CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
CAMPUS TIMÓTEO

Helton Macedo Souza

CONTROLE DE ACESSO VEICULAR UTILIZANDO TECNOLOGIA DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

Timóteo

2018

Helton Macedo Souza

CONTROLE DE ACESSO VEICULAR UTILIZANDO TECNOLOGIA DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

Monografia apresentada à Coordenação de Engenharia de Computação do Campus Timóteo do Centro Federal de Educação Tecnológica de Minas Gerais para obtenção do grau de Bacharel em Engenharia de Computação.

Orientador: Adílson Mendes Ricardo

Timóteo

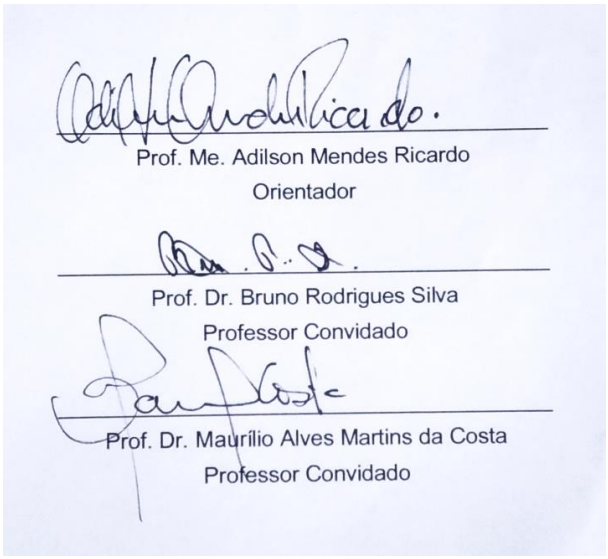
2018

Helton Macedo Souza

Controle de acesso veicular utilizando tecnologia de identificação por radiofrequência

Monografia apresentada ao Curso de Engenharia de Computação do Centro Federal de Educação Tecnológica de Minas Gerais, campus Timóteo para obtenção do título de Engenheiro de Computação.

Trabalho aprovado. Timóteo, 09 de Julho de 2018:



Timóteo
2018

Dedico este trabalho

a minha família.

Agradecimentos

Agradeço primeiramente a Deus por sempre me ouvir, ser fonte de segurança, tranquilidade e paz nos momentos difíceis pelos quais passei durante essa caminhada.

Agradeço a minha família pelo apoio e conselhos durante essa jornada, agradeço também pela paciência e por sempre me motivar a continuar batalhando até o fim.

Agradeço ao meu professor orientador Adílson Mendes Ricardo que mesmo antes de iniciar essa etapa de TCC já estava aberto a conversas e me ajudando a direcionar as ideias para meu trabalho, agradeço a suas orientações no decorrer do trabalho, por estar disposto a me ajudar com as duvidas e com as dificuldades que encontrei. Agradeço também a professora Deisymar Botega Tavares pelas conversas e sugestões no decorrer do trabalho desde o inicio no surgimento da ideia até a conclusão do trabalho ajudando a direcionar o projeto.

Por fim, agradeço aos amigos que conheci e fizeram parte dessa caminhada vivenciando comigo alegrias e dificuldades durante o curso.

“Não existe triunfo sem perda, não há vitória sem sofrimento, não há liberdade sem sacrifício.”

J.R.R. Tolkien

Resumo

Com a evolução da tecnologia e sua aplicação cada vez mais em processos, sempre buscando agilidade e praticidade, surgiu também a necessidade de proteção, ou seja um meio de se aplicar essa tecnologia de forma segura. Diversas tecnologias surgiram visando o controle físico e lógico, responsáveis por garantirem a integridade e a confidencialidade em um processo. Uma dessas tecnologias que tem se destacado na automatização e identificação de objetos é a de identificação por radiofrequência ou comumente chamada, RFID -*Radio-Frequency IDentification*. A RFID é amplamente utilizada no segmento de cadeias de suprimentos e permite a identificação em tempo real do objeto, permitindo uma automatização do processo. Este trabalho de pesquisa atua no controle físico realizando uma verificação de usuários e seus veículos no acesso ao interior de uma organização ou instituição e, como estudo de caso será aplicada no CEFET-MG campus Timóteo. Atualmente é realizado um controle manual dos veículos pelos vigilantes. O presente trabalho de pesquisa parte desse controle manual como base para a modelagem de um sistema de banco de dados integrado a ferramentas RFID para automatizar esse processo, identificando e verificando as permissões dos usuários no acesso à instituição, digitalizando essas informações, permitindo o uso de diversas funcionalidades como cadastros, controles e relatórios, segundo os princípios da segurança da informação: a integridade, a confidencialidade e a disponibilidade.

Palavras-chave: Controle físico, RFID, radiofrequência, automatização, controle de acesso veicular.

Abstract

With the evolution of technology and its application more and more in processes, always seeking agility and practicality, also arose the need for protection, or a means to apply this technology safely. Several technologies have emerged aiming at the physical and logical control, responsible for guaranteeing integrity and confidentiality in a process. One of these technologies that has stood out in the automation and identification of objects is the one of radiofrequency identification or commonly called, RFID. RFID is widely used in the supply chain segment and allows the real-time identification of the object, allowing automation of the process. This research work focuses on physical control by performing a verification of users and their vehicles in the access to the interior of an organization or institution and as a case study will be applied at the CEFET-MG campus Timóteo. Nowadays a manual control of the vehicles is carried out by the vigilantes. The present research work is based on this manual control as the basis for the modeling of a database system integrated with RFID tools to automate this process, identifying and verifying the users' access permissions to the institution, digitizing this information, allowing the use of various functionalities such as registers, controls and reports, according to the principles of information security: integrity, confidentiality and availability.

Keywords: Physical control, RFID, radiofrequency , automation, vehicular access control.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

De acordo com Finkenzeller (2010), os procedimentos de identificação automática (Auto-ID) tornaram-se populares em indústrias de serviços, logística de vendas e distribuição, cadeia de suprimentos e sistemas de fluxo de materiais. Existem procedimentos de identificação automática para fornecer informações sobre pessoas, animais, bens e produtos em trânsito.

O código de barras que desencadearam uma revolução nos sistemas de identificação há algum tempo, são considerados insuficientes em um número cada vez maior de casos. Na vida cotidiana o mais comum é a utilização de cartões inteligentes com base em um campo de contato para se realizar o transporte de dados (FINKENZELLER, 2010).

No entanto, o contato usado no cartão inteligente muitas vezes é impraticável, uma transferência de dados sem contato entre o dispositivo de transporte de dados e o seu leitor é mais viável. No caso ideal, a energia necessária para operar o dispositivo eletrônico de transporte de dados também seria transferida do leitor usando tecnologia sem contato. Devido aos procedimentos utilizados para a transferência de energia e dados, os sistemas de identificação sem contato são chamados de sistemas de identificação por radiofrequência ou simplesmente RFID - *Radio-Frequency IDentification* (Identificação por radio-frequência) (FINKENZELLER, 2010).

A captura de dados por RFID apresenta inúmeras vantagens em relação a outras tecnologias, em especial a capacidade de leitura de informações em tempo real, sem a necessidade de um campo visual entre o leitor e a etiqueta, podendo até mesmo existir obstáculos entre eles, conforme descreve Glover e Bhatt (2006).

1.1 Problema

De acordo com Sêmola (2014) durante décadas e em alguns casos as informações são tratadas de forma centralizadas e pouco automatizadas. Com o passar do tempo surgiram investimentos na área de tecnologia da informação e a praticidade na aquisição da informação relacionada a automatização dos processos passou a ser uma necessidade.

A partir disso criou-se uma dependência em relação à informação, digitalizada, compartilhada e distribuída e aos elementos da infraestrutura que a mantém (SÊMOLA, 2014). Com isso viu-se a necessidade de se criar meios de proteção físicos e lógicos. Dentro do controle físico está o controle de acesso veicular, talvez sendo a primeira barreira da instituição ou organização no quesito segurança. Quando se diz respeito ao controle de acesso veicular muitos negligenciam esta prática devido aos custos para a implantação de sistemas de segurança falham em manter este controle. Também existe o fato de que muitas instituições e/ou organizações realizam uma verificação manual, isto é, não automatizada, o que pode levar a falhas humanas e tornar o processo custoso e com um menor controle sobre as informações.

O campus do CEFET em Timóteo permite que professores, servidores e alunos utilizem o estacionamento interno para carros e motos, contudo a verificação não automatizada do acesso a parte interna não permite um controle apropriado para gerir o uso deste recurso disponibilizado pela instituição.

Futuramente o campus do CEFET em Timóteo poderá passar por ampliações o que aumentaria o fluxo de pessoas circulando e eventualmente o número de veículos com acesso a parte interna. Assim neste contexto surge uma questão: Como controlar o acesso veicular a partes internas de instituições e organizações de uma forma adequada, atribuindo também a este controle os três princípios da segurança da informação (integridade, confidencialidade e disponibilidade) ao processo?

1.2 Justificativa

O uso de dispositivos de segurança tornou-se necessário para o acesso a prédios, estacionamentos, escritórios entre outros locais que necessitam de restrição quanto ao seu acesso. Em casos como estes poderiam ser implantados sistemas de segurança para se realizar uma verificação e validação do usuário. Entre algumas tecnologias para este fim estão a biometria, o scanner de retina, a fechadura eletrônica e o reconhecimento facial (RAMOS, 2012).

Algumas destas tecnologias possuem um custo elevado, como o scanner de retina, ou expõem o usuário fazendo com que ele tenha que ir até o equipamento de leitura ou verificação o que poderia apresentar um risco a sua segurança física. Uma alternativa seria a verificação manual o que torna o processo custoso e pode estar sujeito a falhas humanas.

De acordo com Ahson e Ilyas (2008) a tecnologia RFID trás uma ampla gama de utilizações, sendo este um importante aspecto, ajudando organizações e indivíduos a realizar ganhos substanciais de produtividade e eficiência, mantendo as características do processo.

As áreas em que a tecnologia RFID vem aparecendo principalmente são a logística, gestão da cadeia de abastecimento e suprimentos, acervo de bibliotecas, implantes médicos, controle de acesso, segurança da aviação e aplicações de segurança nacional.

A tecnologia de identificação por radiofrequência se apresenta como uma alternativa para se automatizar um procedimento de controle de acesso em um determinado local permitindo um controle apropriado de entrada e saída das pessoas que estão utilizando este recurso.

1.3 Objetivos

Este trabalho tem como objetivo geral analisar e comparar a viabilidade, quanto a facilidade, da implantação de um sistema de controle de acesso automatizado utilizando a tecnologia de identificação por radiofrequência em relação ao sistema de controle manual, assegurando a integridade, confidencialidade e disponibilidade das informações coletadas. Também, objetivam-se mais especificamente:

1. Investigar e simular a tecnologia RFID.
2. Implementar um protótipo de sistema de identificação de usuários usando RFID
3. Comparar o sistema atual com o sistema proposto.

1.4 Estrutura do texto

O texto está estruturado da seguinte forma:

- O capitulo 1 faz uma introdução ao trabalho apresentando o problema, a motivação e os objetivos para este trabalho.
- O capitulo 2 desenvolve a fundamentação teórica necessária para a realização da proposta.
- O capitulo 3 retrata os trabalho relacionados recentemente dentro dessa areá, mostrando a abordagem e os meios utilizados para se chegar a solução.
- No capitulo 4 são evidenciados os materiais e as etapas dos procedimentos ou métodos a serem seguidos para o desenvolvimento do trabalho.
- O capitulo 5 apresenta o desenvolvimento e modelagem da proposta, assim como os testes realizados.
- O capitulo 6 são apresentados os resultados obtidos, a comparação entre os dois modelos manual e automatizado.
- No capitulo 7 está presente a conclusão e considerações finais do trabalho, assim como as ideias para trabalhos futuros.

2 Fundamentação teórica

2.1 Redes sem fio

O termo *wireless*, que quer dizer sem fio, possui alguns sinônimos tais como: comunicação sem fio e rede sem fio. A comunicação sem fio baseia-se no estabelecimento da comunicação por meio do ar, usando como meio de transporte o espaço. Redes sem fio enviam e recebem dados, combinando conectividade de equipamentos e mobilidade do usuário. Os modos de transmissão das redes sem fio utilizam as seguintes tecnologias: *spread spectrum* (rádio), infravermelho ou microondas (MENDES, 2007).

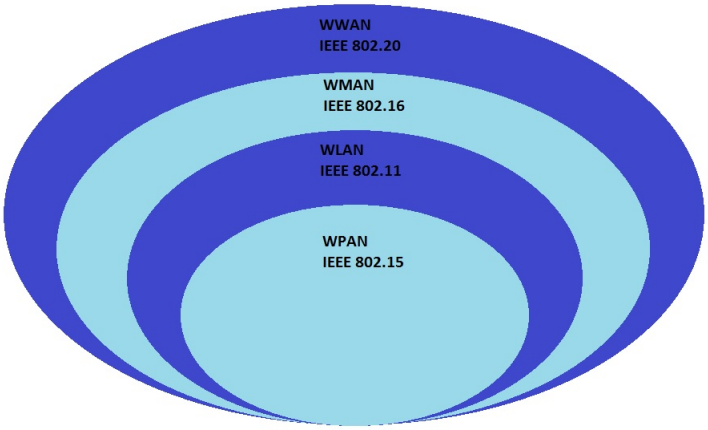
Muitas tecnologias e padrões para LANs sem fio foram desenvolvidos na década de 1990, um padrão em particular de padrões se destacou: a LAN sem fio IEEE - *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos) 802.11, também conhecida como *Wi-Fi* (KUROSE, 2013).

As WLANs - *Wireless Local Area Network* (Rede de área local sem fio) podem ser encontradas em campus universitários, em edifícios comerciais e em vários outros lugares (FOROUZAN, 2009).

O IEEE é uma associação profissional técnica sem fins lucrativos. Seu objetivo é desenvolver padrões técnicos consensuais nos campos das engenharias elétrica, eletrônica e de computação para uso das indústrias. Um dos seus grupos de trabalho foi denominado 802.11, que engloba uma série de especificações que definem como deve ser a comunicação entre dispositivos de uma rede sem fio (ENGST; FLEISHMAN, 2003).

A figura 1 trás a classificação das redes sem fio de acordo com o seu alcance.

Figura 1 – Classificação das redes sem fio



Fonte: Adaptado de Júnior (2012)

Nas subseções a seguir será tratado sobre essas classes que sugiram dentro da tecnologia de redes sem fio.

2.1.1 *Wireless Wide area network* - WWAN

WWAN - *Wireless Wide Area Network* (Rede de longa distância sem fio) é uma rede de grande alcance, também conhecida como rede continental, já que sua área de cobertura se estende por um país ou até mesmo por um continente. As redes de telefonia móvel são as principais representantes nesse escopo de rede (JÚNIOR, 2012).

2.1.2 *Wireless Metropolitan Area Network* - WMAN

WMAN - *Wireless Metropolitan Area Network* (Redes metropolitanas sem fio), esta classe se refere a redes metropolitanas: redes de uso corporativo que atravessam cidades ou estados. Essa conexão é utilizada na prática entre os provedores de acesso e seus pontos de distribuição até os contratantes.

O WMAN é referenciado pelo padrão IEEE 802.16, que foi criado para substituir o padrão IEEE 802.11b no que diz respeito à transmissão de dados a longa distância. Os testes iniciais utilizando o padrão 802.11b e antenas de alta potência não conseguiram alcançar os resultados esperados, pois, eram necessários vários repetidores na sua extensão para conseguir atingir distâncias consideráveis para a tecnologia (JÚNIOR, 2012).

O novo padrão 802.16 utiliza um espectro variável, implementando faixas de frequência entre 10 e 60 GHz, com um padrão alternativo que utiliza frequências entre 2 e 11 GHz. Isto possibilita atingir altas taxas de transferência a distâncias consideráveis.

Desenvolvido dentro do padrão 802.16 um sistema se sobressai, o *WiMax* - *Worldwide Interoperability for Microwave Access* (Interoperabilidade Mundial para Acesso de Micro-Ondas), o *WiMax* foi desenvolvido para atender a demanda de um acesso à Internet móvel (sem fio) e de banda larga na conexão entre o assinante residencial/corporativo e a provedora do serviço de acesso, serviço este que atualmente é atendido por conexões com fio, que usam a infra-estrutura da rede telefônica, de televisão a cabo ou especializada.

De modo simplificado, no *WiMax* um equipamento em uma torre (semelhante às de telefonia celular) transmite o sinal aos assinantes que, por sua vez, utilizam um equipamento especializado para a recepção do sinal, um modem ou modulador de sinal, que pode ficar, por exemplo, no telhado de uma casa ou de um prédio, ao lado do computador de mesa, ou até mesmo embutido em *notebooks* ou dispositivos portáteis (SOARES; SILVA, 2009).

2.1.3 *Wireless Local Area Network* - WLAN

WLAN - *Wireless Local Area Network*(Rede de área local sem fio), trata-se uma rede com alcance limitado a um raio de 100 a 300 m, comumente usadas em escritórios, shoppings, residências, instituições de ensino, entre outros, como alternativa de acesso a internet ou extensões de redes convencionais.

A principal tecnologia dessa categoria é o *Wi-Fi - Wireless Fidelity* (fidelidade sem fio) que tem a designação IEEE 802.11n que opera em 2,4GHz e 5,0GHz de forma simultânea ou não, com taxas de transmissão de 65 Mbps a 600 Mbps dependendo da versão (TANENBAUM; WETHERALL, 2011).

Em virtude da grande utilização das redes locais houve uma diminuição dos custos com os equipamentos e consequentemente a popularização de redes particulares comuns nos dia de hoje, não só nos grandes centros urbanos, mas também sendo uma alternativa ou complemento a redes cabeadas.

Com o passar do tempo e o surgimento de novas técnicas e/ou métodos o padrão 802.11 foi ganhando variações e evoluindo suas características, nos últimos anos o principal padrão utilizado é o 802.11n, mas outros já estão em desenvolvimento ou sendo implementados como o 802.11ac e 802.11ad entre outros (KUROSE, 2013).

Segundo Tanenbaum e Wetherall (2011) o padrão 802.11 evoluiu com o passar do tempo e assim aprimorando e ganhando novos recursos e especificações.

Abaixo uma tabela contendo as características das variações do padrão 802.11.

Tabela 1 – Padrões 802.11

Padrão	Taxa máxima de Transmissão	Frequêcias	Compatibilidades
802.11a	54 Mbps	5 GHz	Não
802.11b	11 Mbps	2.4 GHz	Não
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz ou 5 GHz	802.11b/g
802.11ac	1.3 Gbps	2.4 GHz ou 5 GHz	802.11b/g/n
802.11ad	7 Gbps	2.4 GHz , 5 GHz e 60 GHz	802.11b/g/n/ac

Fonte: Adaptado de Tanenbaum e Wetherall (2011)

- 802.11b

  Este foi o primeiro padrão para comunicação *wireless* utilizado em larga escala e com ele teve-se a possibilidade de se realizar a comunicação e interação entre dispositivos de diversos fabricantes.

  Nas redes de padrão 802.11b, utiliza-se uma frequência de 2,4 GHz, permitindo assim a transmissão de até 11 Mbps com um alcance de no máximo 100 metros. Essa velocidade pode ser alterada dependendo do número de obstáculos presentes na transmissão.

  O distanciamento do ponto de acesso faz com que o sinal diminua até que se perca totalmente e através de alguns softwares específicos, é possível realizar a medida da qualidade do sinal (TANENBAUM; WETHERALL, 2011).

- 802.11b+

  Esse padrão foi uma evolução do padrão 802.11b. Com ele é possível se conectar a uma rede de até 22 Mbit/s, o dobro do anterior 802.11b, porém para que isso seja realmente

possível, as duas placas *wireless* devem ser trabalhar com o padrão 802.11b+ e estarem bem próximas do ponto de acesso. Caso ocorra a mesclagem de dispositivos, como por exemplo, 802.11b e 802.11b+, a taxa de transmissão cairá para 11 Mbps respeitando o dispositivo com a taxa mais baixa (BULHMAN; CABIANCA, 2016).

- 802.11a

  Esse padrão começou a ser desenvolvido primeiro que o padrão 802.11b, porém ficou pronto depois. Com ele é possível trabalhar a uma velocidade teórica de 54 Mbps e empregando uma frequência de 5 GHz. Também é possível compartilhar dados com os padrões 802.11b e 802.11b+ lembrando que a velocidade será sempre à do dispositivo mais lento (FOROUZAN, 2009).

- 802.11g

  Esse padrão é a evolução dos padrões anteriores, ele faz a junção do melhor do 802.11b (alcance do sinal) e do 802.11a (taxa de transmissão). Com ele é possível chegar aos 54 Mbps. Porém como os outros padrões caso alguém se conecte a rede *WiFi* com uma placa que não seja 802.11g a rede inteira começará a trabalhar a uma velocidade de 11 Mbps. Um ponto a se considerar é que o 802.11g não consegue trabalhar com placas do tipo 802.11a (TANENBAUM; WETHERALL, 2011).

- 802.11n

  O padrão 802.11n trouxe a possibilidade de utilização de canais com 40 MHz de banda, permitindo praticamente duplicar as taxas de transferência por canal. Além disso, permite que 2 canais adjacentes (sem superposição) de 20 MHz sejam combinados para formar um único canal de 40 MHz (TANENBAUM; WETHERALL, 2011).

  Desta forma, os canais do padrão 802.11n podem ser configurados como 20MHz, 40MHz, ou conversão automática de 40/20 MHz. Os canais com conversão automática operam em 40 MHz, mas podem automaticamente retornar para 20MHz, quando existe interferências.

  Em relação a banda de 2,4 GHz, isto não representa um ganho significativo porque podem existir apenas 3 canais de 20 MHz que não se superpõem, mas em relação a banda de 5GHz os resultados são bastante satisfatórios. Quando se utiliza o padrão 802.11n com canais de 20MHz na banda de 2,4GHz pode-se atingir até 288,9Mbps. De forma semelhante, na banda de 5 GHz, qualquer canal disponível pode ser designado com largura de 40 MHz, permitindo atingir uma taxa expressiva de 600 Mbps (BULHMAN; CABIANCA, 2016).

- 802.11ac

  Assim como os padrões anteriores, o padrão 802.11ac explora justamente estes itens como aumento da largura de banda empregada, aumento da eficiência espectral e relação sinal/ruído de modo a permitir o aumento da taxa de transmissão.

  O padrão 802.11ac possui largura de banda de 80/160 MHz e utilizará apenas a faixa de 5 GHz, que é menos congestionada de dispositivos e, portanto, menos poluída de

fontes interferentes. Este padrão foi desenvolvido entre 2011 e 2013, com previsão de lançamento somente para o início de 2020. O padrão trabalha com multiestações de transferência sem-fio de na escala de Gbps em *link* único de transferência, graças ao conceito de extensão de interface, já implementado no modelo 802.11n (BULHMAN; CABIANCA, 2016).

- 802.11ad

  Atualmente, desenvolvido pela *Samsung Electronics* a tecnologia *Wi-Fi* que opera na frequência de 60GHz, permite velocidades de transmissão de dados de até 7,2 Gbps, a velocidade máxima possível com dispositivos eletrônicos de consumo existentes .

  Diferentemente do 2,4 GHz, tecnologia já muito utilizada e 5GHz *Wi-Fi*, o padrão 802.11ad utiliza 60GHz nos equipamentos e mantém a velocidade máxima, eliminando a interferência de co-canal, independentemente do número de dispositivos que utilizam a mesma rede. Ao fazer isso, a nova tecnologia da *Samsung* elimina a lacuna entre as velocidades teóricas e reais, e exibe a velocidade real que é 10 vezes mais rápido do que a de 2,4 GHz e 5GHz nas tecnologias *Wi-Fi* atuais (BARION, 2016)

2.1.4 Wireless Personal Area Network - WPAN

Uma WPAN - *Wireless Personal Area Network* (Rede de área pessoal sem fio) é uma agrupamento de dispositivos em rede situada dentro de um curto alcance (normalmente 10 metros). O atributo "pessoal" decorre da fato de que este conjunto de dispositivos possivelmente pertencem a um indivíduo formando sua rede pessoal sem fio.

As principais características da tecnologia WPAN são o baixo consumo de energia, operar no espectro não licenciado (902 MHz a 928 MHz, 2.400 MHz a 2.483, 5 MHz e 5.725 MHz a 5.850 MHz), baixo custo e o tamanho relativamente menor dos dispositivos (JÚNIOR, 2012).

O padrão para WPAN definido pelo IEEE é o 802.15, dentro do escopo de WPAN surgiram diversas tecnologias como *Bluetooth (802.15.1), ZigBee (802.15.4), Ultra-wideband (802.15.4) e RFID (802.15.4)*.

- *Bluetooth*

  Bluetooth é o nome dado ao protocolo de rádio baseado em saltos de frequências de curto alcance (10 a 100 metros) que visa complementar ou substituir ás redes convencionais cabeadas, cujo meio físico de transmissão é o cabo de par trançado, cabo coaxial e fibra óptica.

  Este protocolo surgiu em 1994 após a empresa de dispositivos móveis Ericsson, hoje a Sony-Ericsson, identificar a deficiência que os dispositivo tinham em estabelecer uma conexão entre si como, por exemplo: fones de ouvido, aparelhos celulares, impressoras, periféricos e etc.

  O *Bluetooth* opera na faixa de frequências de 2,4 GHz a 2,483 GHz que não precisa de autorização para ser utilizada e adotou o espalhamento espectral por salto de frequên-

cia *(Frequency-Hopping)* de modo a garantir uma comunicação robusta em uma faixa de frequências compartilhada com outras aplicações como o *WI-FI* e ISM (Industrial, Científica e Médica).

Uma piconet é uma rede *Bluetooth* formada por até 8 dispositivos, sendo 1 mestre e os demais escravos. Todos os dispositivos estão sincronizados ao relógio e sequência de salto de frequência *(hopping)* do mestre.

Em uma piconet toda comunicação ocorre entre mestre e escravos. Não existe comunicação direta entre escravos em uma piconet.

Em um determinado local podem existir várias piconets independentes. Cada piconet tem um canal físico diferente, isto é um dispositivo mestre diferente e um relógio e sequência de salto de frequência independentes (TUDE, 2013).

- *ZigBee*

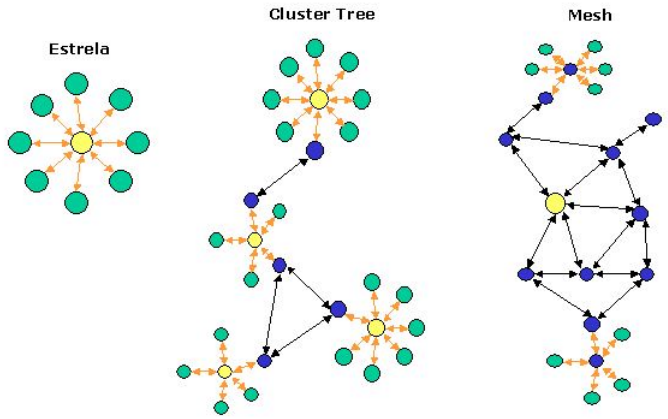
  ZigBee é um padrão que foi definido por uma aliança de empresas de diferentes segmentos do mercado, chamada "*ZigBee Alliance*". Este protocolo foi projetado para permitir comunicação sem fio confiável, com baixo consumo de energia e baixas taxas de transmissão para aplicações de monitoramento e controle. Para implementar as camadas MAC (*Medium Access Control*) e PHY (*Physical Layer*) o *ZigBee* utiliza a definição 802.15.4 do IEEE, que opera em bandas de frequência livres.

  O padrão *ZigBee* pode ser empregado em diversos tipos de aplicações. Algumas destas estão relacionadas abaixo:

  - Automação e Controle Predial (Segurança, Controle de Acesso e Iluminação)
  - Monitoramento ambiental
  - Controle Industrial (gerenciamento de ativos, controle de processos, etc.)
  - Periféricos para PC (Teclado, *mouse e joystick*)
  - Controle remoto de produtos eletrônicos
  - Automação residencial e comercial
  - Saúde Pessoal (Monitoração de pacientes, acompanhamento de Exercício Físico)

A figura 2 abaixo mostra alguns exemplos de topologias utilizadas em redes *ZigBee*.

Figura 2 – Topologias



Fonte:Frias (2004)

Os componentes integrantes da rede são o coordenador, os roteadores e os "*end devices*". O Coordenador inicia a rede definindo o canal de comunicação usado, gerencia os nós da rede e armazena informações sobre eles. Os Roteadores são responsáveis pelo encaminhamento das mensagens entre os nós da rede. Já um "*end devices*" pode ser um dispositivo bem mais simples, só se comunicando com outro nó da rede.

Nas redes *ZigBee* um dispositivo pode permanecer um longo tempo sem ter que se comunicar. Além disso o tempo de acesso a rede é muito pequeno, cerca de 30 mili segundos. Outra característica importante é o tamanho reduzido dos pacotes de dados que trafegam na rede (FRIAS, 2004).

- *Ultra-wideband*

  Segundo Fujimura (2006) a tecnologia *Ultra WideBand*(UWB) oferece uma solução para a otimização do ambiente de comunicação. Diferente da usual tecnologia de transmissão *wireless*, baseada em banda estreita (a largura de banda é menor que 20% da frequência central) e na difusão em frequências separadas, o UWB beneficia-se principalmente pelo fato de propagar o sinal por uma faixa de frequência muito extensa (utilizando espalhamento espectral).

  As tecnologias *wireless* desenvolvidas para a conexão entre dispositivos (tais como o *Wi-Fi* e o *Bluetooth*) não são otimizadas para a utilização de modelos em que múltiplas larguras de banda são utilizadas. Apesar da faixa de transmissão alcançar valores consideráveis para o *Wi-Fi*, por exemplo, a tecnologia tem limitações quanto a consumo de energia elétrica e de largura de banda.

  Entre os benefícios mais importantes do *Ultra Wideband* tem-se:

  - Elevada taxa de dados
  - Custo reduzido dos equipamentos pelo uso dispositivos de baixa potência
  - Imunidade a múltiplos caminhos do sinal entre o emissor e o receptor

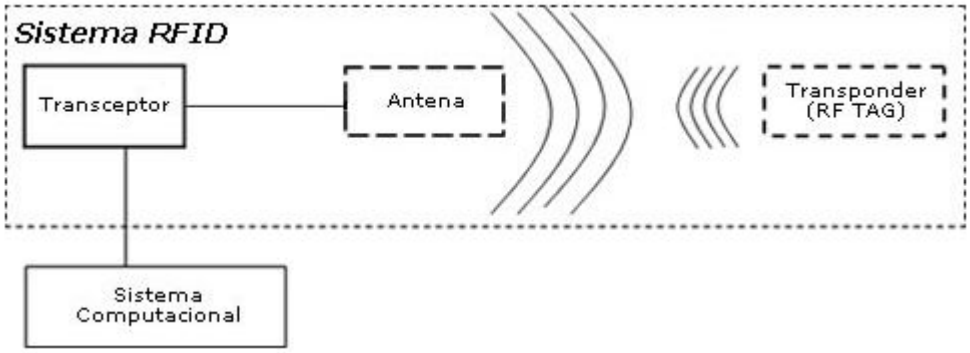
  - Canais codificados para cada comunicação fim-a-fim (*user-code*)
  - Precisão na comunicação (seletividade dos receptores) em comunicação simultânea

- *RFID*

  RFID - *Radio-Frequency IDentification*(Identificação por Radiofrequência), é uma tecnologia sem fio (*wireless*) destinada a coleta de dados. Tal qual o código de barras, o RFID faz parte do grupo de tecnologias de identificação e captura de dados automáticos. Seu surgimento remonta há várias décadas, mas o crescimento massivo de seu uso vem se percebendo nos últimos anos, em especial pela redução do custo de seus componentes.

  O princípio de funcionamento da tecnologia RFID é muito simples, como podemos ver na figura 3 um transceptor/leitor transmite um sinal de radiofrequência através de uma antena para um transponder/etiqueta e essa etiqueta responde com algum tipo de dado e o transceptor é conectado a um sistema operacional que faz uso e trata essas informações (MARTINS, 2017).

Figura 3 – Diagrama geral de um sistema RFID



Fonte: Martins (2017)

2.2 Tecnologia de identificação por radiofrequência

Segundo Martins (2017) está tecnologia teve inicio durante a segunda guerra mundial, sendo utilizado nos sistemas de radares para a identificação de alvos no ar para que pudessem se preparar no caso de ataques detectando-os a uma longa distância, contudo não era possível distinguir se o objeto era aliado ou inimigo devido aos dois emitirem a mesma frequência de sinal.

Os alemães conseguiram contornar este problema presente nos sistemas de radares até então, eles desenvolveram uma técnica que consistia em girar os aviões quando estes estivessem retornando a base e assim modificar o sinal de rádio que seria recebido pelos radares, com isso poderia se averiguar se era aliado ou inimigo, este foi considerado o primeiro sistema de identificação por radiofrequência. Este modelo é um sistema de radio frequência passivo pois somente o radar emitia a radiofrequência sem que seja enviada uma resposta a seguir.

Posteriormente os ingleses vieram a desenvolver um identificador por radiofrequência o IFF - *Identify Friend or Foe*(Identificar amigo ou inimigo), instalavam-se transmissores nos aviões e quando estes passavam por algum radar enviando sinais de radiofrequência começavam a transmitir um sinal de resposta para identifica-los como amigo ou inimigo. Este foi o primeiro sistema ativo de identificação por radiofrequência.

Os modelos modernos de identificação por radiofrequência utilizam esse mesmo principio do IFF, nesta nova arquitetura, um sinal de radiofrequência é enviado por um dispositivo leitor que possui uma antena, a uma etiqueta, o qual é ativada pelo sinal de radiofrequência (sistemas passivos) ou transmitindo seu próprio sinal em resposta (sistemas ativos). Este dispositivo leitor também pode gravar novos dados na etiqueta, no caso de um sistema de leitura/escrita, desde que a etiqueta permita a regravação de dados (MARTINS, 2017).

2.2.1 Sistemas RFID

Segundo Lahiri (2005) a tecnologia de identificação por radiofrequência utiliza ondas de rádio para identificar automaticamente objetos físicos sejam eles seres vivos ou objetos inanimados, assim o conjunto de objetos identificáveis utilizando RFID inclui praticamente tudo que existe neste planeta.

2.2.2 Componentes RFID

A tecnologia RFID e os sistemas que a empregam tem em sua estrutura dois componentes essenciais, a etiqueta e o leitor. Em casos que se utilizam frequência de rádio mais altas como a UHF também tem-se uma antena como parte fundamental da implementação, sendo que esta é a responsável por emitir as ondas de rádio.

2.2.2.1 Etiquetas

Etiqueta é o componente deste sistema que carrega a informação a ser coletada e responde ao leitor quando este emite o sinal. As etiquetas recebem o sinal e usam a energia para refletir o sinal enviando as informações de volta ao leitor. As etiquetas podem ser de diferentes tamanhos ou tipo dependendo da necessidade ou aplicação (GLOVER; BHATT, 2006).

A figura 4 mostra alguns exemplos de etiquetas em seus diferentes formatos e características.

Figura 4 – Exemplos de etiquetas

Fonte: James (2016)

Existem três tipos de etiquetas :

- Etiquetas passivas

  As etiquetas passivas não possuem fonte de alimentação própria e funcionam a partir da energia enviada pelo sinal do leitor. Por isso, são incapazes de iniciar uma comunicação por conta própria. É o tipo mais usado por serem mais simples e baratas, pois não possuem bateria nem transmissor. Pela ausência de bateria, normalmente, possuem uma vida útil maior e, sem o transmissor, são capazes apenas de refletir o sinal vindo do leitor (GLOVER; BHATT, 2006).

- Etiquetas semi-passivas

  As etiquetas semi-passivas que já possuem uma bateria utilizada para alimentação do circuito e de sensores. Contudo, quanto a relação com o leitor, funcionam do mesmo modo que as passivas, ou seja, dependem dele para realizar uma comunicação (GLOVER; BHATT, 2006).

- Etiquetas ativas

  As etiquetas ativas possuem uma fonte de alimentação própria capaz de alimentar o circuito e permitir a emissão de sinais próprios e a comunicação com o leitor. São mais caras, seu tempo de vida é limitado pela duração da bateria e o alcance desse tipo é superior em comparação com as passivas. Além disso, com uma bateria integrada, essas etiquetas permitem um aumento da capacidade computacional e a incorporação de sensores. Por isso, também são maiores e mais complexas (GLOVER; BHATT, 2006).

2.2.2.2 Leitor

Os leitores são utilizados para reconhecer e coletar as informações das etiquetas que estão dentro do alcance do sistema. Este leitor envia uma energia por radiofrequência através de uma ou mais antenas, está energia alimenta uma etiqueta que esteja próxima e assim retorna o sinal com a informação nela contida.

Assim como as etiquetas os leitores também podem ter diversos formados e características conforme a necessidade e aplicação (LAHIRI, 2005).

Na figura 5 são apresentados alguns modelos de leitores.

Figura 5 – Exemplos de leitores

Fonte: James (2016)

2.2.2.3 Antena

Segundo Lahiri (2005) a comunicação entre o leitor e a etiqueta é feita de forma sem fio, para isso se utiliza a antena que é responsável por emitir os sinais de radiofrequência, a antena ativa a etiqueta e também lê o dado contido nela e em certas ocasiões pode escrever na etiqueta também.

Apesar de o termo antena ser utilizado genericamente, seria mais correto utilizar a expressão sistema de propagação, pois os sistemas RFID utilizam dois métodos de acoplamento: proximidade eletromagnética ou indutiva e propagação por ondas eletromagnéticas. A figura 6 mostra uma antena que geralmente é utilizada em aplicações que utilizam a frequência UHF.

Figura 6 – Exemplo de Antena UHF

Fonte:RFID Journal(2011)

2.2.3 Classificação de frequências

Segundo Lahiri (2005) as frequências em RFID são classificadas conforme suas características, a principal diferença diz respeito ao alcance de leitura do sistema. A classificação de frequência é feita desta maneira:

- *Low Frequency - LF*

  Low Frequency(Frequência baixa) é a faixa de frequência que corresponde ao intervalo de 30Khz a 300Khz. Muitas aplicações RFID utilizam esta faixa de frequência, principalmente 125Khz. Normalmente são utilizadas etiquetas passivas nessa faixa de frequência. Tem uma baixa velocidade de transferência, contudo são pouco afetadas por ambientes com interferências de metais, umidade entre outros.

- *High Frequency - HF*

  High Frequency(Frequência alta) é o intervalo de 3Mhz até 30Mhz. Aplicações RFID HF costumam utilizar a frequência de 13,56Mhz em sua operação. Assim como a frequência LF possuem baixa transferência de dados, e também certa tolerância a interferências, mas estas possuem um alcance de coleta maior que a anterior.

- *Ultra High Frequency - UHF*

  Ultra High Frequency - UHF(Frequência ultra alta) Corresponde ao intervalo de 300Mhz a 1Ghz. Possui duas frequências mais utilizadas a 868Mhz e 915Mhz e quando usado etiqueta ativa o mais comum é utilizar 315Mhz e 433Mhz. Possuem alta taxa de transferência de dados, contudo sofrem bastante com interferências, devido a isso seu uso é muito utilizado em cadeias de suprimentos.

- *Microwave Frequency - MF Microwave Frequency*(Frequência de microondas) são as frequências superiores a 1Ghz possuem alta transferência de dados, mas seu desempenho é muito baixo quando se tem interferências limitando assim sua utilização. As frequências mais utilizadas são a de 2,45Ghz e 5,8Ghz.

Essas faixas de frequência são controladas pelo governo afim de não interferir em outras aplicações, e a escolha de determinado tipo dependerá da aplicação e suas necessidades (LAHIRI, 2005).

Abaixo uma tabela que cita algumas regulamentações em alguns países.

Tabela 2 – Classificação de frequências

Pais/Região	LF	HF	UHF	MF
USA	125-134Khz	13,56Mhz	902-928Mhz	2,45 - 8Ghz
Europa	125-134Khz	13,56Mhz	865-868Mhz	2,45Ghz
Japão	125-134Khz	13,56Mhz	Não permitido	2,45Ghz
Cingapura	125-134Khz	13,56Mhz	923-925Mhz	2,45Ghz
China	125-134Khz	13,56Mhz	Não permitido	2,45Ghz

Fonte: Adaptado de Lahiri (2005)

2.2.4 Padrões ISO

A ISO - *International Organization for Standardization* (Organização Internacional de Normalização) é uma entidade com sede em Genebra na Suíça, é um entidade que contribui com comitês e grêmios para o desenvolvimento de padrões em diversas áreas. Assim sendo a tecnologia RFID possui alguns padrões ISO adotados (FINKENZELLER, 2010).

2.2.4.1 Identificação animal

Os padrões ISO 11784, 11785 e 14223 são padrões utilizados em sistemas RFID para a identificação de animais.

- ISO 11784

  Este padrão define a estrutura de código a ser utilizada na identificação de animais, contudo apenas o código é definido, nenhuma característica de transmissão entre uma etiqueta RFID e um leitor é especificada (LAHIRI, 2005).

  O código de identificação para animais tem um total de 64 *bits*, o código nacional é gerenciado por cada pais conforme suas próprias especificações. Os *bits* de 27 a 64 podem ser utilizados para diferenciar diferentes tipos de animais como raças, regiões do país ou criadores (FINKENZELLER, 2010).

Tabela 3 – ISO 11784 - *bits*

Bit	**Informação**	**Descrição**
1	Aplicação Animal (1) / Aplicação não animal (0)	Especifica se o transponder é usado para identificação de animais ou para outros fins.
2 - 15	Reservado	Reservado para futuras aplicações
16	Segue bloco de dados (1)/ Sem bloco de dados(0)	Especifica se os dados adicionais serão transmitidos após o código de identificação
17 - 26	Código de país conforme ISO / IEC 3166	Especifica o país de uso (o código 999 descreve um transponder de teste)
27 - 64	Código de identificação nacional	Número de registro único, específico do país

Fonte: Adaptado de Finkenzeller (2010)

- ISO 11785

  Este padrão define o método utilizado na transmissão para os dados da etiqueta e as especificações do leitor para ativar os dados na etiqueta. Um objetivo central no desenvolvimento desse padrão foi para facilitar a coleta de dados das etiquetas de diversos fabricantes diferentes usando um leitor comum. Um leitor de identificação de animais em conformidade com o padrão reconhece e diferencia entre as etiquetas que utilizam um sistema *full duplex* ou *half-duplex* (modulação de carga) e etiquetas que usam um sistema sequencial (FINKENZELLER, 2010).

- ISO 14223

  Este padrão define a interface de RF e a estrutura de dados das etiquetas ativas. Se baseia nos padrões mais antigos como o 11784 e 11785 e apresenta um desenvolvimento dessas normas.

  Enquanto as etiquetas de acordo com ISO 11785 apenas transmite um código de identificação programado permanentemente, em etiquetas ativas há a possibilidade de gerenciar uma área de memória maior. Como resultado, os dados podem ser lidos, escritos e protegidos contra alterações (FINKENZELLER, 2010).

2.2.4.2 Cartões inteligentes sem contato

De acordo com Finkenzeller (2010) e Lahiri (2005) existem três padrões distintos para esta categoria são eles as ISO 10536, ISO 14443 e ISO 15693.

- ISO 10536

  O padrão ISO 10536 também chamado de "Cartões de identificação - cartões de circuitos integrados sem contato" descreve a estrutura e os parâmetros operacionais dos cartões inteligentes sem contato. Ele consiste de 4 seções, características físicas, dimensões e locais das áreas de acoplamento, sinais eletrônicos e procedimentos de resgate e resposta aos protocolos de reinicialização e transmissão.

- ISO 14443

  O padrão ISO 14443 chamada de "Cartões de identificação - Cartão de circuitos integrados de proximidade", este protocolo aborda cartões de proximidade que possibilita a leitura a uma faixa de distância de 7-15cm e descreve o método operacional e seus parâmetros de operação. O padrão compreende as 4 partes, características físicas, interferência por radiofrequência, inicialização e anticolisão e protocolos de transmissão .

- ISO 15693

  O padrão ISO 15693 também chamado de "Cartões de identificação - Circuito de cartões integrados sem contato. Os cartões descritos neste padrão possui uma distancia de leitura de até 1m. Este padrão tem estas 3 seguintes partes, características físicas, interface aérea e inicialização e protocolo anti-colisão e transmissão (FINKENZELLER, 2010).

2.2.4.3 Outros padrões ISO

Conforme Finkenzeller (2010) existem diversos padrões ISO para esta tecnologia, além dos já citados estes outros tem importância dentro do cenário.

- ISO 69873

  Denominado como portadores de dados para ferramentas e dispositivos de aperto é um padrão que especifica a dimensão e o espaço para montagem em ferramentas.

- ISO 10374

  A ISO 10374 foi designado para a identificação de contêiner. Este padrão descreve um sistema de identificação automática para recipientes com base em etiquetas microondas.

- ISO 18000 *series*

  Existe uma grande quantidade de padrões quando se trata de gerenciamento de itens, abaixo alguns dos principais e relevantes para a tecnologia RFID.

  - ISO 15961: RFID para gerenciamento de itens - Interrogatório, comandos funcionais de etiqueta e outras características de sintaxe.
  - ISO 15962: RFID para gerenciamento de itens: sintaxe de dados.
  - ISO 15963: Identificação única da etiqueta de RF e autoridade de registro para gerenciar a singularidade.
  - ISO 18000: RFID para gerenciamento de itens: interface de ar.
    Este padrão contém as seguintes partes :
    Parte 1:Parâmetro genérico para comunicação de interface de ar para frequências aceitas globalmente
    Parte 2: Parâmetros para comunicação de interface de ar abaixo de 135 kHz
    Parte 3: Parâmetros para Comunicação de Interface Aérea a 13. 56MHz
    Parte 4: Parâmetros para comunicação de interface de ar a 2, 45 GHz
    Parte 5: Parâmetros para comunicação de interface de ar a 5, 8 GHz
    Parte 6: Parâmetros para comunicação de interface de ar - Faixa de frequência UHF
    Parte 7: Parâmetros para comunicação de interface de ar a 433MHz
  - ISO 18001: Tecnologia da informação - RFID para gerenciamento de itens, Requisitos de aplicativos Perfis

2.2.5 EPCglobal

A *EPCglobal, Inc*, é uma instituição sem fins lucrativos, esta organização propõe-se a estabelecer padrões mundiais para projetos desenvolvidos e implementações que utilizam o código EPC e o sistema *EPCglobal Network*.

Segundo Glover e Bhatt (2006) este sistema é um agregado de tecnologias de fornecimento e compartilhamento de informações sobre produtos dentro e fora de uma empresa. Neste padrão constitui-se cinco partes principais:

- EPC: Definição do padrão de código EPC.
- *ID System*: Definição de compatibilidade entre tags e leitores baseados no código EPC.
- *Middleware*: EPCglobal *middleware*.
- *Discovery Services*: Bancos de dados e servidores.
- *EPCIS*: Interface de padronização do fluxo de informações.

2.2.5.1 *EPC - Eletronic Product Code*

De acordo com Finkenzeller (2010) o EPC é um código gravado em uma etiqueta que permite de forma clara e única a identificação de um objeto ou item e também pode ter um número consecutivo que permita identificar cada parte individual do item. Logo abaixo a figura 7 apresenta um exemplo de código EPC com tamanho de 96 *bits*.

Segundo Lahiri (2005) é um método simples e compacto que pode gerar quantidades extremamente grandes de identificadores. Ao mesmo tempo permite que estes códigos sejam agrupados em alguns grupos.

- GTIN - *Global Trade Identity Number* (Número de identidade de comércio global)

  Código global para identificação de produtos e serviços.

- GRAI - *Global Returnable Asset Identifier* (Identificador de ativos retornáveis globais)

  É usado para numeração de ativos retornáveis, como tambores, cilindros de gás, e assim adiante.

- UID - *Unique Identification* (Identificação única).

  Usado para rastreamento de ativos.

- GLN - *Global Location Number*(Número de localização global)

  É usado para representar localização, parceiros comerciais e entidades jurídicas.

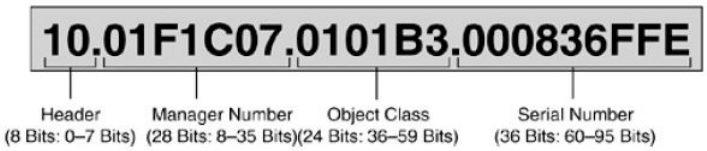
- GIAI - *Global Individual Asset Identifier* (Identificador de ativos individuais globais).

  Usado para identificar ativos individuais, como um estoque em uma empresa.

- SSCC - *Serial Shipping Container Code* (Código de recipiente de transporte em série).

  Usado para identificar unidades de transporte, como uma palete, caixa, papelão.

Figura 7 – Código EPC 96 *bits*



Fonte:Lahiri (2005)

2.2.5.2 Classes de etiquetas EPC

De acordo com Lahiri (2005) a *EPCglobal* definiu algumas classes para as etiquetas RFID, cada classe com capacidades diferentes e para atender as necessidades de cada aplicação.

- Classe 0 / Classe 1

  Tanto as classes 0 e 1 são para etiquetas passivas, estas etiquetas podem ser de 64 ou 96 *bits*. As etiquetas da classe 0 já vem com um código definido de fabrica sem a possibilidade que o cliente possa altera-lo, enquanto que a etiqueta de classe 1 permite que o cliente grave um código EPC conforme desejar.

  As frequências utilizas para a classe 0 é a UHF (900MHz) e a classe 1 abrange as frequências UHF (860 a 930 MHz) e HF (13,86MHz). Todos esses tipos de etiquetas usam a tecnologia de retrodifusão para realizar a comunicação com o leitor.

- Classe 2

  Esta é uma etiqueta passiva regravável que pode armazenar um EPC em conjunto com os dados do usuário. A capacidade mínima de dados do usuário dessa etiqueta é de 224 *bits*. Esta etiqueta usa tecnologia de retrodispersão para comunicação com o leitor.

- Classe 3

  Esta é uma etiqueta ativa regravável que possui uma memória interna para que possam ser gravados dados além do código. Uma etiqueta EPC classe 3 suporta processamento a bordo e capacidade de entrada/saída. Esta etiqueta usa tecnologia de retrodispersão para se comunicar com o leitor.

- Classe 4

  Leitura e escrita com transmissores integrados. Acabam funcionando como mini rádios, podendo se comunicar não apenas com os leitores, mas também com outras etiquetas. Formam redes inteligentes de logística. Cada uma das faixas de frequência tem vantagens e desvantagens para esse tipo de operação.

- Classe 5

  Leitura e escrita com transmissores integrados, todas as funcionalidades da classe 4 somada à capacidade de se comunicar com etiquetas passivas.

2.3 Controle de acesso físico

Segundo Ferreira e Araújo (2008) o controle de acesso físico é toda e qualquer aplicação de procedimento ou uso de equipamentos com o objetivo de proteger ambientes, equipamentos ou informações cujo o acesso deve ter restrição quanto ao seu conteúdo ou acesso. Esse tipo de controle envolve o uso de chaves, trancas, guardas, crachás, biometria e etc., além da aplicação de precedimentos e normas especificados e utilizados por cada organização para esse fim conforme sua necessidade. A política e o investimento, no controle de

acesso físico adotado pela organização, estarão diretamente ligados à importância de seus ativos, observando a relação custo/beneficio. Uma política de controle de acesso físico eficaz depende mais da gestão dos modelos de segurança definidos do que apenas do uso de tecnologia.

2.3.1 Controle de acesso veicular

Segundo Rocha (2018) existe uma grande preocupação a respeito do controle de acesso veicular, restringir o acesso, realizar controle do fluxo e proteção contra pessoas mal intencionadas são só algumas das preocupações que levam a se realizar essa prática. Atualmente algumas tecnologias são implementadas para se realizar esse controle.

- Controle de acesso veicular por biometria

  O controle de acesso por biometria é um dos mais procurados, uma das principais vantagens no uso de controle de acesso por biometria é poder limitar o tempo de permanência de visitantes ou prestadores de serviço dentro da organização, dependendo do que o prestador de serviço ou visitante for fazer, já pode ser estipulado o tempo em que vai permanecer e que áreas vai ocupar. O controle de acesso biométrico também pode ser utilizado com cartão codificado de proximidade e digitação de senha. O sistema de biometria permite o cadastro de todos os dedos das pessoas que vão utiliza-lo e é uma das formas de controle mais eficazes, pois garante a segurança e facilita o controle de fluxo de pessoas que não fazem parte do ambiente.

- Controle de acesso veicular por RFID

  Nesse tipo de controle de acesso veicular, a leitura é feita por rádio frequência. Assim, todas as vezes que o veículo se aproxima por cerca de oito metros de onde se encontra a antena RFID, a leitura de seus dados é realizada. O portão ou cancela somente são abertos após a confirmação do cadastro, ou seja, se as informações contidas no cadastro do veículo forem as mesmas. A tecnologia RFID também pode ser utilizada por meio de chaveiro para entrada e saída por portões de pedestres. Ao aproximar o chaveiro no leitor instalado no portão, os dados do usuário são decodificados e a entrada é permitida.

- Controle de acesso veicular por LPR (*License Plate Recognition*)

  A tecnologia LPR (License Plate Recognition ou Reconhecimento Automático de Placas de Automóveis) é mais um sistema de controle de acesso para organizações. Esse sistema utiliza um módulo eletrônico que reconhece caracteres automaticamente por meio de sensores ópticos para as placas dos veículos. O LPR, na verdade, faz uma checagem dupla, pois autentica antes a placa do veículo e, depois, fica apto para receber os comandos dos controles remotos. Assim, se a placa do veículo não estiver cadastrada no sistema, mesmo que o condutor esteja com o controle remoto não conseguirá abrir o portão.

3 Trabalhos relacionados

Esta seção trás alguns trabalhos realizados utilizando a tecnologia de identificação por radiofrequência para a solução de problemas encontrados.

Segundo Sundar, Hebbar e Golla (2015) as tecnologias existentes são insuficientes para lidar com os problemas do trânsito como controle de congestionamento, veículos de emergência e detecção de veículos roubados. A proposta do trabalho dos autores é criar um sistema de controle de tráfego inteligente baseado em RFID.

O sistema envolve três partes, abordando a primeira parte, cada veículo é equipado com uma etiqueta e quanto estes passam por um leitor é registrado a quantidade de veículos em um determinado tempo estimando assim o congestionamento, assim ele poderá definir quanto tempo a luz verde do semáforo deverá permanecer acesa para agilizar o transito e aliviar o fluxo de veículos.

A segunda parte diz respeito aos veículos de emergência, cada veículo possui um módulo transmissor *ZigBee* e o módulo receptor *ZigBee* será colocado no semáforo quando o veículo acionar as luzes de emergência será enviado um sinal para o semáforo e a luz verde será acesa afim de desobstruir a via.

A terceira parte é responsável pela detecção de veículos roubados, quando algum leitor recebe o sinal de alguma etiqueta dada como sendo de um veículo roubado este envia um SMS para a policia e aciona a luz vermelha do semáforo, então a policia tomará as medidas adequadas.

De acordo com Pereira, Júnior e Almeida (2016) que abordaram um problema presente na sociedade brasileira, as pessoas idosas e/ou deficientes físicos tem dificuldade em encontrar as poucas vagas que lhe se são garantidas por lei, entretanto o principal problema é que essas vagas na maior parte dos casos são ocupadas por pessoas que não possuem nenhuma deficiência física e também não são idosas, apenas são pessoas que se aproveitam da disponibilidade da vaga preferencial sem ter esse direito.

O sistema consiste em instalar em cada vaga preferencial um leitor, uma câmera e um alarme sonoro. Cada cliente com direito teria adquirido previamente uma etiqueta com seus dados pessoais gravados, quando chegasse a uma vaga o leitor realiza a verificação e registra o evento. Caso uma pessoa sem a etiqueta utilizasse a vaga é acionado o alarme sonoro para alerta-lo, após um tempo caso continue indevidamente na vaga a câmera registraria a placa do carro e enviaria para órgãos competentes.

Meireles, Moreira e Silva (2017) implementaram um sistema supervisório para o controle de acesso veicular em um condomínio onde se realizava um controle manual e desejava-se automatizar o processo tendo um ganho de tempo, com a tecnologia RFID implementar um sistema, onde é possível aperfeiçoar o monitoramento dos veículos através de um software, possibilitando o controle do fluxo de veículos e emissão de relatórios diários, semanal, mensal

e anual em tempo real.

O sistema compreende um leitor colocado na portaria de acesso afim de identificar quando um veiculo se aproxima, o *software* recebe os dados e os mostra no monitor presente na portaria caso este veículo tem acesso a cancela é liberada, assim o porteiro só interfere caso o veículo não esteja cadastrado no sistema. Foi apresenta um ganho de tempo considerável, com o controle manual levava-se em torno de 30 segundos desde a aproximação até a abertura da cancela, com a automatização este tempo passou para 2,5 segundos.

Farooq *et al.* (2014) observaram a necessidade de um sistema de controle de acesso se faz necessário em organizações, considerando esta necessidade os autores desenvolveram um sistema de controle de acesso baseado em RFID para ser implementado nos albergues dentro da universidade de Punjab na Índia, este sistema combina identificação por radiofrequência e reconhecimento de imagens por redes neurais.

O sistema de funciona de duas formas, uma fase de registro onde dez imagens do usuário do albergue são capturadas ao emitir uma etiqueta RFID e a fase de reconhecimento onde após a leitura da etiqueta a imagem do usuário é analisada por uma rede neural e em caso positivo o acesso é liberado. Caso os passos anteriores não resultem em uma permissão de acesso, o sistema aciona o alarme e faz uma ligação utilizando um modem GSM para a segurança do local.

4 Materiais e Métodos

Para o desenvolvimento do modelo prático proposto para realizar a análise foram usados os seguintes recursos:

- *Notebook* com as seguintes especificações:
  - Processador: Intel® Core™ i5-4200U CPU de 2.5GHz;
  - Memória RAM: 8GB;
  - Disco Rígido: 1TB, SATA (5400 RPM);
  - Sistema Operacional: *Windows 10 Pro* (Sistema Operacional de 64 bits);
- Plataforma utilizada: *Visual Studio Community* 2017;
- Linguagem de programação: C#;
- *SQL Server 2017 Express*;
- *SQL Server Management Studio*, Versão:17.6;
- Leitor RFID USB 125Khz;
- Etiquetas passivas RFID LF(125Khz);

Para o desenvolvimento do trabalho foram realizadas as seguintes atividades.

1. Analisar como é realizado o controle de acesso veicular atual, os dados contidos nesse controle e como são registradas, armazenadas. Averiguar se é feito algum uso dessas informações como relatórios periódicos.
2. Criar um banco de dados *SQL Server* que contenha as tabelas estruturadas para a implementação e coleta das informações.
3. Desenvolver um sistema na linguagem C# que faça a integração com o banco de dados SQL e os componentes RFID.
4. Instalar os equipamentos RFID, neste caso devido a falta de componentes específicos como a antena e o leitor RFID UHF, será utilizado um leitor com interface USB *plug and play* utilizando a frequência LF ao invés da UHF proposta inicialmente, assim não mais será utilizado etiquetas UHF passando a se utilizar etiquetas LF com uma redução considerável na distância de leitura.
5. Cadastrar as etiquetas no banco de dados designando a um usuário especifico.
6. Cadastrar o restante das informações de cada usuário.

7. Coletar os dados para teste e verificação do desempenho da ferramenta.
8. Comparar o sistema antigo realizado de forma manual com o sistema automatizado e verificar o desempenho de ambos.
9. Ponderar o custo da implementação de um sistema automatizado em relação a produtividade e custo beneficio.

5 Desenvolvimento

Neste capitulo serão apresentados os procedimentos para o desenvolvimento do trabalho.

5.1 Equipamentos RFID

O intuito deste trabalho é apresentar um controle de acesso veicular utilizando identificação por radio frequência tendo como faixa de frequência a UHF.

Nesta faixa de frequência se torna necessária a utilização de uma antena juntamente do leitor para a leitura das etiquetas, muitos dos leitores presentes no mercado já estão sendo fabricados com a antena integrada, permitindo uma variação de acordo com a aplicação. A figura 8 mostra um leitor com antena integrada utilizado em aplicações com frequências UHF.

Figura 8 – Leitor RFID

Fonte: Atlas(2018)

Algumas características:

- Alcance de leitura em torno de 9 metros
- Protocolo *EPCglobal UHF Class 1 Gen 2*
- Frequência: 865-928 MHz
- Interface de comunicação: *Serial e Ethernet*
- Preço médio: $1095,00

Existe também a possibilidade de se trabalhar com dois equipamentos separados, neste caso se utiliza um módulo leitor que pode possuir uma ou múltiplas entradas para se conectar antenas e geralmente a conexão do leitor com a antena se dá por um cabo coaxial. A figura 9 mostra um módulo leitor a esquerda e a direita um antena que emite frequências UHF.

Figura 9 – Leitor e antena

Fonte: (ATLAS, 2018)

Algumas características:

- Alcance de leitura em torno de 9 metros
- Protocolo *EPCglobal UHF Class 1 Gen 2*
- Frequência: 902.75-927.25 MHz
- Interface de comunicação: *Serial e Ethernet*
- 4 entradas para conexão de antenas.
- Preço médio do leitor: $999,00
- Preço médio da antena: $125,00

5.2 Simulação

A proposta do trabalho é apresentar uma solução RFID UHF para o controle, porém conforme mostrado na seção 5.1 os equipamentos possuem um custo elevado o que tornou a sua aquisição inviável. Contudo se viu a possibilidade de simular esta leitura utilizando equipamentos com um valor acessível.

O sistema funciona da mesma forma, mudando exclusivamente os equipamentos RFID, ao invés de um leitor com antena integrada e etiquetas para a frequência UHF é utilizado um leitor com frequência LF mostrado na figura 10 e também etiquetas da mesma faixa de frequência.

Figura 10 – Leitor RFID LF

Fonte: (MSS, 2018)

Enquanto a interface do leitor UHF é ethernet ou serial, o leitor RFID LF possui uma interface USB. Contudo a única alteração necessária no sistema foi a forma com que ele recebe os dados. Apesar da simulação a proposta do trabalho não sofreu limitações e continua realizando tudo que se propôs no objetivo.

5.3 Levantamento do modelo atual

O modelo presente na instituição realiza o controle de maneira manual pelo vigilante, por meio de uma planilha como a que é demonstrada na figura 11 com os servidores, professores e técnicos administrativos do CEFET-MG onde ele registra a data e se o usuário entrou ou saiu da instituição.

Esse modelo além de não permitir um controle adequado está sujeito a falhas humanas, como já constatado. Houve casos de não se registrar o acesso a parte interna ou que tal professor deu entrada mas não saiu da instituição sendo que este, de fato, já não estava mais presente. Poderia ocorrer situações em que o vigilante teria que atender a imprevistos ou urgências e se ausentaria momentaneamente da portaria causando uma defasagem nas informações coletadas.

Figura 11 – Planilha do controle manual

Planilha1

	Servidores	Data:	Data:	Data:	Data:	Data:
1	Adalberto Texeira de Andrade Rocha					
2	Adilson Mendes Ribeiro					
3	Adriana Sales Zardini					
4	Aléssio Miranda Júnior					
5	Alexandre Augusto Gamberini					
6	Alexandre Pereira da Silva					
7	Alisson Brizon D'Angelo Chaib					
8	Alisson Pinto Chaves					
9	Almir Silva Neto					
10	Ana Cristina de Oliveira Santos					
12	André Rodrigues da Cruz					
13	Armim Fraz Isenmann					
14	Aurélio Takão Vieira Kubo					
15	Bianca (Estagiaria)					
17	Bruno Rodruigues Silva					
18	Carla Pricila de Morais Mendes					
19	Carlos Augusto Magalhaes Júnior					
20	Carlos Eduardo Oliveira Andrade					
21	Carlos Frederico Campos Assis					
22	Carolini Tavares Frinhani					
23	Cassio Lourenço Guimares Spinola					
24	Cláudia Mara de Souza					
25	Cristina da Rocha Alves					
26	Cyntia (Estagiaria)					
28	Danilo França do Nascimento					
29	Débora Pereira Coura					
30	Deiymar Pereira Coura					
31	Denis					
32	Douglas Nunes de Oliveira					
33	Elder de Oliveira Rodrigues					
34	Elizabeth de Araujo					
35	Erica Drumond Fontes Silva					
36	Erick Brizon D'Angelo Chaib					
37	Erriston Campos Amaral					
38	Evaldo Sérgio de Souza					
39	Evandro Tolentino					
40	Fabiana da Silva Pereira					
41	Fábio Luiz Rodrigues					
42	Fabrício Almeida de Castro					
43	Felipe Almeida Vieira					
44	Fernanda Vasconcelos Fonseca Tavares					
45	Fernando Castro de Oliveira					
46	Gabriella Caroline Rodrigues					
47	Giselle					
48	Gustavo Henrique dos Santos Ribeiro					
49	Jennifer Catarina de Souza Paula					
50	Jeysa Vanessa Rocha Magalhães Reis					
51	João Henrique					
52	João Batista Queiroz Zuliani					
53	João Paulo de Castro Costa					

Página 1

Planilha1

55	José Agostinho Pimental					
56	José Henrique Gonçalvez					
57	Josyele Ribeiro Caldeira					
58	Júlio César de Jesus Onofre					
59	Leandro Braga de Andrade					
60	Leandro Martins Fernandes					
61	Leonardo Larceda Alves					
62	Liliane Andrade de Souza					
63	Lourenço Godoi Linhares Pires					
64	Luana Dias Lacerda Guerra					
66	Lucas Pantuza Amorim					
67	Luciano Nascimento Moreira					
68	Luiz Antônio Ribeiro					
69	Luiz Carlos Pires Lage					
70	Marcelo de Souza Balbino					
71	Márcia Valéria Rodrigues Ferreira					
72	Márcio José de Castro Justino					
73	Marlene Schettino					
74	Maurílio Alves Martins da costa					
75	Mirela de Castro Santos					
76	Monalisa Mendonça Morais Silva					
78	Nayara Marielle Martins da Costa					
79	Odilon Correa da Silva					
81	Raquel Perreira Soares					
82	Rayane Ferreira da Silva					
83	Rodrigo Gaiba de Oliveira					
84	Romerito Valeriano da Silva					
85	Roney Anderson Nascimento Aquino					
86	Rosana Aparecida Ferreira Nunes					
87	Rutyele Ribeiro Caldeira					
88	Samara Silva Santos					
89	Silvânia Aparecida de Freitas Souza					
90	Solange Carvalho Moreira Rodrigues					
91	Talles Quintão Pessoa					
92	Tatiana Kelly Nunes Bastos					
93	Valmir Dias Luiz					
94	Vania Bevenuti Barbosa					
95	Viviane Cota Silva					
96	Wander Dias de Almeida					
97	Weber Hanry Morais e Feus					
98	Wilian Gomes Dormelas dos Reis					
99	Willy Marlon Dutra Campos					
100	Flavio					
101	Eduardo					
102	Larissa (Estagiaria)					
103	Carolina(Estagiaria)					

Fonte: Autor

As informações coletadas são mais para um controle dos vigilantes do que de uso interno da instituição, contudo seria interessante coletar essas informações e as utilizar para saber se o usuário cadastrado para uso de algum veículo esta presente ou ausente da instituição entre outras situações e tornar essas informações disponíveis para consultas.

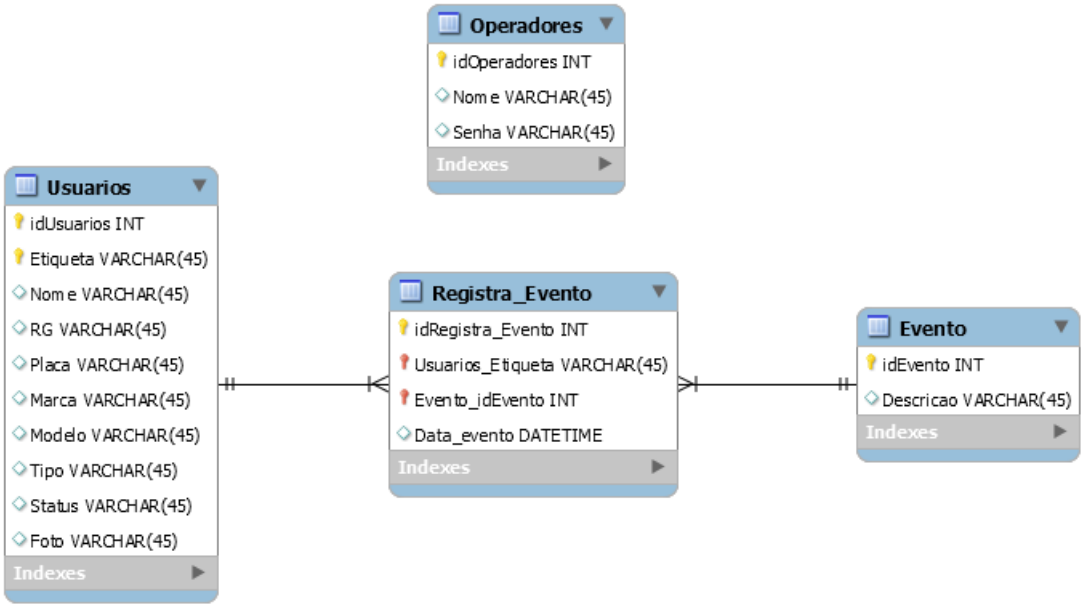
Antes também existia um controle de alunos que com o tempo deixou de existir e seria interessante também realizar essa verificação já que os mesmos fazem uso frequente do recurso. Também não há um histórico adequado destas informações, o que com a automatização seria sanado já que as informações coletadas seriam digitalizadas, tornando fácil o armazenamento por um período satisfatório de tempo. Para escopo deste trabalho não será considerado o acesso de pedestres, tendo como foco somente o controle de acesso veicular.

5.4 Modelagem do banco de dados

Com base nas informações levantadas na etapa anterior e também adaptando a nova proposta foi possível realizar uma modelagem das informações para a criação de um banco

de dados. A figura 12 apresenta o modelo entidade-relacionamento estruturado do banco de dados utilizado na proposta do trabalho.

Figura 12 – Modelo entidade-relacionamento



Fonte: Autor

Descrição das tabelas e campos:

- Usuários
  - idUsuarios: Chave primária e auto incrementada para cada usuário.
  - Etiqueta: Etiqueta RFID contendo um código para cada usuário.
  - Nome: Nome completo do usuário.
  - RG: Documento de identidade.
  - Placa: Placa do veículo cadastrado no sistema.
  - Marca: Marca do veículo.
  - Modelo: Modelo do veículo.
  - Tipo: Tipo do usuário podendo ele ser professor, aluno ou servidor.
  - Status: Contem o valor permitido ou negado, assim verificando se o usuário esta apto a ter o acesso.
- Operadores
  - idOperadores: Chave primária e auto incrementada para cada operador.
  - Nome: Nome de usuário do sistema para cada operador.
  - Senha: Código de acesso ao sistema.

- Evento
  - idEvento : Chave primária e auto incrementada para cada evento.
  - Descrição: Descrição do evento podendo ele ser entrada ou saída.
- Registra_Evento
  - idRegistra_Evento: Chave primária e auto incrementada para cada evento ocorrido.
  - Usuários_Etiqueta: Chave estrangeira da tabela usuários contendo a etiqueta.
  - Evento_idEvento: Chave estrangeira da tabela evento contendo o id evento.
  - Data_evento: Data do acontecimento do evento contendo a data e hora.

Este banco de dados foi implementado utilizando as ferramentas *SQL Server 2017 Express e SQL Server Management Studio na versão 17.6*.

Implementando esse modelo de banco de dados estruturado de acordo com os dados trafegados durante o processo, pode-se fazer um uso adequado das informações, assim existe a opção de gerar diversos relatórios de acordo com a necessidade no momento e também ter um controle melhor sobre os dados registrados ou gerados pelo sistema.

5.5 Desenvolvimento do sistema

O sistema foi desenvolvido na *IDE Visual Studio Community* 2017 que é uma versão para estudantes, produção de software livres e desenvolvimento individual. O desenvolvimento foi realizado utilizando a linguagem C# juntamente com o *Entity Framework* que é uma das principais ferramentas de persistência de dados presentes na plataforma .NET e permite aos desenvolvedores trabalhar com dados na forma de propriedades e objetos específicos do domínio como clientes e produtos, etc, sem ter que relacioná-los com as tabelas do banco de dados e as colunas onde os dados estão armazenados.

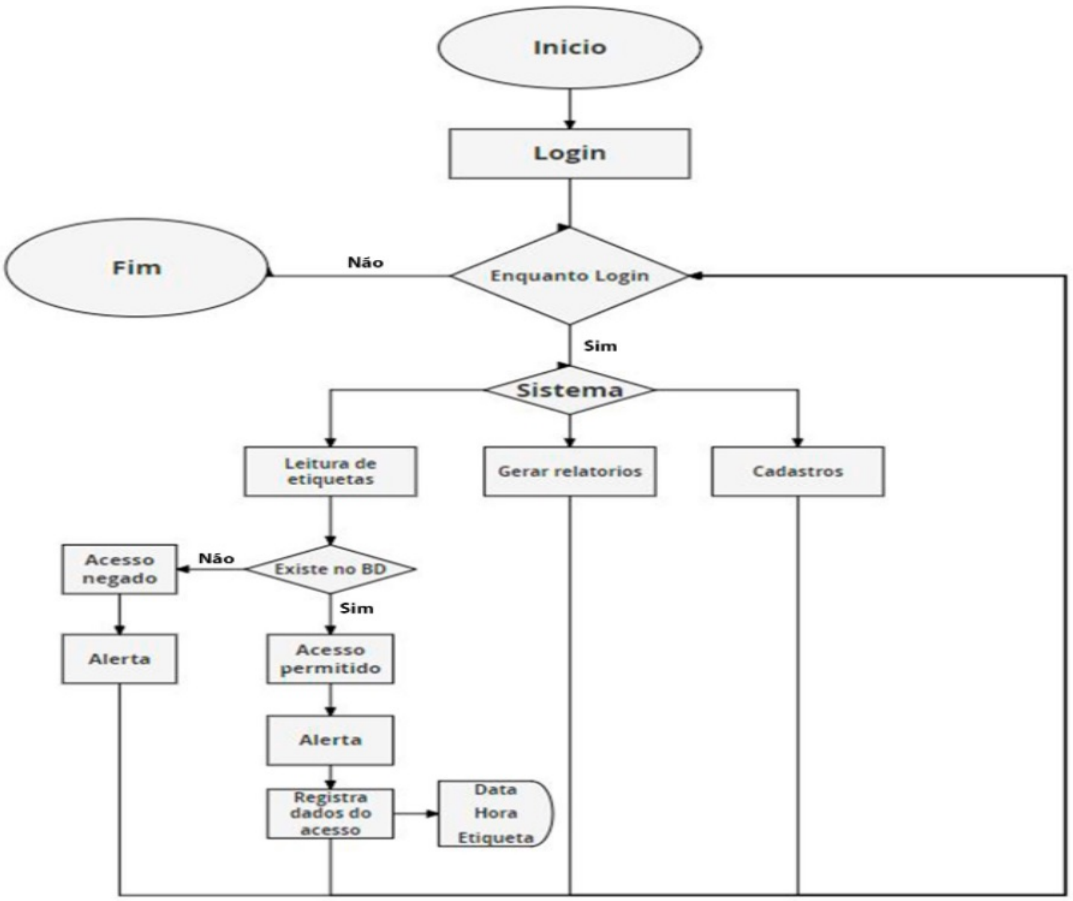
5.5.1 Ambiente do sistema

O sistema pode ser implementado tanto em uma máquina local ou cliente-servidor. O cliente-servidor trás outros benefícios como realizar consultas a fim de saber os alunos dentro do campus, professores e servidores, como também verificar a ausência desse usuário tudo isso sem a necessidade de ligar ou ir até a portaria para que a vigilante faça a conferência.

Durante os testes o sistema foi desenvolvido na máquina física juntamente com o servidor local, no entanto durante o decorrer do trabalho viu-se a oportunidade de trazer outra praticidade em relação a disponibilidade das informações, foi implementado o mesmo banco de dados com as mesma configurações em uma maquina virtual executando o mesmo sistema operacional transformando a aplicação em cliente/servidor.

A figura 13 expõe o fluxograma de como o sistema se porta desde a autenticação do operador até as funcionalidades oferecidas.

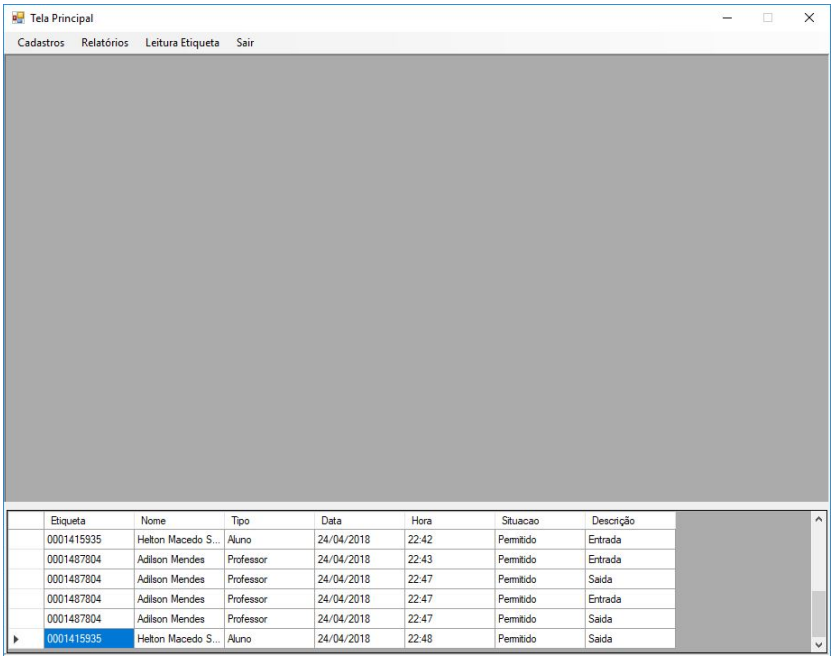
Figura 13 – Fluxograma do sistema



Fonte: Autor

A tela do sistema como mostrado na figura 14 é dividida em duas, a parte superior separada para fazer se realizar as funcionalidades, enquanto que na parte inferior uma *thread* fica executando em *background* atualizando o *grid* com os eventos registrados.

Figura 14 – Tela principal



Fonte: Autor

Operando o sistema é possível realizar os seguintes cadastros:

- Operadores

  Caso exista a necessidade de se cadastrar novos ou excluir/alterar os já existentes no banco.

- Usuários

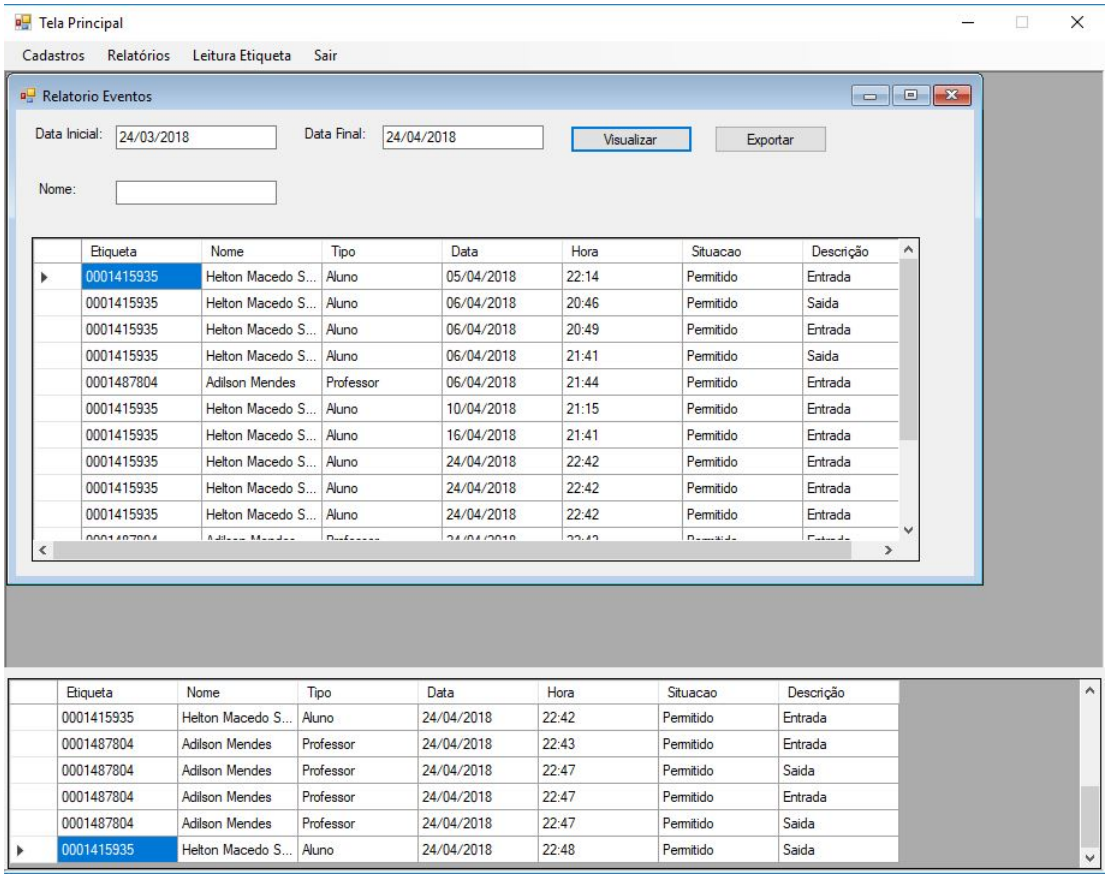
  Cadastrar novos usuários no sistema conforme o surgimentos de novas solicitações, assim como alterar ou excluir os existentes.

O sistema permite a geração dos seguintes relatórios:

- Relatório de usuários cadastrados
- Relatório de veículos cadastrados
- Relatório de Eventos ocorridos

Na figura 15 é apresentado como exemplo o relatório de eventos ocorridos, podendo ser filtrado por data e nome do usuário.

Figura 15 – Relatório de Eventos

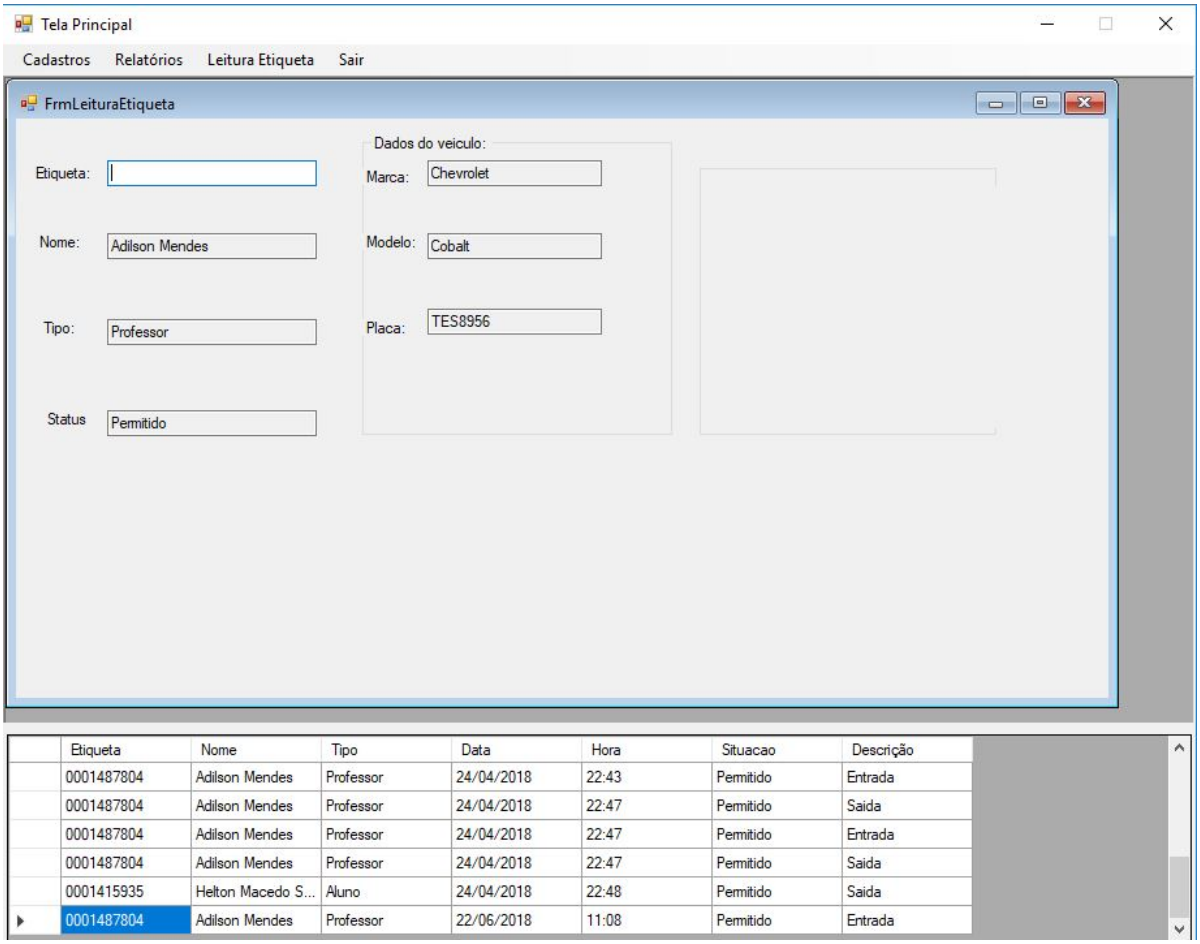


Fonte: Autor

Afim de filtrar as informações e tornar mais prático sua verificação este relatórios possui filtros por data ou nome do usuário. Assim pode-se verificar se este se encontra na instituição ou se está ausente, é possível também exportar o *grid* com as informações em uma planilha.

A leitura da etiqueta demonstrada na figura 16 é utilizada para a identificação e verificação quanto a permissão de acesso ou não é feita ao usuário aproximar a etiqueta do leitor. O sistema captura o código e verifica no banco de dados a situação desta etiqueta, caso não exista este usuário é emitida um alerta na tela e caso contenha tal etiqueta no banco de dados é feita uma análise da situação e emitido na tela os dados do usuário e se o acesso é permitido ou negado.

Figura 16 – Leitura das etiquetas



Fonte: Autor

6 Resultados

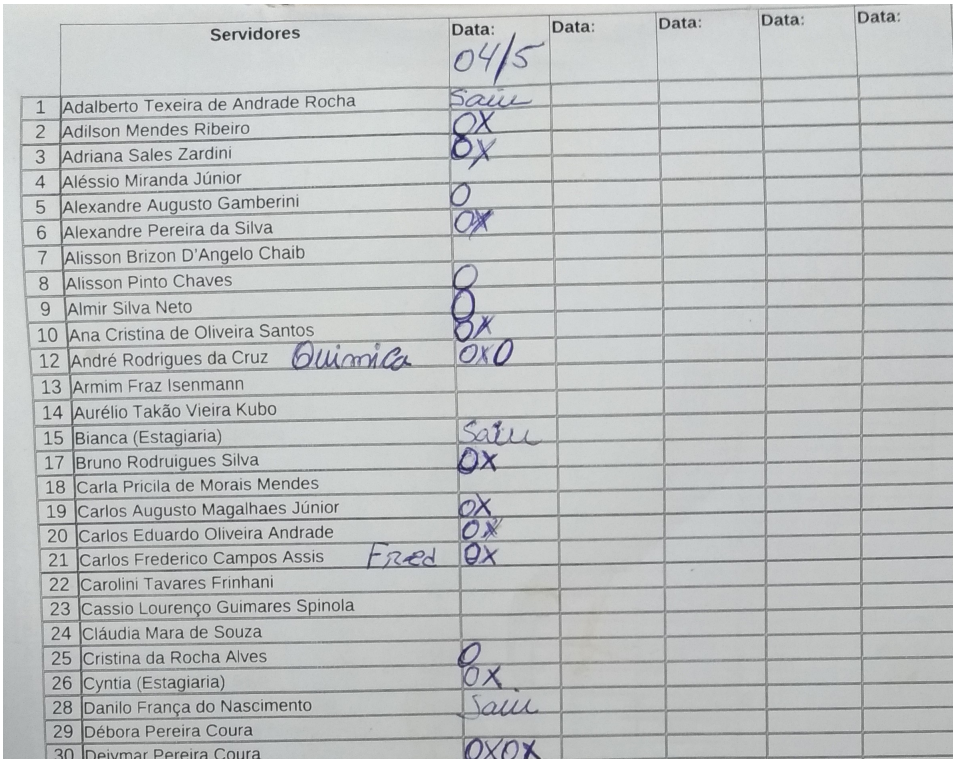
6.1 Integridade da informação

A integridade é um dos três pilares da segurança da informação e corresponde a uma informação precisa, consistente e confiável durante todo o processo. É importante que os dados circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los, comprometê-los ou danificá-los. É importante manter a integridade das informações para que o processo opere corretamente com as informações reais (SÊMOLA, 2014).

Além disso, instruções, orientações e mensagens trocadas entre departamentos e profissionais precisam chegar aos destinatários da mesma forma que foram enviados para não comprometer a comunicação interna e externa. O controle manual pode estar suscetível a falhas humanas, portanto um dos objetivo do trabalho é realizar esse controle garantindo a integridade das informações.

A figura 17 mostra como o controle é realizado pelo vigilante, ele informa manualmente a entrada/saída do usuário, assim como também pode informar uma ausência em caso de licença. Contudo ele informa na data específica e essa verificação não contém o número de vezes do evento ou a hora em que ele ocorreu.

Figura 17 – Controle vigilante

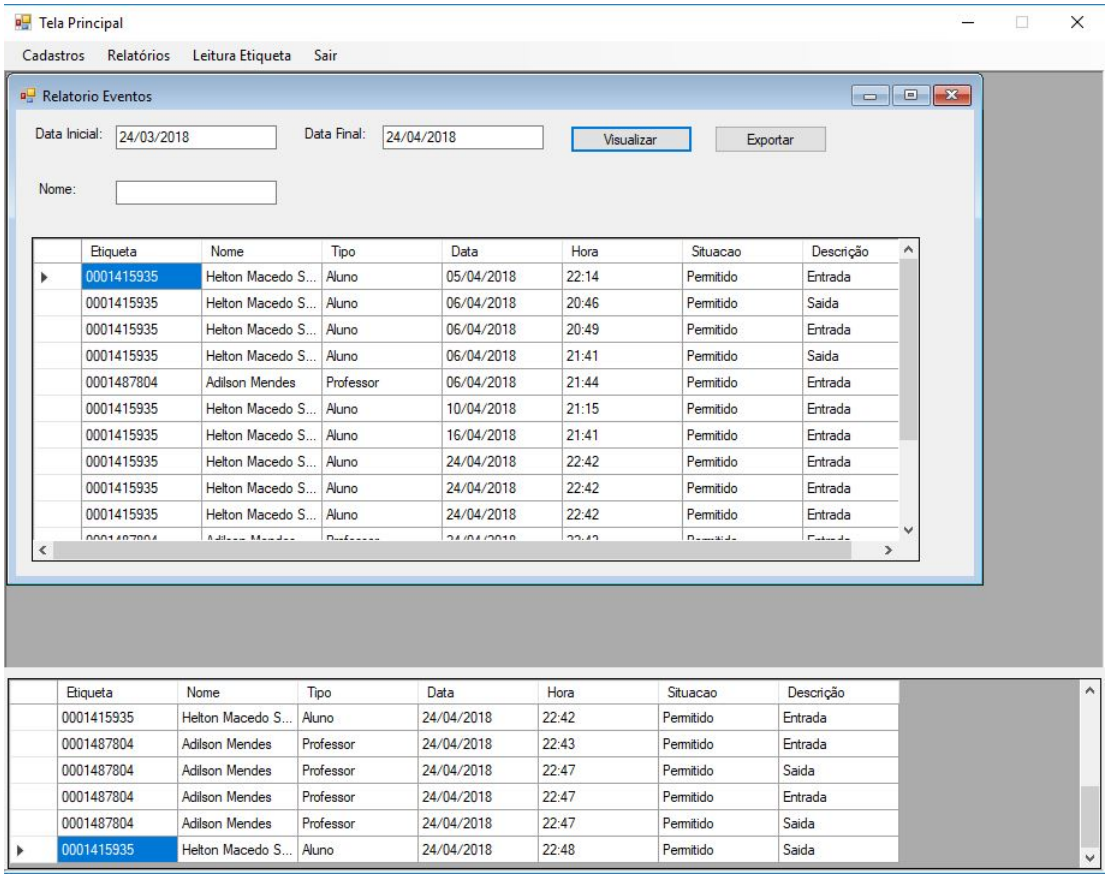


	Servidores	Data: 04/5	Data:	Data:	Data:	Data:
1	Adalberto Texeira de Andrade Rocha	Saiu				
2	Adilson Mendes Ribeiro	OX				
3	Adriana Sales Zardini	OX				
4	Aléssio Miranda Júnior					
5	Alexandre Augusto Gamberini	O				
6	Alexandre Pereira da Silva	OX				
7	Alisson Brizon D'Angelo Chaib					
8	Alisson Pinto Chaves	O				
9	Almir Silva Neto	O				
10	Ana Cristina de Oliveira Santos	OX				
12	André Rodrigues da Cruz Química	OXO				
13	Armim Fraz Isenmann					
14	Aurélio Takão Vieira Kubo					
15	Bianca (Estagiaria)	Saiu				
17	Bruno Rodruigues Silva	OX				
18	Carla Pricila de Morais Mendes					
19	Carlos Augusto Magalhaes Júnior	OX				
20	Carlos Eduardo Oliveira Andrade	OX				
21	Carlos Frederico Campos Assis Fred	OX				
22	Carolini Tavares Frinhani					
23	Cassio Lourenço Guimares Spinola					
24	Cláudia Mara de Souza					
25	Cristina da Rocha Alves	O				
26	Cyntia (Estagiaria)	OX				
28	Danilo França do Nascimento	Saiu				
29	Débora Pereira Coura					
30	Deivmar Pereira Coura	OXOX				

Fonte: Autor

Com os testes realizados percebe-se que a automatização do processo permite um controle apropriado das informações, eliminando possíveis falhas humanas como preenchimento errado do controle manual, ausência do vigilante, entre outros. A figura 18 mostra o controle dos dados digitalizados pela aplicação possibilitando realizar filtragens e controles.

Figura 18 – Controle no sistema



Fonte: Autor

6.2 Confidencialidade da Informação

Confidencialidade é o uso da informação apenas por pessoas autorizadas, toda informação deve ser protegida de acordo com o seu grau de sigilo de seu conteúdo, visando a limitação de seu acesso ou uso apenas as pessoas a quem é destinada (SÊMOLA, 2014).

O acesso a aplicação só se dá por operadores cadastrados e autenticados, com isso o acesso as funcionalidades como identificação dos usuários, cadastros e geração de relatórios fica restrito apenas as pessoas autorizadas e que realmente tenham que fazer o uso das informações.

6.3 Disponibilidade da Informação

A disponibilidade está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas implantados, ou seja, se eles podem ser consultados a qualquer momento pelos colaboradores. A facilidade de lidar e tratar essas informações também é levada em questão quando se trata de praticidade, uma filtragem dos dados afim de disponibilizar o que é realmente relevante para o processo (SÊMOLA, 2014).

Devido a aplicação ser cliente/servidor as informações possuem uma acessibilidade maior, como as informações são digitais e registradas no banco de dados é possível aplicar filtros de acordo com a necessidade e as informações que são desejadas. Também seria possível acessar as informações, relatórios de qualquer lugar da rede que possui o sistema cliente.

Com a disponibilidade das informações é possível verificar os usuários com acesso, automóveis registrados e o controle de qualquer ponto da rede e assim averiguar se o veículo vinculado a um professor ou aluno esta na unidade caso precise entrar em contato com o mesmo.

6.4 Modelo atual e modelo proposto

Um dos objetivos deste trabalho consiste em analisar a viabilidade da implantação de um controle automatizado em relação ao manual utilizado atualmente. Conforme os resultados obtidos no trabalho proposto pode-se ponderar e comparar com o modelo usado atualmente pela instituição.

O controle manual torna o processo custoso e trabalhoso, dependente de um esforço humano como recurso. O vigilante pode muitas vezes deixar de fazer suas funções tidas como prioritárias para realizar esse controle, ou mesmo deixar de faze-lo visto que no momento tem que realizar estas outras funções. Este controle se torna deficitário se o vigilante não estiver presente no momento do acesso ou saída do veículo, as informações ficam defasadas ou o vigilante teria que percorrer todo o recinto periodicamente para averiguar os veículos presentes e atualizar o seu controle. O registro manual, como tem o fator humano no processo, existe a possibilidade de ocorrerem erros em seu preenchimento.

Com o controle manual as informações também não possuem acessibilidade nem conseguem ser usadas com efetividade, pois as planilhas ficam com os vigilantes e caso alguém da instituição queira ter acesso o mesmo tem que se dirigir a eles e procurar dentre todas as planilhas preenchidas. Por isso fica complicado utilizar essas informações para saber se algum usuário esta presente ou ausente na instituição ou verificar a frequência e regularidade de acesso dos usuários.

A utilização da tecnologia RFID neste processo permitem maior integridade e disponibilidade das informações e tornando o processo fluido e agregando usabilidade com as funcionalidades implementadas ao processo.

Este trabalho de pesquisa trás uma automatização de todo este processo, as informações se tornam digitais e são facilmente tratadas podendo servir como consultas, estatísticas e controle do recurso. O fator humano é excluído do processo e junto dele suas deficiências descritas acima, assim também o vigilante pode dar foco as suas atividades principais e só intervir no processo de controle e identificação em caso de necessidade.

Utilizando a RFID na identificação do usuário a verificação foi simplificada, agora o leitor captura o código da etiqueta e envia para o sistema, este acessa o banco de dados e confirma se usuário pode ter acesso ou não e registra o evento ocorrido.

Outro aspecto levantado para este trabalho seria que ao usar a tecnologia RFID com alcance maior (Frequência UHF) o usuário tem uma menor exposição em relação a sua segurança física já que o mesmo não precisaria sair do veiculo ou abrir a janela para que o leitor realizasse a leitura, pois o sistema garante um alcance de leitura em torno de 8 a 10 metros. Mesmo o trabalho simulando a identificação utilizando frequências LF, não houve empecilhos nem modificações a não ser a troca dos leitores/antena e etiquetas necessários para se utilizar frequências LF, porém o controle utilizando a tecnologia RFID com frequência UHF é a real intenção da proposta.

7 Conclusão

O presente trabalho de pesquisa foi desenvolvido para analisar a utilização da tecnologia de identificação por radiofrequência (RFID) e suas aplicações a fim de automatizar o controle de acesso veicular em uma área de acesso controlado. A investigação e os estudos sobre o RFID mostraram que, geralmente, essa tecnologia é utilizada para a identificação de objetos e é vista como uma sucessora do código de barras devido a sua maior disponibilidade de recursos. Cada aplicação requer uma frequência de acordo com suas necessidades e a frequência UHF, que permite um alcance em torno de 10 metros, é comumente utilizada em aplicações de cadeia de suprimentos.

Este trabalho de pesquisa foi planejado para realizar a identificação e o controle das informações dos usuários por meio da implementação de uma RFID UHF, permitindo assim uma maior liberdade tanto do processo quanto dos usuários. Devido a limitações financeiras em relação a obtenção dos equipamentos foi realizada uma alteração na proposta, usando-se um leitor LF. Contudo a pesquisa não sofreu restrição significativa, exceto pela redução no poder de mobilidade da solução, e por isso as funcionalidades foram contempladas igualmente, mesmo para outras frequências.

Conforme proposto a utilização do método descrito nesse trabalho de pesquisa permite um controle do acesso veicular e uma gestão das informações de forma satisfatória, agregando ao processo integridade, confiabilidade, disponibilidade e automação.

De forma geral este trabalho de pesquisa obteve resultados significativos: as informações coletadas como cadastro dos usuários, registros dos eventos de entrada e saída permanecem íntegras desde sua geração, tratamento até a armazenagem.

Outro ponto que foi alcançado é a confidencialidade das informações, visto que somente pessoas autenticadas teriam acesso ao sistema e consequentemente as informações, a identificação e cadastros de usuários ficam restritos somente a pessoas que realmente precisam fazer uso delas.

E por fim a disponibilidade. O tempo e acessibilidade em um sistema é um fator importante para avaliar a praticidade de lidar com as informações circuladas no processo, assim implementando a aplicação como cliente-servidor permitiu-se que as informações fossem coletadas, tratadas e analisadas de qualquer aplicação cliente inserida na rede.

Assim pôde-se cumprir as metas estipuladas ao comparar o modelo proposto com o modelo atual. O modelo proposto oferece diversos benefícios em relação ao controle manual, a simplificação e automatização do processo de controle e identificação, adicionando os três princípios da segurança informação (integridade, disponibilidade e confidencialidade) no tratamento das informações e oferecendo praticidade aos operadores e aos usuários. Esta é uma implementação viável tanto pelos benefícios relatados quanto pela facilidade com que seria implementada e, portanto, dependendo apenas dos custos dos equipamentos.

Trabalhos futuros:

- O aplicação proposta no trabalho já funciona como cliente/servidor, contudo poderia-se implementar a tecnologia de identificação por radiofrequência de forma que esta possa ser utilizada em rede, uma ampliação do campus por exemplo poderia trazer a necessidade de se ter outras portarias realizando controles e identificações.
- Utilizar a tecnologia de identificação por radio frequência de para que possa realizar uma integração aumentando suas funcionalidades, assim além de verificar os veículos, se verificasse também os usuários que adentrassem a pé ou por outros meios, permitindo assim até um controle do fluxo de alunos dentro do campus.
- Juntamente com a aplicação de identificação e controle poderia ser implementado também uma solução que realizasse a abertura automática do portão, em decorrência de entradas e saídas autorizadas pelo controle.

Referências

AHSON, S. A.; ILYAS, M. *RFID handbook: applications, technology, security, and privacy*. [S.l.]: CRC press, 2008. Citado na página 13.

ATLAS, R. S. *Atlas*. 2018. Disponível em: <https://www.atlasrfidstore.com>. Acesso em: 20 Mar. 2018. Citado na página 38.

BARION, R. *IEEE 802.11 ad – o padrão Wi-Fi revoluciuonário*. 2016. Disponível em: <http://www.entelco.com.br/blog/ieee-802-11-ad-o-padrao-wi-fi-revoluciuonario/>. Acesso em: 12 set. 2017. Citado na página 19.

BULHMAN, H. J.; CABIANCA, L. A. *Redes LAN/MAN Wireless II: Funcionamento do Padrão 802.11*. 2016. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialrwlanman2/default.asp>. Acesso em: 10 out. 2017. Citado nas páginas 18 e 19.

ENGST, A. C.; FLEISHMAN, G. *The wireless networking starter kit: the practical guide to Wi-Fi networks for Windows and Macintosh*. [S.l.]: Peachpit Press, 2003. Citado na página 15.

FAROOQ, U. *et al.* Rfid based security and access control system. *International Journal of Engineering and Technology*, IACSIT Press, v. 6, n. 4, p. 309, 2014. Citado na página 34.

FERREIRA, F. N. F.; ARAÚJO, M. T. *Politica de segurança da informação*. [S.l.]: Ciência Moderna, 2008. Citado na página 31.

FINKENZELLER, K. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. [S.l.]: John Wiley & Sons, 2010. Citado nas páginas 12, 27, 28 e 30.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. [S.l.]: AMGH Editora, 2009. Citado nas páginas 15 e 18.

FRIAS, R. N. *ZigBee*. 2004. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialzigbee/default.asp>. Acesso em: 8 out. 2017. Citado na página 21.

FUJIMURA, C. A. *Conhecendo a tecnologia Ultra Wide Band*. 2006. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialuwbI>. Acesso em: 10 out. 2017. Citado na página 21.

GLOVER, B.; BHATT, H. *RFID essentials*. [S.l.]: "O'Reilly Media, Inc.", 2006. Citado nas páginas 12, 23, 24 e 29.

JAMES, G. *RFID Technology*. 2016. Disponível em: <http://www.gjbs.co.uk/images/technology/RFID/RFIDTags.jpg>. Acesso em: 3 out. 2017. Citado nas páginas 24 e 25.

JÚNIOR, A. L. d. C. *Redes sem Fio*. 2012. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredespbaid/default.asp>. Acesso em: 3 out. 2017. Citado nas páginas 15, 16 e 19.

KUROSE, J. F. *Computer networking: A top-down approach featuring the internet, 3/E*. [S.l.]: Pearson Education India, 2013. Citado nas páginas 15 e 17.

LAHIRI, S. *RFID sourcebook*. [S.l.]: IBM press, 2005. Citado nas páginas 23, 25, 26, 27, 28, 30 e 31.

MARTINS, V. A. *RFID (Identificação por Radiofrequência)*. 2017. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialrfid/default.asp>. Acesso em: 12 set. 2017. Citado nas páginas 22 e 23.

MEIRELES, A. M. R.; MOREIRA, L. R.; SILVA, M. F. da. Sistema supervisório para controle de fluxo de veículos através de rfid. *Revista Expressão Católica*, v. 4, n. 2, 2017. Citado na página 33.

MENDES, D. R. *Redes de Computadores*. [S.l.]: Editora Novatec, 2007. Citado na página 15.

MSS, E. *MSS Eletrônica*. 2018. Disponível em: <http://www.msseletronica.com/>. Acesso em: 12 Mar. 2018. Citado na página 39.

PEREIRA, J. C. B.; JÚNIOR, L. F. d. S.; ALMEIDA, R. J. P. d. Sistema automatizado de vaga veicular para deficientes físicos e idosos utilizando a tecnologia rfid. *Nanbiquara*, v. 5, n. 2, 2016. Citado na página 33.

RAMOS, M. P. Controle de acesso biométrico. *Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina*, 2012. Citado na página 13.

ROCHA, E. C. *Controle de acesso veicular: como fazer da forma certa*. 2018. Disponível em: <http://mtgtech.com.br/controle-de-acesso-veicular>. Acesso em: 12 Jul. 2018. Citado na página 32.

SÊMOLA, M. *Gestão da segurança da informação*. [S.l.]: Elsevier Brasil, 2014. v. 2. Citado nas páginas 12, 47, 48 e 49.

SOARES, B. T. ; SILVA, A. P. d. *Wi-Fi e WiMAX I: As Tecnologias de Rede Sem Fio*. 2009. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialww1/default.asp>. Acesso em: 5 set. 2017. Citado na página 16.

SUNDAR, R.; HEBBAR, S.; GOLLA, V. Implementing intelligent traffic control system for congestion control, ambulance clearance, and stolen vehicle detection. *IEEE Sensors Journal*, IEEE, v. 15, n. 2, p. 1109–1113, 2015. Citado na página 33.

TANENBAUM, A. S.; WETHERALL, D. J. *Computer Networks*. [S.l.]: Pearson, 2011. Citado nas páginas 17 e 18.

TUDE, E. *Bluetooth*. 2013. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialblue/>. Acesso em: 6 out. 2017. Citado na página 20.

Anexos

ANEXO A – Código Fonte

Listing A.1 – FrmTelaPrincipal

```
1
2  using ControleRFID.View;
3  using System;
4  using System.Collections.Generic;
5  using System.ComponentModel;
6  using System.Data;
7  using System.Drawing;
8  using System.IO.Ports;
9  using System.Linq;
10 using System.Text;
11 using System.Threading;
12 using System.Threading.Tasks;
13 using System.Windows.Forms;
14 using ControleRFID.Servico.Servico;
15
16 namespace ControleRFID
17 {
18     public partial class FrmTelaPrincipal : Form
19     {
20         string str = "Data Source=.;Initial Catalog=AMS;Integrated Security=
               True";
21         private SerialPort RFID;
22         private string DispString;
23
24         LeituraServico _leituraServico = new LeituraServico();
25
26         delegate void SetTextCallback(string texto);
27
28         public FrmTelaPrincipal()
29         {
30             this.FormBorderStyle = FormBorderStyle.FixedSingle;
31             this.StartPosition = FormStartPosition.CenterScreen;
32             InitializeComponent();
33             this.Show();
34
35             //Thread t = new Thread(Eventos);
36             //t.Start();
37
38             timer1.Interval = 5000;
39             timer1.Enabled = true;
40             timer1.Start();
41
42       }
43
44
45
```

```
46
47          public void Eventos()
48          {
49              while (Application.OpenForms.OfType<FrmTelaPrincipal>().Count() >
                    0) {
50
51                  for (int i = 0; i < 50; i++)
52                  {
53
54                  }
55              }
56
57
58          }
59
60
61          private void DefinirTexto(string texto)
62          {
63              //this.textBox1.Text = texto;
64          }
65          private void rel torioToolStripMenuItem_Click(object sender,
                EventArgs e)
66          {
67              FecharFormulariosFilhos();
68              var frmRelEventos = new FrmRelEventos();
69              frmRelEventos.Anchor = System.Windows.Forms.AnchorStyles.Top;
70              frmRelEventos.MdiParent = this;
71              // this.Hide();
72              frmRelEventos.Show();
73          }
74
75          private void relat rioUsuariosToolStripMenuItem_Click(object sender,
                EventArgs e)
76          {
77              FecharFormulariosFilhos();
78              var frmRelUsuario = new FrmRelUsuario();
79              frmRelUsuario.MdiParent = this;
80              //this.Hide();
81              frmRelUsuario.Anchor = System.Windows.Forms.AnchorStyles.Top;
82              frmRelUsuario.Show();
83
84          }
85
86
87
88          private void usu riosToolStripMenuItem_Click(object sender,
                EventArgs e)
89          {
90              FecharFormulariosFilhos();
91              var formCadUsuario = new FrmCadastroUsuario();
92              formCadUsuario.MdiParent = this;
93              //this.Hide();
```

```
94              formCadUsuario.Anchor = System.Windows.Forms.AnchorStyles.Top;
95              formCadUsuario.Show();
96          }
97
98          private void operadorToolStripMenuItem_Click(object sender, EventArgs
                e)
99          {
100             FecharFormulariosFilhos();
101             var frmCadOperador = new FrmCadOperador();
102             frmCadOperador.Anchor = System.Windows.Forms.AnchorStyles.Top;
103             frmCadOperador.MdiParent = this;
104             // this.Hide();
105             frmCadOperador.Show();
106         }
107
108
109         private void FecharFormulariosFilhos()
110         {
111             // percorre todos os formul rios abertos
112             for (int i = Application.OpenForms.Count - 1; i >= 0; i--)
113             {
114                 // se o formul rio for filho
115                 if (Application.OpenForms[i].IsMdiChild)
116                 {
117                     // fecha o formul rio
118                     Application.OpenForms[i].Close();
119                 }
120             }
121         }
122
123         private void leituraEtiquetaToolStripMenuItem_Click(object sender,
                EventArgs e)
124         {
125             FecharFormulariosFilhos();
126             var frmLeituraEtiquete = new FrmLeituraEtiqueta();
127             frmLeituraEtiquete.Anchor = System.Windows.Forms.AnchorStyles.Top
                    ;
128             frmLeituraEtiquete.MdiParent = this;
129             // this.Hide();
130             frmLeituraEtiquete.Show();
131         }
132
133         private void relat rioVeiculosToolStripMenuItem_Click(object sender,
                EventArgs e)
134         {
135             FecharFormulariosFilhos();
136             var frmRelVeiculo = new FormRelVeiculos();
137             frmRelVeiculo.Anchor = System.Windows.Forms.AnchorStyles.Top;
138             frmRelVeiculo.MdiParent = this;
139             // this.Hide();
140             frmRelVeiculo.Show();
141         }
```

```
142
143         private void timer1_Tick(object sender, EventArgs e)
144         {
145             var list = _leituraServico.ObterEventos();
146             dataGridView1.DataSource = list;
147             dataGridView1.Columns.RemoveAt(0);
148             //dataGridView1.Columns.RemoveAt(6);
149             dataGridView1.Columns[3].DefaultCellStyle.Format = "dd/MM/yyyy";
150             dataGridView1.Columns[4].DefaultCellStyle.Format = "HH:mm";
151             var dgvCount= dataGridView1.Rows.Count;
152             if(dgvCount > 0)
153             dataGridView1.CurrentCell = dataGridView1.Rows[dgvCount - 1].
                    Cells[0];
154         }
155
156         private void sairToolStripMenuItem_Click(object sender, EventArgs e)
157         {
158             Application.Exit();
159         }
160     }
161 }
```

Listing A.2 – FrmLeituraEtiqueta

```
1
2 using System;
3 using System.Collections;
4 using System.Collections.Generic;
5 using System.ComponentModel;
6 using System.Data;
7 using System.Drawing;
8 using System.Linq;
9 using System.Text;
10 using System.Threading.Tasks;
11 using System.Windows.Forms;
12 using ControleRFID.Servico.Servico;
13
14
15
16 namespace ControleRFID
17 {
18     public partial class FrmLeituraEtiqueta : Form
19     {
20
21
22         List<Pessoa> pessoas = new List<Pessoa>();
23         LeituraServico _leituraServico = new LeituraServico();
24
25         public FrmLeituraEtiqueta()
26         {
27             InitializeComponent();
28             //Pessoa p1 = new Pessoa("Helton", "0001415935", "aluno", "
```

```
                Permitido");
29              //Pessoa p2 = new Pessoa("Adilson", "0001487804", "Professor", "
                    Permitido");
30              //pessoas.Add(p1);
31              //pessoas.Add(p2);
32              //var list = _leituraServico.ObterEventos();
33              //dataGridView1.DataSource = list;
34              //dataGridView1.Columns.RemoveAt(0);
35              //dataGridView1.Columns.RemoveAt(6);
36              //dataGridView1.Columns[3].DefaultCellStyle.Format = "dd/MM/yyyy
                    ";
37              //dataGridView1.Columns[4].DefaultCellStyle.Format = "HH:mm";
38          }
39
40          private void label2_Click(object sender, EventArgs e)
41          {
42
43          }
44
45
46          private void textBox1_KeyUp(object sender, KeyEventArgs e)
47          {
48
49
50              if (e.KeyCode == Keys.Enter)
51              {
52                  string entrada = textBox1.Text;
53                  textBox1.Text = "";
54
55
56                  // Teste nova fun   o
57                 var listaUsuario = _leituraServico.ObterPorTag(entrada);
58
59                  if (listaUsuario == null)
60                  {
61                      MessageBox.Show("Usuario n o cadastrado", "Aviso",
                            MessageBoxButtons.OK, MessageBoxIcon.Warning);
62
63                  }
64                  else
65                  {
66                      int idEvento = _leituraServico.BuscaIdEvento(entrada);
67
68                      _leituraServico.CadastrarEvento(listaUsuario.Etiqueta,
                            idEvento);
69
70                      textBox2.Text = listaUsuario.Nome;
71                      textBox3.Text = listaUsuario.Tipo;
72                      textBox4.Text = listaUsuario.Status;
73                      textBox5.Text = listaUsuario.Marca;
74                      textBox6.Text = listaUsuario.Modelo;
75                      textBox7.Text = listaUsuario.Placa;
```

```
76                  }
77                  //Inserir na tabela registra eventos
78
79
80              }
81          }
82      }
83  }
```

Listing A.3 – FrmRelVeiculos

```
1  using System;
2  using System.Collections.Generic;
3  using System.ComponentModel;
4  using System.Data;
5  using System.Drawing;
6  using System.Linq;
7  using System.Text;
8  using System.Threading.Tasks;
9  using System.Windows.Forms;
10 using ControleRFID.Servico.Servico;
11
12 namespace ControleRFID.View
13 {
14     public partial class FormRelVeiculos : Form
15     {
16         UsuarioServico _usuarioServico = new UsuarioServico();
17         public FormRelVeiculos()
18         {
19             InitializeComponent();
20         }
21
22         private void button1_Click(object sender, EventArgs e)
23         {
24             var list = _usuarioServico.ObterVeiculos();
25
26             dataGridView1.DataSource = list;
27             dataGridView1.Columns.RemoveAt(0);
28         }
29     }
30 }
```

Listing A.4 – FrmRelEventos

```
1 using ControleRFID.Servico.Servico;
2 using System;
3 using System.Collections.Generic;
4 using System.ComponentModel;
5 using System.Data;
6 using System.Drawing;
7 using System.Linq;
8 using System.Text;
```

```
 9 using System.Threading.Tasks;
10 using System.Windows.Forms;
11 using Utils;
12
13 namespace ControleRFID.View
14 {
15     public partial class FrmRelEventos : Form
16     {
17         LeituraServico _leituraServico = new LeituraServico();
18         public FrmRelEventos()
19         {
20             InitializeComponent();
21
22             Mascara.addMask(textBox1, Mascara.MaskType.Data);
23             Mascara.addMask(textBox2, Mascara.MaskType.Data);
24
25             textBox1.Text = DateTime.Today.AddMonths(-1).ToShortDateString();
26             textBox2.Text = DateTime.Today.ToShortDateString();
27
28         }
29
30         private void button1_Click(object sender, EventArgs e)
31         {
32             DateTime dtInicial;
33             DateTime dtFinal;
34
35             try
36             {
37                 dtInicial = DateTime.TryParse(textBox1.Text, out dtInicial) ?
                       dtInicial : DateTime.MinValue;
38                 dtFinal = DateTime.TryParse(textBox2.Text, out dtFinal) ?
                       dtFinal : DateTime.MaxValue;
39
40                 dtFinal = new DateTime(dtFinal.Year, dtFinal.Month, dtFinal.
                       Day, 23, 59, 59);
41             }
42             catch
43             {
44                 dtInicial = DateTime.MinValue;
45                 dtFinal = DateTime.MaxValue;
46             }
47             if (textBox3.TextLength <= 0)
48             {
49                 var list = _leituraServico.ObterEventos(dtInicial, dtFinal);
50                 dataGridView1.DataSource = list;
51                 dataGridView1.Columns.RemoveAt(0);
52                 //dataGridView1.Columns.RemoveAt(6);
53                 dataGridView1.Columns[3].DefaultCellStyle.Format = "dd/MM/
                       yyyy";
54                 dataGridView1.Columns[4].DefaultCellStyle.Format = "HH:mm";
55             }
56             else
```

```
57              {
58                  var list = _leituraServico.ObterEventos(dtInicial, dtFinal,
                        textBox3.Text);
59                  dataGridView1.DataSource = list;
60                  dataGridView1.Columns.RemoveAt(0);
61                  //dataGridView1.Columns.RemoveAt(6);
62                  dataGridView1.Columns[3].DefaultCellStyle.Format = "dd/MM/
                        yyyy";
63                  dataGridView1.Columns[4].DefaultCellStyle.Format = "HH:mm";
64              }
65
66          }
67
68          private void FrmRelEventos_Load(object sender, EventArgs e)
69          {
70
71          }
72      }
73  }
```

Listing A.5 – Login

```
1  using System;
2  using System.Collections.Generic;
3  using System.ComponentModel;
4  using System.Data;
5  using System.Drawing;
6  using System.Linq;
7  using System.Text;
8  using System.Threading.Tasks;
9  using System.Windows.Forms;
10 using ControleRFID.Servico.Servico;
11
12
13 namespace ControleRFID
14 {
15     public partial class Login : Form
16     {
17         OperadorServico _operadorServico = new OperadorServico();
18
19         public Login()
20         {
21             this.StartPosition = FormStartPosition.CenterScreen;
22             InitializeComponent();
23
24             textBox2.PasswordChar = '*';
25         }
26
27         private void button1_Click(object sender, EventArgs e)
28         {
29             if (textBox1.Text == "" || textBox2.Text == "")
30             {
```

```
31                  MessageBox.Show("Preencher Usuario e Senha", "Alerta",
                        MessageBoxButtons.OK, MessageBoxIcon.Warning);
32
33              }
34              else
35              {
36                  try
37                  {
38                      Cursor.Current = Cursors.WaitCursor;
39
40                      if (_operadorServico.ObterLogin(textBox1.Text, textBox2.
                            Text) == true)
41                      {
42                          var formTelaPrincipal = new FrmTelaPrincipal();
43                          this.Hide();
44                          formTelaPrincipal.Show();
45                      }
46                      else
47                      {
48                          //txtUsuario.Text = "";
49                          textBox2.Text = "";
50                          if (MessageBox.Show("Usu rio e Senha incorretos", "
                                Aviso", MessageBoxButtons.OKCancel,
                                MessageBoxIcon.Exclamation) == DialogResult.
                                Cancel)
51                          {
52                              this.Close();
53                          }
54                      }
55                  }
56                  catch (Exception ex)
57                  {
58                      //txtUsuario.Text = "";
59                      textBox2.Text = "";
60                      if (MessageBox.Show(ex.ToString(), @"Usu rio e Senha
                            incorretos", MessageBoxButtons.OKCancel,
                            MessageBoxIcon.Exclamation) == DialogResult.Cancel)
61                      {
62                          this.Close();
63                      }
64                  }
65                  Cursor.Current = Cursors.Default;
66              }
67      }
68
69          private void button2_Click(object sender, EventArgs e)
70          {
71              Application.Exit();
72          }
73       }
74  }
```

Listing A.6 – FrmCadastroUsuario

```
1  using System;
2  using System.Collections.Generic;
3  using System.ComponentModel;
4  using System.Data;
5  using System.Drawing;
6  using System.Linq;
7  using System.Text;
8  using System.Threading.Tasks;
9  using System.Windows.Forms;
10 using ControleRFID.Servico.Servico;
11
12
13 namespace ControleRFID
14 {
15     public partial class Login : Form
16     {
17         OperadorServico _operadorServico = new OperadorServico();
18
19         public Login()
20         {
21             this.StartPosition = FormStartPosition.CenterScreen;
22             InitializeComponent();
23
24             textBox2.PasswordChar = '*';
25         }
26
27         private void button1_Click(object sender, EventArgs e)
28         {
29             if (textBox1.Text == "" || textBox2.Text == "")
30             {
31                 MessageBox.Show("Preencher Usuario e Senha", "Alerta",
                       MessageBoxButtons.OK, MessageBoxIcon.Warning);
32
33             }
34             else
35             {
36                 try
37                 {
38                     Cursor.Current = Cursors.WaitCursor;
39
40                     if (_operadorServico.ObterLogin(textBox1.Text, textBox2.
                           Text) == true)
41                     {
42                         var formTelaPrincipal = new FrmTelaPrincipal();
43                         this.Hide();
44                         formTelaPrincipal.Show();
45                     }
46                     else
47                     {
48                         //txtUsuario.Text = "";
49                         textBox2.Text = "";
```

```
50                          if (MessageBox.Show("Usu rio e Senha incorretos", "
                                Aviso", MessageBoxButtons.OKCancel,
                                MessageBoxIcon.Exclamation) == DialogResult.
                                Cancel)
51                          {
52                              this.Close();
53                          }
54                      }
55                  }
56                  catch (Exception ex)
57                  {
58                      //txtUsuario.Text = "";
59                      textBox2.Text = "";
60                      if (MessageBox.Show(ex.ToString(), @"Usu rio e Senha
                            incorretos", MessageBoxButtons.OKCancel,
                            MessageBoxIcon.Exclamation) == DialogResult.Cancel)
61                      {
62                          this.Close();
63                      }
64                  }
65                  Cursor.Current = Cursors.Default;
66              }
67      }
68
69          private void button2_Click(object sender, EventArgs e)
70          {
71              Application.Exit();
72          }
73      }
74  }
```

Listing A.7 – FrmCadOperador

```
1  using System;
2  using System.Collections.Generic;
3  using System.ComponentModel;
4  using System.Data;
5  using System.Drawing;
6  using System.Linq;
7  using System.Text;
8  using System.Threading.Tasks;
9  using System.Windows.Forms;
10 using ControleRFID.Servico.Servico;
11
12
13 namespace ControleRFID
14 {
15     public partial class Login : Form
16     {
17         OperadorServico _operadorServico = new OperadorServico();
18
19         public Login()
```

```
20          {
21              this.StartPosition = FormStartPosition.CenterScreen;
22              InitializeComponent();
23
24              textBox2.PasswordChar = '*';
25          }
26
27          private void button1_Click(object sender, EventArgs e)
28          {
29              if (textBox1.Text == "" || textBox2.Text == "")
30              {
31                  MessageBox.Show("Preencher Usuario e Senha", "Alerta",
                        MessageBoxButtons.OK, MessageBoxIcon.Warning);
32
33              }
34              else
35              {
36                  try
37                  {
38                      Cursor.Current = Cursors.WaitCursor;
39
40                      if (_operadorServico.ObterLogin(textBox1.Text, textBox2.
                            Text) == true)
41                      {
42                          var formTelaPrincipal = new FrmTelaPrincipal();
43                          this.Hide();
44                          formTelaPrincipal.Show();
45                      }
46                      else
47                      {
48                          //txtUsuario.Text = "";
49                          textBox2.Text = "";
50                          if (MessageBox.Show("Usu rio e Senha incorretos", "
                                Aviso", MessageBoxButtons.OKCancel,
                                MessageBoxIcon.Exclamation) == DialogResult.
                                Cancel)
51                          {
52                              this.Close();
53                          }
54                      }
55                  }
56                  catch (Exception ex)
57                  {
58                      //txtUsuario.Text = "";
59                      textBox2.Text = "";
60                      if (MessageBox.Show(ex.ToString(), @"Usu rio e Senha
                            incorretos", MessageBoxButtons.OKCancel,
                            MessageBoxIcon.Exclamation) == DialogResult.Cancel)
61                      {
62                          this.Close();
63                      }
64                  }
```

```
65                  Cursor.Current = Cursors.Default;
66              }
67      }
68
69          private void button2_Click(object sender, EventArgs e)
70          {
71              Application.Exit();
72          }
73      }
74  }
```

Listing A.8 – Entidades

```
1  namespace ControleRFID.Dominio
2  {
3      using System;
4      using System.Data.Entity;
5      using System.ComponentModel.DataAnnotations.Schema;
6      using System.Linq;
7
8      public partial class ModeloRFID : DbContext
9      {
10         public ModeloRFID()
11             : base("name=ModeloRFID")
12         {
13         }
14
15         public virtual DbSet<Evento> Evento { get; set; }
16         public virtual DbSet<Operadores> Operadores { get; set; }
17         public virtual DbSet<Registra_evento> Registra_evento { get; set; }
18         public virtual DbSet<sysdiagrams> sysdiagrams { get; set; }
19         public virtual DbSet<Usuarios> Usuarios { get; set; }
20
21         protected override void OnModelCreating(DbModelBuilder modelBuilder)
22         {
23             modelBuilder.Entity<Evento>()
24                 .Property(e => e.descricao)
25                 .IsUnicode(false);
26
27             modelBuilder.Entity<Operadores>()
28                 .Property(e => e.Nome)
29                 .IsUnicode(false);
30
31             modelBuilder.Entity<Operadores>()
32                 .Property(e => e.Senha)
33                 .IsUnicode(false);
34
35             modelBuilder.Entity<Registra_evento>()
36                 .Property(e => e.Etiqueta)
37                 .IsUnicode(false);
38
39             modelBuilder.Entity<Usuarios>()
```

```
40                  .Property(e => e.Etiqueta)
41                  .IsUnicode(false);
42
43              modelBuilder.Entity<Usuarios>()
44                  .Property(e => e.Nome)
45                  .IsUnicode(false);
46
47              modelBuilder.Entity<Usuarios>()
48                  .Property(e => e.RG)
49                  .IsUnicode(false);
50
51              modelBuilder.Entity<Usuarios>()
52                  .Property(e => e.Placa)
53                  .IsUnicode(false);
54
55              modelBuilder.Entity<Usuarios>()
56                  .Property(e => e.Marca)
57                  .IsUnicode(false);
58
59              modelBuilder.Entity<Usuarios>()
60                  .Property(e => e.Modelo)
61                  .IsUnicode(false);
62
63              modelBuilder.Entity<Usuarios>()
64                  .Property(e => e.Tipo)
65                  .IsUnicode(false);
66
67              modelBuilder.Entity<Usuarios>()
68                  .Property(e => e.Status)
69                  .IsUnicode(false);
70          }
71      }
72  }
73
74  namespace ControleRFID.Dominio
75  {
76      using System;
77      using System.Collections.Generic;
78      using System.ComponentModel.DataAnnotations;
79      using System.ComponentModel.DataAnnotations.Schema;
80      using System.Data.Entity.Spatial;
81
82      [Table("Evento")]
83      public partial class Evento
84      {
85          [Key]
86          public int idEvento { get; set; }
87
88          [Required]
89          [StringLength(50)]
90          public string descricao { get; set; }
91      }
```

```
92 }
93
94 namespace ControleRFID.Dominio
95 {
96     using System;
97     using System.Collections.Generic;
98     using System.ComponentModel.DataAnnotations;
99     using System.ComponentModel.DataAnnotations.Schema;
100    using System.Data.Entity.Spatial;
101
102    public partial class Operadores
103    {
104        [Key]
105        public int idOperador { get; set; }
106
107        [Required]
108        [StringLength(50)]
109        public string Nome { get; set; }
110
111        [Required]
112        [StringLength(50)]
113        public string Senha { get; set; }
114    }
115 }
116
117 namespace ControleRFID.Dominio
118 {
119     using System;
120     using System.Collections.Generic;
121     using System.ComponentModel.DataAnnotations;
122     using System.ComponentModel.DataAnnotations.Schema;
123     using System.Data.Entity.Spatial;
124
125     public partial class Registra_evento
126     {
127         [Key]
128         public int idRegistra { get; set; }
129
130         [Required]
131         [StringLength(50)]
132         public string Etiqueta { get; set; }
133
134         public int id_evento { get; set; }
135
136         public DateTime data_evento { get; set; }
137     }
138 }
139
140 using System;
141 using System.Collections.Generic;
142 using System.ComponentModel;
143 using System.Linq;
```

```
144 using System.Text;
145 using System.Threading.Tasks;
146
147 namespace ControleRFID.Dominio
148 {
149     public class RelatorioEvento
150     {
151
152         public int idRegistra { get; set; }
153
154         [DisplayName("Etiqueta")]
155         public string Etiqueta { get; set; }
156
157         [DisplayName("Nome")]
158         public string Nome { get; set; }
159
160         [DisplayName("Tipo")]
161         public string Tipo { get; set; }
162
163         [DisplayName("Data")]
164         public DateTime data_evento { get; set; }
165
166         [DisplayName("Hora")]
167         public DateTime hora_evento { get; set; }
168
169         [DisplayName("Situacao")]
170         public string Situacao { get; set; }
171
172         [DisplayName("D e s c r i   o")]
173         public string decr_evento { get; set; }
174
175     }
176 }
177
178 using System.ComponentModel;
179
180 namespace ControleRFID.Dominio
181 {
182     public class RelatorioUsuario
183     {
184
185         public int idUsuarios { get; set; }
186
187         [DisplayName("Etiqueta")]
188         public string Etiqueta { get; set; }
189
190         [DisplayName("Nome")]
191         public string Nome { get; set; }
192
193         [DisplayName("RG")]
194         public string RG { get; set; }
195
```

```
196         [DisplayName("Marca")]
197         public string Marca { get; set; }
198 
199         [DisplayName("Modelo")]
200         public string Modelo { get; set; }
201 
202         [DisplayName("Placa")]
203         public string Placa { get; set; }
204 
205 
206         [DisplayName("Tipo")]
207         public string Tipo { get; set; }
208 
209         [DisplayName("Status")]
210         public string Status { get; set; }
211         }
212 }
213 
214 
215 using System;
216 using System.Collections.Generic;
217 using System.ComponentModel;
218 using System.IO;
219 using System.Linq;
220 using System.Text;
221 
222 namespace ControleRFID.Dominio
223 {
224     public class RelatorioVeiculo
225     {
226         public int idUsuarios { get; set; }
227 
228         [DisplayName("Marca")]
229         public string Marca { get; set; }
230 
231         [DisplayName("Modelo")]
232         public string Modelo { get; set; }
233 
234         [DisplayName("Placa")]
235         public string Placa { get; set; }
236 
237         [DisplayName("Status")]
238         public string Status { get; set; }
239 
240     }
241 }
242 
243 
244 using System;
245 using System.Collections.Generic;
246 using System.ComponentModel;
247 using System.IO;
```

```
248 using System.Linq;
249 using System.Text;
250
251 namespace ControleRFID.Dominio
252 {
253     public class RelatorioVeiculo
254     {
255         public int idUsuarios { get; set; }
256
257         [DisplayName("Marca")]
258         public string Marca { get; set; }
259
260         [DisplayName("Modelo")]
261         public string Modelo { get; set; }
262
263         [DisplayName("Placa")]
264         public string Placa { get; set; }
265
266         [DisplayName("Status")]
267         public string Status { get; set; }
268
269     }
270 }
```

Listing A.9 – LeituraServico

```
1  using System;
2  using System.Collections;
3  using System.Collections.Generic;
4  using System.Linq;
5  using System.Text;
6  using System.Threading.Tasks;
7  using ControleRFID.Dominio;
8
9  namespace ControleRFID.Servico.Servico
10 {
11     public class LeituraServico
12     {
13         ModeloRFID Db = new ModeloRFID();
14
15         public Usuarios ObterPorTag(string etiqueta)
16         {
17             var listaUsuario = Db.Set<Usuarios>().FirstOrDefault(x => x.
                   Etiqueta == etiqueta);
18
19
20
21             return listaUsuario;
22         }
23
24         public void CadastrarEvento(string etiqueta,int idEvento) {
25             try
```

```
26              {
27                  Db.Set<Registra_evento>().Add(new Registra_evento
28                  {
29                      Etiqueta = etiqueta,
30                      data_evento = DateTime.Now,
31                      id_evento = idEvento
32                  });
33                  Db.SaveChanges();
34              }
35              catch (Exception ex)
36              {
37                  Console.WriteLine(ex);
38
39              }
40
41
42
43          }
44
45          public int BuscaIdEvento(string etiqueta)
46          {
47              int idEvento;
48              var user1 = (from registraEvento in Db.Set<Registra_evento>()
49                           where registraEvento.Etiqueta == etiqueta
50                           select new {
51                                  registraEvento.idRegistra,
52                                  registraEvento.id_evento}).OrderByDescending(
                                      x => x.idRegistra).FirstOrDefault();
53
54
55              if (user1==null)
56              {
57                  idEvento = 1;
58              }
59
60              else if (user1.id_evento == 2)
61              {
62                  idEvento = 1;
63
64              }
65              else
66              {
67                  idEvento = 2;
68              }
69
70              return idEvento;
71          }
72          public List<RelatorioEvento> ObterEventos() {
73
74                  var listaEventos = (from registraEvento in Db.Set<
                        Registra_evento>()
75                                      join evento in Db.Evento on
```

```
                                    registraEvento.id_evento equals
                                    evento.idEvento
76                                  join usuario in Db.Usuarios on
                                    registraEvento.Etiqueta equals
                                    usuario.Etiqueta
77                                  select new RelatorioEvento
78                                  {
79                                      Etiqueta = registraEvento.Etiqueta,
80                                      Nome = usuario.Nome,
81                                      Tipo = usuario.Tipo,
82                                      data_evento = registraEvento.
                                        data_evento,
83                                      hora_evento = registraEvento.
                                        data_evento,
84                                      Situacao = usuario.Status,
85                                      decr_evento = evento.descricao
86                                  }).ToList();
87
88
89              return listaEventos;
90          }
91
92      public List<RelatorioEvento> ObterEventos(DateTime dtInicial,DateTime
            dtFinal)
93      {
94
95          var listaEventos = (from registraEvento in Db.Set<Registra_evento
                >()
96                              join evento in Db.Evento on registraEvento.
                                id_evento equals evento.idEvento
97                              join usuario in Db.Usuarios on registraEvento
                                .Etiqueta equals usuario.Etiqueta
98                              where (registraEvento.data_evento >=
                                dtInicial && registraEvento.data_evento
                                <= dtFinal)
99                              select new RelatorioEvento
100                             {
101                                 Etiqueta = registraEvento.Etiqueta,
102                                 Nome = usuario.Nome,
103                                 Tipo = usuario.Tipo,
104                                 data_evento = registraEvento.data_evento,
105                                 hora_evento = registraEvento.data_evento,
106                                 Situacao = usuario.Status,
107                                 decr_evento = evento.descricao
108                             }).ToList();
109
110
111         return listaEventos;
112     }
113
114     public List<RelatorioEvento> ObterEventos(DateTime dtInicial,
            DateTime dtFinal,string nome)
```

```
115         {
116
117             var listaEventos = (from registraEvento in Db.Set<Registra_evento
                    >()
118                                 join evento in Db.Evento on registraEvento.
                                        id_evento equals evento.idEvento
119                                 join usuario in Db.Usuarios on registraEvento
                                        .Etiqueta equals usuario.Etiqueta
120                                 where (registraEvento.data_evento >=
                                        dtInicial && registraEvento.data_evento
                                        <= dtFinal && usuario.Nome.Contains(nome)
                                        )
121                                 select new RelatorioEvento
122                                 {
123                                     Etiqueta = registraEvento.Etiqueta,
124                                     Nome = usuario.Nome,
125                                     Tipo = usuario.Tipo,
126                                     data_evento = registraEvento.data_evento,
127                                     hora_evento = registraEvento.data_evento,
128                                     Situacao = usuario.Status,
129                                     decr_evento = evento.descricao
130                                 }).ToList();
131
132
133
134             return listaEventos;
135         }
136     }
137
138 }
```

Listing A.10 – OperadorServico

```
1  using ControleRFID.Dominio;
2  using System;
3  using System.Collections.Generic;
4  using System.Linq;
5  using System.Text;
6  using System.Threading.Tasks;
7
8  namespace ControleRFID.Servico.Servico
9  {
10     public class OperadorServico
11     {
12         public ModeloRFID Db = new ModeloRFID();
13
14         public void CadastrarOperador(string _nome, string _senha)
15         {
16             try
17             {
18                 Db.Set<Operadores>().Add(new Operadores
19                 {
```

```
20                      Nome = _nome,
21                      Senha = _senha
22
23                  });
24                  Db.SaveChanges();
25              }
26              catch (Exception ex)
27              {
28                  Console.WriteLine(ex);
29              }
30          }
31          public bool ObterLogin(string login,string senha)
32          {
33              var usuario = Db.Set<Operadores>().FirstOrDefault(x => x.Nome.
                    ToLower() == login.ToLower() && x.Senha == senha);
34
35              if (usuario != null)
36              {
37                  return true;
38              }
39              else
40                  return false;
41          }
42
43 }
44 }
```

Listing A.11 – UsuarioServico

```
1  using System;
2  using System.Collections.Generic;
3  using System.Linq;
4  using System.Text;
5  using System.Threading.Tasks;
6  using ControleRFID.Dominio;
7
8
9
10 namespace ControleRFID.Servico.Servico
11 {
12     public class UsuarioServico
13     {
14         public ModeloRFID Db = new ModeloRFID();
15
16         public void CadastrarUsuario(string _nome, string _rg, string
               _etiqueta, string _placa, string _tipo, string _status, string
               _marca, string _modelo)
17         {
18             try
19             {
20                 Db.Set<Usuarios>().Add(new Usuarios
21                 {
```

```
22                      Nome = _nome,
23                      Etiqueta = _etiqueta,
24                      RG = _rg,
25                      Placa = _placa,
26                      Tipo = _tipo,
27                      Status = _status,
28                      Marca = _marca,
29                      Modelo = _modelo
30                      //to =  222
31                      });
32                  Db.SaveChanges();
33              }
34              catch (Exception ex)
35              {
36                  Console.WriteLine(ex);
37
38              }
39          }
40
41          public List<RelatorioUsuario> ObterUsuarios()
42          {
43
44              var listaEventos = (from usuario in Db.Set<Usuarios>()
45                                  select new RelatorioUsuario
46                                  {
47                                     Etiqueta=usuario.Etiqueta,
48                                     Nome= usuario.Nome,
49                                     Marca= usuario.Marca,
50                                     Modelo= usuario.Modelo,
51                                     Placa = usuario.Placa,
52                                     RG = usuario.RG,
53                                     Status = usuario.Status,
54                                     Tipo = usuario.Tipo,
55                                  }).ToList();
56
57
58              return listaEventos;
59          }
60
61          public List<RelatorioVeiculo> ObterVeiculos()
62          {
63
64              var listaEventos = (from usuario in Db.Set<Usuarios>()
65                                  select new RelatorioVeiculo
66                                  {
67
68                                      Marca = usuario.Marca,
69                                      Modelo = usuario.Modelo,
70                                      Placa = usuario.Placa,
71                                      Status = usuario.Status,
72
73                                  }).ToList();
```

```
74
75
76                  return listaEventos;
77              }
78          }
79  }
```

ANEXO B – SQL Banco de dados

Listing B.1 – SQL Banco de dados

```
1
2 USE [master]
3 GO
4 /****** Object:  Database [RFID]    Script Date: 11/07/2018 10:59:49 ******/
5 CREATE DATABASE [RFID]
6  CONTAINMENT = NONE
7  ON  PRIMARY
8 ( NAME = N'RFID', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL14.
      SQLEXPRESS\MSSQL\DATA\RFID.mdf' , SIZE = 8192KB , MAXSIZE = UNLIMITED,
      FILEGROWTH = 65536KB )
9  LOG ON
10 ( NAME = N'RFID_log', FILENAME = N'C:\Program Files\Microsoft SQL Server\
      MSSQL14.SQLEXPRESS\MSSQL\DATA\RFID_log.ldf' , SIZE = 8192KB , MAXSIZE =
      2048GB , FILEGROWTH = 65536KB )
11 GO
12 ALTER DATABASE [RFID] SET COMPATIBILITY_LEVEL = 140
13 GO
14 IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
15 begin
16 EXEC [RFID].[dbo].[sp_fulltext_database] @action = 'enable'
17 end
18 GO
19 ALTER DATABASE [RFID] SET ANSI_NULL_DEFAULT OFF
20 GO
21 ALTER DATABASE [RFID] SET ANSI_NULLS OFF
22 GO
23 ALTER DATABASE [RFID] SET ANSI_PADDING OFF
24 GO
25 ALTER DATABASE [RFID] SET ANSI_WARNINGS OFF
26 GO
27 ALTER DATABASE [RFID] SET ARITHABORT OFF
28 GO
29 ALTER DATABASE [RFID] SET AUTO_CLOSE OFF
30 GO
31 ALTER DATABASE [RFID] SET AUTO_SHRINK OFF
32 GO
33 ALTER DATABASE [RFID] SET AUTO_UPDATE_STATISTICS ON
34 GO
35 ALTER DATABASE [RFID] SET CURSOR_CLOSE_ON_COMMIT OFF
36 GO
37 ALTER DATABASE [RFID] SET CURSOR_DEFAULT  GLOBAL
38 GO
39 ALTER DATABASE [RFID] SET CONCAT_NULL_YIELDS_NULL OFF
40 GO
41 ALTER DATABASE [RFID] SET NUMERIC_ROUNDABORT OFF
42 GO
```

```
43 ALTER DATABASE [RFID] SET QUOTED_IDENTIFIER OFF
44 GO
45 ALTER DATABASE [RFID] SET RECURSIVE_TRIGGERS OFF
46 GO
47 ALTER DATABASE [RFID] SET  DISABLE_BROKER
48 GO
49 ALTER DATABASE [RFID] SET AUTO_UPDATE_STATISTICS_ASYNC OFF
50 GO
51 ALTER DATABASE [RFID] SET DATE_CORRELATION_OPTIMIZATION OFF
52 GO
53 ALTER DATABASE [RFID] SET TRUSTWORTHY OFF
54 GO
55 ALTER DATABASE [RFID] SET ALLOW_SNAPSHOT_ISOLATION OFF
56 GO
57 ALTER DATABASE [RFID] SET PARAMETERIZATION SIMPLE
58 GO
59 ALTER DATABASE [RFID] SET READ_COMMITTED_SNAPSHOT OFF
60 GO
61 ALTER DATABASE [RFID] SET HONOR_BROKER_PRIORITY OFF
62 GO
63 ALTER DATABASE [RFID] SET RECOVERY SIMPLE
64 GO
65 ALTER DATABASE [RFID] SET  MULTI_USER
66 GO
67 ALTER DATABASE [RFID] SET PAGE_VERIFY CHECKSUM
68 GO
69 ALTER DATABASE [RFID] SET DB_CHAINING OFF
70 GO
71 ALTER DATABASE [RFID] SET FILESTREAM( NON_TRANSACTED_ACCESS = OFF )
72 GO
73 ALTER DATABASE [RFID] SET TARGET_RECOVERY_TIME = 60 SECONDS
74 GO
75 ALTER DATABASE [RFID] SET DELAYED_DURABILITY = DISABLED
76 GO
77 ALTER DATABASE [RFID] SET QUERY_STORE = OFF
78 GO
79 USE [RFID]
80 GO
81 ALTER DATABASE SCOPED CONFIGURATION SET IDENTITY_CACHE = ON;
82 GO
83 ALTER DATABASE SCOPED CONFIGURATION SET LEGACY_CARDINALITY_ESTIMATION = OFF;
84 GO
85 ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET
       LEGACY_CARDINALITY_ESTIMATION = PRIMARY;
86 GO
87 ALTER DATABASE SCOPED CONFIGURATION SET MAXDOP = 0;
88 GO
89 ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET MAXDOP = PRIMARY;
90 GO
91 ALTER DATABASE SCOPED CONFIGURATION SET PARAMETER_SNIFFING = ON;
92 GO
```

```
93 ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET PARAMETER_SNIFFING =
       PRIMARY;
94 GO
95 ALTER DATABASE SCOPED CONFIGURATION SET QUERY_OPTIMIZER_HOTFIXES = OFF;
96 GO
97 ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET
       QUERY_OPTIMIZER_HOTFIXES = PRIMARY;
98 GO
99 USE [RFID]
100 GO
101 /****** Object:  Table [dbo].[Evento]    Script Date: 11/07/2018 10:59:49
       ******/
102 SET ANSI_NULLS ON
103 GO
104 SET QUOTED_IDENTIFIER ON
105 GO
106 CREATE TABLE [dbo].[Evento](
107   [idEvento] [int] IDENTITY(1,1) NOT NULL,
108   [descricao] [varchar](50) NOT NULL,
109  CONSTRAINT [PK_Evento] PRIMARY KEY CLUSTERED
110 (
111   [idEvento] ASC
112 )WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
       ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
113 ) ON [PRIMARY]
114 GO
115 /****** Object:  Table [dbo].[Operadores]    Script Date: 11/07/2018 10:59:50
       ******/
116 SET ANSI_NULLS ON
117 GO
118 SET QUOTED_IDENTIFIER ON
119 GO
120 CREATE TABLE [dbo].[Operadores](
121   [idOperador] [int] IDENTITY(1,1) NOT NULL,
122   [Nome] [varchar](50) NOT NULL,
123   [Senha] [varchar](50) NOT NULL,
124  CONSTRAINT [PK_Operadores] PRIMARY KEY CLUSTERED
125 (
126   [idOperador] ASC
127 )WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
       ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
128 ) ON [PRIMARY]
129 GO
130 /****** Object:  Table [dbo].[Registra_evento]    Script Date: 11/07/2018
       10:59:50 ******/
131 SET ANSI_NULLS ON
132 GO
133 SET QUOTED_IDENTIFIER ON
134 GO
135 CREATE TABLE [dbo].[Registra_evento](
136   [idRegistra] [int] IDENTITY(1,1) NOT NULL,
137   [Etiqueta] [varchar](50) NOT NULL,
```

```
138   [id_evento] [int] NOT NULL,
139   [data_evento] [datetime] NOT NULL,
140  CONSTRAINT [PK_Registra_evento] PRIMARY KEY CLUSTERED
141 (
142   [idRegistra] ASC
143 )WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
       ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
144 ) ON [PRIMARY]
145 GO
146 /****** Object:  Table [dbo].[Usuarios]    Script Date: 11/07/2018 10:59:50
       ******/
147 SET ANSI_NULLS ON
148 GO
149 SET QUOTED_IDENTIFIER ON
150 GO
151 CREATE TABLE [dbo].[Usuarios](
152   [idUsuarios] [int] IDENTITY(1,1) NOT NULL,
153   [Etiqueta] [varchar](50) NOT NULL,
154   [Nome] [varchar](50) NOT NULL,
155   [RG] [varchar](50) NOT NULL,
156   [Placa] [varchar](50) NOT NULL,
157   [Marca] [varchar](50) NOT NULL,
158   [Modelo] [varchar](50) NOT NULL,
159   [Tipo] [varchar](50) NOT NULL,
160   [Status] [varchar](50) NOT NULL,
161   [Foto] [varbinary](50) NULL,
162  CONSTRAINT [PK_Usuarios] PRIMARY KEY CLUSTERED
163 (
164   [idUsuarios] ASC
165 )WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
       ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
166 ) ON [PRIMARY]
167 GO
168 USE [master]
169 GO
170 ALTER DATABASE [RFID] SET  READ_WRITE
171 GO
```