Controle de Acesso YSNP

Diego Oliveira de Andrade [1] – Faculdade de Tecnologia de Carapicuíba

Gabriel Martins Monteiro da Silva [2] – Faculdade de Tecnologia de Carapicuíba

Prof. Me. Jadir Custódio Mendonça Jr. [3] – Faculdade de Tecnologia de Carapicuíba

RESUMO

YSNP: Controle de Acesso, é um sistema para gerenciar, de maneira eficaz, o acesso das pessoas que necessitam entrar no campus. Este *artigo* tem como objetivo geral demonstrar que o sistema, de controle de acesso, utilizado atualmente possui falhas, mostrando que não há uma certeza de quem está adentrando esta instituição. Esse novo sistema proposto, que será concluído e futuramente implementado, será automatizado, utilizando-se das tecnologias Arduíno e RFID, sendo ambos de baixo custo. Para poder entrar no campus o usuário deve possuir um cartão, válido, que irá identificá-lo, mostrando seus dados e uma foto, facilitando a conferência feita pelo segurança, caso seja um visitante, o utilizador do sistema (segurança), deverá efetuar um cadastro mediante a solicitação de um documento oficial com foto, vincular um cartão temporário a este individuo, ao qual este cartão deverá ser devolvido em sua saída.

Palavras-chave: Controle de Acesso. Arduíno. RFID. Sistema.

ABSTRACT

YSNP: Access Control is a system to effectively manage access for people who need to enter in the campus. This article has as general objective to demonstrate that the system of access control, currently used has flaws, showing that there is no certainty of whom is entering this institution. This new system proposed, that will be complete and implement in the future, will be automated, using Arduíno and RFID technologies, both of which are inexpensive. In order to enter the campus, the user must have a valid card, which will identify him / her, show his / her data and a photo, facilitating the security checking, if he is a visitor, the system user (security officer), will register the visitor by requesting his/her document with a photo. He/she will receive a temporary card which will be returned when he/she leaves the campus.

Keywords: *Access Control. Arduíno. RFID. System.*

---

[1] Aluno do CST em Análise e Desenvolvimento de Sistemas – *e-mail*: diego.andrade14@fatec.sp.gov.br
Aluno do CST em Análise e Desenvolvimento de Sistemas – *e-mail*: gabriel.silva143@fatec.sp.gov.br
[3] Mestre em Engenharia Elétrica– *e-mail*: Jadircmj@hotmail.com

1 INTRODUÇÃO

Um aspecto muito importante nas Organizações é a questão da segurança patrimonial bem como a segurança de seu pátio humano. A empresa detém seus ativos físicos e para tanto, necessita preservá-los. Igualmente há de se pensar na integridade de seus colaboradores e stakeholders. O serviço de segurança empresarial tem sido realizado, via de regra, pela contratação de empresas terceirizadas, especializadas nos serviços de portaria e segurança. Há que se identificar todos que buscam adentrar suas instalações. E isso não é diferente numa Instituição de Ensino Superior.

Atualmente, na Faculdade de Tecnologia de Carapicuíba, o controle de acesso vem sendo feito de maneira burocrática e insegura. Para adentrar o campus deve-se apenas mostrar uma carteirinha de identificação, a qual não é inteiramente confiável, pois esta pode ser facilmente falsificada ou utilizada por outra pessoa que não seja seu verdadeiro proprietário. Caso o indivíduo não a possua, este deve preencher, ele mesmo, um formulário contendo seus dados pessoais, podendo até usar um nome fictício e, mesmo assim, poderá adentrar a instituição. Há, assim, uma vulnerabilidade da segurança quando do acesso às instalações do campus. O sistema atual se mostra falho, devido ao procedimento em que os usuários são submetidos para adentrar ao Campus. Eles são indagados se possuem uma carteirinha que é fornecida pela instituição, confeccionada tão somente por um simples pedaço de papel, com a impressão dos dados do aluno e da instituição, mostrando-se ser de fácil falsificação, pois basta que o aluno ou outra pessoa qualquer, a apresente, em geral, há uma certa distância, dificultando a conferência efetuada pelo segurança ficando quase impossível verificar a foto contida nesse documento, se de fato é ou não do portador. O usuário apenas mostra essa carteirinha e em alguns casos, como a foto fica ainda desfocada, mesmo que, o segurança a tenha em mãos e não apenas a visualize à certa distância, deixa o segurança sem a certeza de que realmente se trata do proprietário desse documento. Além disso, uma vulnerabilidade atual, é que, caso o usuário não possui tal carteirinha, este dever inserir seus dados, em uma folha que previamente contém os campos exigidos para sua identificação, porém como esse procedimento é feito pelo próprio usuário, este pode tranquilamente colocar qualquer tipo de informação nesse cadastro, podendo este ser verídico ou não, pois não há um acompanhamento bem como uma conferência no ato deste cadastramento que assegure de que tais dados fornecidos sejam verdadeiros ou não. Tendo em vista que o atual sistema de controle de acesso à instituição apresenta algumas falhas, as quais impactam não apenas a segurança patrimonial, mas também a segurança física. Como resolver tal problema de

segurança no controle de acesso? Deve-se haver um novo sistema que contenha alguns procedimentos mais apropriados.

Este artigo tem por objetivo apresentar o Sistema de Controle de Acesso YSNP a fim de que possa ser adotado e implantado no Campus da Faculdade de Tecnologia de Carapicuíba, apresentar o sistema, *You Shall Not Pass* (YSNP) controle de acesso, que de maneira simples, barata e eficaz, permite controlar o acesso de pessoas no Campus, através de um circuito eletrônico, constituído de uma placa de Arduíno e um leitor RFID (*Radio Frequency Identification*), sistema de identificação por rádio frequência, tornando este projeto de baixo custo, uma vez que ambos os componentes custarão para a instituição menos de quatro mil reais.

Esse novo sistema propõe que cada usuário tenha um cartão de acesso válido, o qual terá, além de seus dados pessoais, registrado sua foto. Quando esse cartão é passado no leitor RFID, no momento do acesso, o operador do sistema poderá de maneira simples e eficaz verificar se realmente se trata de tal usuário, pois no monitor aparecerão todos os dados do portador, bem como se este catão está registrado no sistema como válido, podendo fazer a comparação entre a foto cadastrada com o usuário. Caso se trate de um aluno, regularmente matriculado na instituição e, seu cartão não esteja válido no momento de sua entrada, o mesmo não poderá adentar até que seu cartão seja validado pelo operador do sistema, que por sua vez deverá verificar junto à direção acadêmica da instituição a veracidade da matrícula desse aluno. Por se tratar de um mecanismo eletrônico, se mostra mais eficaz no quesito segurança, pois somente poderá entrar quem possuir este cartão, o qual deverá estar válido. Caso o aluno perca seu cartão, deverá imediatamente informar tal ocorrido à instituição, que por sua vez, comunicará aos operadores do sistema que bloquearão o cartão, para que, caso alguém o encontrar não possa adentrar a instituição. O aluno deverá solicitar outro cartão de acesso à instituição, sendo esta solicitação cobrada ou não. Tal decisão de cobrança ficará a critério da instituição. O operador poderá cadastrá-lo como visitante informando-o do procedimento a ser tomado junto a secretaria da instituição, para que o aluno ou usuário que tenha perdido seu cartão possa efetuar seu acesso à Unidade. No caso de um visitante, o operador irá cadastrá-lo e associar um cartão que ficará validado somente durante o período de sua permanência na instituição.

O sistema registrará somente uma entrada por cartão. Dessa forma o cartão ficará indisponível para registrar uma eventual “segunda” entrada sem que antes seja registrada sua saída, para se evitar casos em que o usuário queira disponibilizar seu cartão para outra pessoa,

que esteja do lado de fora da instituição de forma a ter seu acesso liberado. O agente de segurança deverá efetuar a conferência dos usuários, na sua entrada e saída pelos dados apresentados no monitor mediante a leitura do cartão.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 *Radio Frequency Identification* - RFID

Segundo Duroc e Kaddour (2012), RFID (*Radio Frequency Identification*) é uma tecnologia que teve início em meados da década de 80. Seu funcionamento se dá, com a identificação sendo realizada por meio da radiofrequência e, dependendo do tipo de chip que se utiliza, o seu alcance pode variar. Para a comunicação, é necessária uma Tag RFID, um cartão ou um chaveiro que contenha um chip RFID, conforme Figura 1, o qual pode enviar e receber sinais de um leitor específico. Após esta troca de sinais, um software possui o papel de decodificar e transformar esse sinal em informações úteis.

Sun (2012) aponta que uma *Tag* RFID pode possuir em seu funcionamento dois modos: ativo e passivo. O modo Ativo, a Tag possui sua própria bateria, não tendo a necessidade do leitor fornecer corrente, isso possibilita que o alcance seja maior que uma Tag do tipo passiva. Já neste modo (passivo), a Tag fica dependente do leitor, pois para enviar um sinal, é necessário que seja enviada uma corrente, torando o seu alcance menor, em relação à Tag Ativa.

Segundo Seufitelli et al (2009) a tecnologia RFID vem se mostrando de grande utilidade. Sua agilidade e flexibilidade é bem maior, quando comparamos ao código de barras. Atualmente existem muitas aplicações para esta tecnologia, como por exemplo, o controle de acesso de pessoas e veículos, controle de estoque e localização de animais. O emprego desta tecnologia vem crescendo consideravelmente e consequentemente, seu custo passou a apresentar uma redução atrativa viabilizando o espectro de aplicações do RFID.

Figura 1 – RFID e Tags

Fonte: Site FilipeFlop - https://www.filipeflop.com/produto/kit-modulo-leitor-rfid-mfrc522-mifare/

2.2. Arduíno

Arduíno teve seu início na Itália, no ano de 2005. Seu propósito era disponibilizar uma plataforma para construir projetos com o custo bem menos elevado em comparação com os outros que já estavam no mercado. Trata-se de uma plataforma open-source de prototipagem e de baixo custo. O Arduíno adota o conceito open-source, com isso, seu software e hardware são abertos para qualquer pessoa que deseje alterá-lo ou copiá-lo. Conforme Mork (2013) devido a este fato de a tecnologia empregada ser de baixo custo, para projetos que se utilizam de microcontroladores são cada vez mais comuns a utilização do Arduíno. Projetos e sistemas podem ser desenvolvidos com conhecimento básico de eletrônica, desde simples controles de luzes até automatização de residências, usando-se o Arduíno. Foi desenvolvido para que sua compreensão e programação sejam fácil, adaptável a sistemas operacionais diferentes.

O Arduíno transforma através de sensores ligados a ele, sinais do mundo físico para a programação e vice-versa. Possui um controlador com pinos de entrada e saída de dados. A linguagem de programação utilizada é baseada em C/C++, com algumas alterações. O fato de o Arduíno possuir um microcontrolador possibilita facilmente a criação de inúmeras aplicações diferentes, além de permitir a reutilização de componentes, apenas reprogramando-o, transformando-o em uma grande ferramenta para projetos rápidos (DI RENNA et al, 2013). A Figura 2 apresenta um Arduíno Uno.

Figura 2 - Arduíno

Fonte: Site Oficial Arduíno - https://store.Arduíno.cc/usa/Arduíno

2.3 Controle de acesso

O principal objetivo do procedimento de controle de acesso é que somente pessoas que possuem permissão possam entrar em determinados locais, fazendo com que pessoas não autorizadas, busquem a autorização, ou caso contrário, não poderão adentrar aos mesmos. Em

diferentes instituições, organizações, há sistemas de controle de acesso, por vezes informatizados, para facilitar a operação de identificação dos passantes. Estes sistemas têm como objetivo também, automatizar este processo de validação do acesso, ajudando assim na preservação dos bens daquele determinado local (BRENNER e BIZARRIA, 2011).

Para realizar o controle do acesso tem-se que definir os ambientes que serão controlados, tendo como foco a entrada bem como sua saída. Estes ambientes devem ser controlados também por meio físicos e detectores eletrônicos (BRENNER e BIZARRIA, 2011).

Todos os acessos são salvos em um servidor, onde neste também são realizadas as regras e as pessoas que são permitidas acessar áreas em que o sistema monitora e controla. Este acesso pode ser gerenciado através de biometria, cartões de proximidade ou senhas, possibilitando um controle estatístico da movimentação e estão inseridos em todos os níveis de segurança dos bens de uma instituição.

3 PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma pesquisa exploratória e descritiva. Foi utilizado o método de abordagem indutivo, que parte de um caso único, com uma conexão ascendente, do específico para o geral (LAKATOS & MARCONI, 2009). Trata-se ainda, de uma pesquisa experimental, por meio de um estudo de caso junto à Instituição de Ensino Superior (IES), Faculdade de Tecnologia de Carapicuíba, cujo experimento é um sistema de controle de acesso de pessoas em suas dependências – alunos, professores, terceiros, a partir do uso do Arduíno e leitor RFID, após observações dos principais pontos de vulnerabilidade que demandam modificações para segurança local.

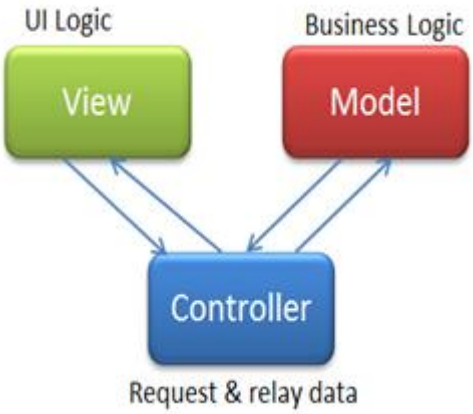
4 DESENVOLVIMENTO

O Controle de Acesso YSNP é um sistema eletrônico que controla o acesso de pessoas ao interior do campus da IES, objeto de estudo. Esse sistema foi desenvolvido na linguagem de programação JAVA, em conjunto com o Arduíno (baseado na linguagem C/C++, com algumas modificações) para desenvolvimento da parte eletrônica, e um leitor RFID (*Radio Frequency IDentification*), para efetuar os registros de entrada e saída. Para persistência dos dados dos transeuntes que utilizarão o sistema foi utilizado o banco de dados MySql, o qual, além de ser gratuito, responde adequadamente à demanda que lhe é exigida.

Em seu desenvolvimento foi utilizado o padrão MVC (*Model View Controller*) conforme fluxograma da Figura 3. Este padrão de arquitetura de software possui um processo

simples, onde a camada Controller é o elemento principal, executando a maior parte das tarefas. Ele faz a interação entre as outras camadas da aplicação (*Model e View*). No caso do YSNP controle de acesso, é esta camada quem faz a interface da aplicação com o banco de dados. A camada Model é onde contém os dados da aplicação e as regras de negócio. Por fim, na camada View é responsável pela apresentação dos dados para o usuário (telas do sistema).

Figura 3: Fluxograma do modelo MVC



Fonte: Code Project - https://www.codeproject.com/Articles/552846/Why-s-How-s-of-Asp-Net-MVC-Part

Para fazer a persistência dos dados, foi utilizado o padrão DAO (Data Access Object) em conjunto com o padrão MVC. Este padrão nos permite mudar como os dados são armazenados sem que a lógica do negócio seja influenciada, tornando mais simples o entendimento das classes e de fácil manutenção. As classes DAO tem a responsabilidade de manter a comunicação entre o SGBD (Sistema Gerenciador de Banco de Dados). Ele fornece as operações principais para a aplicação: o CRUD, que permite Criar (Create), Ler (Read), Alterar (Updade) e Deletar (Delete) informações da base de dados. Ao realizar a comunicação entre o SGBD ele transforma os dados que vem da base em objetos e vice-versa.

Assim que é inicializado o sistema YSNP, irá aparecer a tela de login, conforme Figura 4, onde o usuário deverá colocar seu UserName e sua senha.

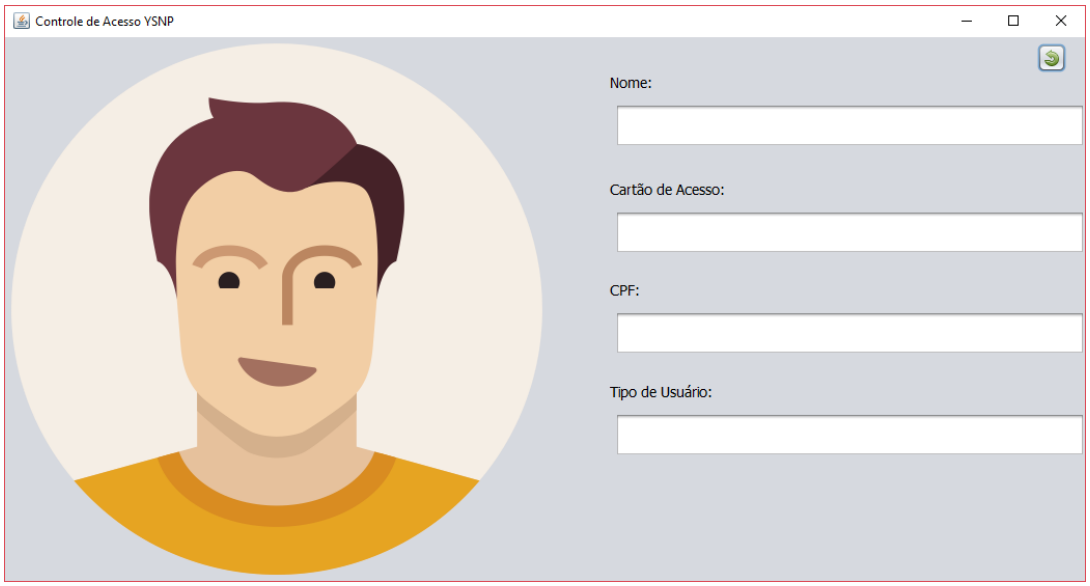
Após inserir seus dados na tela de login e clicar no botão entrar, o sistema irá procurar no banco de dados se este utilizador existe, caso o utilizador não exista ou erre algum dos dados exigidos para acessar o sistema, não terá acesso ao sistema.

Figura 4 – Tela de Login

Fonte: Elaborada pelos autores

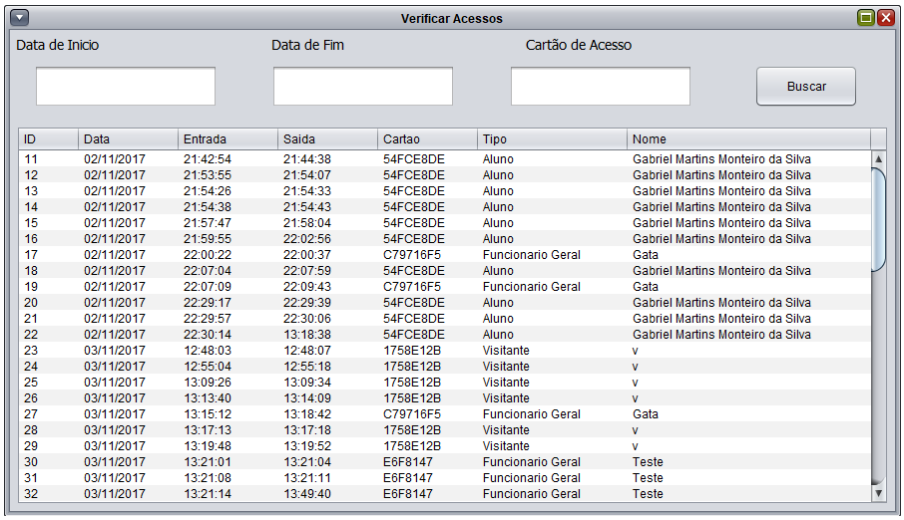
O sistema conta com as seguintes funcionalidades: controle de acesso, onde o utilizador do sistema possa efetivamente fazer o controle de acesso ao Campus (Figura 5), registrando automaticamente as entradas e saídas; a função de verificar acessos (Figura 6) se trata de um relatório onde o utilizador pode verificar quem entrou e saiu do Campus, mostrando que horas o usuário registrou sua entrada e sua saída, o dia desses registros bem como qual o tipo do usuário; nas funções gerenciar usuário (Figura 7), gerenciar segurança (Figura 8) e gerenciar login (Figura 9) o utilizador poderá efetuar as quatro operações básicas realizadas em banco de dados, podendo cadastrar, alterar, excluir ou procurar dados que estão salvos no banco.

Figura 5: Tela de Controle de Acesso



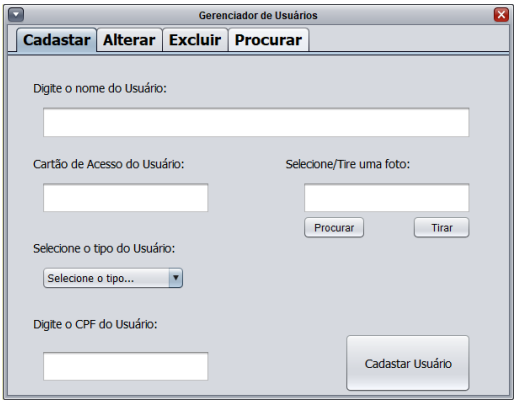
Fonte: Elaborada pelos autores

Figura 6: Tela de Verificar Acessos



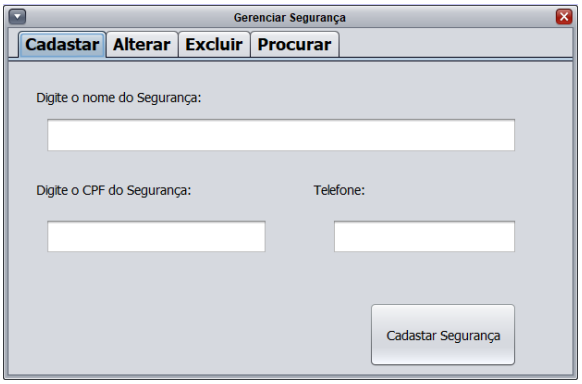
Fonte: Elaborada pelos autores

Figura 7: Tela de Gerencia de Usuário



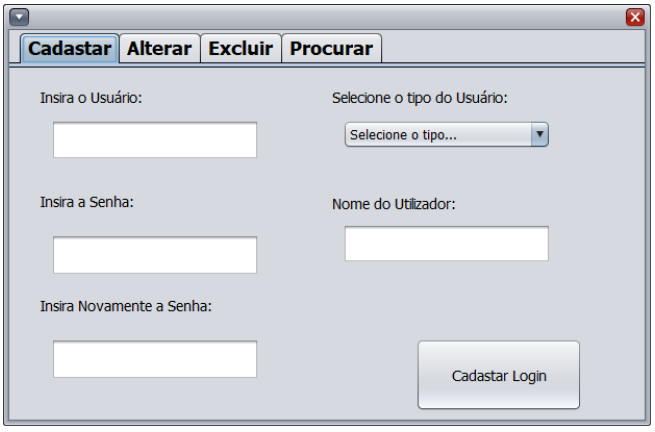
Fonte: Elaborada pelos autores

Figura 8: Tela de Gerencia de Segurança



Fonte: Elaborada pelos autores

Figura 9: Tela de Gerencia de Login



Fonte: Elaborada pelos autores

Para este sistema, existem três tipos de perfil de acesso: o Administrador, o Diretor e o Segurança. O administrador terá acesso a todas as funcionalidades do sistema: a tela de "Controle de Acesso", a tela de "Gerenciar Usuário", "Gerenciar Segurança", "Verificar Acessos" e "Gerenciar Login". O Segurança terá disponível somente as funções de "Controle de acesso" e "Gerenciar usuário". O Diretor terá disponível as funções de "Controle de acesso", "Gerenciar Usuário", "Gerenciar Segurança" e "Verificar Acessos".

Para que esse sistema possa registrar as entradas e saídas, o usuário precisará passar a Tag no leitor de RFID, que mostrará seus dados no monitor, sendo verificado pelo utilizador do sistema (Segurança). Caso o usuário possua uma Tag compatível com essa tecnologia RFID e que não esteja devidamente registrada no sistema, não terá acesso até que o utilizador realize seu cadastro inserindo seus dados pessoais, tirar uma foto e validando sua Tag.

Serão utilizadas duas plataformas do Arduíno bem como dois leitores RFID. Um conjunto ficará responsável para registrar a entrada e o outro para registrar a saída. Ambos irão trabalhar de forma sincronizada de modo que o usuário não consiga efetuar duas entradas ou duas saídas com a mesma Tag, ainda que, por inocência, queira emprestar sua Tag para outra pessoa utilizá-la.

Em caso de ser um visitante, o utilizador do sistema irá registrá-lo, na aba cadastrar contida na função gerenciar usuário, seus dados serão inseridos no sistema e será liberada uma Tag de acesso a qual só será válida enquanto estiver dentro do Campus, devendo esta ser obrigatoriamente devolvida em sua saída. Após o visitante registrar sua saída, a Tag que ele utilizou será automaticamente desvinculada deixando-a disponível para ser utilizada para outro visitante, para o qual esse processo deverá ser realizado novamente.

Os custos do Projeto têm as seguintes projeções: em média, R$ 30,00 (trinta reais) a placa de Arduíno, R$15,00 (quinze reais) o leitor de RFID e em média, R$ 1,00 (um real) cada cartão plástico, compatível a essa tecnologia. Este sistema necessitará de duas plataformas Arduíno bem como dois leitores RFID, onde ambos irão trabalhar de forma sincronizada, um registrando somente a entrada e o outro a saída, impedindo assim que o usuário registre duas entradas ou duas saídas, caso este usuário, mesmo que de maneira despretensiosa, venha a emprestar seu cartão a outro usuário que esteja fora do Campus. Tendo em vista que, no semestre de 2017-2, há 2.197 alunos matriculados na Fatec e 1.100 alunos matriculados na Etec (que também têm acesso ao Campus), acrescentando-se os funcionários administrativos e professores de ambas as instituições, perfazendo aproximadamente um total de 3.500 acessos diários ao campus, conforme Tabela 1, há a

necessidade de, em média, 3.500 cartões, o que corresponde ao valor de R$ 3.500,00, pelo valor unitário de cada um a R$ 1,00. Para que este projeto seja implementado, portanto, a instituição investirá aproximadamente R$ 3.590,00, sem considerar o custo operacional da Equipe Técnica para implantação. Para que este sistema funcione o mesmo deve possuir os equipamentos citados anteriormente bem como um computador com uma configuração simples: o Hardware com processador duo core ou superior, 1Gb ou mais de memória RAM, periféricos tais como, mouse, teclado e Webcam e como Software de operação, o Sistema Operacional Windows 7 ou superior, Java e banco de dados MySQL. Para que as pessoas possam acessar a instituição, devem possuir um cartão de acesso, que seja válido. Se não possuir tal cartão o operador do sistema, a equipe de segurança efetuará um cadastro como visitante para esta pessoa, associando um cartão, o qual deverá ser devolvido quando da saída do Campus.

Tabela 1 – Quantidade de acessos diários, referente ao segundo semestre de 2017

Cálculo de Acessos Campus FATEC/ETEC Carapicuíba				
	Matrículas	Funcionários	Professores	Terceiros
FATEC	2.197	19	64	24
ETEC	1.100	20	76	
SUBTOTAL	3.297	39	140	24
TOTAL	3.500			

Fonte: Secretarias Acadêmicas Fatec-Etec Carapicuíba

5 RESULTADOS E DISCUSSÃO

Após uma análise dos procedimentos utilizados atualmente no processo de controle de acesso à IES objeto de estudo, foi verificado que existe a necessidade de melhorias na conferência dos usuários bem como nos procedimentos ao quais estes são submetidos. Desta forma, para que este controle seja feito de maneira mais adequada, além de facilitá-lo, sugere-se que o sistema apresentado no Desenvolvimento possui viabilidade de implantação pelo baixo custo às duas Instituições. Tendo em vista que estes novos procedimentos serão quase todos automatizados, ficando apenas o procedimento de identificação física de responsabilidade por parte do segurança, que terá a função de comparar o usuário com a sua foto que está registrada no sistema bem como identificar e registrar os visitantes, tornando

assim mais apropriado o controle quanto aos usuários à instituição, deixando-a mais segura, pois só adentrará às suas dependências aquele que possuir um cartão válido e estiver de acordo com as características físicas presentes em seu cadastro.

6 CONSIDERAÇÕES FINAIS

Conclui-se que é de suma importância que haja uma melhoria nos procedimentos utilizados no controle de acesso, uma vez que o atual controle apresenta diversas falhas das quais, facilmente pessoas mal-intencionadas conseguem entrar na instituição sem maiores problemas, podendo agir pelos seus interesses, dado que sua identificação nos modelos atuais fica praticamente impossível pois a atual identificação pode ser falsificada ou utilizada por outra pessoa.

O diferencial da proposta deste projeto, com relação ao atual procedimento realizado, está no controle onde a usuário somente poderá registrar uma entrada por vez, sendo que para haver outro registro de entrada com o mesmo cartão deverá antes registrar sua saída, pois mesmo que o usuário registre sua entrada e, de maneira indevida, disponibilize seu cartão para outra pessoa que esteja fora da instituição, este cartão não poderá registrar uma nova entrada sem antes ter registrado a efetiva saída.

REFERÊNCIAS

BRENNER, Gabriel Pitágoras Silva; BIZARRIA, Walter. **Sistema de Controle de Acesso com Biometria da Digital. VIII SEGET- Simpósio de Excelência em Gestão e Tecnologia (2011).** Disponivel em <https://www.aedb.br/seget/arquivos/artigos11/44914520.pdf>. Acesso em 25 set 2017.

DI RENNA, Roberto Brauer; BRASIL, Rodrigo Duque Ramos; CUNHA, Thiago Elias Bitencourt; BEPPU, Mathyan Motta; FONSECA, Erika Guimarães Pereira da. **Introdução ao kit de desenvolvimento Arduíno.** Tutoriais PET-Tele. Universidade Federal Fluminense - UFF. Escola de Engenharia - TCE. Curso de Engenharia de Telecomunicações - TGT. Niterói – RJ, Junho (2013). Disponível em: www.telecom.uff.br/pet/petws/downloads/tutoriais/Arduíno/Tut_Arduíno.pdf. Acesso em: 28 Out 2017.

DUROC, Y.; KADDOUR, D. **RFID potential impacts and future evolution for Green projects.** Energy Procedia, v. 18, p. 91-98, 2012.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 6. ed. São Paulo: Atlas, 2009. 315p.

MORK, S. **Programação com Arduíno:** Começando com Sketches. Porto Alegre: Bookman, 2013.

SEUFITELLI, Claudia Boechat; HENRIQUE, Daniele FONTES; ROSA, Sérgio Inácio da; CARVALHO, Rogério **Atem de. Tecnologia RFID e seus benefícios.** Revista VÉRTICES, Campos dos Goytacazes/RJ, v. 11, n. 1/3, p. 19-26, jan./dez. 2009.

SUN, C. **Application of RFID technology for logistics on internet of things.** AASRI Conference on Computational Intelligence and Bioinformatics, v. 1, p. 106-111, 2012.

"O conteúdo expresso no trabalho é de inteira responsabilidade do(s) autor(es)."