ULBRA CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
COMUNIDADE EVANGÉLICA LUTERANA "SÃO PAULO"
Recredenciado pela Portaria Ministerial nº 3.607 - D.O.U. nº 202 de 20/10/2005

PLÍNIO CARDOSO DE OLIVEIRA

SISTEMA DE CONTROLE DE ACESSO A AMBIENTES FÍSICOS COM DESTRAVAMENTO DE FECHADURAS ELETRÔNICAS POR MEIO DE NFC (*NEAR FIELD COMMUNICATION*)

Palmas – TO

2013

PLÍNIO CARDOSO DE OLIVEIRA

SISTEMA DE CONTROLE DE ACESSO A AMBIENTES FÍSICOS COM DESTRAVAMENTO DE FECHADURAS ELETRÔNICAS POR MEIO DE NFC (NEAR FIELD COMMUNICATION)

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. MSc. Jackson Gomes de Souza.

Palmas – TO

2013

PLÍNIO CARDOSO DE OLIVEIRA

SISTEMA DE CONTROLE DE ACESSO A AMBIENTES FÍSICOS COM DESTRAVAMENTO DE FECHADURAS ELETRÔNICAS POR MEIO DE NFC (NEAR FIELD COMMUNICATION)

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de Informação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. MSc. Jackson Gomes de Souza.

Aprovada em dezembro de 2013.

BANCA EXAMINADORA

_____

Prof. M. Sc. Jackson Gomes de Souza
Centro Universitário Luterano de Palmas

_____

Prof. M. Sc. Madianita Bogo Marioti
Centro Universitário Luterano de Palmas

_____

Prof. M. Sc. Fabiano Fagundes
Centro Universitário Luterano de Palmas

Palmas – TO
2013

De tudo o que se tem ouvido, a suma é: Teme a Deus, e guarda os seus mandamentos; porque isto é o dever de todo homem.
Eclesiastes 12:13

RESUMO

Esse trabalho tem como objetivo implementar o projeto de uma fechadura elétrica, que é uma trava mecânica controlada eletronicamente, utilizando a tecnologia NFC (*Near Field Communication*) existente em telefones móveis, principalmente os smartfones e cartões magnéticos. Também será utilizada no projeto a plataforma *Arduino* que é uma tecnologia empregada para criar protótipos microcontrolados. O chip da plataforma será responsável por interligar a fechadura elétrica com o leitor NFC.

PALAVRAS-CHAVE: *Arduino*; NFC, Fechadura Eletrônica

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Há muito tempo o registro de informações e o armazenamento de dados são medidas comuns nas empresas, pois facilitam a tomada de decisões e, consequentemente, geram resultados mais benéficos. Com a evolução dos sistemas computacionais houve um aumento dessa prática, por ter se tornado mais acessível o trabalho de armazenamento de dados, por exemplo, com a diminuição do custo por MB em discos rígidos. Entretanto, um problema encontrado em guardar esses dados, é prover meios de garantir que eles estejam seguros contra ataques ou catástrofes.

É importante notar que a mesma tecnologia que proporcionou a evolução nas formas de armazenamento de dados, também facilitou a criação de sistemas que preservem esse patrimônio das instituições.

A implantação de sistemas de segurança geralmente produz transtornos, pois sua utilização está na contra mão do conforto de seus usuários. Como um dos intuitos desses mecanismos é barrar o acesso de pessoas não autorizadas, esses sistemas acabam dificultando também o acesso de quem possui permissão.

Contudo, vêm sendo desenvolvidas variadas técnicas de segurança como senhas, chaves e reconhecimento biométrico para serem usadas conforme a necessidade do projeto e para minimizar os incômodos causados por sua implantação. Cada uma dessas técnicas tem suas vantagens e desvantagens, que devem ser adaptadas ao ambiente organizacional onde forem instaladas.

Independentemente das técnicas utilizadas, é importante que todas as possíveis vulnerabilidades sejam minimizadas ou extintas. Para haver proteção eficiente é necessário que sejam tomadas medidas contra vulnerabilidades lógicas, as relacionadas à rede e sistemas, e vulnerabilidades físicas, que são danos ou acessos presenciais (físicos) aos equipamentos responsáveis pelo armazenamento e processamento dos dados.

A segurança de ambientes físicos deve ser tratada com a mesma importância que se emprega aos ataques virtuais, pois os prejuízos causados por eles podem atingir proporções idênticas. Em muitas situações os danos aos ativos da organização acontecem de forma não intencional por pessoas desavisadas, mas

esse problema pode ser solucionado fazendo-se uso de mecanismos que bloqueiem ou diminuam o acesso desses indivíduos.

Dentro de um ambiente organizacional é normal que existam funcionários que necessitem de acesso a diferentes ambientes físicos. Como geralmente a locomoção desses funcionários é grande, o ideal é que exista um sistema seguro, mas que não seja desgastante para os seus usuários.

A utilização de senhas em fechaduras é relativamente lenta se comparada a outras técnicas, pois para se ter um sistema confiável é necessário que o usuário faça uso de vários dígitos na senha. Outra tecnologia que pode ser utilizada é a biometria, que identifica o usuário por suas características físicas e comportamentais, mas essa tecnologia tem um custo elevado, principalmente conforme os níveis de complexidade empregados, que vão desde a utilização de impressões digitais ao reconhecimento da face e da retina.

Outro mecanismo utilizado nas fechaduras são as chaves mecânicas e eletrônicas, a vantagem delas é que são rápidas, como a biometria, e seguras como as senhas. Com a popularização dos telefones celulares, ultimamente eles estão sendo usados em projetos para ter mais uma funcionalidade que é de trabalhar como chave de acesso em sistemas de segurança físico.

O presente trabalho visa abordar essa área de segurança de ambientes físicos expondo normas regulamentadoras e políticas de segurança que tratam do tema. Dentro deste contexto, tem como objetivo implementar um projeto de uma fechadura elétrica utilizando a tecnologia NFC (*Near Field Communication*) existente em telefones móveis, principalmente os smartfones, e cartões magnéticos.

A tecnologia NFC será utilizada como meio de transmissão para enviar uma chave do dispositivo (celular ou cartão) até o leitor que está conectado à fechadura. A placa *Arduino* é responsável por verificar esse código de acesso, e abrir a fechadura elétrica caso a chave esteja correta.

Este trabalho está estruturado da seguinte forma: Metodologia, contemplando os principais conceitos envolvidos no projeto; Materiais e métodos empregados para o desenvolvimento do sistema de controle de acesso; resultados e discursões acerca do trabalho; considerações finais e por fim, as referências bibliográficas das fontes de informações que foram utilizadas durante os estudos.

2. REFERENCIAL TEÓRICO

Nesse capítulo será apresentado o referencial teórico acerca dos temas envolvidos no trabalho. A primeira seção, sobre Segurança Organizacional, discorre sobre os conceitos gerais relacionados à segurança e descreve a importância que ela tem para empresas e organizações, ela também aborda sobre o controle de acesso a ambientes físicos informando a sua relevância para a segurança em geral. As duas seções finais tratam sobre a tecnologia NFC e a plataforma *Arduino*. A exposição dessas duas seções tem o objetivo de demostrar o funcionamento destas tecnologias, que serão utilizadas para a criação de uma solução de segurança para sistemas de controle de acesso a ambientes físicos.

2.1 Segurança Organizacional

A Segurança Organizacional é uma área abrangente que envolve pessoas e equipamentos no propósito de proteger tudo o que se tem valor para a empresa. Como aborda Hori (2003, p.18) a segurança é um serviço essencial que permeia toda a organização, ela está diretamente ligada à sobrevivência e ao bom funcionamento da empresa.

Devido a sua importância, a Segurança Organizacional é um tema que precisa ser tratado a nível gerencial, pois conforme Lessa (2004, p.9), as decisões sobre a segurança da empresa devem vir de uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do negócio.

Hori (2003, p.72) alerta que é necessário que toda a gerência tenha consciência da importância da segurança da informação tendo uma participação ativa nas aprovações das estratégias a serem adotadas. Dessa forma, as diretrizes de segurança da empresa serão mais respeitadas, pois a influência da gerência sobre assuntos como segurança terá mais efeitos do que se partisse de um setor inferior a esses gestores.

Assim como uma corrente é tão forte quanto o seu elo mais fraco, a segurança de uma empresa será nivelada a partir do ponto que oferece menos segurança, (LESSA, 2004, p.9), por isso, será gravemente comprometida se for negligenciado alguma parte potencialmente vulnerável. É importante que sejam

analisados todos os tipos de ataques e vulnerabilidades aos quais a empresa está exposta, pois não podem ser ignorados fatores internos, como os atos cometidos pelos próprios funcionários, e nem externos, como catástrofes naturais.

Conhecer os riscos é a primeira etapa para conseguir se defender deles, pois assim é possível realizar planejamentos e alcançar o melhor nível de segurança dentro dos recursos disponíveis. Segundo Caruso e Steffen (1999, p.65) “a etapa final da análise de risco é a geração do plano de segurança da organização”, que, segundo o autor, deve se preocupar com medidas e procedimentos para que falhas ou sinistros não ocorram.

Em meio a esse contexto, a informação tem se tornado de grande importância dentro da lista dos ativos das instituições. Na seção seguinte será abordada a dimensão dessa importância e as características de segurança requeridas por esses ativos.

2.1.1 Segurança da Informação

Como define a ABNT NBR ISO/IEC 27002 (2005), que aborda a gestão da segurança, a informação é um patrimônio que, como qualquer outro patrimônio importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido. O vazamento ou a destruição de informações podem levar ao fechamento de uma organização, por isso ela não deve ser tratada como simplesmente uma responsabilidade da área de informática, mas deve ser uma preocupação de toda a gerência da empresa.

“Nesse mundo globalizado onde as informações atravessam fronteiras (...), a proteção do conhecimento é de vital importância para a sobrevivência das organizações” (NAKAMURA e GEUS, 2003, p. 35). Da mesma forma que são criados projetos para viabilizar a sobrevivência da instituição no decorrer do tempo, também é necessário o planejamento de políticas de segurança que garantam a proteção da organização.

Cada estrutura organizacional necessita de características e níveis específicos de segurança para os seus dados. Segundo Spanceski (2004) os itens relevantes ao assunto, que precisam ser abordados na área de segurança, são:

Confidencialidade: é a característica necessária nos sistemas de segurança para que os dados não sejam compreendidos por terceiros caso venham a interceptar a comunicação entre remetente e destinatário(s).

Integridade: Informações erradas podem induzir o receptor da mensagem a tomar decisões incorretas, que prejudiquem a organização, por isso a integridade é a garantia de que a mensagem recebida pelo destinatário é a mesma que foi enviada pelo remetente, sem alterações.

Disponibilidade: o acesso à informação, em muitos casos, é essencial para o funcionamento de uma instituição. Sendo assim, é necessário que os dados sempre estejam disponíveis aos usuários autorizados.

Autenticidade: A autenticidade tem a responsabilidade de verificar se o suposto autor da mensagem é realmente quem ele diz ser, sendo que o mesmo também vale para o caso do destinatário.

Implantar sistemas de segurança demanda investimentos como aquisição de equipamentos e, em muitos casos, geram grandes transtornos. Por esses motivos que, no projeto desses sistemas, devem ser identificados os requisitos de segurança mais necessários para que possam ser priorizados os pontos relevantes.

Um exemplo de sistema que permite priorizar características de segurança é um serviço de e-mails, que valoriza a confidencialidade dos dados. Os provedores de e-mails podem até ficar suspensos por algum tempo, mas se o conteúdo das contas de e-mails for lido por pessoas não autorizadas, a empresa prestadora do serviço poderá passar por graves transtornos.

Assim, se faz necessária a criação de normas de segurança pelos próprios gestores, as quais necessitam ser registradas e formalizadas em um documento da política de segurança, tema que será tratado com mais detalhes na seção seguinte.

2.1.2 Política de segurança

Segundo a Publicação de Boas Práticas de Segurança do TCU (TCU, 2007) uma política de segurança é um conjunto de princípios e regras que norteiam a gestão de segurança de informação de uma instituição. Pela crescente importância da informação para as instituições, a segurança da informação ultrapassou a abordagem de ser simplesmente tecnológica e se tornou um assunto de nível estratégico.

Conforme orienta a ABNT NBR ISO/IEC 27002 (2005), a política de segurança é um tema que deve ser discutido e definido pelos gestores para estabelecer regras e procedimentos institucionais de segurança. Convém que a direção institua uma política clara e demonstre apoio e comprometimento com a segurança da informação por meio da criação e manutenção desta norma para toda a organização.

Conforme Peixoto e Moura (2004, p.6), para que exista segurança é necessário que todas as pessoas envolvidas na organização estejam comprometidas com esse propósito. Por isso existe a necessidade de que a gerência difunda a política de segurança, e incentive o respeito aos procedimentos com o intuito de fazer com que as regras sejam acatadas. Com relação ao possível descumprimento das regras, a implantação de penalidades é um mecanismo que pode ser utilizado para fortalecer o cumprimento da política implantada.

Apesar de que o estímulo ao respeito às regras e normas precise vir da gerência, cada nível de uma organização tem a sua responsabilidade em relação à segurança. A Figura 1 demonstra como estão divididas as atribuições entre esses níveis.

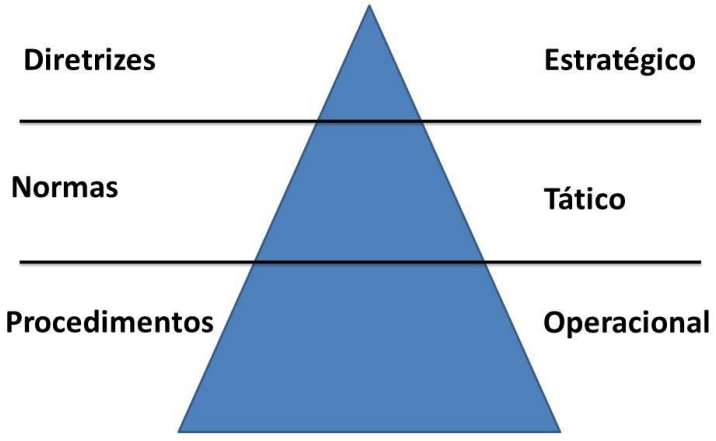

Figura 1: Níveis organizacionais (LESSA, 2004 apud SÊMOLA, 2003, adaptada).

No nível estratégico, é responsabilidade da gerência definir as regras de segurança com base no modelo de negócio da organização. As diretrizes impostas têm o objetivo de declarar os valores que devem ser seguidos para que a informação tenha o nível de segurança adequado.

As normas do nível tático são regras gerais utilizadas em todos os segmentos da instituição, elas definem procedimentos genéricos sem especificar métodos técnicos das operações. Os assuntos que geralmente são abordados por elas são atividades do cotidiano dos funcionários como acesso a arquivos no banco de dados, utilização da rede, realização de backup etc.

No nível operacional são descritos os procedimentos técnicos para realizar as atividades relacionadas ao manuseio dos bens da organização. Esses procedimentos geralmente são os que mais sofrem alterações com o tempo, porque pequenas mudanças na tecnologia utilizada na segurança os afetam primeiro.

A ABNT NBR ISO/IEC 27002 (2005) recomenda que sejam abordados vários assuntos no documento da política de segurança, alguns deles são:

- **Comprometimento da direção com a política de segurança:** O documento deve deixar claro que a gerência está de acordo com as normas e metas estabelecidas. Dessa forma, a direção fará com que o documento tenha mais credibilidade dentro da empresa;
- **Segurança em recursos humanos:** As questões da política relacionadas à segurança de recursos humanos definem as responsabilidades de funcionários, fornecedores e terceiros em relação ao uso e à proteção de recursos. Antes de serem assinados contratos devem ser esclarecidas as condições impostas pela política de segurança da empresa, e, só depois de aceitos os temos da política da empresa, o contrato poderá ser firmado;
- **Gerenciamento de incidente:** A política de segurança da organização deve prover mecanismos que minimizem os danos na ocorrência de catástrofes. É aconselhado que ela aborde sobre o gerenciamento de riscos e procedimentos em caso de incidentes, e que forneça o contato de pessoas e órgãos de apoio.

Os assuntos tratados na política de segurança de uma empresa podem variar muito dependendo do modelo do negócio, pois cada estrutura requer um nível de segurança adequado aos possíveis riscos e possuem características específicas que devem ser atendidas. Mesmo com essa subatividade dos temas da política de segurança, Wadlow (2000, p.15) descreve com mais detalhes do que a norma ABNT

NBR ISO/IEC 27002 (2005) as questões que devem ser levadas em consideração na criação desse documento:

- **O que deve ser protegido:** Descreve de forma detalhada os tipos de níveis de segurança esperados pela empresa. Por exemplo, caracterizando os ativos como: confidenciais, sensíveis e acessíveis;
- **Método de proteção:** Descreve em alto nível as prioridades de proteção. Por exemplo, prioridades organizacionais (como saúde e segurança humana), conformidade com a legislação e preservação dos interesses da empresa;
- **Responsabilidade:** Descreve as responsabilidades de cada classe de usuários. Por exemplo, descreve as responsabilidades de usuários como: contratados, convidados e administradores de sistemas;
- **Uso adequado:** Descreve como os participantes da empresa deverão ou não usar a rede. Por exemplo: os convidados não podem acessar a rede interna e os administradores têm acesso a todos os documentos da empresa;
- **Diretoria de análise de segurança:** É uma equipe formada por três funcionários da empresa que têm cargos de diretores ou outro nível superior. Entre as funções dessa equipe está a de aplicar penalidades aos colaboradores e fornecedores da empresa que descumprirem as normas da política de segurança;
- **Penalidades:** As penalidades foram classificadas por Wadlow (2000, p.19) em três níveis: crítica, séria e limitada. As penalidades críticas são recomendações de demissão ou para a abertura de ação legal; as sérias são recomendações para demissão e desconto de salário, e as limitadas são recomendações para desconto de salário, repreensão formal e suspensão não remunerada.

Segundo Wadlow (2000, p.19) as recomendações feitas pela equipe de segurança são sujeitas à administração executiva da empresa, que poderá ou não acatar essas recomendações.

A política de segurança para correspondentes bancários do banco Santander (2013) faz uso dos pontos citados pela ABNT NBR ISO/IEC 27002 (2005) e também pelos temas abordados por Wadlow (2000). Santander (2013) menciona a responsabilidade dos correspondentes em resguardar as informações sigilosas da mesma forma que a ABNT NBR ISO/IEC 27002 (2005, p.8) fala da importância em definir as responsabilidades pela gestão da segurança da informação.

Seguindo os pontos mencionados por Wadlow (2000, p.19), a política de segurança do banco Santander (2013) cita que a violação dos procedimentos de segurança pode acarretar em rescisão de contrato, penalidades civil e penal.

A segurança de ambientes físicos é um assunto que também deve ser tratado na política de segurança, descrevendo as responsabilidades dos usuários desses ambientes e a forma de utilização. Por ser uma parte importante para esse trabalho ela será tratada com mais detalhes na seção seguinte.

2.1.3 Segurança física e de ambiente

A segurança física e de ambiente visa à proteção da área física de uma instituição contra todos os possíveis incidentes, sejam eles naturais ou intencionais. O tema é bem abrangente, pois, como é abordado na ABNT NBR ISO/IEC 27002 (2005), ele precisa compreender problemas desde a falta de energia elétrica até inundações.

A ABNT NBR ISO/IEC 11515 (1990), que é uma norma pautada na segurança física de dados, relaciona uma série de fatores que influenciam na segurança dos ambientes físicos, alguns deles são:

- A **localidade** onde a edificação está situada influencia na segurança, pelo fato de que precisa ser estudada a ocorrência de catástrofes ambientais. Com isso, se for instalado um prédio em uma área onde é frequente o acontecimento de fenômenos como descargas atmosféricas, é necessário que sejam tomadas medidas de segurança em relação a esses fenômenos;
- O ideal é que o prédio que acomodará a empresa seja **projetado especificamente** para esse fim, mas caso isso não seja possível, é necessário que sejam feitas as **modificações necessárias**, pois o

modelo do edifício pode facilitar ou dificultar a implantação de sistemas de segurança;

- Tanto **temperaturas** baixas como altas danificam equipamentos, principalmente os eletrônicos. Com isso, o **clima** está diretamente ligado à vida útil dos dispositivos de armazenamento e processamento de dados.

Pelo fato de que os ativos requerem aspectos de segurança específicos, é aconselhável que dentro de uma empresa também sejam criadas diferentes zonas de segurança para acomodar os ativos de acordo com sua prioridade. Esse procedimento tem o objetivo de proteger os bens conforme as suas características. Por exemplo, um ambiente que guarda fitas de backup precisa ser devidamente protegido em relação ao acesso físico, mas não necessita ter um sistema redundante de energia elétrica, como em uma sala de servidores que não podem parar de realizar o processamento de dados.

A divisão de áreas para acomodar os bens da empresa também ajuda a melhorar o desempenho da segurança em geral, pois assim é possível direcionar recursos para áreas mais críticas. Conforme citam Peixoto e Moura (2004, p.10) dessa forma também é possível conseguir economizar em investimentos, uma vez que é aceitável deixar de implantar mecanismos de segurança pelo fato de que o ativo não requer esse cuidado.

Outro fator que deve ser levado em consideração é a segurança dos ambientes em relação aos funcionários da organização. A ABNT NBR ISO/IEC 27002 (2005) sugere que as áreas onde estão localizados os ativos mais valiosos apenas sejam divulgadas aos funcionários somente quando for necessário. Em situações onde o processamento dos dados é realizado em um prédio separado dos demais anexos da organização, é aconselhável que seja evitada a implantação de placas indicativas que identifiquem a finalidade dessa edificação. Dessa forma, evita-se que terceiros venham a conhecer a localização dessa área vital das empresas, que é o setor de processamento de dados.

O controle de acesso físico é uma parte que compõe a segurança física e de ambiente pelo fato de ser responsável por controlar o trânsito de pessoas nas áreas

seguras da instituição. As características necessárias de um sistema dessa área serão tratadas com mais detalhes na seção seguinte.

2.1.4 Controle de acesso físico

O controle de acesso físico é um conjunto de regras e procedimentos que têm o objetivo de registrar e restringir o ingresso de pessoas não autorizadas em instalações. Segundo Bauer (2006, p.12) esse controle visa a impedir que indivíduos sem as devidas permissões tenham acesso a ambientes físicos, com o intuito de proteger os equipamentos que tratam ou armazenam as informações, buscando a prevenção de possíveis perdas, roubos ou vazamentos de informações.

Em muitas empresas o controle do acesso físico não tem a mesma relevância se comparada à segurança lógica. É necessário que da mesma forma em que os acessos lógicos requerem nome de usuário e senha dos usuários para acessar os sistemas pela rede, os acessos físicos da empresa também precisam ser gerenciados, permitindo a entrada de pessoas somente aos locais previamente definidos pela administração.

A ABNT NBR ISO/IEC 27002 (2005) orienta que o pedido para a liberação de acesso aos ambientes necessita ser formal e de responsabilidade de um gerente designado para essa função. Nessa requisição é necessário que sejam descritas informações a respeito dos motivos da liberação desse acesso e registradas informações como data e pessoas envolvidas.

As regras do controle de acesso que, por exemplo, delimitam o período de acesso a uma determinada sala, devem ser analisadas e registradas no documento da política de segurança da organização, tomando como base os requisitos do ambiente (ABNT NBR ISO/IEC 27002, 2005, p.65). As permissões fornecidas a cada indivíduo devem admitir apenas as necessidades imprescindíveis ao cumprimento do seu objetivo, deixando bloqueadas as entradas em ambientes desnecessários.

A ABNT NBR ISO/IEC 27002 (2005) orienta que o gestor precisa analisar regularmente o direito de acesso dos usuários por meio de processos formais. Esse procedimento é necessário pelo fato de que as funções dos usuários podem mudar no decorrer do tempo, e com isso é preciso regular suas permissões em relação as suas novas funções.

Implantar esse processo de controlar as permissões dos funcionários aos ambientes físicos é uma tarefa que aumenta o trabalho da empresa e também gera incômodos aos funcionários. Moura e Peixoto (2004, p.6) afirmam que se as medidas de segurança forem um entrave para o trabalho das pessoas, isso trará prejuízos para a empresa, pois essas medidas podem diminuir a produtividade dos funcionários.

Por isso, Nakamura e Geus (2003, p.47) alertam para o fato de que a administração da segurança de uma organização é uma tarefa complexa, dessa forma as medidas devem ser dimensionadas, para que a produtividade dos usuários não seja afetada. Consequentemente, um dos motivos de não se usar o controle de acesso nos ambientes dentro de uma empresa é o transtorno que eles acarretam aos utilizadores durante o expediente de trabalho.

Mesmo com esses empecilhos, o controle de acesso não pode ser ignorado em algumas áreas de uma empresa como o a sala de servidores que armazenam e processam dados. O importante para se ter um bom sistema de segurança é analisar as características do local com o intuito de projetar um sistema que se adeque ao ambiente para não atrapalhar o trabalho e que esteja de acordo com a disponibilidade financeira.

O NFC é uma tecnologia que pode ajudar os gestores em controlar áreas que requerem esse controle de acesso, além de beneficiar os usuários, pois ela tem o objetivo de ser uma tecnologia de fácil utilização em situações que requerem comodidade. A seção seguinte demonstra as características dessa tecnologia que pode ser utilizada como uma opção de controle de acesso.

2.2 NFC (Near Field Communication)

Conforme descreve Simões (2008), o NFC (Near Field Communication) é uma tecnologia de transmissão de dados sem fio para curtas distâncias, dessa forma os dispositivos não precisam estar conectados fisicamente para realizar a transferência de dados. Ele não tem a pretensão de ser mais veloz do que outros tipos de transmissão, como o bluetooth, mas possui características peculiares que o diferenciam das tecnologias já existentes (ATOJI, 2010).

O NFC está presente principalmente em cartões e celulares smartphones. Devido ao seu tamanho reduzido, foi projetado para não ter baterias energéticas. No

entanto, por possuir um chip responsável por emitir os dados gravados, é necessário que se tenha energia disponível para realizar o procedimento de leitura dos dados contidos no chip.

Na seção seguinte será demostrado qual e como é o funcionamento da tecnologia que possibilita o NFC não possuir baterias ou conexões diretas com uma rede elétrica.

2.2.1 Transmissão de energia sem fio

Para possibilitar que os dispositivos NFC consigam fazer operações sem estarem conectados a uma fonte de energia, é utilizada uma tecnologia que é estudada desde o século XX por Nikola Tesla (FRANCA, NETO e OLIVEIRA, 2003). O cientista buscou maneiras de enviar energia entre dispositivos fisicamente distantes por ondas eletromagnéticas, dispensando a necessidade de fios. O NFC utiliza desse mecanismo para obter do próprio dispositivo que irá ler os dados a energia necessária ao seu funcionamento.

Conforme define Assis (2012, online) o fenômeno da propagação das ondas eletromagnéticas corresponde ao processo físico no qual a energia irradiada por um equipamento emissor de ondas atinge outro dispositivo que capta esses sinais. A Figura 2 demonstra quais são as partes que compõem um sistema de transmissão de energia sem fio e como é realizado esse procedimento.

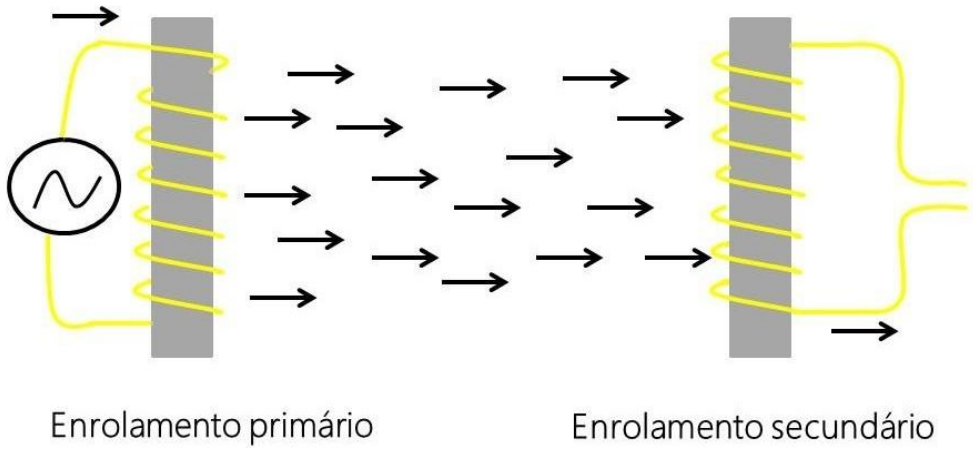

Figura 2: Transmissão de energia sem fio

O modelo apresentado na Figura 2 é formado por duas bobinas, que são fios enrolados de forma espiral, e uma fonte de energia elétrica ligada nas duas

extremidades dos fios que envolvem a bobina do enrolamento primário. Devido às características das ondas eletromagnéticas, Gondim (2010) diz que é necessário um caminho livre de obstáculos entre o transmissor e o receptor para a viabilidade da transmissão.

Conforme menciona Real (2008, p.2) quando uma corrente elétrica passa por um fio, ela gera um campo eletromagnético que é irradiado pelo ar e até mesmo no vácuo. Esse fenômeno é o descrito na Figura 2 em que a fonte de energia insere uma corrente elétrica no enrolamento primário, e essa corrente faz emitir ondas eletromagnéticas que são recebidas no enrolamento secundário.

As ondas que chegam ao segundo enrolamento são novamente convertidas em uma corrente elétrica. Com isso, a segunda bobina pode ser conectada a um dispositivo eletrônico para funcionar como fonte de energia.

A potência emitida pelo transmissor e a potência captada pelo receptor são diferentes, pois as perdas energéticas são proporcionais à distância entre os aparelhos. Esse problema inviabiliza o uso em equipamentos com alto consumo energético, e isso fez com que essa tecnologia fosse inviável em muitas aplicações como a transmissão de energia sem fio para condicionadores de ar e televisores.

Apesar da energia sem fio sofrer muitas perdas durante a transmissão, ela pode ser utilizada em pequenos dispositivos, como no caso de um emissor de dados NFC, que possui um chip com baixo consumo de energia e que foi projetado para funcionar quando estiver perto do seu leitor.

Dessa forma, ao se aproximar o dispositivo NFC de um leitor para realizar a transferência dos dados, o leitor envia a energia necessária para alimentar o dispositivo. Portanto, mesmo se o NFC estiver em um telefone celular que se encontra com a bateria descarregada, poderá ser realizado o procedimento de transferência dos dados normalmente (FILHO, 2010, p.58).

A forma de transmissão dos dados nos dispositivos NFC também faz uso das ondas eletromagnéticas e, da mesma forma que a transmissão de energia, ela também foi projetada para funcionar a curtas distâncias nos dispositivos NFC.

2.2.2 Transmissão de dados NFC

Segundo Dantas (2002, p.9) o sinal é a entidade que é transmitida em um sistema de comunicação; e o transmissor é responsável por converter, de alguma

maneira, a informação na fonte para uma forma de sinal. Em um sistema de comunicação eletromagnético as informações são transformadas em sinais que se propagam pelo ar ou pelo vácuo.

Essa conversão de informação em sinal, citada por Dantas (2002, p.9), é denominada modulação. Conforme Casagrande (2008) a modulação é a mudança de uma ou mais características de uma onda de acordo com outro sinal (que são os dados a serem transmitidos).

Para Real (2008), os dados da comunicação podem ser transmitidos por diversas formas numa onda, fazendo com que os dados alterem características como: amplitude, frequência e fase da onda. Por exemplo, em um sistema de modulação por amplitude as informações provocam alterações na amplitude da onda, dessa forma essas variações serão entendidas como as informações enviadas do transmissor para o receptor.

Segundo Laskoski, Marcondes e Szerementa (2006), “portadora” é o nome dado à onda eletromagnética responsável pelo transporte de informação no meio de transmissão. A Figura 3 demonstra como é realizado esse processo de unir a onda portadora com os dados que o remetente pretende enviar.

Figura 3: Processo de modulação

A onda portadora é uniforme, mas quando ela se une com os dados a serem enviados no processo de modulação ela sofre alterações na sua estrutura e se transforma em uma onda modulada conforme apresentado na Figura 3. No receptor a onda sofre o processo inverso chamado de demodulação, assim é descartada a onda portadora e o que fica são os dados.

Segundo a ISO/IEC 18092 (2004), a frequência da onda portadora utilizada nos dispositivos NFC é de 13,56 MHz. Assim, os aparelhos NFC que contêm as

informações a serem transmitidas enviam os dados embutidos em uma onda nessa frequência com o intuito de que o receptor abstraia as informações contidas nessa onda.

A frequência da onda portadora influencia diretamente na qualidade do sinal recebido pelo receptor e pela quantidade de dados que a onda pode enviar em um período de tempo. A Tabela 1 apresenta algumas faixas de frequência e demonstra aplicações que fazem uso das mesmas.

Tabela 1: Faixa de frequência e suas aplicações

Frequência	Aplicação
3 a 30 Hz	Comunicação com submarinos
300 Hz a 3 kHz	Comunicação com minas
30 a 300 KHz	Comunicação internacional, navegação, rádio em alguns países
300 KHz a 3 MHz	Navegação, rádio AM
3 a 30 MHz	Rádios HM
30 a 300 MHz	Rádios FM, televisão, aviação
300 MHz a 3 GHz	Televisão aberta, celulares, redes sem fio
3 a 30 GHz	Redes sem fio, satélites
30 a 300 GHz	Radares, radioastronomia, armas avançadas

Fonte: REAL (2008).

As aplicações que necessitam transportar mais dados por segundo utilizam frequências mais altas, mas as frequências baixas têm a característica de conseguir chegar a pontos mais distantes do que as altas frequências.

A capacidade de transmissão de dados em uma determinada onda está diretamente relacionada com sua frequência. Quanto maior a frequência, maior a quantidade de dados que podem ser enviados por intervalo de tempo. Além da capacidade de transmissão, a frequência também é determinante no alcance da onda e nos meios nos quais ela é capaz de penetrar (VILELA, 2012, p.6).

A ISO/IEC 18092 (2004) delimita que a maior taxa de transferência entre os dispositivos NFC seja de 424 kbps por segundo, a uma distância de trabalho de 20 centímetros entre o leitor e o emissor dos dados. Apesar de a faixa de frequência utilizada pela tecnologia possibilitar a comunicação com distâncias maiores, a norma definidora não utilizou esta característica da onda.

Atoji (2010) explica que a distância de operação dos dispositivos NFC é curta para ser inerentemente segura, no que diz respeito a tentativas de interceptação. Esse procedimento dificulta que outros aparelhos possam capturar os dados durante a transmissão. A segurança é uma das características que possibilita a utilização do NFC em sistemas que necessitam de proteção para o sigilo dos dados, por isso ele já é utilizado em sistemas de pagamento, conforme cita Oxford (2012).

Segundo Mazzola (2000), as transmissões de dados realizadas entre equipamentos ocorrem de três formas: simplex, half-dupex e full-duplex. A tecnologia NFC faz uso do simplex e half-dupex. A Figura 4 demonstra o modo de funcionamento desses diferentes modelos.

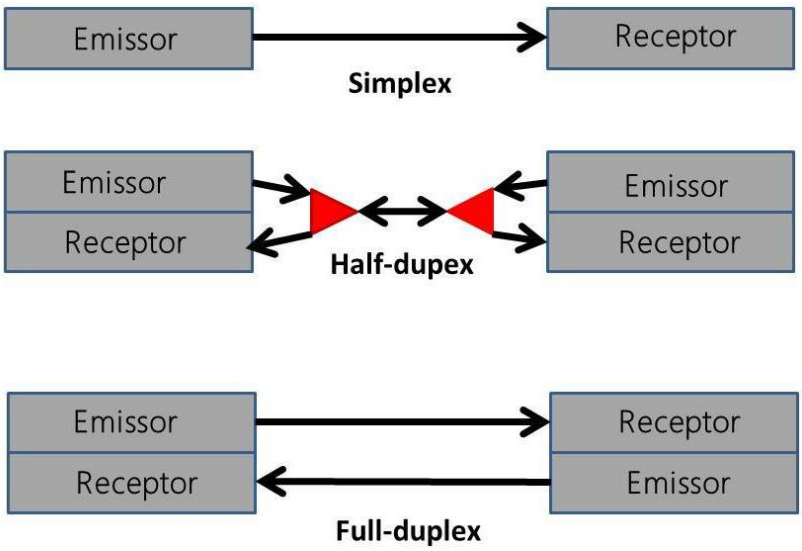

Figura 4: Transmissão de dados

A Figura 4 demonstra o sentido da transmissão e a quantidade de canais utilizados entre as duas partes. A forma como são empregados esses canais é especificada por Mazzola (2000) como:

- **Simplex:** a informação é transmitida em uma única direção. Nesse modelo as duas partes somente operam com procedimentos bem definidos que são uma enviar e a outra receber os dados;

- **Half-dupex:** “quando a transmissão é feita nos dois sentidos, mas não ao mesmo tempo”. Assim, uma parte precisa esperar a outra desocupar o meio de transmissão para poder enviar os dados; e
- **Full-duplex:** “quando a transmissão é feita nos dois sentidos simultaneamente”. Nesse modelo existem dois canais de comunicação possibilitando o envio simultâneo de informações.

Os dois primeiros modos são utilizados nas formas de comunicação do NFC. De acordo com Filho (2010) “a tecnologia NFC tem três modos de operação diferentes: modo leitura/escrita, modo pear-to-pear e modo de emulação de cartões”:

Modo leitura/escrita: “neste modo o dispositivo NFC ativo inicia uma operação em uma tag passiva”. Dessa forma o modelo da comunicação é do tipo simplex, pois os dados trafegam em um único sentido da tag ao leitor NFC;

Modo pear-to-pear: dois dispositivos podem trocar dados entre si e, como Atoji (2010) afirma que os dispositivos compartilham uma única banda de frequência, o modo pear-to-pear é classificado como half–duplex, pois esse modo utiliza somente um canal de comunicação;

Modo emulação de cartões: o próprio dispositivo NFC age como sendo uma etiqueta NFC, funcionando para o leitor um dispositivo de somente leitura. Nesse modo a comunicação é classificada como simplex novamente, pois apesar de que o dispositivo possa enviar dados, ele está no modo de somente leitura.

Dessa forma, de acordo com Atoji (2010), os dispositivos NFC podem trabalhar de modo ativo ou passivo:

Ativo: “ambos os dispositivos são capazes de gerar seus sinais de radiofrequência para a comunicação”.

Passivo: “apenas um dispositivo (denominado iniciador) gera o sinal de radiofrequência para comunicação”.

A Figura 5 demonstra como é realizada a transferência dos dados em uma comunicação passiva. O leitor NFC envia as ondas eletromagnéticas responsáveis por alimentar o dispositivo passivo, e quando o seu chip for energizado ele envia outra onda de volta ao leitor contendo os dados que estão internamente na sua memória.

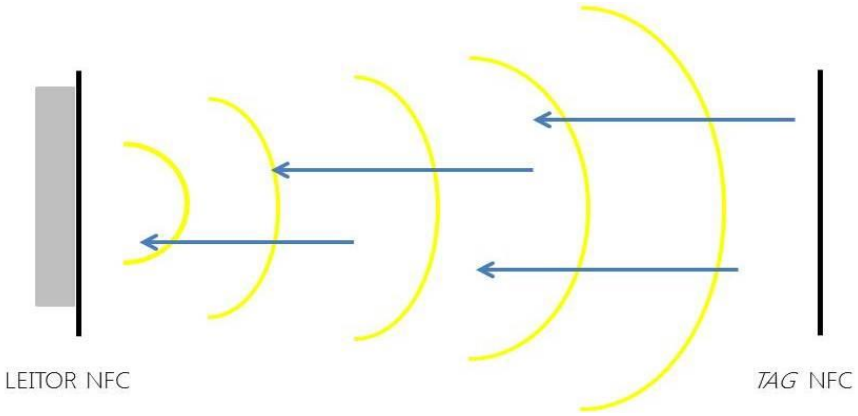

Figura 5: Comunicação NFC passiva

A comunicação ativa se diferencia da comunicação passiva (Figura 5) pelo fato de não serem emitidas ondas para alimentar os dispositivos, o que não é necessário, pois tanto o leitor como a etiqueta que contêm os dados possuem energia própria.

Um exemplo de sistemas ativos é a comunicação de dois celulares no modo pear-to-pear. Neste modelo, ambos não precisam enviar ondas eletromagnéticas pois os dois dispositivos possuem baterias para alimentarem os chips que enviam a onda portadora com as informações. Um exemplo de sistema passivo é a leitura de cartões NFC, assim o leitor precisa transmitir energia para que o chip do cartão seja alimentado e possa enviar os dados.

Como foi demonstrado no decorrer desta seção e também como comenta Simões (2008, p.23), a tecnologia NFC possui características no seu projeto de ser uma tecnologia que proporcione segurança na transmissão dos dados por limitar a conexão somente em pequenas distâncias. Mas outras tecnologias também podem ser incorporadas ao NFC, como a criptografia dos dados e pedido de permissão para efetuar uma transferência.

Na seção seguinte será abordado sobre a plataforma de prototipagem eletrônica *Arduino* que, no contexto deste trabalho, será integrada a dispositivos NFC no intuito de ser criado um sistema de segurança para o controle de acesso físico.

2.3 Arduino

Segundo *Arduino* (2013, online), “*Arduino* é uma plataforma de prototipagem eletrônica open-source baseado em *hardware* e *software* flexíveis e de fácil

manuseio”. A plataforma permite a criação de projetos para diversas áreas como robótica, educação, medicina e qualquer outra atividade na qual possa ser utilizado o processamento eletrônico.

A plataforma *Arduino* é composta de uma placa eletrônica (*hardware*) e de um ambiente de desenvolvimento (*software*) para criação dos projetos pelos usuários (PINTO, 2011, p.49). Já existem no mercado outros *hardwares* como o da Philips e *softwares* de gravação, como o Matlab, mas o intuito da plataforma *Arduino* é ter *hardware* e *software* próprio que facilite o trabalho de iniciantes e pessoas com pouco conhecimento em eletrônica. A plataforma *Arduino* foi projetada com a finalidade de ser de fácil entendimento, programação e aplicação, além de funcionar em diversos sistemas operacionais (FONSECA e BEPPU, 2010).

O *software* de desenvolvimento dos códigos e a documentação desse projeto podem ser baixados gratuitamente no site oficial da plataforma: http://www.arduino.cc. Como a maioria dos *softwares* livres, a plataforma *Arduino* também é aberta a sugestões de melhorias.

Como aborda Melo (2010, p.1) as placas da plataforma *Arduino* podem ser utilizadas para desenvolver artefatos interativos de forma independente ou conectadas a um computador. Os dois formatos de utilização seguem o mesmo princípio de funcionamento de um sistema computacional que é a interação das etapas: entrada, processamento e saída, a Figura 1 apresenta como é o fluxo dos dados entre esses componentes.

Figura 6: Sistema computacional (FONSECA e BEPPU, 2010, p.2, adaptada)

Entrada: O primeiro bloco da Figura 1 é responsável por receber ou captar dados, nos sistemas *Arduino* esses dados podem ser provenientes de sensores, computadores ou comandos enviados por usuários.

Processamento: A parte de processamento é responsável por executar as ações pré-definidas levando em consideração os dados provenientes da etapa de

entrada. Na plataforma *Arduino* essa tarefa é realizada pelo microcontrolador que armazena internamente o código com as regras de execução.

Saída: A saída de um sistema computacional é o resultado da etapa de processamento dos dados, na plataforma *Arduino* essas saídas podem ser impulsos elétricos que acionam equipamentos como: lâmpadas e eletrodomésticos, ou até mesmo enviam uma mensagem para um celular.

Como aborda Pinto (2011, p.49) “o elemento inteligente da placa é o microcontrolador”, ele é o principal componente da placa, pois todo código é armazenado e processado nele. Devido sua importância, o microcontrolador será tratado com mais detalhes na seção seguinte.

2.3.1 Microcontrolador

Como abordam Fonseca e Beppu (2010) “um microcontrolador (também denominado MCU) é um computador em um chip, que contém processador, memória e periféricos de entrada/saída”. Dessa forma, um microcontrolador é um sistema computacional composto pelas estruturas básicas necessárias para desenvolver o trabalho de processamento de dados.

O mercado conta com uma diversidade de microcontroladores com diferentes características de tamanho, preço e poder de processamento. A Tabela 2 apresenta alguns modelos de diferentes fabricantes informando a frequência de trabalho, quantidade de memória RAM (Random Access Memory) e memória ROM (Read Only Memory) que cada chip contém.

Tabela 2: Microcontroladores

Fabricante	Microcontrolador	Frequência	RAM	ROM
Intel	87C51-24	24 MHz	256 B	4 KB
Philips	P87C51MB2	24 MHz	2 KB	4 KB
Atmel	AT89C5115	40 MHz	512 B	18 KB
Dallas	DS87C550	33 MHz	1 KB	8 Kb

Fonte: Adaptação de Zelenovisky e Mendonça (Online).

Como abordam Nichel e Bessa (2010, p.3), o aumento da frequência influencia no aumento da capacidade de processamento. Dessa forma pode ser

observado que o poder de processamento dos microcontroladores é menor do que os dos computadores pessoais, pois estes, geralmente, trabalham com frequência superior a GHz. Como demostra a Tabela 2, a faixa de frequência de trabalho dos microcontroladores fica em MHz.

Como pode ser visto nas duas últimas colunas da Tabela 2, os microcontroladores possuem entre os seus componentes as memórias RAM e ROM. E, assim como a frequência, Santos (2009, p.11) fala que elas representam um fator crucial no desemprenho dos microcontroladores.

Para Livi e Silveira (2006, p.10) RAM é a memória utilizada pelos usuários para desenvolver programas. Seu uso restringe-se ao período em que o equipamento está em funcionamento. Se a máquina não receber energia mesmo em um curto espaço de tempo, todo o conteúdo da memória RAM será apagado, ou seja, é uma memória volátil.

Segundo Livi e Silveira (2006, p.10) a ROM é uma porção de memória que não depende de energia para manter o seu conteúdo, ou seja, é uma memória não volátil. Dessa forma, a ROM pode ser utilizada para gravar códigos que não podem ser apagados quando o chip for desenergizado.

A plataforma *Arduino* utiliza os microcontroladores da fabricante Atmel e são empregados diferentes modelos de chips para serem acomodados aos vários tipos de placas que a plataforma possui (ARDUINO, online, 2013). Cada modelo dos microcontroladores da plataforma possui diferentes tamanhos de memória e frequência de processamento.

Arduino (online, 2013), declara que pode ser utilizada a linguagem de programação C para realizar a criação do código para os microcontroladores da plataforma *Arduino*. Entretanto, para facilitar a criação do código pelos utilizadores da plataforma, foi desenvolvida uma linguagem própria, como será demostrado na seção seguinte.

2.3.2 Linguagem de programação para *Arduino*

Como o intuito da plataforma é de ser de fácil aprendizado, se faz necessária a utilização de uma linguagem de programação de alto nível para esconder as peculiaridades do *hardware* dos programadores. Para isso, a plataforma *Arduino* escolheu a linguagem C\C++ para ser utilizada como referência, preservando a sua

sintaxe clássica na declaração de variáveis, nos operadores, nos ponteiros, nas estruturas e em muitas outras características da linguagem (MELO, 2012. p.7).

Segundo *Arduino* (online, 2013), os programas *Arduino* podem ser divididos em três principais partes:

Estruturas: A estrutura compreende as estruturas de controle, operadores aritméticos e booleanos. Os ponteiros que tem na linguagem C, também estão presentes na plataforma *Arduino*.

Valores: Os valores abrangem os tipos de dados suportados pela plataforma, ela aceita a maior parte dos tipos das linguagens de alto nível como: *int*, *float*, *bolean* e etc. Mas o diferencial é que ela possui tipos como *higth* e *low* para declarar que algum pino do *chip* seja colocado com 5 volts ou 0 volts.

Funções: A plataforma contém várias funções específicas para microcontroladores, a exemplo disso temos as funções digitais e analógicas que são utilizadas para realizar o controle dos pinos que são a interface de entrada e saída de dados.

Os códigos para *Arduino* apresentam a peculiaridade de necessitar de duas funções, *setup*() e *loop*(), que são específicas da linguagem. As funções *setup*() e loop() são de carácter obrigatório, ou seja, mesmo que não necessária a sua utilização deverão constar no código utilizado (SANTOS, 2009, p.20):

setup(): rotina inserida no inicio do programa para determinar as configurações necessárias ao programa (PINTO, 2011, p.141).

loop(): função executada após a configuração (setup()). Será executada continuamente enquanto a energia não for desligada (PINTO, 2011, p.141).

Os códigos escritos usando o ambiente de desenvolvimento *Arduino* são chamados de sketches, e esses arquivos ficam salvos com a extensão .Ino (ARDUINO, 2013).

A forma de como os programas são criados na plataforma *Arduino* se parecem com outras linguagens como Java, a diferença é que a plataforma *Arduino* precisa de mais uma fase, que é a gravação do código no microcontrolador. As fases do processo de criação de um programa com a plataforma estão expostas na Figura apresentando as quatro fases que são: criar, compilar, gravar e executar.

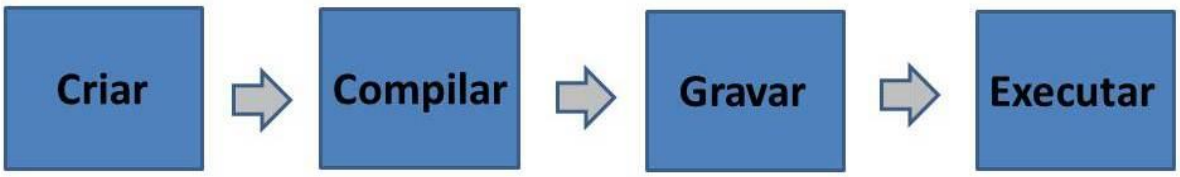

Figura 7: Fases de desenvolvimento de uma aplicação (Fonte: Adaptação de Santos, 2009)

A primeira fase do processo apresentado na Figura 7 é a criação do código pelo usuário. Nessa fase são criadas as estruturas lógicas e declaradas as bibliotecas utilizadas no código. Em seguida o código é passado por um compilador, que, segundo *Arduino* (2010, online), transforma o código legível em instruções de máquina.

Como mostra a Figura 7, depois que o código é compilado ele vai para a fase de gravação, nessa fase o programa é enviado do computador para a memória do microcontrolador. A última fase, que é a execução do código, acontece espontaneamente assim que microcontrolador é energizado, isso acontece pelo fato de que toda a estrutura dos códigos *Arduino* são escritos dentro da função *loop*().

Segundo a *Arduino* (2013, online), são realizadas várias etapas no processo de compilação, essas etapas como podem ser visto na Figura 8, são: verificação, transformação e junção do código do usuário para que ele fique no formato em que o microcontrolador possa processar.

Figura 8: Compilação

As etapas da compilação são descritas da seguinte forma:

- **Verificação:** Na primeira fase é executada uma verificação para certificar que o código está escrito corretamente;
- **Transformação:** em seguida o código é transformado em linguagem de máquina que é o formato que será gravado na memória do microcontrolador;

- **Junção:** Na fase de junção o código escrito pelo usuário é unido às bibliotecas utilizadas no código.

O resultado do processo de compilação, apresentado na Figura 8, pelas fases de verificação, transformação e junção, é um único arquivo que pode ser enviado ao chip para ser gravado na memória.

Conforme cita Melo (2012, p.9), a plataforma conta com diversas bibliotecas que trabalham em áreas como comunicação serial, sensorialmente e controle de motores. Além disso, segundo *Arduino* (2013) a plataforma permite aos usuários criarem suas próprias bibliotecas para serem utilizadas nos seus projetos e disponibilizadas para outras pessoas.

2.3.3 Shields

Com o objetivo de aumentar as funcionalidades da placa *Arduino*, várias empresas de *hardware* desenvolveram placas eletrônicas adicionais denominadas *Shields* (PINTO, 2011, p.51). Essas placas desempenham trabalhos como: sensores de temperatura, transmissores de mensagens da rede de celulares e leitores de dados NFC.

As *Shields* são acopladas as placas *Arduino* como na Figura 9 que tem uma placa *Arduino* Uno conectada a uma *Shield Ethernet* em sua parte superior.

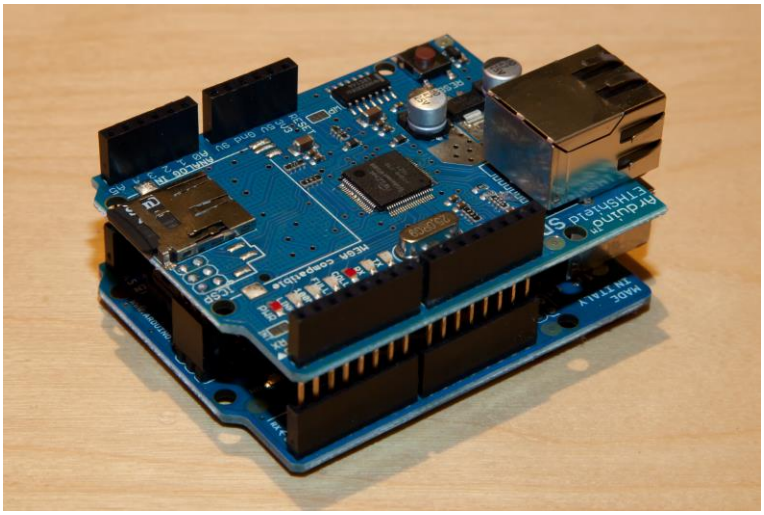

Figura 9: *Shield* Ethernet

Alguns modelos de *Shilds* são projetados para encaixar fisicamente nas placas *Arduino* conforme o exemplo da Figura 9. As *Shields* enviam e recebem dados funcionando como uma interface para as placas *Arduino*.

Assim como as placas *Arduino*, as *Shields* existem em diversos modelos. Alguns desses modelos estão expostos no site oficial da plataforma: http://www.arduino.cc, e outros modelos podem ser encontrados em outros fabricantes como: http://www.seeedstudio.com/depot/.

No decorrer desta seção pode ser visto que a plataforma apresenta flexibilidade tanto nas placas quanto na programação, possibilitando que sejam criados projetos simples e também os que requerem mais recursos.

3. MATERIAIS E MÉTODOS

Nessa seção serão apresentados os materiais e métodos utilizados na realização da parte prática desse trabalho.

3.1 Materiais

3.1.1 Fechadura elétrica

A fechadura elétrica, apresentada na Figura 10, é um dispositivo que destrava a tranca de segurança quando recebe uma tensão de 12 volts nas suas conexões. A fechadura também funciona utilizando a chave mecânica convencional, o que ajuda quando falta energia para abrir a fechadura.

Figura 10: Fechadura eletrônica

O modelo da fechadura utilizado no projeto foi o da *Soprano serie FE780*, mas grande parte das fechaduras sequem o mesmo padrão de funcionamento e acionamento. O projeto requer que a fechadura tenha o acionamento com um pulso elétrico de 12 volts, dessa forma podem ser empregados outros tipos de fechaduras para a criação do trabalho.

3.1.2 *Shield* NFC

A *shield* NFC, ilustrada na Figura 11, é uma placa que lê e grava informações em dispositivos com a tecnologia NFC em uma distância média de alcance de 10 cm. A placa também possibilita a troca de dados com outros dispositivos, como celulares, quem possuam a tecnologia NFC.

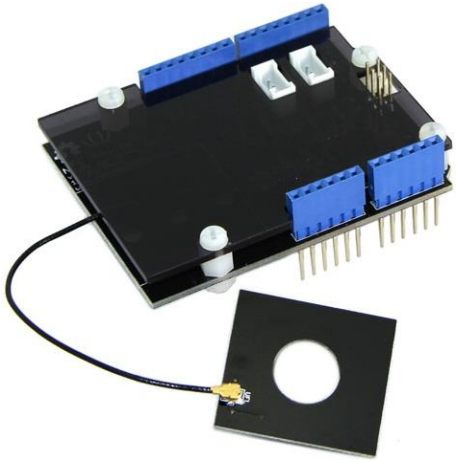

Figura 11: *Shield* NFC

O modelo do leitor utilizado no projeto foi a *Shield Elecfreaks v 1.6*, e assim como em grande parte das placas de expansão da plataforma *Arduino*, essa *shield* tem o formato para ser encaixada nos modelos convencionais de placas como *Arduino Uno*. Dessa forma, a placa dispensa a necessidade de soldar fios para realizar a ligação da *Shield* com a placa *Arduino*, necessitando apenas que seja gravado o código no microcontrolador para começar o uso.

A placa utiliza o protocolo de comunicação serial SPI para realizar o envio e recebimento de dados da placa ao qual está acoplada. A alimentação energética da *shield* é obtida da placa *Arduino* à qual está acoplada.

3.1.3 Placa *Arduino* Uno

O *Arduino Uno,* apresentada na Figura 12, é uma placa que utiliza o microcontrolador *Atmega 328,* de 16 MHz. A placa possui dois conectores para realizar a alimentação da placa, um dos conectores é do formato USB que tem a entrada de 5 Volts, o outro conector utiliza a tensão de 12 volts.

Figura 12: *Arduino* Uno

A comunicação da placa com o computador é realizada pela mesma porta USB que fornece energia pela placa. Ao ser acoplada a um computador, a placa é conectada a uma porta serial.

3.1.4 Relé

O relé, ilustrado na Figura 13, é um dispositivo que funciona como um interruptor eletromecânico, pois ao fornecer corrente elétrica nos terminais de acionamento o relé fecha o contado entre os terminais secundários.

Figura 13: Relé

O relé é utilizado principalmente para acionar dispositivos de alto consumo utilizando baixas tensões, uma vez que, dessa forma, possibilita que uma pequena corrente de entrada nos terminais de acionamento controle a abertura ou o fechamento dos contatos secundários.

3.1.5 Dispositivos NFC

Os componentes utilizados no projeto para realizar a abertura da fechadura foram: cartão NFC; adesivo NFC, e celular. Esses componentes funcionam como dispositivos de armazenamento que são lidos quando aproximados de um equipamento de leitura, e cada dispositivo possui um número identificador (Id) gravado em sua memória.

Figura 14: Cartão NFC

Os cartões NFC, como o apresentado na Figura 14, são cartões plásticos que trabalham com a transmissão de dados por rádio frequência, ou seja, sem contato. A capacidade de armazenamento desse cartão é de 8 Kb, e a memória utilizada é do tipo *EEPROM*, dessa forma é possível apagar e escrever várias vezes no cartão.

Figura 15:TecTiles

Tectiles, como o apresentado na Figura 15, são adesivos NFC desenvolvidos pela *Samsung* para serem utilizados inicialmente pelos seus telefones celulares. O principal uso desses adesivos é abrir um determinado site, que esteja armazenado em sua memória, quando ele for aproximado de um celular Samsung, mas por possuir um Id, ele foi útil no projeto para abrir a fechadura.

Figura 16: Samsung Galaxy S4

O *Samsung Galaxy S4* é um celular que possui a tecnologia NFC embutida no seu *hardware* e *software*, com ele é possível escrever e ler dados em dispositivos NFC. A antena NFC necessária para transferir os dados fica localizada na bateria do celular, e atualmente a *Samsung* tem utilizado os chips NFC da *Broadcom* em seus celulares.

3.1.6 Biblioteca PN532

A biblioteca PN532 tem a finalidade de fornecer métodos que realizem a transferência de dados entra as placas *Arduino* e as *shields* NFC. Essa biblioteca utiliza a transferência de dados serial para realizar a comunicação entre as placas, dessa forma, é necessário apenas quatro fios conectados aos dispositivos para que seja possível a transferência dos dados.

Essa biblioteca é produzida pela *Adafruit* e pode ser adquirida gratuitamente no site http://www.adafruit.com. Junto com a biblioteca estão exemplos de códigos para executar tarefas como escrever e ler dados nas *shields* NFC.

3.2 Métodos

Esta seção apresenta os métodos utilizados para a confecção desse trabalho, cujas etapas estão definidas em quatro: escolha dos componentes, montagem dos componentes, criação do código e testes. A disposição dos métodos no decorrer do texto segue a ordem cronológica que eles foram executados no trabalho.

Escolha dos componentes: As placas da plataforma *Arduino* utilizadas no projeto, que são a placa *Arduino* e a *shield* NFC, foram escolhidas buscando a maior conectividade entre elas. Dessa forma, foram selecionados modelos que se encaixavam para não necessitar a utilização de solda.

Foi feita uma pesquisa sobre os tipos de fechaduras eletrônicas disponíveis no mercado, o que permitiu perceber que elas possuem o funcionamento similar, e assim foi selecionado o modelo descrito na seção materiais. A escolha desse modelo foi motivada pela sua característica de trabalhar com baixas tensões elétricas, no caso 12 volts, o que facilita no manuseio dos componentes durante a criação do projeto.

Montar componentes: Depois de selecionar e reunir todos os componentes do projeto, foi realizada a montagem dos mesmos. A montagem envolveu a composição do projeto, ou seja, a reunião dos componentes físicos (relé, transistor, fechadura elétrica e placa *Arduino*) para a criação da solução proposta.

Criação do código: Nessa etapa foi buscada a biblioteca PN532 para prover a comunicação da *shield* NFC com a placa *Arduino Uno*. Depois de adquirir a biblioteca, foi implementado o *software* e instalado no microcontrolador da placa.

Teste: Após finalizado o projeto foram realizados testes para verificar se os equipamentos possibilitavam a abertura da fechadura.

Muitos dos componentes apresentados nessa seção, como placa *Arduino Uno* e *shield* NFC *Elecfreaks*, podem ser substituídos por outros modelos similares, desde que apresentem o mesmo comportamento diante das situações que foram empregados neste projeto. No capítulo seguinte é apresentada a utilização desses componentes, juntamente com os métodos, esclarecendo as suas respectivas finalidades no contexto deste trabalho.

3 RESULTADOS E DISCUSSÃO

Nesta seção é apresentado o processo de criação do projeto utilizando os componentes e métodos apresentados na seção anterior. A seção também expõe um comparativo entre o projeto e as tecnologias similares que estão no mercado, esse comparativo tem o objetivo de abstrair a viabilidade da utilização de um sistema como esse diante das soluções já existentes.

Por último, a seção apresenta os resultados obtidos com os testes, informando os pontos que foram alcançados dos objetivos iniciais (propostos no projeto de pesquisa apresentado em 2013-1) e novas informações que foram descobertas no decorrer do trabalho.

A Figura 17 demostra uma visão geral das partes que integram o projeto, e expõe como foi feita a ligação entre esses componentes (o leitor NFC, a placa *Arduino Uno* e a fechadura elétrica).

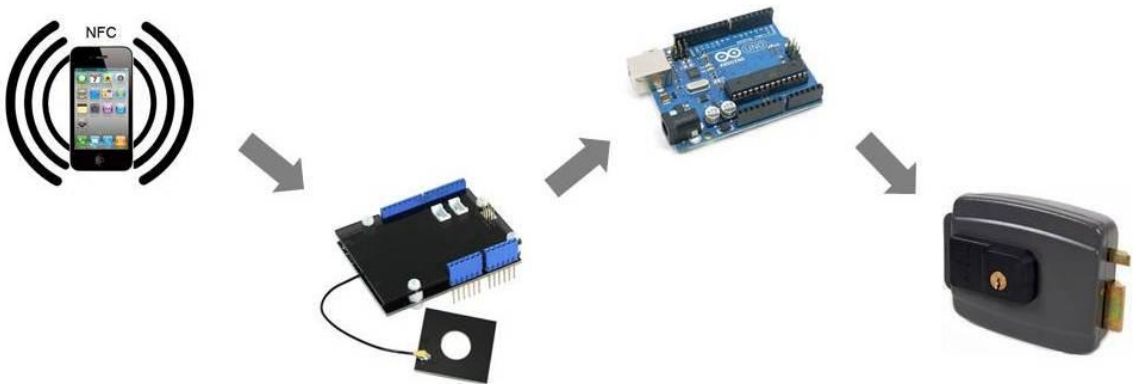

Figura 17: Visão geral do projeto

O leitor NFC fica ligado à placa *Arduino*, que por sua vez está conectada à fechadura eletrônica, na mesma disposição em que está na Figura 17. Dessa forma, quando um dispositivo NFC, que pode ser um celular, cartão ou qualquer outro aparelho que contenha essa tecnologia, aproximar-se do leitor NFC, os dados de identificação do dispositivo são enviados para a placa *Arduino.* Posteriormente é verificado se esse dispositivo é cadastrado para abrir a fechadura, caso seja verdadeiro, a placa *Arduino* envia um sinal para que a fechadura seja aberta.

Da forma que estão articulados os componentes do projeto, a fechadura é aberta sem a necessidade de que seja pressionado nenhum botão, com isso, essa

solução de controle de acesso proposta nesse trabalho vem de encontro à necessidade citada no referencial teórico, em que um dos motivos de não serem implantados sistemas de controle de acesso, são os transtornos que eles causam para os usuários que trabalham nesses ambientes.

A seguir é exposto o início da parte prática desse sistema de controle de acesso físico. A princípio é demonstrado o trabalho realizado nos componentes físicos, e posteriormente é apresentada a parte do *software* do projeto.

3.1 Construção do sistema

Como o projeto é composto por partes independentes, essas referidas partes podem ser desenvolvidas em qualquer ordem, desde que estejam prontas para concretizar a integração ao final. No presente trabalho foi seguida ordem de primeiro realizar a montagem dos componentes físicos, e posteriormente criar o *software* que gerencia esses componentes.

3.1.1 Montagem

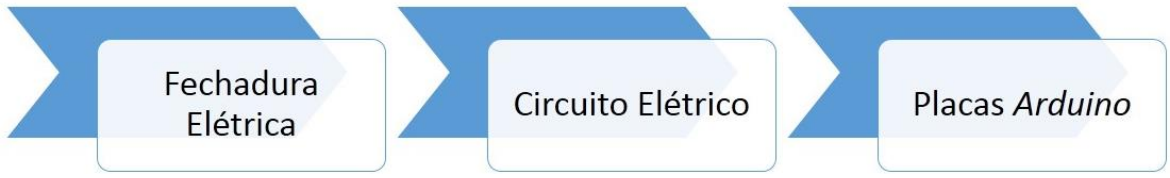

Figura 18: Montagem dos componentes físicos

A montagem dos componentes físicos do projeto foi dividida em três fases conforme é ilustrado na Figura 18. A primeira etapa da parte prática do trabalho foi realizada na fechadura elétrica, a qual foi instalada em uma bancada de madeira para simular o ambiente de uma porta (Figura 19), para isso foi fixada uma dobradiça entre a fechadura e a madeira no intuito de possibilitar à fechadura o mesmo movimento de abrir e fechar uma porta.

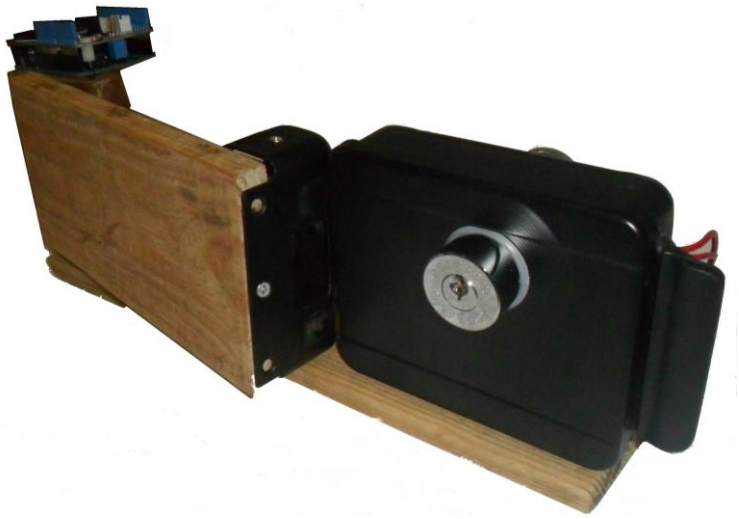

Figura 19: Fechadura Fixada

Para que a fechadura seja acionada pela placa *Arduino Uno*, se faz necessário um circuito que intermedie a ligação entre a placa e a fechadura. Isso acontece porque a fechadura elétrica funciona com uma tenção de 12 volts, e a saída da placa *Arduino* é de apenas 5 volts. O circuito elétrico utilizado no projeto para fazer essa ligação está exposto na Figura 20. A criação desse circuito consiste em soldar o transistor na entrada do relé, dessa forma o circuito apresenta uma entrada, que fica ligada ao *Arduino Uno*, e uma saída, ligada na fechadura elétrica.

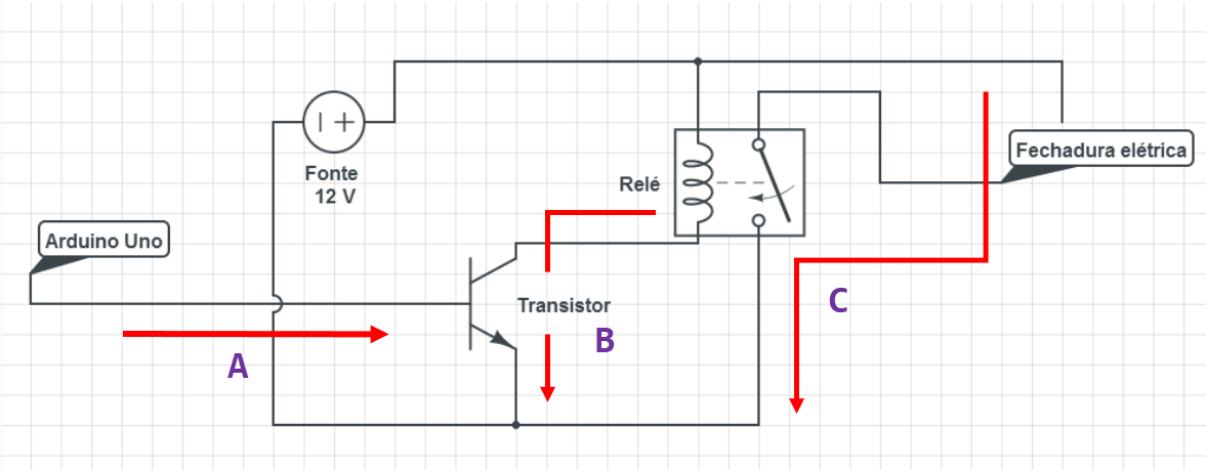

Figura 20: Conexão *Arduino* Fechadura

As setas vermelhas da Figura 20 indicam o sentido da corrente elétrica no momento em que o circuito é acionado. Após ser lido e identificado que o dispositivo NFC tem autoridade para abrir a fechadura, a placa *Arduino* envia um sinal de 5 volts durante 0,1, segundos conforme ilustra a seta A da Figura 20.

Ao chegar a tensão de 5 volts na base do transistor, ele funcionará como um interruptor fechado, fazendo que passe uma corrente elétrica, conforme a seta B, e aciona o relé. Com o relé no modo fechado a corrente elétrica seguirá no sentido da seta C, e isso fará com que seja enviada energia elétrica para a fechadura, e consequentemente a trava seja aberta.

As placas da plataforma *Arduino (Arduino Uno e shield NFC)*, foram escolhidas de forma que dispensassem a utilização de soldas para realizar a integração entre as duas. Dessa forma, a montagem das duas placas foi realizada efetuando o encaixe entre elas, conforme foram projetadas para serem utilizadas.

3.1.2 Software

Todo o código responsável por controlar o sistema de segurança fica gravado na placa *Arduino Uno*, dessa forma esse código também controla o funcionamento do leitor NFC. A seguir, o Código-fonte 1 apresenta o código-fonte que foi utilizado para realizar as configurações iniciais do *software* que lê o id dos dispositivos que se aproximam do leitor.

```
1:#include <PN532.h>
2:#define SCK 13
3:#define MOSI 11
4:#define SS 10
5:#define MISO 12
6:PN532 nfc(SCK, MISO, MOSI, SS);
7:void setup(void)
8:{
9:    Serial.begin(9600);
10:    nfc.begin();
11:    nfc.SAMConfig();
12:}
```

Código-fonte 1: Configurações iniciais

Na linha 1 do Código-fonte 1 é incluída a biblioteca PN532, que será utilizada para realizar a leitura do id dos dispositivos. Essa biblioteca realiza a comunicação

da placa *Arduino* com a *shield* NFC de forma serial, e para isso ela utiliza quatro pinos (10 a 13), que são definidos nas linhas 2 a 5 do Código-fonte 1.

Dentro da configuração (função *setup()*), são realizadas as etapas:

- Definição da velocidade de transmissão dos dados, que é 9600 bps (linha 9);
- Inicialização do driver (linha 10) e definição do modo de funcionamento, que é para leitura e escrita (linha 11).

Cada dispositivo NFC possui um identificador (ID) único, por isso, esta característica foi escolhida para identificar o dispositivo e acionar a abertura da fechadura caso esse ID esteja cadastrado no código.

Dentro da função *loop()*, que é executada durante todo o tempo que a placa fica ligada, foi criado o código que lê o id do dispositivo NFC e envia o sinal de 5 volts para abrir a fechadura caso o id do cartão esteja liberado para fazer isso.

```
13:void loop(void) {
14: int id = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A);
15:           if (id != 0)
16:         {
17:                     digitalWrite(p8, HIGH);
18:                      delay(100);
19:                     digitalWrite(p8, LOW);
20:}
21:}
```

Código-fonte 2: Código de controle

Na linha 14 do Código-fonte 2, foi declarada uma variável para receber o ID do dispositivo a ser lido, e posteriormente é comparado esse valor. No código apresentado não está realizando restrição para os tipos de IDs, pois no condicional da linha 15 só é verificado se o ID é diferente de 0. Nesse referido condicional é o local do código onde deve ser inserido os IDs que devem ter permissão para abrir a fechadura, e assim realizar a restrição de acesso requerida pelos sistemas de segurança.

Depois de ser considerado válido o ID, é enviado um sinal de 5 volts para o pino 8, que acionará a abertura da fechadura elétrica. Para que a trava da fechadura seja liberada, é suficiente que o pino 8 da placa seja ativado por 0,1 segundos,

conforme está exposto nas linhas 18 e 19, pois a fechadura necessita apenas de um pulso elétrico para liberar a trava.

Ligando os três componentes expostos nesta seção (fechadura montada no tablado de madeira, circuito elétrico de intermediação e placa *Arduino* com o *software*) obtém-se o sistema de controle de acesso, pois caso os dados contidos no dispositivo NFC estiverem previamente cadastrados na memória na placa *Arduino,* a placa envia um sinal elétrico para que a fechadura eletrônica seja destravada. Logo esse sistema permite a abertura da fechadura sem que exista contato físico do usuário.

3.2 Discussões

Ao final da implementação do projeto foi possível foi possível perceber que as tecnologias utilizadas, NFC e *Arduino*, apresentaram as características que propunham desempenhar. O dispositivo NFC mostrou que é possível desenvolver projetos que sejam de rápida utilização, pois ao aproximar um equipamento com a tecnologia NFC, o dispositivo foi acionado sem necessitar nenhuma configuração.

A plataforma *Arduino* se mostrou de fácil manuseio e também com baixos custos tanto das placas quando das *Shields*, com isso foi possível desenvolver a fechadura eletrônica com poucos recursos e de fácil utilização para os usuários. Os valores dos componentes utilizados na implementação do projeto estão expostos na Tabela 3.

Tabela 3: Custos do Projeto

[1]Componente	Valor (R$)
Fechadura elétrica	**88,00**
Placa *Arduino* Uno V.3	**34,00**
Shield NFC Elecfreak	**78,00**
Transistor TIP41	**1,50**
Relé	**12,00**
Total	**213,50**

[1] A fechadura elétrica, o transistor e o relé foram comprados na cidade de Palmas no ano do desenvolvimento desse trabalho. A *shield* NFC e a placa Arduino Uno foram compradas em uma loja virtual da Web no mesmo ano.

Somando os valores dos componentes da Tabela 1 obtém-se um custo relativamente baixo se comparado às fechaduras presentes no mercado. Figura 21 e Figura 22 apresentam modelos existentes no mercado, com função semelhante à proposta nesse trabalho.

[2]Figura 21: Fechadura Biométrica **[3] Figura 22: Fechadura à Cartão**

A fechadura biométrica apresentada na Figura 21 foi encontrada com o valor de R$ 960,00, e a fechadura com abertura com sensor de proximidade com o valor de R$ 1230,00. Realizando um comparativo entre as fechaduras encontradas no mercado e o custo do projeto, pode-se observar que existe uma redução de 70% a 75% entre o custo total do projeto e os valores das fechaduras existentes.

As fechaduras elétricas encontradas no mercado que podem ser utilizadas no projeto são do tipo de embutir, ou seja, são encaixadas externamente nas portas. Esse fator faz com que a estética seja prejudicada pois a fechadura fica exposta, mas esse limitação é ocasionada pela falta de outros modelos de fechaduras, e não pela estrutura dos outros componentes do projeto.

Para realizar a parte de testes do trabalho, os dispositivos foram aproximados a uma distância média de 3 centímetros da *Shield* NFC que realiza a leitura dos dados. Essa aproximação dura menos que um segundo, afastando posteriormente o dispositivo NFC da *Shield* de leitura depois de ser executado esse procedimento.

Foi possível abrir a fechadura elétrica com os três dispositivos expostos no capítulo dos materiais utilizados: celular; adesivo NFC e cartão NFC, e seguindo a

---

[2] http://www.madeiramadeira.com.br/

[3] http://www.inteligenthome.com.br/

distância de 3 centímetros citada anteriormente, os dispositivos não apresentaram erros no procedimento de leitura. O cartão NFC e o adesivo NFC abriram instantaneamente a fechadura ao serem aproximados do leitor, mas o celular necessitou que o dispositivo NFC seja ligado pare realizar o procedimento de abrir a fechadura.

Por padrão o dispositivo NFC do celular se encontra no modo desligado, mas se o usuário deixar o dispositivo NFC ligado, o celular apresentará a mesma facilidade para abrir a fechadura como no cartão e adesivo NFC.

Findada a análise do trabalho apresentado, constata-se que os benefícios trazidos em praticidade de uso e economia são visíveis quando adotado em um ambiente propício como em uma empresa que necessita de maior rigor na segurança física. As características da solução de segurança desenvolvida nesse projeto, viabiliza a instalação dessa fechadura elétrica nas diversas portas que compões o prédio de uma empresa, dessa forma, proporcionará segurança aos ativos dessa empresa que ficam armazenados nesses ambientes.

4 CONSIDERAÇÕES FINAIS

Este trabalho apresentou conceitos de segurança da informação com ênfase no acesso físico. O material apresentado fez relações dos temas abordados por autores da área com normas regulamentadoras vigentes no mercado. Por meio da revisão de literatura foi possível perceber a relevância que a área de segurança física tem para a segurança das organizações, e esse fato demonstra a importância do desenvolvimento de trabalhos como o que esta monografia apresenta para essa área de segurança.

Com o intuito de desenvolver um sistema de controle de acesso físico, foram abordadas no trabalho duas tecnologias para a criação do projeto que foram: a plataforma *Arduino* e a tecnologia de transmissão de dados NFC.

Sobre a plataforma *Arduino* foi apresentado o seu funcionamento demostrando componentes do *hardware*, como o microcontrolador, características da linguagem de programação utilizada e as placas de expansão denominada *shield*. Acerca da tecnologia NFC foi apresentado os modos de funcionamento, a forma de transmissão dos dados e como a tecnologia transmite energia entre os dispositivos sem que haja contato físico.

A partir dos estudos realizados e das conclusões obtidas, foi implementado o projeto de uma fechadura eletrônica com abertura pela tecnologia NFC. A plataforma *Arduino* foi utilizada no projeto para atender a necessidade de controlar a fechadura elétrica, e paralelamente realizar a validação dos dados dos usuários. A tecnologia NFC foi empregada para identificar o usuário enviando dados ao leitor instalado na placa *Arduino Uno*.

Durante a pesquisa das fechaduras elétricas existentes no mercado, foi observado que os modelos encontrados não possuem a capacidade de registrar o acesso dos usuários, provavelmente essas fechaduras existam, mas pode-se concluir que elas não são tão populares. Como foi citado no referencial teórico, o registro de acesso é uma medida requisitada nas políticas de segurança, dessa forma, o projeto apresentado expõe vantagens nesse sentido, pois a facilidade de modificação do projeto proporcionada pela plataforma *Arduino,* possibilita que sejam desenvolvidos módulos para realizar o registrado o acesso desses usuários.

Uma evolução deste trabalho é a expansão para diversas áreas, como a integração de várias fechaduras elétricas, como a desenvolvida, para que seja realizado o monitoramento centralizado do estado das fechaduras e o registo de acesso dos usuários. A disponibilidade de realizar a conexão entre linguagens de programação e a plataforma *Arduino*, possibilita que esse projeto seja explorado em outros trabalhos por alunos do curso de computação, pois esses alunos podem explorar áreas como a programação para dispositivos móveis e até mesmo a mineração de dados para descobrir padrões de acesso dos usuários em uma área onde exista esse registro.

5. REFERÊNCIAS

ARDUINO. **Site Oficial**. Online. Disponível em: <http://www.arduino.cc>. Acesso em 13 de maio de 2013.

ASSIS, M. S. **Introdução à propagação das ondas eletromagnéticas**. São Paulo. 2012. Disponível em: < http://www.iecom.org.br/encom_2012/Introducao_a_ Propagacao.pdf >. Acesso em: 19 de maio de 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma ABNT NBR ISSO/IEC 27002**. Tecnologia da Informação – Código de prática para gestão da segurança da informação, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR 11515** Critérios de segurança física relativos ao armazenamento de dados, 1990**.**

INTERNATIONAL STANDARD . **ISO/IEC 18092.** Telecommunications and infomation exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1**),** 2004.

ATOJI, R. I. **Bluetooth e NFC: Estudo de caso.** [monografia]. São Paulo. 2010.

BAUER, C. A. **Política de Segurança da Informação para Redes Corporativas**. Rio Grande do Sul. 2006. Disponível em: <http://tconline.feevale.br/tc/files/0001 _621.pdf>. Acesso em: 24 de março de 2013.

BERNARDES, M.C. **Algumas recomendações para um modelo de governança da segurança da informação** [Editorial]. Fonte, ano 04, n 07. Jul./dez., 2007.

CASAGRANDE, J. H. B. **Redes de computadores e a camada física.** 2008. Disponível em: http://www.sj.cefetsc.edu.br/~msobral/RCO2/docs/casagrande/ MODULO3/cap9/cap9.pdf>. Acesso em: 25 de maio de 2012.

FILHO, O. L. S. F. **Comunicação NFC (*Near Field Communication*) entre dispositivos ativos.** 2010. Disponível em: <http://www.cin.ufpe.br/~tg/2010-2/olsff.pdf>. Acesso em: 26 de maio de 2013.

FONSECA, E. G. P. BEPPU, M. M. **Apostila Arduino.** 2010. Disponível em: < http://www.telecom.uff.br/pet/petws/downloads/tutoriais/arduino/Tut_Arduino.pdf>. Acesso em: 14 de maio de 2013.

FRANCA, A. G. R; NETO, H. A. B. C. OLIVEIRA, L. C. **Transmissão de energia sem fio**. Disponível em: http://www.ifs.edu.br/snct2012/Arquivos/119_1.pdf Acesso em: 19 de maio de 2013.

GUIMARÃES, A. G; LINS, R. A; OLIVEIRA. **Segurança com Redes Privadas Virtuais**. Rio de Janeiro: Brasport, 2006. 209 p.

GUINDANI, Alexandre. **Gestão da Continuidade do Negócio**. 2008. Disponível em: <http://www.upis.br/posgraduacao/revista_integracao/gestao_continuidade.pdf>. Acesso em: 16 de abril de 2013.

GODIM, F. P. **Transmissão de energia elétrica sem fio.** 2010. Disponível em: <http://www.dee.ufc.br/anexos/TFCs/2011-1/Monografia%20-%20Felipe%20Pontes%20Gondim.pdf>. Acesso em: 26 de maio de 2013.

HORI, A. S. **Modelo de gestão de risco em segurança da informação: Um estudo de caso no mercado brasileiro de cartões de crédito.** 2003. Disponível em: < http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2216/74539.pdf?sequence=2>. Acesso em: 11 de junho de 2013.

LESSA, B. N. **Gestão estratégica da segurança da informação.** 2004. Disponível em: <http://www.oocities.org/siliconvalley/vista/4747/mono.pdf>. Acesso em: 10 de junho de 2013.

MAGUIRE, F. **O Futuro da Tecnologia sem contato**. [Editorial]. The Review, n 1, Jan, 2012.

MAZZOLA, V.B. **Arquitetura de redes de computadores.** 2000. Disponível em: <http://www.joinville.udesc.br/portal/professores/flavio/materiais/Redes.pdf>. Acesso em: 25 de maio de 2013.

MELO, J. L. G. G. **Mini curso Arduino.** 2012. Disponível em: < http://www.eletrica.ufpr.br/~james/Laboratorio%20V/arquivos/Mini%20Curso%20Arduino.pdf >. Acesso em 14 de maio de 2013.

NAKAMURA, E. T; GEUS, P. L. **Segurança de Redes em Ambientes Corporativos**. 2 ed. - São Paulo: Futura, 2003. 472 p.

NICHEL, E. M. BESSA, W. K. S. M. **Sistema embarcado com Acesso sem-fio.** 2010. Disponível em: < http://www.eletrica.ufpr.br/ufpr2/tccs/157.pdf>. Acesso em: 05 de junho de 2013.

OXFORD, T. **O Futuro do NFC**. [Editorial]. The Review, n1, jan 2012.

PEIXOTO, W. A. C. MOURA. H. **Segurança física.** 2004. Disponível em: < http://hmoura5.br.tripod.com/PDF/apuesa.pdf>. Acesso em 09 de junho de 2013.

REAL, L. F. O. C. **Transmissão sem fio, ondas, campos magnéticos e seus efeitos na saúde humana**. [monografia]. São Paulo. 2008.

SANTANDER. **Política de segurança da informação para correspondente bancário do Santander.** Disponível em: < http://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf>. Acesso em: 08 de maio de 2013.

SAINT PAUL. NFC, **Near Field Communication**. Disponível em: <http://www.rfid.ind.br/o-que-e-nfc#nfcvrfid>. Acesso em: 03 de abril de 2013.

SPANCESKI, F. R. **Política de segurança da informação-Desenvolvimento de um modelo voltado para instituições de ensino.** 2004. Disponível em: < http://hotsites.cnps.embrapa.br/blogs/pesq/wp-content/uploads/2009/08/ist_2004_ francini_politicas.pdf>. Acesso em: 09 de junho de 2013.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Boas práticas em segurança da informação**. 2 ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação. 2007.

ZELENOVISKY, R. MENDONÇA, A. **Arquitetura de microcontroladores modernos**. Online. Disponível em: <http://www.mzeditora.com.br/artigos/mic_ modernos.htm>. Acesso em: 05/06/2013.

WADLOW, T. A. Segurança de redes: **Projeto e gerenciamento de redes seguras**. Rio de Janeiro. Campus. 2000.