UMA PROPOSTA DE UTILIZAÇÃO DA TECNOLOGIA RFID E INTELIGÊNCIA ARTIFICIAL COMO SISTEMA DE CONTROLE DE ACESSO DE PESSOAS NO ÂMBITO DE PRÉDIOS PÚBLICOS

A PROPOSAL FOR THE USE OF RFID TECHNOLOGY AND ARTIFICIAL INTELLIGENCE AS AN ACCESS CONTROL SYSTEM FOR PEOPLE IN PUBLIC BUILDINGS

Sandro Rogério Ferreira Gomes [1]; Rosa Cristina Ferreira Bezerra [2]; Antônio Raimundo Amorim da Silva [3]; Dércio Luiz Reis [4]

RESUMO: A utilização da tecnologia RFID (*Radio-Frequency Identification* ou Identificação por Radiofrequência) vem sendo adotada em sistemas de controle de acesso devido à sua eficiência, conveniência e flexibilidade. O presente artigo, por meio de uma pesquisa bibliográfica, analisa o uso da RFID para controle de acesso de servidores e visitantes às dependências de prédios públicos, discutindo suas características, principais tecnologias, vantagens, desafios de segurança e as soluções implementadas para mitigar riscos de intrusão. Com o auxílio da literatura, observou-se que essa tecnologia possui diversas vantagens e aplicações, e que não veio para substituir outras tecnologias, podendo, inclusive, trabalhar em conjunto. A pesquisa enfatiza a importância da combinação de RFID com tecnologias como a IA, para aumentar a segurança e o controle. Ao final, é apresentada uma proposta de um sistema de controle de acesso, baseado em RFID, integrado com um sistema de IA, que permita um monitoramento de segurança em áreas sensíveis de prédios públicos.

Palavras-Chaves: Gestão; Sistema; Identificação; Radiofrequência.

ABSTRACT: The use of RFID (Radio Frequency Identification) technology has been adopted in access control systems due to its efficiency, convenience, and flexibility. This paper, through bibliographic research, analyzes the application of RFID for controlling the access of employees and visitors to public building facilities, discussing its characteristics, main technologies, advantages, security challenges, and the solutions implemented to mitigate security and intrusion risks. Supported by the literature, it was observed that this technology offers several advantages and applications and does not replace other technologies but can even operate in conjunction with them. The research highlights the importance of combining RFID with technologies such as AI to enhance security and control. In conclusion, a proposal is presented for an RFID-based access control system, integrated with an AI system, allowing for the monitoring of security in sensitive areas of public buildings.

Keywords: Management; System; Identification; Radio frequency.

1. INTRODUÇÃO

[1] Comando Militar da Amazônia (CMA) / email: sandrorecife2014@gmail.com
[2] Superintendência da Zona Franca de Manaus (SUFRAMA) / email: rosacrisfb@gmail.com
[3] Superintendência da Zona Franca de Manaus (SUFRAMA) / email: antonio.amorim@suframa.gov.br
[4] Universidade Federal do Amazonas (UFAM) / email: dercioreis@ufam.edu.br

O controle de acesso é uma das principais preocupações no gerenciamento da segurança de edifícios, especialmente em instalações sensíveis, como unidades corporativas e governamentais. A tecnologia RFID é uma das principais soluções para gerenciar o acesso físico de pessoas de maneira eficiente, utilizando crachás ou cartões de proximidade que permitem ou restringem o acesso, de acordo com o nível de autorização designada para o portador. Este artigo explora, principalmente, como a RFID se integra aos sistemas de controle de acesso, e descreve seus benefícios, os principais desafios, especialmente os relacionados à segurança.

As tecnologias que dão forma a chamada Indústria 4.0 (I4.0), possui, entre os seus princípios, a orientação a serviços, que consiste no desenvolvimento de softwares customizados, utilizando a internet dos serviços, integrando os usuários e máquinas através de programas adaptáveis a cada necessidade. Esses *softwares*, são literalmente feitos sob medida (SOUZA; CAVALLARI JUNIOR; DELGADO NETO, 2017). Sistemas de localização em tempo real ou *real time location system* – RTLS, são sistemas sem fio, que permitem o rastreamento de pessoas, fluxos de trabalho e materiais, tornando possível o monitoramento de características como velocidade, temperatura e umidade. Dentre estas tecnologias, pode-se mencionar o *bluetooth*, infravermelho e RFID (BUDAK; USTUNDAG, 2015 *apud* VIEIRA et al., 2018). A integração de um sistema de controle de acesso baseado em RFID com aplicações de Inteligência Artificial (IA), atuando para analisar a movimentação de servidores e visitantes dentro das instalações do prédio, é uma inovação significativa para que o sistema não seja apenas uma ferramenta burocrática de autorização de entrada nas instalações.

A tecnologia RFID, no controle de acesso, em shoppings, prédios residenciais, industriais e comerciais, vem sendo utilizada há bastante tempo. A importância dessa tecnologia consiste na garantia da agilidade na checagem de dados e na liberação de entrada e saída de pessoas, transmitindo confiabilidade, segurança e dinamismo na utilização dos dados coletados, sendo possível a tomada de inúmeras ações com a integração com outras tecnologias e plataformas (SANTINI, 2008).

Sistemas de controle de acesso inteligente, baseados em RFID, são cada vez mais populares, o que torna as organizações mais seguras, tornando-se a ferramenta mais conveniente na gestão de pessoal, com alta segurança e confiabilidade (TING, 2016, *apud* WANG et al., 2018).

Estudos anteriores, tais como, a abordagem do controle de acesso de pessoas em ambiente restrito utilizando a tecnologia RFID (OLIVEIRA et al., 2018), e ainda, a utilização de um sistema de controle inteligente de acesso em escritórios baseado na mesma tecnologia (WANG et all., 2018), demonstram a viabilidade de um sistema de RFID, e exemplifica como esta tecnologia pode ser inserida de forma simples nas instituições (TEIXEIRA, 2011).

2. REFERENCIAL TEÓRICO

Neste tópico, serão apresentadas as principais opiniões de especialistas referentes a esta temática, abrangendo o tema principal RFID, expondo informações sobre sua origem e utilização enfatizando sua aplicação no controle de entrada e saída de pessoas em instituições públicas.

2.1 Sistema RFID

Stanton (2004) e Pizzeti (2007) definem a *Radio Frequency Identification* (Identificação por Radiofrequência – RFID) como uma tecnologia de identificação que utiliza a radiofrequência para o intercâmbio de dados, permitindo realizar remotamente o armazenamento e recuperação de

informações usando uma etiqueta de rádio para identificação (PETENATE, 2019) e poderá ser afixada ou incorporada em um produto ou até em seres vivos.

O RFID tem sua estrutura formada de uma etiqueta plana, adesiva, de dimensões reduzidas, contendo um microchip em conjunto com sensores especiais e dispositivos que permitem a codificação e leitura dos dados contidos na mesma (PETENATE, 2019). O microchip da etiqueta é feito de silício, e permite armazenar inúmeras informações. Um sistema de RFID é composto por leitores configurados em rede, etiquetas, e um servidor para gerenciar a rede. As etiquetas são dispositivos eletrônicos que contêm um código que pode ser lido por um leitor remoto. A leitura ocorre quando um leitor específico envia ondas de radiofrequência à etiqueta, que repassa seus dados armazenados de volta ao leitor (PIZZETTI, 2007).

Uma determinada frequência de rádio é modulada por um leitor que transmite para uma tag, que recebe e, através de um elemento de acoplamento, repassa-as para o seu microchip (CIRIACO, 2009). A energia necessária será fornecida pelo leitor, por meio das ondas de rádio, sempre que a *tag* não possuir bateria própria, o que permitirá que ela permaneça ativa quando estiver sob a área coberta pelo leitor. Assim, acontece a comunicação por meio da radiofrequência, em ambos os sentidos (ZIMPEL et al., 2015, PULMANN, 2015).

As principais tecnologias RFID passíveis de utilização para controle de acesso a prédios envolvem diferentes tipos de *tags*, leitores e frequências. Para o desenvolvimento de um projeto de um controle de acesso como é proposta do presente artigo, é necessário que sejam tomadas decisões técnicas que atendam aos requisitos estabelecidos. É necessária a definição sobre a frequência do sinal de RFID a ser utilizado, o tipo de *tag*, o protocolo de comunicação, e as tecnologias a serem empregadas no controle de acesso e de segurança do sistema.

2.1.1 Frequências de RFID

Conforme Dastres (2022) As frequências **LF (Low Frequency)** de 125 kHz a 134 kHz e a **HF (High Frequency)** de 13,56 MHz não são recomendadas para o tipo de aplicação proposta por este trabalho, pois possuem um alcance curto, de 0,10 metros e 1 metro respectivamente, o que exige que o portador se aproxime muito dos dispositivos de leitura, o que não é conveniente para controles de acesso de grande fluxo de usuários. A **UHF (Ultra High Frequency)** de 300 MHz a 3 GHz, possui um alcance de leitura de até 10 metros ou mais, permitindo também seu uso em sistemas de controle de estacionamento. Esta tecnologia, entretanto, é mais suscetível a interferências e tem a necessidade de termos uma linha de visão entre a tag e o dispositivo leitor, o que precisa ser previsto nos projetos em que a escolha recaia sobre este tipo de equipamento.

Estão disponíveis no mercado três tipos de Tags: as Passivas, as ativas e as semiativas. As passivas não possuem fonte de energia própria e dependendo da energia fornecida pelo leitor RFID para transmitir dados. São as mais comuns em sistemas de controle de acesso e basicamente são apresentadas no formato de cartões de proximidade, crachás de funcionários. As tags ativas possuem uma fonte de energia interna (bateria), o que permite que sejam detectadas a distâncias maiores. Normalmente são empregadas em aplicações que requerem longos alcances, como portais de veículos. Já as tags semiativas utilizam baterias internas para alimentar circuitos internos, mas dependem do sinal de leitura para a transmissão dos dados ocorra.

2.1.2 Protocolos de Comunicação

Os protocolos de comunicação normalmente empregados em sistemas RFID são o ISO/IEC 14443, o ISO/IEC 15693 e o EPC Gen 2 (ISO 18000-6C).

O ISO/IEC 14443 é um protocolo de comunicação utilizado em cartões RFID de alta frequência (HF), como os cartões MIFARE e NFC. O protocolo ISO/IEC 15693 é um protocolo que permite sua leitura em maiores distâncias em HF. O protocolo EPC Gen 2 (ISO 18000-6C) é o protocolo utilizado principalmente em sistemas RFID de ultra-alta frequência (UHF), com alcance e capacidade de leitura elevados, utilizado em controle de acesso de veículos.

2.1.3 Tecnologias mais usadas no controle de acesso

As tecnologias mais utilizadas no controle de acesso são:

a) Cartões de Proximidade (Proximity Cards) que utilizam RFID em LF ou HF, amplamente usados em edifícios corporativos e residenciais;
b) MIFARE, tecnologia popular baseada em HF, com maior segurança e armazenamento de dados, usada para crachás de funcionários e cartões de transporte;
c) NFC (Near Field Communication), baseada em RFID HF, que permite a comunicação entre dispositivos (como smartphones e leitores), facilitando o uso de celulares para controle de acesso;
d) UHF para Veículos, utilizado para controle de acesso em estacionamentos e portões de segurança, com emprego de *tags* ativas ou passivas que podem ser lidas a distâncias maiores.

Essas são tecnologias amplamente empregadas por sua segurança, versatilidade e facilidade de integração em sistemas de controle de acesso. Os principais parâmetros para a definição da tecnologia mais adequada ao projeto, depende dos requisitos de segurança, da conveniência e do escopo de custo de cada aplicação.

2.1.4 Segurança

Um dos principais requisitos de um sistema de controle de acesso é a segurança do sistema. Sistemas de controle de acesso baseados em RFID devem evitar a entrada de pessoas não autorizadas, para isso, diversas medidas podem ser implementadas, incluindo criptografia, autenticação e práticas de proteção física e digital. Aqui serão apresentadas algumas das implementações mais comuns:

a) Criptografia;
   - Criptografia nos Dados da *tag*, que consiste em utilizar a criptografia para proteger os dados armazenados nas *tags* RFID. A transmissão das informações não é transmitida em texto claro, evitando a interceptação e a clonagem;
   - Criptografia do Canal de Comunicação, técnica em que, além da criptografia nos dados da *tag*, é possível criptografar o canal de comunicação entre a *tag* e o leitor RFID, tornando mais difícil interceptar ou alterar as informações transmitidas.
b) Autenticação Mútua;
   Esta técnica implementa uma rotina de identificação mútua entre a *tag* e o leitor, garantindo que os elementos se identifiquem antes de qualquer troca de dados. Dessa forma, o leitor RFID verifique se as *tags* são genuínas, e a *tag* só transmita informações quando o leitor for legítimo.
c) Desafio-Resposta;

São sistemas de autenticação baseados em desafio-resposta. O leitor envia um desafio criptográfico para a *tag* usando uma chave secreta compartilhada, exigindo uma resposta correta. Como o desafio é alterado em cada interação, não há como uma tentativa de reutilização ocorra.

d) Controle de Acesso Baseado em Servidor;
Neste tipo de controle de segurança, os dados lidos pelos leitores são enviados para um servidor central e validados. Ou seja, a liberação de acesso não se dá pela leitura dos dados da *tag*. O servidor verifica se o portador tem o acesso autorizado com base em credenciais dinâmicas, como horário de acesso permitido, função do usuário, locais em que o acesso será concedido, entre outras condições previamente estabelecidas.
Outra possibilidade é o Sistema em Camadas em que as informações da *tag* podem ser apenas parte de um sistema maior, que pode incluir o reconhecimento biométrico ou códigos PIN adicionais, criando uma autenticação em múltiplos fatores (MFA).

e) Bloqueio de *tags* Não Autorizadas;
A configuração de Listas de Controle de Acesso (listas brancas e negras) permite que o controle autorize somente *tags* que estejam em uma lista de controle, bloqueando automaticamente as que são clonadas ou duplicadas.
A implementação de UIDs (Identificadores Únicos) protegidos é outra possibilidade. Esta implementação implementa um identificador único (UID) para cada tag, a ser utilizado para verificação da sua autenticidade. UIDs criptografados ou que se alteram dinamicamente pode evitar a clonagem.

f) Proteção Física e Geográfica;
Por meio de um ajuste do Alcance do Leitor é possível impedir que o leitor capte sinais de *tags* fora da área desejada, evitando ataques de "*sniffing*" (escuta) em que as comunicações RFID são interceptadas à distância.
Outra técnica é a instalação de barreiras físicas ou "gaiolas de Faraday" ao redor de áreas sensíveis, impedindo que sinais RFID sejam lidos de fora do prédio.

g) Biometria como Fator de Autenticação Adicional;
Outra técnica empregada é a autenticação em Múltiplos Fatores (MFA) em que o RFID é combinado com outras formas de autenticação, como biometria (impressão digital, reconhecimento facial, etc.) ou a digitação de um código PIN. Isso cria uma camada extra de segurança, onde a simples posse da *tag* RFID não garante o acesso.

h) Proteção contra Clonagem e Skimming;
Na Proteção Anticlonagem são utilizadas *tags* RFID avançadas, como MIFARE DESFire ou iClass, que possuem proteções contra clonagem e replicação.
Podem ser utilizados também bloqueadores RFID, mais comuns em ambientes de alta segurança, em que os funcionários podem usar carteiras ou capas de bloqueio RFID para evitar que suas *tags* sejam lidas sem autorização (*skimming*).

i) Monitoramento e Log de Acessos;
Uma importante implementação de segurança é a implantação de sistemas de monitoramento contínuo. Esses sistemas registram todas as tentativas de acesso, incluindo acessos bem-sucedidos e falhas de autorização, permitindo que os registros sejam auditados para detectar comportamentos anômalos e tentativas de intrusões. Podem também contar com alertas em tempo real onde mensagens automáticas são emitidas se

detectadas tentativas de acesso suspeitas ou falhas repetidas, o que permite uma resposta rápida da segurança.

j) Atualizações e Gestão de Chaves.
Uma ação fundamental para a manutenção da segurança de sistemas de controle de acesso é a manutenção das atualizações do *firmware* do RFID e seus componentes, com patches de segurança para corrigir eventuais vulnerabilidades. A Gestão de Chaves Seguras, no caso de sistemas que usam chaves criptográficas (como MIFARE ou DESFire), garante que as chaves sejam armazenadas e geridas de maneira segura, evitando que sejam comprometidas.

Com a combinação de todas essas técnicas, é possível aumentar significativamente a segurança de um sistema de controle de acesso baseado em RFID, protegendo contra a entrada de pessoas não autorizadas e minimizando os riscos de clonagem ou ataque.

2.2 Controle de pessoas em órgãos públicos

O controle de acesso às dependências em um prédio público necessita de mecanismos que facilitem o fluxo dos veículos e dos pedestres sem a parada para a identificação, que acaba causando atraso, que pode ser evitado por meio da utilização de ferramentas inteligentes (ZAGONEL; MACHADO; MÔNEGO, 2017).

Para Faria, Marra e Resende (2020), o setor público necessita se adequar aos novos tempos e implementar mudanças, mas se depara com a visão burocrática dos indivíduos e pela falta de criatividade dos gestores. Em contrapartida, Marques, Borges e Almada (2018), Marques *et al.*, (2014) e Matos e Schommer (2013) afirmam que as organizações públicas estão buscando constantes mudanças para que a prestação de serviço seja cada vez mais eficiente, por meio da utilização das novas tecnologias.

A função da tecnologia nesses casos é a substituição do ser humano em atividades simples e rotineiras, que podem ser realizadas de forma remota, contribuindo significativamente no atendimento das atividades finalísticas da instituição, tendo como resposta o aumento da segurança e da conveniência, melhora na qualidade do serviço, otimização da administração de tempo e dinheiro, e a padronização da gestão de unidades (CHAGAS; PIMENTEL, 2017).

Para esses autores, a identificação dos servidores através deste sistema pode substituir o ponto eletrônico, gerando relatórios que documentem as entradas e saídas nas dependências da instituição.

2.3 Modelo e elementos principais do sistema RFID

O RFID se caracteriza como uma tecnologia de Identificação por meio de radiofrequência (VIEIRA et al., 2013) para capturar dados e permitir a leitura de um transponder, na maioria dos projetos sem a necessidade de campo visual direto e através de objetos construídos pelos mais diversos materiais como plástico, vidro ou madeira.

Segundo Puhlmann (2015), o RFID é uma tecnologia poderosa e multifuncional usada para a identificação, rastreamento e gerenciamento em uma enorme lista de produtos, documentos, animais ou pessoas. Os sistemas de RFID são geralmente compostos pelo leitor com a antena, o transponder, (*Tag*, RF *Tag*, etiqueta eletrônica), e computador ou outro tipo de controlador conforme ilustrado na Figura 1.

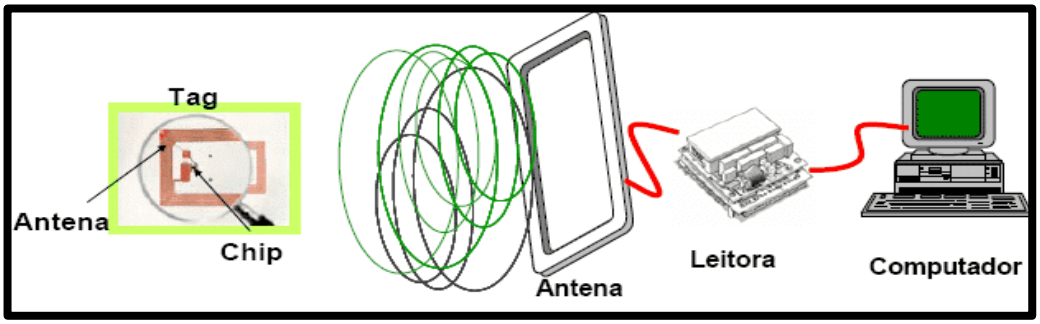


Figura 1. Sistema de RFID genérico. Fonte: Puhlmann (2015)

Seria impossível a listagem de todos os dispositivos necessários devido a diversidade de dispositivos utilizados hoje na aplicação do RFID em seus diversos setores. Cada empresa tem suas especificações e preferências na utilização desses dispositivos, e assim, possui seus específicos hardwares e softwares. Apresenta-se no Quadro 1 os dispositivos fundamentais que fazem parte de um sistema com a utilização de RFID (CARDOSO, 2000).

Quadro 1. Elementos Estruturantes do RFID

ELEMENTO ESTRUTURANTE	DESCRIÇÃO
Transponder (Tags)	Transmite e responde aos comandos que chegam por radiofrequência. Sua estrutura básica é bem simples: um chip capaz de armazenar informações e uma resistência fazendo o papel de antena, envoltos por algum material como plástico ou silicone, em um determinado formato.
Tags Passivas	Não possuem fonte de alimentação própria e funcionam a partir da energia enviada pelo sinal do leitor. É o tipo mais usado por serem mais simples e baratas, pois não possuem bateria nem transmissor.
Tags 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 muito superior em comparação com as passivas.
Antena	Transforma a energia eletromagnética guiada pela linha de transmissão em energia eletromagnética irradiada e vice-versa. O tipo de antena utilizada, assim como o seu layout, são fatores determinantes para o alcance das tags.
Leitor	Realiza a comunicação com as Tags através da antena e repassar a informação para o software.
Controlador	É responsável por controlar o leitor. Eles podem variar em complexidade, sendo desde um pequeno leitor embarcado em um palmtop ou celular até um microcomputador com sistema servidor e várias funcionalidades.

Fonte: Elaborado pelos autores adaptado de Cardoso, 2000, Dobkin (2012), Glover (2007), Greef (2002), Heckel (2018), Santini (2008).

Segundo FAHL (2005) e AHSON e ILYAS (2008), para que se possa utilizar um sistema de controle de entrada e saída de pessoas usando a tecnologia RFID, sem causar problemas, e com o máximo de aproveitamento, existem algumas recomendações de inclusões de hábitos ou mudanças de conduta aos usuários. Fazendo bom uso do equipamento e respeitando essas recomendações, pode-se garantir o funcionamento adequado do sistema.

As principais recomendações para a utilização dessa tecnologia descrita acima estão descritas no Quadro 2.

Quadro 2. Recomendações

RECOMENDAÇÕES	DESCRIÇÃO
Porte da Tag	O usuário do sistema deve estar sempre de posse da sua *tag* RFID, pois sem ela, o leitor não poderá identificar a sua passagem e localização.
Uso da Tag	O usuário não pode trocar ou emprestar a sua *tag*, pois enquanto um ID estiver cadastrado no sistema associado a um nome, a *tag* deve ser de uso pessoal e intransferível.
Leitura da Tag	O usuário deve sempre se certificar de que a sua *tag* realmente foi lida pelo leitor. Esta verificação pode ser efetuada através de mensagens visuais ou avisos sonoros. Pode ocorrer de o leitor demorar alguns segundos para reconhecer a *tag*, por uma interferência momentânea por exemplo. Caso a tag não seja reconhecida pelo leitor, o registro do acesso no banco de dados não será realizado.

Fonte: Elaborado pelos autores adaptado de FAHL (2005) e AHSON e ILYAS (2008).

3. PERCURSO METODOLÓGICO

A metodologia utilizada neste artigo foi a pesquisa bibliográfica e documental, baseada em materiais que já foram publicados, principalmente em artigos científicos, teses e dissertações disponibilizados pela internet em diversos bancos de pesquisa.

Segundo Gil (2017), a pesquisa bibliográfica tem a finalidade de conhecer os posicionamentos de diversos autores sobre o assunto em pauta, permitindo alcançar o objetivo com conceitos válidos, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões.

Nesse sentido, o objetivo da pesquisa bibliográfica foi identificar, através das informações sugeridas pelas propostas dos autores, no que diz respeito ao controle de acesso de pessoas em ambientes restrito, utilizando a tecnologia RFID, fosse proposto por esse artigo uma solução para o controle de fluxo de pessoas dentro uma instituição pública.

A estrutura proposta compõe-se de um sistema operacional em modo servidor de rede que hospeda um servidor de banco de dados e um servidor web. O processo de implantação de um sistema está apresentado na Figura 2.

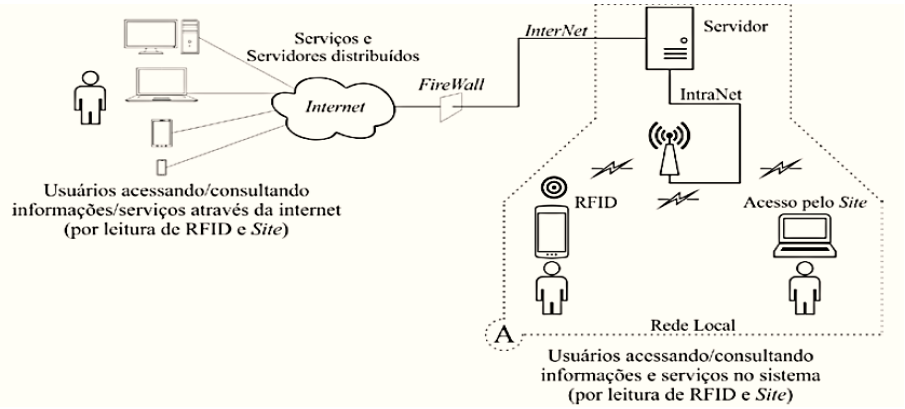


Figura 2. Estrutura de um projeto. Fonte: Hippert; Longo; Moreira (2019)

4. RESULTADOS

Como proposto na Figura 3, constante no percurso metodológico, o sistema funcionará com a instalação de leitores no portal de acesso da entrada dos servidores e terceirizados, na portaria de entrada dos visitantes, e em pontos previamente selecionados dos prédios, notadamente em pontos que cubram áreas sensíveis do prédio, permitindo assim a captura de informações sobre o deslocamento das pessoas e, no caso de servidores e de terceirizados, substituirá o ponto eletrônico. Nesta configuração, o sistema possibilitará a captura de informações para alimentação do banco de dados a ser analisado pelos algoritmos de IA. Após o horário de expediente, o sistema alertará sobre a permanência de pessoal nos prédios e fornecerá informações sobre sua movimentação e localização presumida.

Para atender a estes requisitos, o projeto prevê o uso de um sistema RFID de ultra alta frequência (UHF), com alcance e capacidade de leitura elevados, utilizando o protocolo EPC Gen 2 (ISO 18000-6C), o que permitirá atender aos requisitos de distância para a captura de dados das *tags*, bem como a diretiva de segurança do sistema.

Cada servidor terá um crachá com um chip/etiqueta previamente cadastrada no software de controle, com as informações básicas para a sua identificação, como: nome, matrícula ou identificação, cargo, setor de trabalho e outros.

No caso dos visitantes, será feita a entrega de um crachá genérico, que será na mesma hora, linkado com a foto da carteira de identidade ou outro documento utilizado, e informações que permitam um controle básico de trânsito. A devolução do documento só será efetuada após a entrega do crachá com a *tag* de identificação.

Todas as antenas estarão ligadas ao *data center*, e transmitirão todas as informações de acesso e movimentação por meio da rede lógica. Nas portarias e no portal do prédio principal, haverá terminais de alimentação que serão utilizados para a inserção de informações referentes aos visitantes e para consulta dos dados cadastrados. A figura 3 mostra o fluxograma proposto para o sistema.

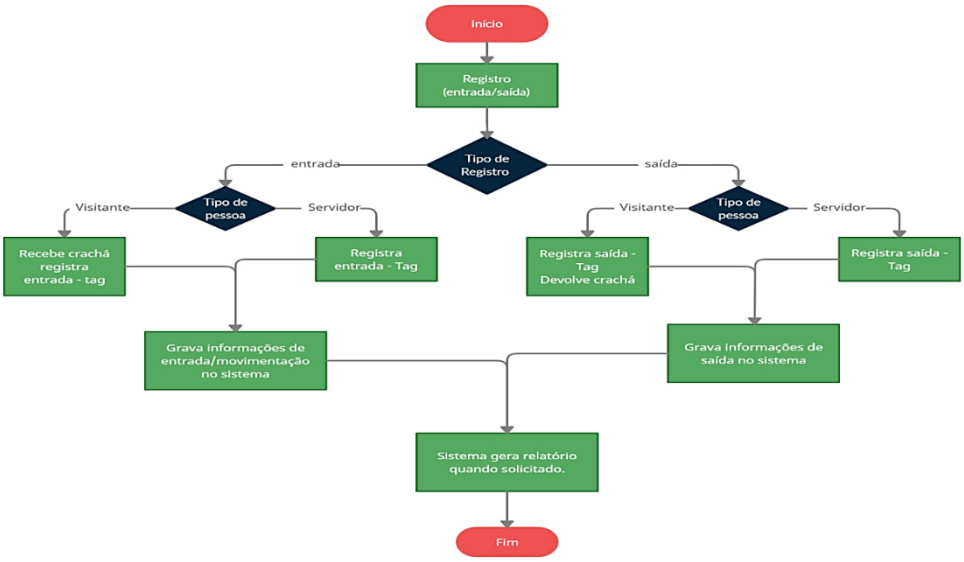


Figura 3. Fluxograma da Proposta do Sistema. Fonte: Elaborado pelos autores (2023)

Um sistema de controle de acesso RFID, não representa um grande impacto ou intensas mudanças de rotina no cotidiano das pessoas. A praticidade e a discrição são características marcantes da aplicação de controle de entradas e saídas usando a tecnologia RFID. Após a instalação e o cadastramento dos usuários, o usufruto desta tecnologia será quase imperceptível. O servidor ou visitante poderá passar por leitores localizados em pontos estratégicos, registrar a sua movimentação e ao final do mês, poderá consultar um relatório com o seu histórico de movimentações nas dependências da instituição. Existe a possibilidade de uma má leitura, fazendo com que o usuário tenha que repetir o procedimento de identificação, no entanto, ao comparar com outras tecnologias, como código de barras e biometria, o RFID apresenta melhores resultados.

As vantagens são: controle de acesso de servidores e visitantes em tempo real, com localização precisa dos deslocamentos; avaliação da produtividade dos e prestadores de serviços, acompanhamento dos visitantes; sistema prático e de fácil manuseio; de baixo custo de investimento; confecção de relatórios para geração do ponto eletrônico de frequência dos servidores. Em contrapartida temos as seguintes desvantagens: falta de colaboradores treinados para manusear o equipamento e o software; sistema de redundância; dependência de energia elétrica para funcionar.

5. CONCLUSÃO

A tecnologia RFID surgiu há várias décadas, entretanto está em crescimento contínuo e a cada dia aumenta o número de aplicações, devido, principalmente, a redução dos custos dos componentes. Com a sua popularidade, o custo com a implementação em larga escala tende a reduzir. Um sistema de controle de fluxo de pessoas utilizando a tecnologia de RFID pode se adequar muito bem a situações reais vividas nas instituições. Esse sistema possui uma grande utilidade, pois através da aplicação de controle de fluxo desenvolvido, é possível controlar o acesso a áreas consideradas restritas, registrar o horário de entrada e saída de cada usuário e até o deslocamento deles pela empresa ou instituição.

Nesse intuito, este trabalho foi norteado pela relevância em expor, com o auxílio da literatura e de pesquisas realizadas, o grande diferencial competitivo que esta tecnologia possui em comparação com as demais. O campo de aplicação desta tecnologia é vasto e permite a sua utilização na identificação animal e até em sistemas de pagamento automático.

No entanto, durante as pesquisas para a elaboração deste artigo, verificou-se que é necessário um mínimo de conhecimento para entender esta tecnologia e, que através de uma simulação de aplicação, é possível verificar sua viabilidade e uso real.

A tecnologia RFID está consolidada como uma das principais ferramentas para controle de acesso em edifícios, oferecendo conveniência, eficiência e flexibilidade. No entanto, a segurança continua sendo um desafio, especialmente devido à vulnerabilidade da comunicação sem fio. A implementação de medidas robustas de criptografia, autenticação e integração com outras tecnologias, como biometria e IA, é fundamental para garantir que os sistemas RFID continuem sendo seguros e eficazes no futuro. A evolução dessa tecnologia e suas soluções de segurança permitirão que a RFID continue sendo uma escolha atraente para sistemas de controle de acesso em um mundo cada vez mais conectado.

REFERÊNCIAS

Cardoso, F. de S. (2000). Contribuição ao desenvolvimento de um sistema de identificação por rádio frequência para aplicações hospitalares. Dissertação (Mestrado em Engenharia Biomédica) — Área de Instrumentação Biomédica, Universidade Federal da Paraíba, João Pessoa.

Ciriaco, Douglas (2024). Como funciona o RFID? Disponível em https://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm, acessado em 15 de abril de 2024.

Chagas, João Maros Ayrolla Navega; Pimentel, Julia Silva (2017). Aplicação de tecnologia smart card e RFID no ambiente universitário – Rio de Janeiro: UFRJ/ Escola Politécnica.

Cunha, R. P. O. (2005). Uso da tecnologia RFID no gerenciamento de uma cadeia de suprimentos. Dissertação (Bacharelado) — Engenharia da Computação, Faculdade de Engenharia de Sorocaba, Sorocaba.

Dastres Roza ; Soori, Mohsen; Asamel, Mohammed (2022). Radio frequency identification (RFID) based wireless manufacturing systems, a review. Independent Journal of Management & Production, ISSN-e 2236-269X, Vol. 13, Nº. 1, pags. 258-290

Dobkin, D. M. (2008). The RF in RFID passive UHF RFID in practice. [S.l.]: Elsevier.

Duarte, J. A. M (2005). Automação do sistema de ordem de serviço e formação de trens em pátios. In: Revista Ferroviária. Disponível em: Acesso em 20 mar 2021.

Fahl, C. R. (2005). Um estudo sobre a viabilidade de implantação de etiquetas inteligentes como vantagem competitiva em um centro de distribuição. Dissertação (Monografia) — Instituto Paulista de Ensino e Pesquisa - Centro de Pós-graduação, Gestão de Negócios em Logística e Transportes, Campinas.

Gil, Antonio Carlos (2017). Como elaborar projetos de pesquisa – 6ª ed. – São Paulo : Atlas.

Glover, B.; Bhatt, H. (2007). Fundamentos de RFID. [S.l.]: Alta Books.

Greff, P. de A. (2009). Especificação de um sistema para monitoramento de atividades de natação usando RFID. Dissertação (Tecnólogo) — Curso Superior de Tecnologia em Sistemas de

Telecomunicações, Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina - Campus São José, São José - SC, Outubro.

Hippert, M. A. S.; Longo, O. C.; Moreira, A. C. (2019). RFID na edificação: proposta de modelo de sistema para organização das informações de manutenção. Ambiente Construído, Porto Alegre, v. 19, n. 4, p. 155-173, out./dez.

UFRJ (2024). Identificação por rádio frequência. Disponível em https://www.gta.ufrj.br/grad/15_1/rfid/etiquetas.html, acesso em 21 mar 2024.

Nunes, Joao Victor; Fernandes, Thiago Rocha; Oliveira, Sonagno de Paiva (2015). Aplicação do sistema RFID no controle de acesso de veículos em condomínios. XXXV Encontro Nacional De Engenharia De Produção.

Oliveira, S. B. Z. de; Lima, D. R. G. de; Oliveira, L. da S. (2018). Controle de acesso de pessoas em ambientes restrito, utilizando a tecnologia rádio frequência e identificação - (RFID).

Pizzetti, M. C. (2007). Uma abordagem estratégica de integração da tecnologia RFID. 80f. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Florianópolis.

Puhlmann, H. F. W. (2021). Introdução à tecnologia de identificação RFID. Disponível em: https://www.researchgate.net/publication/277954223, PESQUISADO EM 20 março de 2021.

Santini, Arthur Gambin. (2008). RFID: Conceitos, aplicabilidade e impactos. 1ª ed. Rio de Janeiro: Ciência Moderna.

Souza, P. H. M. de; Cavallari Jr., S. J.; Delgado Neto, G. G. (2017). Indústria 4.0: contribuições para setor produtivo moderno. XXXVII Encontro Nacional De Engenharia De Produção.

Teixeira, Tiago (2011). Controle de fluxo de pessoas usando RFID. 72 p. Monografia (Curso Superior de Tecnologia em Sistemas de Telecomunicações) – Instituo Federal de Santa Catarina.

Vieira, Jéssica Mota et al. (2015). Análise do sistema RFID para monitoração de equipamentos de laboratórios. Revista Principia - Divulgação Científica e Tecnológica do IFPB, Paraíba, n. 22, p. 23-27. ISSN 2447-9187.

Vieira, I. M. M.; Muniz, E. C. L.; Santos, C. J.; Oliveira, H. B. J.; Souza, L. C. G. (2019). O uso da RFID em sistemas hospitalares: uma análise de periódicos internacionais. Gepros. Gestão da Produção, Operações e Sistemas, v. 14, n. 2, p. 55 - 74. DOI: 10.15675/gepros.v14i2.2160 . Acessado em: 19 Mar 2021.

Wang, Xiaoxu; Wang, Yuesheng (2018). An office intelligent access control system based on RFID. The 30th chinese control and decision conference (2018 ccdc). Acessado em: 20 Mar 2024.

Zagonel, Mateus Victorio; Machado, Cristian Cleder; Mônego, Cassiano (2017). Tecnologia RFID: um estudo de caso para controle de acesso em escolas. Revista de Engenharia, Computação e Tecnologia, v. 01, n. 01, p. 31-38, novembro.

Zimpel, C. et al. (2015). RFID e rastreabilidade de estoque. Paraná Cooperativo – Técnico e Cientifico. Curitiba, v. 11, n. 130, p. 01-80, Dezembro.