O uso de plataforma de prototipagem eletrônica Open Source na automação: o caso do acesso aos laboratórios de Informática do IFNMG Campus Januária

Arley Oliveira Da Mota
arley.msn@hotmail.com
IFNMG

Anderson Rodrigues de Moura
andersonrdm17@gmail.com
IFNMG

Paulo Vitor do Carmo Batista
paulovitorsi@gmail.com
IFNMG

Joselice Ferreira Lima
joselice.f.lima@gmai.com
IFNMG

Resumo: Este artigo apresenta o uso da prototipagem eletrônica no processo de automação das portas de acesso aos laboratórios do IFNMG Campus Januária, utilizando tecnologias open source. No desenvolvimento da proposta utilizou-se da revisão de literatura que subsidiou a construção do protótipo e possibilitou a análise de trabalhos relacionados. Como resultado obteve-se um protótipo de baixo custo, replicável e de alto desempenho.

Palavras Chave: Automação - Open Source - Arduino - Acesso - Baixo Custo

1. INTRODUÇÃO

A automação de acesso a ambientes é um processo utilizado há várias décadas. Entretanto o uso de ferramentas *open source* para esse fim é um tanto quanto recente. Segundo Mota e Seruca (2015) o software *open source* constitui hoje uma fonte, ainda pouco explorada, de ferramentas úteis para o desenvolvimento dessas novas tarefas. Como o *software*, o *hardware open source* começou a se destacar neste processo de automação com surgimento dos embarcados: o *Arduino* em 2005 e o *Raspyberry* em 2006, tendo em vista que o conceito de automação surgiu por volta de 1946.

A automação é definida pelo conjunto de serviços provido por sistemas tecnológicos integrados como o melhor meio de satisfazer as necessidades básicas de segurança, comunicação, gestão energética e conforto de uma habitação (MURATORI e BÓ, 2011).

Entre outras coisas, os benefícios fizeram com que a demanda por esta tecnologia aumentasse significativamente. Até 2014, cerca de trezentas mil residências no Brasil já possuíam equipamentos de Automação Residencial, e 78% dos consumidores brasileiros estavam interessados em adotá-la (AURESIDE, 2014). Entende-se que esse interesse poderia ser maior se fossem utilizadas tecnologias de *software* e *hardware open source*, gerando assim uma ferramenta de baixo custo.

Tais tecnologias podem ser adotadas em residências, salas comerciais, instituições públicas e privadas. Soeiro et al. (2014) descreve um sistema de controle de horários de aula utilizando leitores biométricos e ferramentas *open source* para controle de horários de professores. Em Oliveira et al. (2014) é apresentado o uso da tecnologia RFID (Identificação por Rádio Frequência) na identificação e gerenciamento do acervo em uma biblioteca. Já no trabalho de Brenner e Bizarria (2011) é desenvolvido um sistema de controle de acesso utilizando biometria digital no entanto são utilizadas soluções de *hardware* e *software* proprietários.

No IFNMG - *Campus* Januária para se ter acesso aos laboratórios do ensino superior, o professor interessado deve-se dirigir à secretaria onde estão guardadas as chaves de cada laboratório e fazer a requisição da chave do laboratório desejado, desde que ela esteja disponível. Nota-se, que não há um controle efetivo de acesso aos laboratórios, visto que não existe um relatório com horários de acesso, impossibilitando assim a aplicação de algum tipo de penalidade às pessoas que venham a praticar danos ou furtos ao patrimônio público. A partir da lacuna identificada, pergunta-se: como viabilizar tal acesso diminuindo as falhas diagnosticadas e garantindo uma maior eficiência?

O objetivo deste artigo é apresentar o processo de desenvolvimento de um protótipo de uma ferramenta que utiliza tecnologias *open source* para automação das portas de acesso aos laboratórios de informática do IFNMG - *Campus* Januária. Constata-se sua relevância por apresentar uma tecnologia de baixo custo, código aberto e grande efetividade em sua proposta.

O artigo está estruturado a partir desta introdução, e conta na segunda seção com a revisão de literatura onde são abordados os conceitos de automação, tecnologias *open source*, meios de comunicação e controle de acesso; na terceira seção fala-se sobre os sistemas de controle de acesso existentes; na quarta seção estão os materiais e métodos onde são descritas as técnicas de construção do protótipo; na quinta seção encontram-se os detalhes do protótipo desenvolvido, e por fim as considerações finais.

2. REVISÃO DE LITERATURA

2.1. AUTOMAÇÃO

A automação surgiu na indústria com intuito de permutar ou reduzir a mão-de-obra humana nos processos de produção. Por volta da década de 80, a automação passou a ser utilizada em residências e prédios propiciando diversos benefícios como: segurança, conforto pessoal e economia de energia (FINDER, 2011).

A Domótica termo que se refere à automação doméstica, originou-se da palavra latina "domus" (casa) com a junção de "robótica" (controle automatizado de algo). É descrita pelo conjunto de serviços providos por sistemas tecnológicos integrados como o melhor meio de satisfazer as necessidades básicas de segurança, comunicação, gestão energética e conforto de uma habitação (MURATORI e BÓ, 2011).

Existem outras ramificações da automação, como automação predial, industrial e comercial. A ideia é a mesma, no entanto se diferenciam por estar em contexto distintos. Entretanto, na automação residencial, a AURESIDE (2016) evidencia como benefício o conforto, a segurança, a comodidade, a acessibilidade, a economia de tempo e o esforço. Já Rocha et al. (2012) destaca a redução dos custos dos processos, aumento da produtividade e a redução na execução dos tempos das atividades.

Neste sentido nota-se a importância da utilização de tecnologias *open source* visto que são um arranjo de *hardware* e *software* livres. Leal (2012) cita que um *software* livre é um programa que fornece o código-fonte gratuitamente para os usuários, possibilitando modificações e melhoramentos por qualquer pessoa. Neste mesmo conceito surgiu o *hardware* livre, em que o *design* do *hardware* e o código-fonte do *software* são regidos por licenças, às quais destacam-se a GPL (*General Public License*), LGPL (*Lesser General Public License*) e BSD (*Berkeley Software Distribution*) que permitem o uso e alterações por toda a comunidade (ARAÚJO, 2011).

2.2. ARDUINO E RASPBERRY

O *Arduino* (plataforma de prototipagem eletrônica) surgiu na Itália em 2005, e é constituído de uma plataforma de *hardware* e *software open source*. Para Alves (2013) objetivo era criar uma ferramenta de prototipagem eletrônica de custo acessível e flexível, além de possibilitar que pessoas não especialistas em programação e/ou em eletrônica pudessem desenvolver aplicações de objetos e ambientes interativos. Existem componentes responsáveis por estender a capacidade do *Arduino*. Aos conectados sobre a PCB (Placa de Circuito Impresso), denominam-se *shields*, como por exemplo o *ethernet shield* que realiza a comunicação cabeada com a rede através da interface RJ45 (*Registered Jack*); o LCD *shield* que exibe os *feedbacks* programados em tela, e os teclados que possibilitam a entrada de dados. Os que utilizam fios para realizar a conexão com a PCB, denominam-se módulos, como por exemplo o leitor de RFID (ARDUINO, 2016).

O *Raspberry* é considerado um minicomputador pessoal *open source*. Foi criado pela *Raspberry Pi* e lançado em 2006 no Reino Unido, com o objetivo de desenvolver um produto com preço acessível, tamanho reduzido e com diversas funcionalidades capazes de integrar facilmente o desenvolvimento de projetos eletrônicos com software (Cruz e Lisboa 2014). Existem três modelos do *Raspberry*, dos quais se diferenciam basicamente pela a memória RAM (*Random Access Memory*) e o número de portas USB (*Universal Serial Bus*). No primeiro modelo nomeado A, pode-se verificar 256 MB (*Mega Bytes*) de RAM e uma porta USB. Já no segundo, o B, verifica-se 512 MB de RAM, duas portas USB e uma porta RJ45. O último modelo, o B+, foi acrescido de mais duas portas USB, se comparado ao modelo B.

2.3. MEIOS DE COMUNICAÇÃO

Para que dois ou mais sistemas computacionais distintos se comuniquem, é necessário que ambos estabeleçam regras de conversação. Esta regra ou padrão de comunicação é conhecida como protocolo. Para Tanenbaum (2003) um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação. O *Ethernet* e IEEE 802.11 - *Wi-Fi*, são os protocolos mais populares atualmente. Entre outras particularidades que os distingue, a utilização ou não de fios é a principal delas.

Segundo Tanenbaum (2003) o *Ethernet* é uma tecnologia de comunicação em rede local com meio de transmissão (cabos) compartilhado, padronizado como padrão IEEE 802.3. Em constante evolução, esta tecnologia é amplamente utilizada em instituições, indústrias e residências. Já a conexão *Wi-Fi* criada no início dos anos 90, estabelece uma comunicação sem fio, muito conhecida por usuários de dispositivos móveis, por oferecer comodidade, praticidade e mobilidade.

3. SISTEMA DE CONTROLE DE ACESSO

Para Brenner e Bizarria (2014) efetivar o controle de acesso é necessário estabelecer alguns perímetros, com acesso isolado, partindo de partes mais externas para as mais internas, focando tanto a entrada dos indivíduos quanto a saída. Estes perímetros para Souza (2010, p. 17), normalmente são delimitados e controlados por barreiras físicas e tecnologias de detecção. Um exemplo, neste caso, seria a utilização de porta como barreira e um mecanismo tecnológico que possibilite a validação e autenticação das informações fornecidas pelo usuário, possibilitando assim seu acesso. Outro aspecto ligado ao ramo de controle de acesso é a autorização, que se refere a proteger contra acesso não autorizado, uma informação ou recurso computacional, estabelecendo o que um usuário está permitido a fazer no sistema (SILVA, 2008, p. 9).

Definir medidas de identificação e estabelecer a autenticação, torna-se fundamental para a o controle dos acessos, pois Silva (2008, p. 7) destaca que:

> ... autenticação provê a garantia da identidade de um usuário, ou seja, é responsável por verificar se um requerente é quem ele diz ser, por meio de suas credencias, sendo que suas credencias são as evidências que um requerente apresenta para estabelecer sua identidade como um usuário válido (SILVA 2008, p. 7).

Os mecanismos de identificação defendidos pelos autores Silva (2008, p. 7), Pinheiro (2008, p. 16) e Peixinho et al. (2013, p. 122) baseiam-se em três paradigmas: algo-que-você-sabe (mecanismo de senhas e suas variações); algo-que-você-tem (*smartcards*, chips, *token*, etc.) ou algo-que-você-é (impressão digital, formato da íris, voz, face, etc).

Algo-que-você-sabe

Nesse princípio, o sistema solicita ao usuário que informe algo que somente ele sabe, o caso da senha por exemplo. Para Peixinho et al. (2013, p. 122) este princípio em geral é o menos seguro, pois um atacante pode tentar adivinhar a senha de um usuário. Outros problemas identificados por Silva (2008, p. 8) com a utilização deste princípio são: um intruso pode penetrar em um computador do sistema e ler o arquivo de senhas; alguém pode adivinhar uma senha mal escolhida; um intruso pode quebrar uma senha, tentando exaustivamente todas possíveis combinações ou palavras de um vocabulário.

Algo-que-você-tem

O usuário deve fornecer o dado que recebeu no momento em que se registrou para ter acesso. De acordo com Brenner e Bizarria (2014) consiste basicamente em ter posse de chaves,

cartões, carteiras e demais *tokens* de acesso que associados à utilização de senhas, possibilitam uma maior segurança.

Algo-que-você-é

Para Peixinho et al. (2013, p. 122) este princípio mostrou ser a forma mais segura de autenticação, pois envolve uma característica intrínseca. Neste caso, pode-se utilizar a biometria da íris, da digital, enfim, algum comportamento ou morfologia.

Entretanto, a utilização de qualquer mecanismo de identificação puro, para Brenner e Bizarria (2014) não provê garantia suficiente da identidade de um requerente, sendo necessário desenvolver um sistema de autenticação que possa utilizar mais de um tipo de identificação para provar sua identidade. Um exemplo seria o identificador RFID associado a uma senha.

4. MATERIAS E MÉTODOS

A pesquisa caracteriza-se como aplicada e experimental, que visa a obtenção de conhecimento e geração de produto (protótipo). Na revisão bibliográfica utilizou-se publicações para elaboração do texto e estruturação da proposta, baseando-se na necessidade de se identificar ferramentas e métodos para sua estruturação (JUNG, 2004).

Na construção do protótipo, decidiu-se pela utilização de tecnologias *open source,* onde foi empregada a plataforma *Arduino* (*Arduino* mega, *ethernet shield*, protoboard, modulo leitor RFID), que foi programada para controlar juntamente com o Sistema Gerenciador de Acesso (SGA), responsável pela gestão da ferramenta.

Na montagem do protótipo utilizou-se um *led* para simular a fechadura elétrica. Para acoplá-la a basta substituir o *led* por ela e adicionar mais um componente eletrônico chamado relé, não sendo necessário alterar qualquer parte do código-fonte responsável pela gerência da placa. O resultado da montagem é apresentado na Figura 1 abaixo, que mostra todas as conexões necessárias para o funcionamento correto do protótipo.

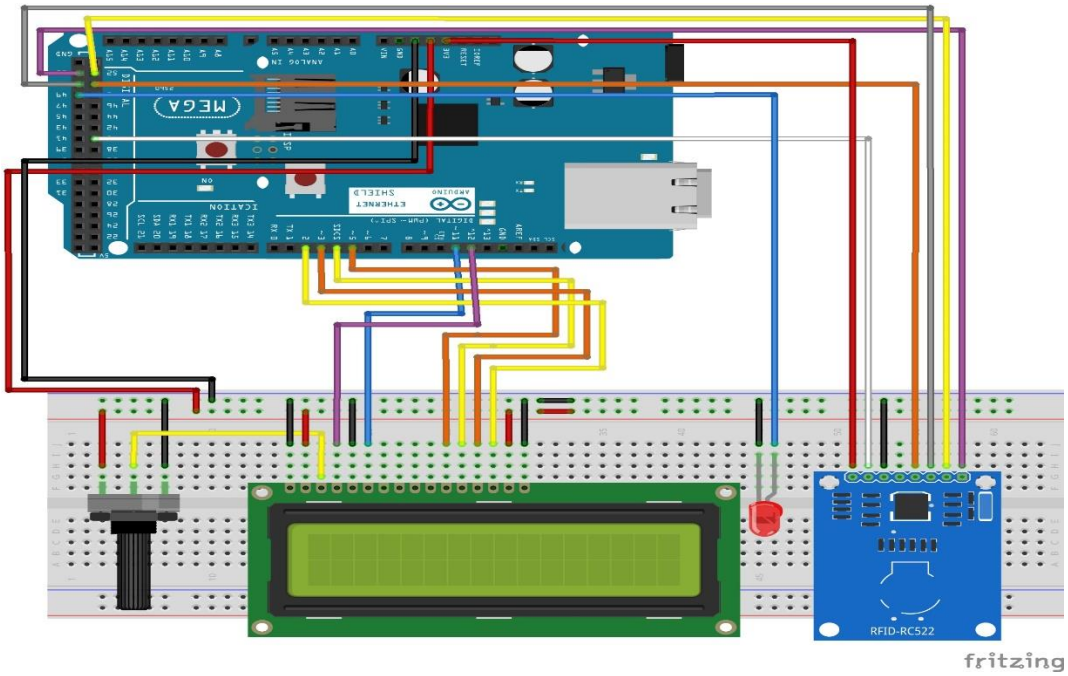

Figura 1: Esquema de conexões

Após implementada a estrutura física, direcionou-se os esforços para o desenvolvimento do SGA. Após o levantamento de requisitos, obteve-se o diagrama mostrado na Figura 2.

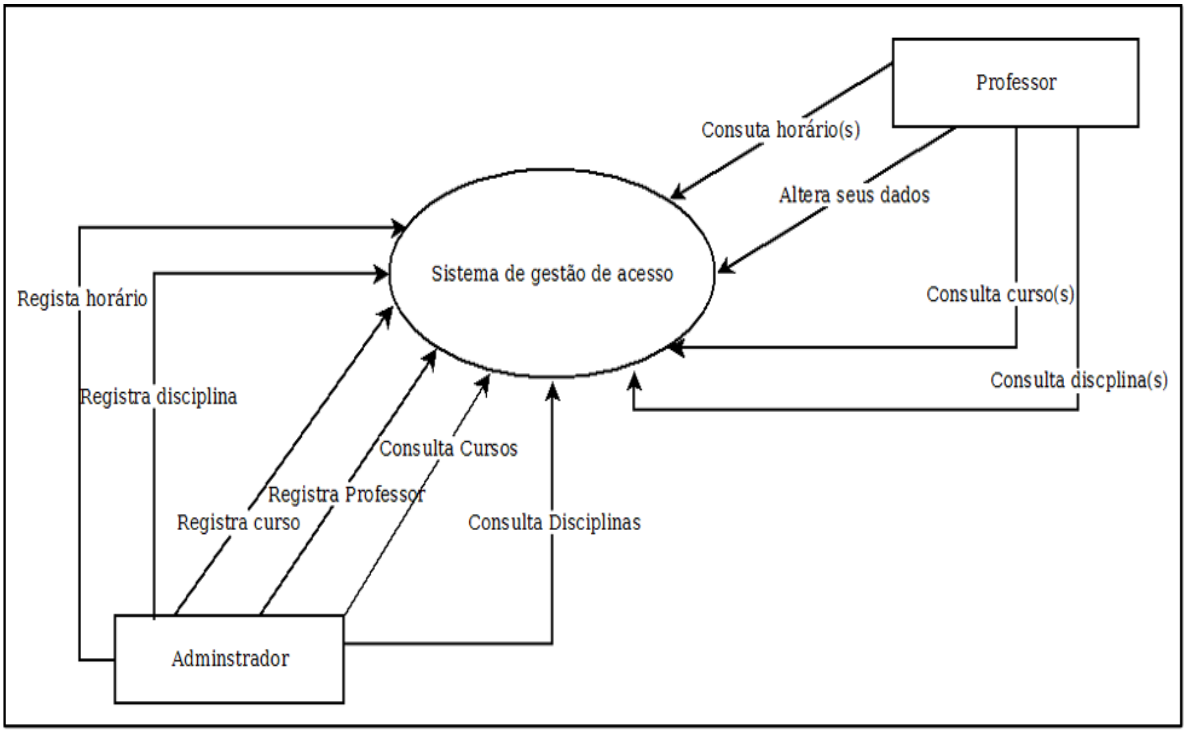

Figura 2: Diagrama de Contexto

É importante ressaltar que no levantamento de requisitos do sistema, identificou-se a necessidade de criação de dois tipos de usuários: o professor e o administrador, que consequentemente possui maiores privilégios. O administrador é o responsável por gerenciar professores, cursos, disciplinas e horários. Isto torna-se necessário visto a importância de se controlar quem teve acesso aos laboratórios. Já o professor pode apenas consultar informações de acesso e alterar seus dados.

Na programação do SGA, foi utilizado o *framework Codeigniter*, desenvolvido em PHP e para implementação do seu ambiente de gerenciamento utilizou-se o NetBeans 8.0. A comunicação entre o *Arduino* e o SGA deu-se através do pacote do XAMPP que é contém os principais servidores de código aberto, como o APACHE, o MYSQL e o PHP. Já a troca de informações entre o SGA e o *Arduino* é feita utilizando JSON. Na programação *frontend* utilizou-se os *frameworks BootStrap* e MDL (*Material Design Lite*), que utilizam HTML e CSS com bibliotecas em *JavaScript*.

Por fim, para o desenvolvimento do SGA, utilizou-se a metodologia ágil *Scrum*, responsável pela gestão e planejamento de projetos de software, assegurando assim que uma funcionalidade só estará pronta após ser testada.

5. VISÃO DO PROTÓTIPO

O protótipo foi construído com o objetivo de instalar um sistema de controle de acessos aos laboratórios de informática, que são utilizados por professores de vários cursos ofertados pelo IFNMG - *Campus* Januária.

Abaixo, a Figura 3 demonstra os dispositivos utilizados e existentes no ambiente atual, bem como as conexões realizadas entre o SGA, que está hospedado no servidor, e o *hardware*.

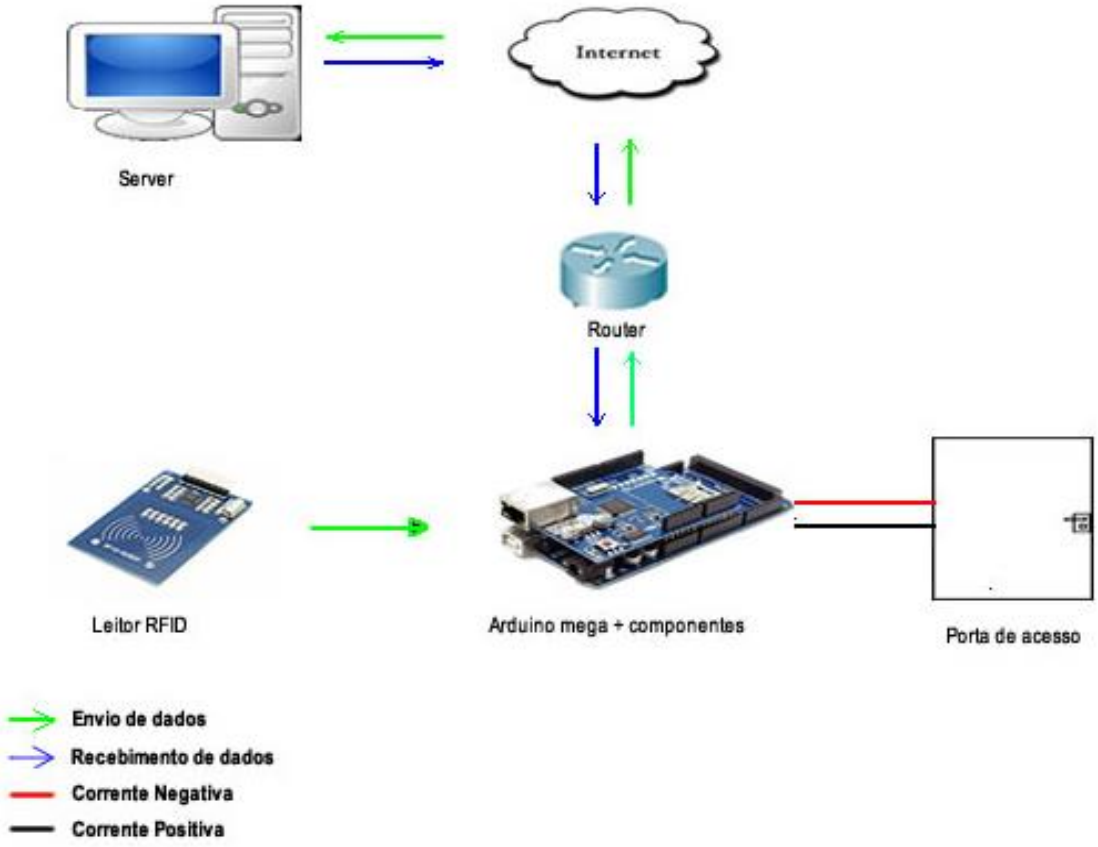

Figura 3: Diagrama de conexões

O protótipo apresentado neste artigo possui um tipo de autenticação e duas formas de acessos (chaves e *tag* RFID). Na fase de testes do protótipo foram utilizados um notebook como servidor da aplicação SGA e o esquema de conexões detalhado na Figura 1.

Para realizar o acesso aos laboratórios, o usuário deverá utilizar sua *tag* RFID que será lido pelo *Arduino* e enviado ao SGA, responsável por processar as informações e validar juntamente ao banco de dados as informações fornecidas. Este procedimento pode ser visualizado na Figura 4 abaixo.

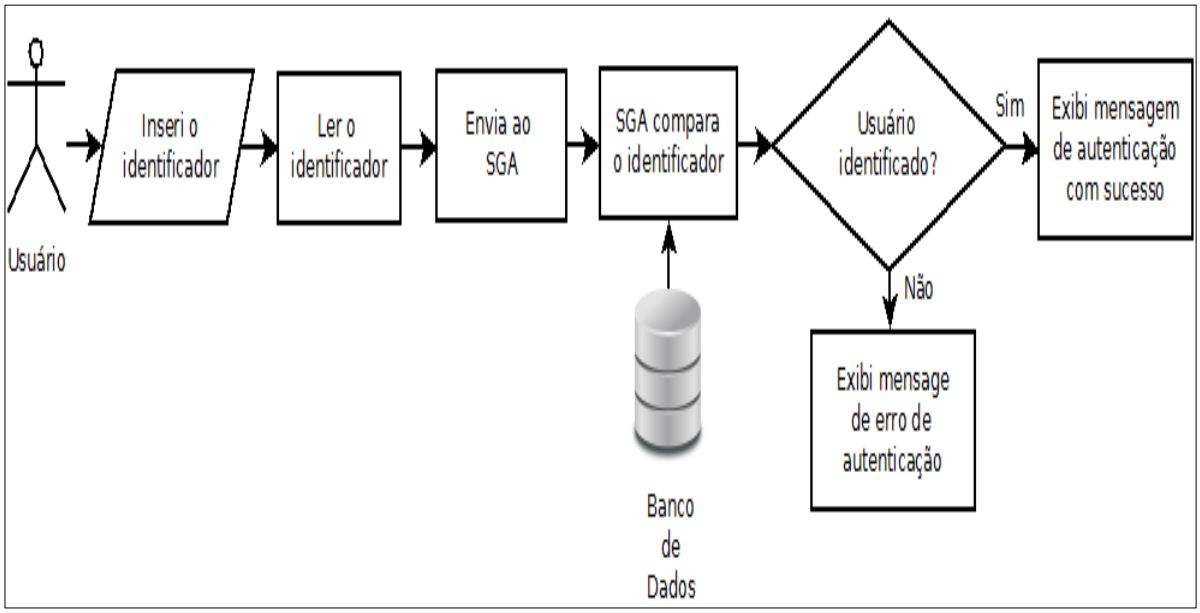

Figura 4: Processo de autenticação

Para ter acesso aos laboratórios o usuário terá que se cadastrar no SGA como pode ser visualizado na Figura 5, e solicitar seu identificador RFID que será associado ao seu perfil.

Figura 5: Tela de cadastro de usuário – versão mobile

Com o cadastro realizado, o usuário consegue realizar o acesso aos laboratórios utilizando uma *tag* RFID como identificação. Para efeito de controle de acesso aos laboratórios, o sistema emite relatórios de entrada e saída dos usuários.

6. CONSIDERAÇÕES FINAIS

O sistema de acesso automático utiliza-se em sua estrutura *hardware* e *software* com tecnologias *open source*. Na configuração do sistema de controle, adotou-se os mecanismos de identificação como bem citado por (Silva 2008, p. 7), Pinheiro (2008, p. 16) e Peixinho et al. (2013, p. 122), baseando então no paradigma de algo-que-você-tem, onde o usuário, para ter acesso aos laboratórios, deve fornecer o dado que recebeu no momento do cadastro.

Por outro lado, mecanismos de automação, geralmente são fabricados e distribuídos por empresas proprietárias, acarretando um custo de desenvolvimento e manutenção. Na maioria das vezes, pequenas empresas ou mesmo órgãos filantrópicos ou escolas públicas não tem acesso a tais tecnologias. Com o uso de bancada de prototipagem de baixo custo, os custos são reduzidos tornado viável a replicação.

Sendo assim, para responder a pergunta inicial “como viabilizar acesso aos laboratórios de informática do IFNMG - *Campus* Januária?” este artigo apresentou uma solução de baixo custo, com utilização de ferramentas *open source*, que através dos testes realizados, comprovou-se a viabilidade de utilização e a capacidade de replicação.

Em trabalhos futuros espera-se utilizar novas tecnologias para melhorar o sistema de segurança, como a utilização da biometria digital associado ao uso da senha.

7. REFERÊNCIAS

Alves, R. M. S.; Armando L. C., Pinto, M. C.; Sampaio, F. F. & Elia, M. F. Uso do Hardware Livre Arduino em Ambientes de Ensino-aprendizagem. Jornada de Atualização em Informática na Educação, v. 1, n. 1, p. 162-187, 2013.

Araújo, F. M. A. Hardware Livre. Congresso de Tecnologia da Informação. Vol. 6, 2011.

Arduino. Shields. 2016. https://www.arduino.cc/en/Main/arduinoShields/, abril 2016.

AURESIDE. Automação residencial teve grande impulso em. 2014. 2014. http://www.aureside.org.br/noticias/automacao-residencial-teve-grande-impulso-em-2014, abril 2016.

AURESIDE. Associação Brasileira de Automação Residencial e Predial. 2016. http://www.aureside.org.br/, abril 2016.

Brenner, Gabriel P. S. & Bizarria, Walter. Sistema de Controle de Acesso com Biometria da Digital. VIII Simpósio de Excelência em Gestão e Tecnologia, 2011.

Cruz, Ariadne A. & Lisboa, Emerson F. WebHome–Automação residencial utilizando Raspberry PI. Revista Ciência e Tecnologia, v. 17, n. 31, 2014.

Finder. Pré – Automação RESIDENCIAL. Revista da empresa Finder. São Paulo, 2014.

Jung, C. F. Metodologia para Pesquisa e Desenvolvimento: aplicada a novas tecnologias, produtos e processos. Axcel Books, 2004.

Leal, C. A. Software Livre: Desconhecimento ou Preconceito. Anais do Congresso Nacional Universidade, EAD e Software Livre. Vol. 1. No. 1, 2012.

Mota, C. & Seruca, I. Free/open source software vs. proprietary software in education. Information Systems and Technologies (CISTI), 10th Iberian Conference on. IEEE, 2015.

Muratori, J. R. & Bó, P. H. D. Automação residencial: historico, definições e conceitos. In O Setor elétrico, number 62, São Paulo. p. 70, 2012.

Oliveira, N. O.; O. R. M. & Amaral, F. V. Gerenciamento de acervo através da tecnologia RFID: a experiência da Biblioteca Universitária da UFLA. XVIII Seminário Nacional de Bibliotecas Universitárias, 2014.

Peixinho, I. C.; Fonseca, F. M. & Lima, F. M. Segurança de Redes e Sistemas. Escola Superior de Redes RNP, Rio de Janeiro/RJ, 2013.

Pinheiro, J. M. Biometria nos Sistemas Computacionais. 1ª Edição. Ciência Moderna, 2008. ISBN: 978-85-7393-738-1, 2008.

Silva, P. H. O. Sistema de segurança de tranca de porta e controle de acesso. 2014. http://repositorio.uniceub.br/bitstream/235/4916/1/20817630.pdf, abril 2016.

Soeiro, R. R.; Costa B. H.; Carneiro, F. D. F; Almeida, N. M. B; Castro, B. F. J. A; Tavares, D. A. B. & Menezes, J. W. M. Sistema de Controle de horários de aula utilizando leitores biométricos. COBENGE - Engenharia: Múltiplos sabres e atuações. Brasil, Juíz de Fora/MG, 2014.

Souza, M. B. Controle de Acesso: Conceitos, Tecnologias e Benefícios. Editora Sicurezza, 2010.

Tanenbaum, A. S. Redes de Computadores. 4a edição, Campus, 2004.