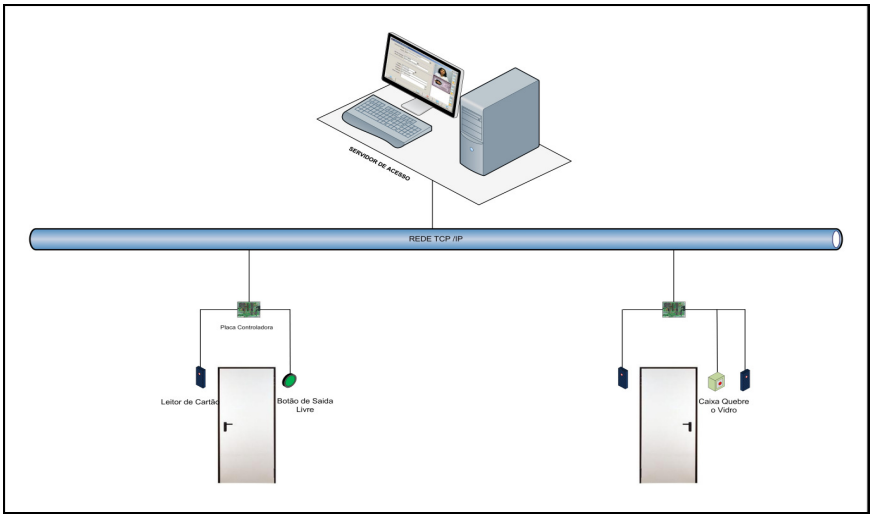

Figura 5: Portas em um sistema de controle de acesso.

5.2.Tecnologias de Identificação

Obviamente os meios de identificação não funcionam de forma isolada, porém é o fator que determina o nível de segurança do sistema e também o custo de implantação do mesmo.

Existem diversas formas de identificação dos indivíduos a um sistema de controle de acesso, porém a escolha da tecnologia utilizada é feita baseada no nível de segurança que se deseja ter no sistema, na área que se deseja implementar controle pois devem ser levadas em considerações as condições físicas do ambiente e a disponibilidade de recursos financeiros para investimentos no sistema. Os critérios de verificação da identificação se resumem em:

- **Algo que só o individuo sabe** que são as senhas numéricas ou alfanuméricas;

- **Algo que só o individuo possui**, ou seja, objetos físicos únicos como de acesso que autorizam o portador, pessoa, veiculo ou objeto a obter o acesso requisitado, como, por exemplo, chaves ou cartões para pessoas, e TAGs ou controles para veículos.
- **Algo que só o individuo é** são características biométricas dos seres humanos que os identificam para os sistemas de controle de acesso.

Existem equipamentos dedicados para cada uma dessas tecnologias de identificação, sendo que todas possuem vantagens e desvantagens e serão descritas em seguida e resumida adiante na tabela 1.

5.2.1. Teclados

Os sistemas com teclados permitem o acesso da pessoa a partir da correta digitação da senha desta forma o dispositivo de bloqueio é liberado. A desvantagem deste sistema é a grande facilidade para copiar a senha e com o tempo o desgaste do teclado facilitará a descoberta das senhas pelas teclas que ficam visivelmente mais desgastadas. Isso não impede que um individuo forneça sua senha para outro, desta forma não há garantia de quem ingressou porém são registrados data e horário dos acessos.

Os sistemas com teclados são indicados somente para áreas com pouco fluxo de pessoas e em áreas restritas. A figura abaixo ilustra um teclado utilizado em sistemas de controle de acesso. O usuário digita uma senha para ter acesso o nível de controle é baixo, pois senha pode ser divulgada. Pouquíssimo usado em segurança, devido à sua fragilidade.

Figura 6: Teclado

5.2.2. CARTÕES

Os cartões são sistemas bastante empregados pelo baixo custo e pela variedade de possibilidades que oferecem os softwares que lhes dão suporte. Podem ser de memória de contato ou de proximidade, para leitura de código de barras ou tarjas magnéticas, sendo que os dois últimos estão deixando de ser utilizados pela quantidade de problemas e pela facilidade de cópia dos cartões, devido a isso não serão abordados nesse trabalho.

Os cartões de proximidade possuem um protocolo de codificação chamado *Wiegand* o qual permite codificação dos cartões em 26 ou 32 bits o que torna praticamente impossível a incidência de cartões repetidos e a cópia de cartões é impossível.

Os cartões de proximidade utilização tecnologia de identificação por rádio freqüência (RFID). Esses cartões podem ser ativos ou passivos.

Os cartões de proximidade passivos possuem um circuito constituído de bobina entre o substrato plástico que dá a forma do cartão, essa bobina é excitada quando aproximada do leitor o qual emite um campo eletromagnético, no mesmo leitor há um receptor que capta o sinal emitido pelo cartão e o envia para placa controladora.

Os cartões ativos de proximidade possuem uma bateria interna para alimentação de seu circuito o qual emite um sinal sem necessidade de estar muito próximo ao leitor, um exemplo de aplicação dos cartões ativos é o serviço de “Sem Parar” oferecidos nos pedágios por suas concessionárias.

Para leitura dos cartões é necessário que sejam instalados leitores em locais estratégicos próximos as áreas de conexão, ou seja, próximo das portas, catracas ou para o caso de veículos ao alcance do motorista. Os leitores são conectados as placas controladoras do sistema os quais farão a interface com o servidor de sistema.

Os leitores conseguem coletar o código dos cartões passivos a uma distancia que varia de 10 a 70 centímetros, dependendo do modelo de leitor, quando maior o alcance maior o custo do mesmo.

Os cartões de proximidade são extremamente seguros, sendo quase impossível copiá-los. Considerando sua durabilidade seu custo pode ser considerado médio. A Figura 7 mostra um exemplo de leitor e cartão de proximidade.

Figura 7: Leitor e Cartão de Proximidade

Este meio de identificação possui um bom nível de segurança. As leitoras de proximidade são especificadas de acordo com a distância máxima admissível para que elas reconheçam o cartão. Uma observação importante em relação aos sistemas que utilizam cartões de proximidade, que pode ser considerada uma desvantagem, é que os cartões de um fabricante não funcionam com leitores de outro e vice versa. Outra desvantagem é que podem ser utilizados por pessoas não autorizadas, seja por extravio, perda, roubo ou furto.

5.2.3. Biometria

É estudo estatístico das características físicas ou comportamentais dos seres vivos. Recentemente este termo também foi associado às pessoas como forma de identificá-las unicamente. Hoje é usada na identificação criminal, controle de ponto, controle de acesso, etc. Como dito anteriormente o reconhecimento do individuo será dado por características físicas do mesmo. Foram criadas leitoras biométricas para aplicações em indústrias, empresas e condomínios, para restringir o acesso de pessoas não autorizadas ao estabelecimento, e ate controlar horários de funcionários com forma de marcar o ponto.

O controle biométrico é extremamente confiável, pois sua estrutura básica consiste no registro de certas características físicas ou comportamentais de cada pessoa, que são comparadas a um arquivo armazenado em seu banco de dados. Esses sistemas se tornaram possíveis com a evolução das técnicas de processamento digital de sinais, utilizando essas técnicas as características são amostradas, digitalizadas e armazenadas em um banco de dados associada a um código. (BRASILIANO, 2003, p.47).

O custo dos equipamentos que permitem registro e leitura de características biométricas é muito alto se comparado aos anteriores, por isso são utilizados somente em áreas consideradas de alta segurança ou de alto risco. (BRASILIANO, 2003, p.48)

Os principais sistemas biométricos existentes são:

- **Geometria da mão:** Este sistema, também chamado de *Hand Key,* utiliza características das mãos. Reconhecem a geometria da mão, analisando comprimento e largura dos dedos, e a área da mão. A certeza na forma de identificar um individuo por este sistema, é pelo fato que 2 pessoas não possuem a geometria de suas mãos iguais. Consiste na utilização de imagens da geometria da mão, palma e dedos por *scanners*, para identificar as pessoas. Armazenam comprimento físico das características coletadas e alguns sinais particulares, como cicatrizes por exemplo. Para realizar acesso, o usuário posiciona sua mão no leitor o qual faz uma comparação entre a leitura realizada e os dados armazenados em seu banco de dados, caso as condições sejam satisfeitas o sistema libera o acesso. É um sistema muito confiável, porém, alem do custo elevado, não pode ser instalado em ambientes externos que tenham incidência de luz solar, pois utiliza pequenos espelhos para realizar leituras das mãos e formar a imagem que será armazenada. A Figura 8 ilustra este tipo de leitor. Observe que na imagem a pessoa está utilizando um anel, se esta pessoa não foi cadastra com esse anel, o sistema não irá liberar seu acesso, pois houve alteração na imagem armazenada, por isso é recomendado que ao fazer cadastro não sejam utilizados adornos, caso isso não seja acatado é necessário que a pessoa não utilize adornos diferentes do qual utilizou quando cadastrada.

Figura 8: Leitor de Geometria das Mãos

Impressões digitais: O reconhecimento de impressões digitais tem sido empregado historicamente principalmente por órgãos de investigação, porém o processo era todo manual, deixando-o lento e a cargo da perícia e acuracidade de cada investigador. Uma grande demanda por softwares de reconhecimento automático aliados ao crescente poder computacional levou órgãos como FBI e Nasa a investirem pesado neste tipo de tecnologia de reconhecimento. (BRASILIANO, 2003, p.52)

Hoje em dia o reconhecimento de impressões digitais está relacionado tanto com a investigação criminal como autenticação em tempo real. No cenário criminal, softwares conhecidos como AFIS (“Automated Fingerprint Identification System”) utilizam grandes bancos de dados,

com imagens completas de impressões digitais visando uma posterior identificação de pistas deixadas na cena de um crime.

Já na autenticação em tempo real são utilizadas técnicas mais leves e denominadas *Finger Scan*, onde não são aplicadas comparações de imagens completas, mas sim um reconhecimento de padrões onde é gerado um modelo a partir da imagem inicial. Essas 15 técnicas devem levar em conta a precisão exigida, possibilidade de erros e requisitos de desempenho.

Figura 9: Leitores de Digitais.

Dentre as principais técnicas de captura de imagens destacam-se três principais:

- **Ótica**: mais usado e mais antigo método. Apresenta problemas de restos de impressões de indivíduos anteriores, porém a qualidade é bastante aceitável e possui hardware de baixo custo.
- **Chips de Silício**: em geral possui uma melhor definição do que as amostras tiradas pelos dispositivos óticos e baseiam-se num chip de silício que utiliza sinais elétricos para a formação da imagem. Usado em celulares e laptops graças ao tamanho reduzido, sendo ainda uma tecnologia cara.
- **Ultra-som**: pode-se dizer que é a tecnologia mais precisa em se tratando de captura de impressões digitais, pois gera imagens de alta definição mesmo em condições adversas (sujeiras) devido à formação da imagem estar baseada em cálculos de distâncias levando em consideração a impedância da pele, o ar e o próprio equipamento.

- **Leitura da Retina ou Iris:** Escaneiam a íris ou retina. No caso de mapeamento de retina a identificação do individuo é feita pelo escaneamento dos vasos sanguíneos do globo ocular. Já o mapeamento da íris se baseia sobre os anéis coloridos em torno da pupila. A identificação pela íris é extremamente precisa, pois esta não sofre alterações pelo tempo ou por lesões. Estes métodos de identificação são os mais precisos, mas possuem a desvantagem de ter altíssimo custo e grande desconforto no momento da leitura e é um equipamento que precisa ser sempre higienizado para evitar que haja contaminações de algumas doenças como conjuntivite, por exemplo. A figura 10 ilustra estes leitores.

Figura 10: Leitores de íris e retina.

- **Identificação da face:** Esta técnica consiste na leitura de pontos delimitadores da face para identificação de tamanhos, proporções, formas e distâncias. Identifica as pessoas mesmo que a face tenha sido alterada por barba, bigodes, sobrancelhas, cor ou cortes de cabelo diferentes. É uma técnica muito nova e que não causa desconforto algum, pois como a captura e leitura é feita por uma câmera o usuário fica a uma distância confortável do ponto de leitura. A principal desvantagem é para o caso de irmãos gêmeos.

Figura 11: Leitor facial.

- **Reconhecimento de Voz:** Reconhece padrões de voz, identificando se o individuo é do sexo masculino ou feminino. Não é muito usado em segurança, pois pode ser facilmente burlado.

Figura 12: Interface de Captura de Voz.

- **Reconhecimento de Caligrafia:** Reconhece a forma com que uma pessoa escreve e posteriormente identifica o individuo que escreveu. Alguns sistemas podem ser burlados de forma que a assinatura e o formato das letras podem ser copiados, porem há tecnologias que não analisam somente a escrita, mas também a forma com que a pessoa escreve (pressão, angulação da caneta ao escrever, tempo de escrita, etc.) ficando assim mais difícil burlar o sistema.

Figura 13: Leitor de Caligrafia.

Dentre os sistemas biométricos apresentados os mais utilizados atualmente são os de leitura de digitais, geometria das mãos, íris e retina, a tabela 1, apresenta um comparativo entre essas tecnologias as quais devem ser levadas em conta em cada projeto, pois todas dependem do ambiente que serão instaladas, das pessoas e da quantidade de pessoas que utilizarão o sistema.

DADOS	DIGITAIS	MÃO	ÍRIS	RETINA
TAMANHO REGISTRO	250 a 1200 bytes	9 bytes	512 bytes	96 bytes
TEMPO CONFIRMAÇÃO	5 - 7 seg	3 - 5 seg	< 2,5 seg	< 2,5 seg
FALSA ACEITAÇÃO	0 %	< 0,1 %	0 %	0 %
FALSA REJEIÇÃO	9,4 %	< 0,1 %	~ 0 %	~ 0 %
OUTROS	Sensor de Calor	Se é mão viva	Íris é estável	Retina é estável
CUSTO RELATIVO	Baixo	Médio	Altíssimo	Altíssimo
VANTAGENS	Conveniente e fácil de usar, baixa infraestrutura de custo, sensores de miniaturização devido a uso de sensor de silicone, ideal para todas as aplicações.	Conveniente e fácil usar. Não afetada por condições de pele, ideal para controle de acesso e tempo e aplicações de freqüência,	Alta taxa de precisão. velocidade alta, ideal em aeroportos e para aplicações financeiras para processo rápido e seguro	Taxas de precisão muito altas
LIMITAÇÕES	Conotação de justiça criminal, desempenho se altera com dedos, secos, oleosos, sujos ou cicatrizados, contato é considerado anti-higiênico em alguns países asiáticos.	Vultoso em tamanho, custo alto, contato considerado anti-higiênico em alguns países asiáticos.	Infraestrutura alta, desconforto público usando o olho, parece com um intruso.	Infraestrutura médio-alta, desconforto público usando o olho.

Tabela 1: Comparativo dos sistemas biométricos.

6 ALGUMAS APLICAÇÕES DE CONTROLE DE ACESSO

As organizações estão investindo cada vez mais na gestão da segurança patrimonial e, conseqüentemente, em sistemas eletrônicos de segurança que permitem o monitoramento em tempo real da movimentação de pessoas e/ou veículos nas dependências ou mesmo nos arredores da organização, todos os registros dessas movimentações são armazenados em banco de dados o que permite consultas posteriores seja de um vídeo, alarmes ou dos eventos de acessos em áreas com sistemas eletrônicos de controle de acesso, tema de estudo neste trabalho.

Conforme capítulo anterior, os sistemas eletrônicos de controle de acesso podem ser instalados em diferentes áreas segregadas entre si por algum dispositivo de bloqueio os quais podem ser portas, cancelas, catracas ou portões.

Na prática esses sistemas são muito utilizados em empresas e condomínios com objetivos distintos.

Em condomínios são utilizados para registro do horário de entrada e saída de condôminos e para controle da entrada de visitantes e prestadores de serviços de forma que essas pessoas devam se identificar na portaria para que o funcionário da portaria verifique com a pessoa que receberá a visita se pode permitir a entrada do visitante.

Em empresas esses sistemas são utilizados também em portarias e recepções com o mesmo objetivo dos condomínios. Porém suas principais aplicações são em áreas nas quais se fazem necessários a segurança da informação e dos demais ativos, ou seja, é interessante ter o controle de acesso a áreas especificas como, por exemplo, setores de desenvolvimento, área de armazenamento de produtos controlados – no caso de indústrias químicas, áreas onde são armazenados documentações confidenciais e nos centro de processamento de dados normalmente chamados de CPDs área de responsabilidade do departamento de tecnologia da informação (TI). Essas áreas além de concentrar as informações da empresa em servidores também armazenam os equipamentos que gerenciam as operações de comunicação como switches, roteadores e centrais telefônicas (PABX).

Com a informatização dos processos e digitalização dos documentos é de extrema importância restringir o acesso físico ao ambiente computacional a pessoas que trabalham e utilizam esse ambiente. O uso de um sistema eletrônico de controle de acesso reduz significativamente os riscos de acesso de pessoas não autorizadas e conseqüentemente o acesso a informações confidenciais ou até mesmo sabotagens dos servidores. (FONTES, 2000, p.42).

Conforme observado no tópico anterior, a utilização de sistemas de controle de acesso em CPDs é de extrema importância com o objetivo de prover a prevenção de acesso não autorizado, dano, perda e interferência às instalações físicas da organização e à sua informação. Os recursos e

instalações de processamento de informações críticas, ou sensíveis do negócio, devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

Em suma os sistemas eletrônicos de controle de acesso podem ser instalados em qualquer área, porém em algumas é necessário que haja um controle mais rigoroso, pois as políticas de segurança devem sem implantadas em conjunto com a política de operação de cada área, ou seja, à medida que as pessoas acessam o interior das entidades mais rigoroso deve ser este controle. A figura 14 ilustra um diagrama de um sistema de controle de acesso, através desta figura é observável a possibilidade de se integrar diferentes dispositivos de bloqueio, desta forma é possível aplicar um sistema eletrônico de controle de acesso em qualquer área que se faça útil a utilização deste tipo de sistema para controle de pessoas e/ou veículos.

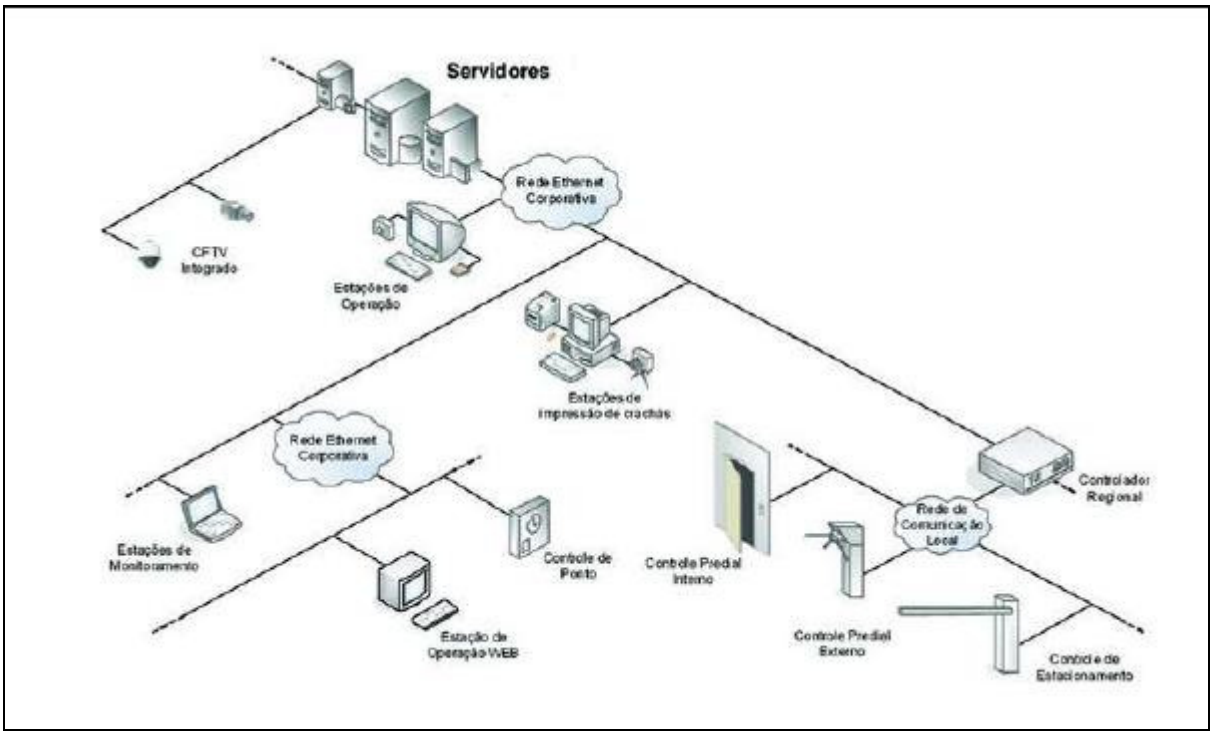

Figura 14: Diagrama de Aplicações de Controle de Acesso.

7 EXEMPLO DE SISTEMA DE CONTROLE DE ACESSO

7.1. Controle de Acesso em um Centro de Processamento de Dados (CPD)

Conforme citado no capitulo anterior é muito importante que haja controle de acesso nos CPDs para minimizar os riscos de acesso físico aos equipamentos contidos nesta área. Devido a importância dada a esta área e para a maioria das empresas, principalmente as de médio e grande porte, será utilizado como exemplo o estudo de caso de um sistema de controle de acesso projetado para a porta de um CPD.

Para escolha do sistema que será utilizado é necessário conhecer todos os requisitos das políticas de segurança relacionadas ao acesso físico ao CPD, mas basicamente essas políticas devem restringir o acesso físico ao ambiente computacional a pessoas que trabalham e utilizam esse ambiente. Na maioria dos casos o acesso ao CPD é permitido somente a alguns funcionários do departamento de TI.

O projeto e instalação do sistema eletrônico de controle de acesso do CPD pode ser feito seguindo as etapas dos próximos tópicos deste capítulo.

7.1.1. Escolha do Sistema

Conforme citado no capítulo 3 deste trabalho a maioria dos sistemas eletrônicos de controle de acesso possuem o mesmo recurso, porém devem atender os requisitos da política de segurança elaborada para o CPD. Em um contexto geral as principais exigências para esta área são:

- Permitir que o CPD seja configurado como área independente;
- Possibilitar que os direitos de acesso a área seja associado a todas as pessoas do departamento de TI ou somente a algumas;
- Possibilitar configuração de tabelas de horários, dias da semana, feriados e dias não úteis de forma que os funcionários não tenham acesso fora do seu período de trabalho;
- Possibilitar que no cadastro do funcionário seja configurado o período de férias deste, para que durante este período seu acesso não seja permitido – principalmente quando a tecnologia de identificação utilizada forem cartões;
- Registrar todos os eventos de acesso, ou tentavas de acesso;
- Gerar alarme caso a porta seja aberta de forma forçada ou mesmo fique aberta por mais tempo que o necessário;
- As placas controladoras devem ter a capacidade de manter o sistema operante mesmo no caso de haver uma falha de comunicação entre as mesmas e o servidor.

A partir dessas informações é possível escolher o sistema que atenda as necessidades do cliente e ofereça uma melhor relação custo x beneficio, vale lembrar que muitos clientes já têm preferência por alguns fabricantes pelo fato de possuírem acordos comerciais, ou simplesmente por outras unidades da empresa já possuírem tal sistema, e todos os *sites* devem ser integrados, até mesmo porque sistemas de fabricantes diferentes não funcionam em conjunto.

Atualmente existem muitos sistemas no mercado, porém alguns são muito conhecidos dentre eles se destacam:

- **Kantech**: Produto fabricado pela empresa Tyco, foi dos primeiros sistemas de controle de acesso instalados no Brasil é um sistema muito estável e atende todos os requisitos necessários para nosso caso, porém, tem custo elevado e sua interface de operação não é "amigável". É utilizado atualmente principalmente em filiais de empresas norte americanas. Caso haja necessidade de expansão do sistema é necessário comprar ampliação do software além do hardware, o que torna a utilização desse sistema inviável para algumas empresas.
- **Facility Commander:** Sistema produzido pela empresa GE Security, neste sistema é possível integrar câmeras, alarmes e controle de acesso em único software. É um sistema de fácil operação, e também muito estável. É utilizado em algumas empresas multinacionais, porém seu custo é elevado comparado a outros produtos, pois não possui representação comercial no Brasil o que torna os serviços de compra e importação também elevados, esses fatores fazem com que o valor de venda seja alto. Outra desvantagem é a dificuldade é o tempo de retorno dos equipamentos da assistência técnica, apesar de raramente apresentarem problemas. Caso haja necessidade de expansão do sistema é necessário comprar ampliação do software além do hardware, o que torna a utilização desse sistema inviável para algumas empresas.
- **Data Plus:** Sistema produzido no Brasil pela empresa Data Quest, a operação deste software e extremamente simples, porém é indicado somente para pequenas aplicações. As desvantagens desse sistema são pela forma de comunicação entre servidor e controladoras ser serial, para maiores distâncias é necessário instalação de conversores de protocolo, o que vai encarecendo o sistema, outra desvantagem é que o sistema opera somente se estiver *on-line* com o servidor, caso haja alguma falha de comunicação entre controladoras e servidor o sistema deixa de funcionar. Sistema de fácil expansão, necessário investir somente em hardware, porém se limita a 32 controladoras.
- **Win Spector:** Sistema produzido no Brasil pela empresa Trilobit. É um ótimo sistema além de atender todos os requisitos exigidos para sistemas eletrônicos de controle de acesso o fabricante oferece opções de customização do sistema para incrementar algumas funções. O

software possui uma versão para pequenas aplicações e versão para maiores aplicações, que podem controlar acesso de até 1.000.000 de usuários. Possui custo intermediário que varia de acordo com a licença de software adquirida. Caso haja necessidade o sistema pode ser expandido facilmente com novo investimento somente em hardware.

Além dos exemplos citados acima todos atendem as políticas adotadas para maioria dos CPDs. Atualmente pela boa qualidade, versatilidade e pelo custo competitivo comparado aos dois primeiros exemplos, o sistema *Win Spector* atende de forma satisfatória o estudo de caso deste trabalho, por isso, os demais tópicos deste capitulo farão algumas referências a este sistema.

7.2.Materiais Utilizados e Instalação

Os sistemas eletrônicos de controle de acesso têm o mesmo principio de funcionamento e são constituídos basicamente com a mesma arquitetura. Os materiais utilizados para instalação de qualquer um deles são os mesmos no que diz respeito à infraestrutura diferindo somente o software e placa controladora, pois na maioria dos casos, são desenvolvidos e produzidos pelo mesmo fabricante. Dos exemplos citados no tópico anterior deste capítulo ambos os fabricantes produzem tanto o software quanto o hardware e, o software de um não é compatível com o hardware do outro e vice versa.

A Figura 15 ilustra os elementos básicos necessários para se controlar acesso em um CPD:

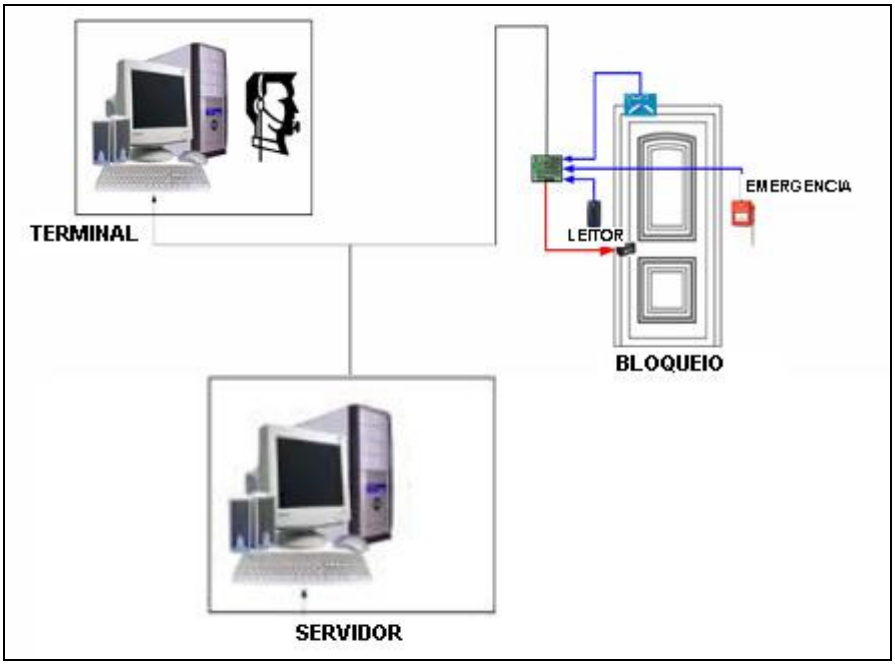

Figura 15: Elementos Necessários Para Controlar Acesso em um CPD.

7.2.1. Servidor

Um elemento fundamental para o funcionamento do sistema é o servidor, conforme citado no capitulo anterior é responsável pelo armazenamento de todas as informações do sistema, tanto de registro de dados dos eventos de acesso quanto de configurações gerais do sistema, portanto é muito importante que a CPU utilizada para esta finalidade atenda os requisitos mínimos informados pelo fabricante do software, no caso deste trabalho esses requisitos são:

- Processador Pentium Dual Core 1.8 GHz;
- Memória RAM de 1 Gb;
- Disco rígido de 10 Gb (dedicado exclusivamente para o sistema);
- Placa de rede 100/1000 Mbits;
- Sistema operacional para servidor Windows 2000 Server ou Windows Server 2003;
- SQL Server 2005 (*Service Pack 2*);
- Win Spector Smart Servidor;

É recomendado que as operações corriqueiras do sistema não sejam realizadas diretamente no servidor, por isso são instalados os terminais, que serão descritos no próximo tópico. No servidor é recomendado que sejam feitas somente as configurações de parâmetros do sistema, as quais podem ser realizadas também nos terminais, porém, são restritas por senhas. A Figura 16 ilustra o principal item de configuração no servidor, que é a configuração de conexão com o banco de dados.

Figura 16: Configuração de Conexão com o Bando de Dados.

7.2.2. Terminal

Para operação do software é instalado em outra CPU o aplicativo denominado de Win Spector Terminal, que possui em sua interface somente os recursos para cadastro do sistema e algumas configurações de hardware, sendo que cada operador é cadastrado individualmente e os recursos são atribuídos conforme necessidade, os requisitos mínimos para o terminal são:

- Processador Pentium Dual Core 1.8 GHz;
- Memória RAM de 1 Gb;
- Disco rígido de 10 Gb (dedicado exclusivamente para o sistema);
- Placa de rede 100/1000 Mbits;
- Windows XP (*Service Pack 2)*
- Win Spector Smart Terminal (sistema permite que até 4 terminais operem simultaneamente).

Esses itens são requisitos mínimos considerando que este terminal será utilizado exclusivamente para operação do sistema, caso este CPU seja utilizada para outras aplicações esses requisitos devem ser revistos.

Neste elemento são realizadas as operações corriqueiras do sistema, ou seja, cadastros de funcionários, prestadores de serviços e visitantes. A Figura 17 ilustra as tarefas que podem ser realizadas no terminal:

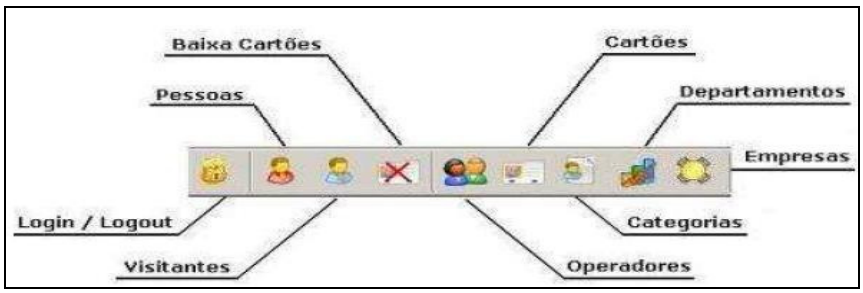

Figura 17: Operações Disponíveis no Terminal.

O software possui botões de atalho para facilitar a operação e a função de cada um desses botões é:

- **Login / Logout**: Opção para entrada de nome de operador e senha, assim como nos sistemas operacionais, é possível que cada operador seja cadastrado de forma a ter privilégios de acesso diferentes aos recursos do sistema;
- **Pessoas**: A operação pessoas permite que sejam cadastradas e fotografadas pessoas quer sejam funcionários, terceiros ou pessoas que se enquadrem em outras categorias

previamente cadastradas. Neste campo são habilitadas as áreas nas quais as pessoas terão acesso;

- **Visitantes**: Como o próprio nome diz, é utilizada para cadastrar e fotografar visitantes e, também, definidas as áreas que o visitante poderá acessar. Uma vez cadastrado, os dados dos visitantes ficam armazenados no banco de dados junto com a foto, desta forma na próxima visita é necessário que o mesmo apresente o número do documento utilizado para o primeiro cadastro;
- **Baixa de cartões**: As pessoas e visitantes recebem um cartão para acessar as dependências da empresa, os funcionários, normalmente, ficam com o cartão até que por algum motivo tenham que o devolver. Os visitantes devolvem o cartão na saída, este campo é utilizado para desvincular o cartão da pessoa, tornando o cartão disponível para ser associado a outra;
- **Operadores**: Campo utilizado para cadastro, exclusão ou edição dos operadores do sistema;
- **Cartões**: Campo utilizado para cadastro, edição ou exclusão de cartões;
- **Categorias**: Campo utilizado para cadastrar categorias, as quais definem qual tipo de vinculo a pessoa tem com a empresa, por exemplo, funcionário, estagiário, terceirizado etc.
- **Departamentos**: Campo utilizado para cadastrar os departamentos existentes na empresa, como administrativo, segurança, engenharia e tecnologia da informação, por exemplo.
- **Empresas**: Campo utilizado para cadastro de empresas as quais podem ter funcionários residentes ou que visitam com freqüência a empresa na qual está implantado o sistema de controle de acesso.

7.2.3. Controladora

A placa controladora utilizada pelo sistema *Win Spector Smart* é denominada TRIW. Esta controladora possui as seguintes características técnicas:

- Alimentação em 12Vdc;
- Interface de comunicação ethernet TCP-IP 10/100 Mbps;
- Entrada para 2 leitores com protocolo *Wiegand*;
- Display para verificação de status e para acessar menu de configuração;
- Micro-interruptores para fazer a configuração local da placa;
- Possui duas saídas de relés acionadas de forma independente;
- Possui um relé de saída de alarme.

A Figura 18 ilustra uma placa controladora TRIW, os bornes verticais são de entrada e os horizontais de saídas.

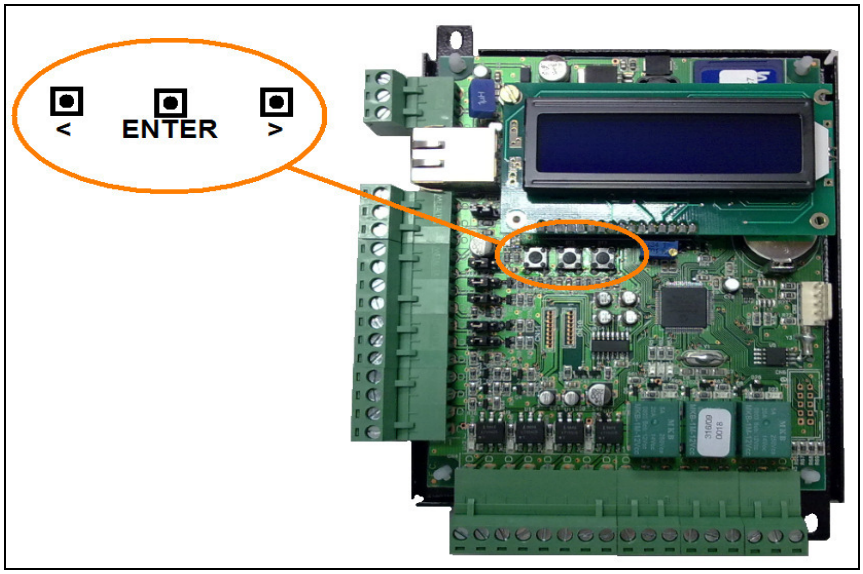

Figura 18: Placa Controladora TRIW.

7.2.4. Leitor / Identificador

O acesso ao CPD na maioria da empresa é realizado por poucas pessoas, em alguns casos alguns funcionários do departamento de tecnologia da informação não têm privilegio de acessar essa área. Por isso a escolha da tecnologia de identificação é fundamental. Cartões podem ser utilizados por pessoas não autorizadas, seja por extravio, perda, roubo ou furto, por se tratar de uma área critica e acessada por poucas pessoas o mais indicado é que se utilize um sistema de identificação biométrico. Um sistema confiável e viável economicamente para pequenas aplicações é o de identificação de impressões digitais.

O leitor biométrico *Control ID* possui saída com o protocolo *Wiegand*, este protocolo é compatível com a maioria das controladoras, inclusive com a TRIW, pois é o protocolo de saída da maioria dos leitores de cartões de proximidade.

Para funcionar desta forma é necessário configurar a saída do leitor biométrico para o modo denominado *Emular Cartão*. Desta forma o tratamento da informação feito pelo sistema é idêntico ao dado através da leitura de um cartão, o diferencial é que é garantido que a pessoa que teve acesso autorizado está ou esteve presente no momento da abertura da porta. Como muitas empresas seguem normas internacionais para o departamento de TI e acesso aos CPDs e muitas dessas normas estão vinculadas a procedimentos adotados para conseguir certificações, como ISO, instalar um sistema de controle de acesso cujo reconhecimento é feito por biometria é um grande e vantajoso diferencial.

A Figura 19 ilustra a arquitetura de interligação do hardware do sistema com o leitor biométrico, é possível notar que a única diferença é o tipo de leitor (identificador) utilizado.

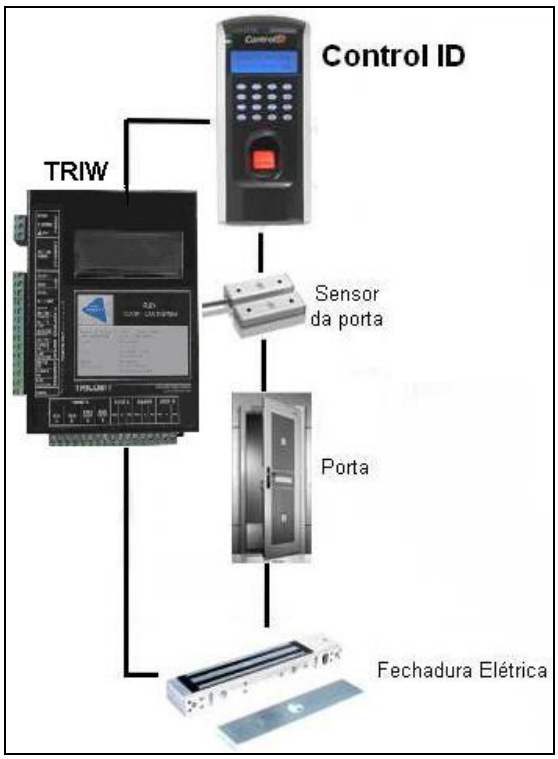

Figura 19: Arquitetura com leitor biométrico de digitais.

7.2.5. Infraestrutura Geral

Para instalar um sistema de controle eletrônico de acesso é necessário alguns cuidados com a infraestrutura, de forma que a controladora fique segura e ao mesmo tempo o mais próxima possível do dispositivo de bloqueio que se deseja controlar, neste caso, uma porta.

Considerando que a controladora ficará acomodada em um gabinete acima da porta, conforme figura 24, são necessários os seguintes materiais para instalação deste sistema:

- Um gabinete de 300x300x150 milímetros com fechadura para acomodação da fonte de alimentação, da TRIW e de um disjuntor;
- Uma TRIW;
- Uma fonte de alimentação 12Vdc 36 Watts para alimentação da TRIW, leitores e fechadura;
- Dois Biométricos para impressões digitais (um acesso de entrada ao CPD e outro para saída);
- Oito metros de cabo manga 6 x 26 AWG para interligar os leitores com a TRIW;
- Quatro metros de cabo paralelo 2 x 0,75 mm para energizar a fechadura eletromagnética;

- Uma fechadura eletromagnética.
- Um sensor magnético (será utilizado para monitorar abertura forçada da porta e também para alertar o operador do sistema que a mesma ficou aberta por mais tempo que o necessário);
- Dispositivo de quebra de vidro (instalado na parte interna do CPD caso haja uma emergência ao quebrar o vidro a porta destrava);
- Ponto de 127 ou 220 Vac com aterramento disponibilizado pelo cliente para energização da fonte de alimentação do sistema;
- Ponto de rede.

A Figura 20 ilustra a forma que deve ser feita a infraestrutura para um sistema de controle de acesso, note que a tubulação de dados é separada da tubulação que levará energia para o gabinete desta forma se evita que haja induções eletromagnéticas que causem interferências na comunicação do sistema.

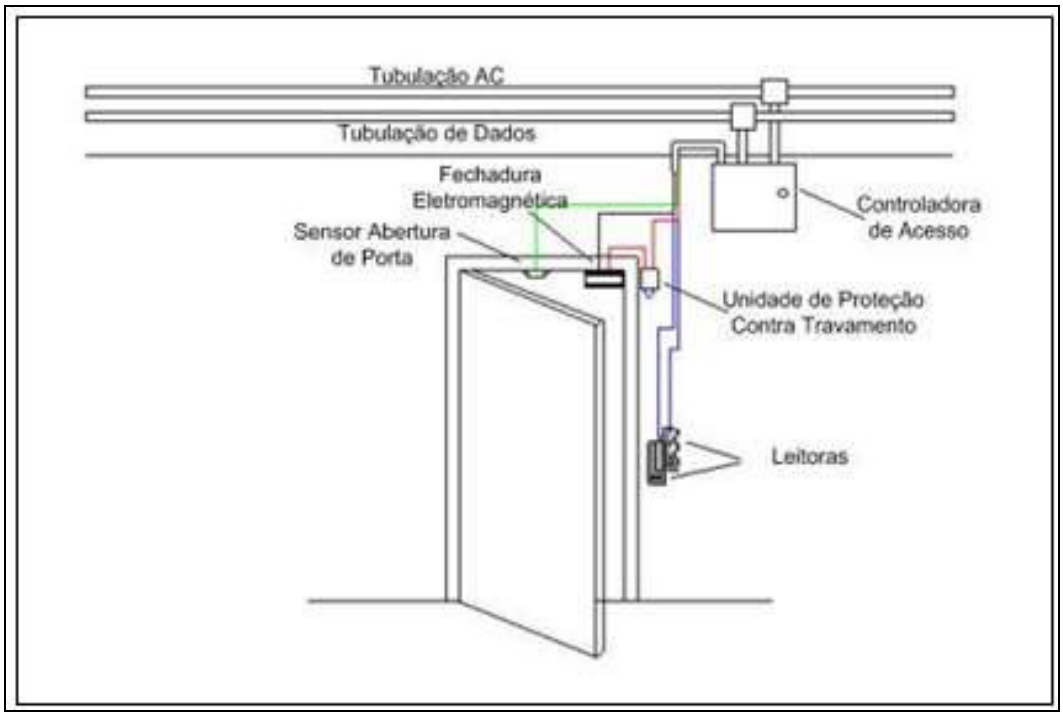

Figura 20: Infraestrutura de instalação de sistema de controle de acesso em uma porta

A Figura 21 é a fotografia de um gabinete utilizado para instalação de três controladoras TRIW, neste caso foi instalado um no break para que o sistema permaneça operante caso haja falta de energia elétrica, pois em muitos casos pessoas aproveitam dessas situações, ou mesmo as provocam, para adentrar os locais controlados por sistemas eletrônicos de segurança.

Figura 21: Exemplo de montagem de gabinete

7.2.6. Configuração dos Parâmetros

Após instalação do software e hardware é necessário que sejam configurados os parâmetros do sistema. Na TRIW basta configurar o endereço IP. No software *Win Spector Smart*, os itens que devem ser configurados são:

- **Áreas:** conforme nomenclatura indicada pelo cliente, no caso deste trabalho foram criadas 4 áreas conforme ilustrado na Figura 22. Note que essas áreas serão utilizadas nas configurações de hardware posteriormente:

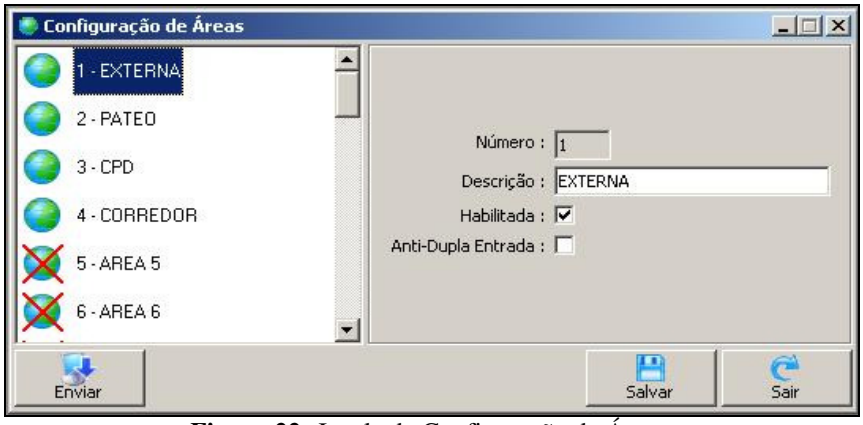

Figura 22: Janela de Configuração de Áreas.

- **Feriados:** Os feriados são cadastrados para que as pessoas não tenham acesso permitido a determinadas áreas em datas especificas, como feriados.

Figura 23: Configuração de Feriados.

- **Hardware:** Campo para configuração da TRIW, como a comunicação entre o servidor e a TRIW é feita por rede TCP-IP é necessário configurar no software o mesmo endereço IP que será configurado a controladora correspondente e a área controlada pela mesma.

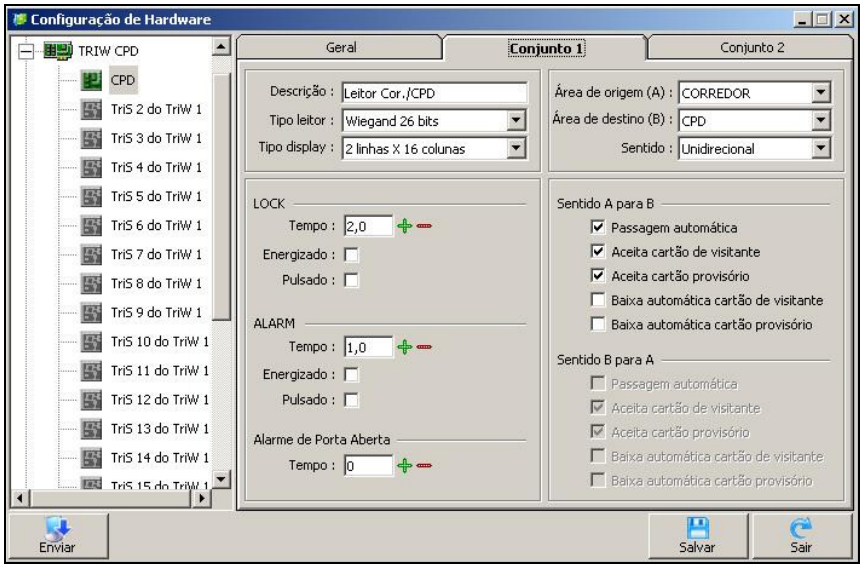

Figura 24: Configuração do leitor de acesso do corredor para o CPD.

7.3.Testes Funcionais

Após o sistema ser instalado e configurado, são realizados testes funcionais. São feitos basicamente dois cadastros, um com acesso permitido. A Figura 25 ilustra um relatório emitido após os testes:

Empresa : 0 - EMPRESA PADRAO
Data : 12/11/2011

Hora	Nome da Pessoa	Cartão	Tipo Acesso
08:10:07	Acesso CPD	0012900599	CARTAO VENCIDO
08:10:12	sem acesso	0000805902	CARTAO VENCIDO
08:10:58	Acesso CPD	0012900599	ACESSO AUTORIZADO
08:11:06	sem acesso	0000805902	ACESSO AUTORIZADO
08:11:44	Acesso CPD	0012900599	AREA DESABILITADA
08:11:50	sem acesso	0000805902	AREA NÃO PERMITIDA
08:12:05	sem acesso	0000805902	AREA NÃO PERMITIDA
08:12:07	Acesso CPD	0012900599	AREA DESABILITADA
08:12:36	Acesso CPD	0012900599	AREA DESABILITADA
08:12:39	sem acesso	0000805902	AREA NÃO PERMITIDA
08:15:12	sem acesso	0000805902	AREA NÃO PERMITIDA
08:15:17	Acesso CPD	0012900599	ACESSO AUTORIZADO
08:15:23	Acesso CPD	0012900599	ACESSO AUTORIZADO
08:15:27	sem acesso	0000805902	AREA NÃO PERMITIDA
08:15:31	sem acesso	0000805902	AREA NÃO PERMITIDA
08:15:40	sem acesso	0000805902	AREA NÃO PERMITIDA
08:15:44	Acesso CPD	0012900599	ACESSO AUTORIZADO
08:15:48	Acesso CPD	0012900599	ACESSO AUTORIZADO
09:02:04	Acesso CPD	0012900599	ACESSO AUTORIZADO
09:02:11	sem acesso	0000805902	AREA NÃO PERMITIDA
09:02:21	sem acesso	0000805902	AREA NÃO PERMITIDA
09:02:27	Acesso CPD	0012900599	ACESSO AUTORIZADO
09:02:31	sem acesso	0000805902	AREA NÃO PERMITIDA
09:02:53	Acesso CPD	0012900599	ACESSO AUTORIZADO
09:03:14	sem acesso	0000805902	AREA NÃO PERMITIDA

Total por Data : 25

Figura 25: Apresentação de um relatório de histórico de acesso filtrado por data e hora.

Note que no relatório aparecem o horário, o nome da pessoa, o número do cartão e o tipo de acesso. Para simular foi feito cadastro de uma pessoa com nome fictício de Acesso CPD e outra pessoa com nome de Sem Acesso, para simulação o cadastro dos cartões também tiveram suas datas de validade configuradas para uma data ultrapassada, isso também restringe o acesso e aparece nas duas primeiras linhas do relatório.

Quando o cartão associado ao cadastro Sem Acesso é apresentado registra no banco de dados a informação de área não permitida e o dispositivo de bloqueio não é liberado. Para o cartão associado ao cadastro Acesso CPD é registrado no banco de dados acesso autorizado e o dispositivo de bloqueio fica liberado pelo tempo configurado nas configurações de hardware.

O Win Spector Smart também permite que o operador monitore todos os eventos de acesso que estejam ocorrendo praticamente em tempo real, considerando que possa haver algum atraso devido ao tráfego de informações na rede TCP-IP. Esta função é denominada **Eventos do Sistema** e monitora tanto os eventos de acesso quanto possíveis problemas de comunicação com as placas controladoras. A figura abaixo ilustra essa função.

Horário	TriW	TriS	Leitor	Evento	Cartão	PIN	Nome
16:09:11	1	1	1	ACESSO SOLICITAD	0018060896	6	CARLUCIO SILVEIRA
16:09:11	1	1	1	ACESSO LIBERADO	0018060896	6	CARLUCIO SILVEIRA
16:09:11	1	1	1	ACESSO REALIZADO	0018060896	6	CARLUCIO SILVEIRA
16:09:13	1	1	1	ACESSO SOLICITAD	0018848900	2	LILIAN BARBOSA
16:09:13	1	1	1	ACESSO LIBERADO	0018848900	2	LILIAN BARBOSA
16:09:13	1	1	1	ACESSO REALIZADO	0018848900	2	LILIAN BARBOSA
16:09:14	1	1	1	ACESSO SOLICITAD	0018848890	----------	----------
16:09:14	1	1	1	CARTAO NAO EXIST	0018848890	----------	----------
16:09:16	1	1	1	ACESSO SOLICITAD	0018141437	3	LUCIANO PERES
16:09:16	1	1	1	ACESSO LIBERADO	0018141437	3	LUCIANO PERES
16:09:16	1	1	1	ACESSO REALIZADO	0018141437	3	LUCIANO PERES
16:10:27	------	------	------	----------	----------	----------	Data e hora enviados com sucesso para o TriW 1

Figura 26: Monitoramento de Eventos do Sistema.

Pode ser observado na Figura 26 que os eventos de acesso validos são apresentados em verde qualquer evento que restrinja o acesso aparece destacado em vermelho. Esta função é muito útil, pois caso uma pessoa tente acessar uma área para qual não é credenciada, possibilita que o pessoal do departamento de segurança verifique os motivos que levaram a pessoa tentar acessar uma área para qual não tem acesso permitido, e se necessário, informar e/ou a advertir.

.

CONCLUSÃO.

Os sistemas eletrônicos de controle de acesso é um recurso muito útil em diversas aplicações, porém é fundamental que seu funcionamento seja integrado com políticas que criem procedimentos funcionais que restrinjam o acesso sem atrapalhar as operações da instituição, ou seja, treinar as pessoas de forma que elas entendam que o sistema é para ajudar garantir a segurança patrimonial da empresa e também a qualidade das operações que sejam confidenciais. Desta forma é fundamental que o projeto técnico seja feito atendendo aos requisitos e conceitos da segurança patrimonial e seguindo as políticas de privacidade dos setores que controlam as áreas envolvidas.

Em locais que há cultura de segurança das informações a utilização de sistemas eletrônicos de controle de acesso são fundamentais para que o acesso físico aos CPDs não sejam limitados a utilização de uma chave para abertura de uma fechadura, por exemplo. Se utilizando cartões como chave de identificação todos os eventos são registrados e como o cartão em praticamente todas as organizações funciona também como identificação física dos funcionários (crachás) a responsabilidade de guarda e utilização do mesmo é atribuída a cada individuo, e como há registro de todos os eventos é natural que cada um assimile essa responsabilidade e a pratique.

Porém, para o bom funcionamento dos sistemas eletrônicos de controle de acesso não basta apenas uma série de procedimentos também é necessário que as instalações sejam feitas atendendo todos os requisitos técnicos do projeto para que sistema opere de forma confiável em tempo integral e que as pessoas sejam treinadas de forma adequada para que entendam e pratiquem as políticas adotadas pela empresa.

As tendências futuras são que as características biométricas devem ser mais utilizadas, porém para isso as empresas estão investindo para que esses sistemas tenham um processamento mais rápido com o objetivo de melhorar seu desempenho e tornar sua aplicação viável em ambiente de alto fluxo de pessoas e/ou veículos.

Desta forma concluo que os sistemas eletrônicos de controle de acesso são um tema interessante por integrar diferentes tecnologias como redes ETHERNET (TCP-IP), leitores e cartões de identificação por rádio freqüência, tecnologias de identificação biométricas e conceitos de cabeamento e elementos eletrônicos com mecânicos, como portas e fechaduras eletromagnéticas dentre outros e também por ser uma ferramenta que pode ser utilizada em todas as instituições que tenham uma ou mais áreas de acesso restrito com a vantagem de todas as informações ficarem armazenas e também serem monitoradas em tempo real permitindo ação imediata de forma estratégica das pessoas do departamento de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS.

BRASILIANO, A.C.R.; BLANCO L. **Planejamento Tático e Técnico Em Segurança Empresarial.** 1. Ed. Sicurezza: São Paulo, 2003.

FONTES, E.; **Vivendo A Segurança Da Informação.** 1. Ed. Sicurezza: São Paulo: 2000.

MANDARINI, M.; **Segurança Corporativa Estratégica.** 1. Ed. Manole LTDA.: Barueri, 2005.

CONTROL ID LEITORES BIOMÉTRICOS informações sobre produtos e manuais < http://www.controlid.com.br/controle-de-acesso/controle-de-acesso-cx-700.php> Acesso em 09 nov. 2011.

HID FABRICANTE DE LEITORES E CARTÕES RFID informações sobre produtos e manuais < http://www.hidglobal.com/portugues/iam/physicalAccess.php> Acesso em 18 set. 2011.

TRILOBIT SISTEMAS DE CONTROLE DE ACESSO manuais do sistema WinSpector Smart e TRIW < http://www.trilobit.com.br/br/seguranca/controledeacesso/downloads/manuais/wspsmart> Acesso em: 18 set. 2011.

.