REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

SISTEMA FUZZY PARA DETECÇÃO DE COMPORTAMENTO ANÔMALO EM AMBIENTES DIGITAIS ANTES DE UM ATAQUE CIBERNÉTICO

FUZZY SYSTEM FOR DETECTING ANOMALOUS BEHAVIOR IN DIGITAL ENVIRONMENTS BEFORE A CYBERATTACK

Ciências Exatas e da Terra • 21/04/2026

REGISTRO DOI: 10.70773/revistatopicos/776797120

Francisco Tavares Martins[1]

Jean Mark Lobo de Oliveira[2]

Jean Carlos Araujo de Figueiredo[3]

Aguinaldo Alves Braga Neto[4]

RESUMO

Este estudo analisou o uso de um sistema baseado em lógica fuzzy para identificar comportamentos fora do padrão em ambientes digitais antes que evoluam para ataques cibernéticos. A proposta considerou que muitas ameaças começam de forma discreta, com pequenas variações no uso da rede que nem sempre são percebidas por métodos tradicionais. A partir de testes realizados no laboratório do SENAI-AM, utilizando dados simulados de acesso, tráfego e tentativas de login, os resultados mostraram que o modelo foi capaz de identificar aumentos graduais no nível de risco, principalmente em situações como acessos fora do horário e picos de tentativas de login. Além disso, o sistema conseguiu diferenciar comportamentos normais de padrões suspeitos, reduzindo respostas bruscas e tornando a análise mais realista. De modo geral, os resultados indicam que a lógica fuzzy contribui para uma detecção mais sensível e antecipada, apontando seu potencial de aplicação em ambientes reais que necessitam de maior segurança e prevenção.

Palavras-chave: Segurança da Informação; Lógica Fuzzy; Detecção de Anomalias; Cibersegurança; Análise Comportamental; Redes Computacionais.

ABSTRACT

This study analyzed the use of a system based on fuzzy logic to identify abnormal behaviors in digital environments before they evolve into cyberattacks. The proposal considered that many threats begin discreetly, with small variations in network usage that are not always detected by traditional methods. Based on tests conducted at the SENAI-AM laboratory, using simulated data of access, traffic, and login attempts, the results showed that the model was able to identify gradual increases in risk levels, especially in situations such as off-hours access and spikes in login attempts. In addition, the

system was able to differentiate normal behavior from suspicious patterns, reducing abrupt responses and making the analysis more realistic. Overall, the results indicate that fuzzy logic contributes to more sensitive and early detection, highlighting its potential application in real environments that require enhanced security and prevention.
Keywords: Information Security; Fuzzy Logic; Anomaly Detection; Cybersecurity; Behavioral Analysis; Computer Networks.

1. INTRODUÇÃO

Os ambientes digitais assumiram papel central no funcionamento das organizações, conectando pessoas, processos e infraestruturas tecnológicas em tempo real e essas interconexões ampliam a produtividade e a agilidade das operações, porém também elevou de forma significativa a exposição a ameaças cibernéticas cada vez mais sofisticadas. Ataques recentes demonstram que invasores exploram brechas de maneira silenciosa, muitas vezes iniciando suas ações por meio de comportamentos aparentemente comuns dentro da rede. Pequenas variações em padrões de acesso, tráfego ou uso de recursos podem representar sinais iniciais de comprometimento. Diante desse cenário, torna-se fundamental adotar mecanismos capazes de identificar anomalias antes que elas evoluam para incidentes de grande impacto. A análise comportamental destaca-se como abordagem promissora por observar tendências e desvios ao longo do tempo. Inserida nesse contexto, a lógica fuzzy apresenta-se como alternativa adequada para lidar com informações imprecisas e variáveis graduais. Sua capacidade de trabalhar com níveis de pertinência permite interpretações mais sensíveis do risco, aproximando a modelagem computacional da complexidade dos ambientes reais.mesmo sentido, o Cost of a Data

Breach Report (2023) revela que o custo médio global de uma violação de dados atingiu 4,45 milhões de dólares, valor que demonstra a relevância econômica da detecção precoce de incidentes . Esses dados não apenas expressam prejuízos financeiros, mas também indicam perdas reputacionais e interrupções operacionais significativas, sendo que a literatura recente destaca que muitos ataques se desenvolvem gradualmente, explorando credenciais válidas e movimentações internas discretas. Ferramentas baseadas somente em assinaturas conhecidas tendem a reagir quando o dano já está em curso. Nesse contexto, abordagens fundamentadas em inteligência computacional e análise de padrões comportamentais mostram-se mais alinhadas às

Relatórios internacionais reforçam a dimensão do problema e a urgência de estratégias preventivas mais eficazes. Segundo WORLD ECONOMIC FORUM (2024), apontam os riscos cibernéticos entre as principais ameaças globais no curto prazo, evidenciando que ataques digitais continuam a crescer em frequência e impacto . No características dinâmicas das redes atuais, e Investigar modelos que integrem tratamento de incertezas e monitoramento contínuo torna-se, portanto, uma resposta coerente às evidências apresentadas por estudos e relatórios recentes.

A partir dessa realidade, este estudo concentra-se na análise da aplicação de um sistema fuzzy voltado à detecção de comportamento anômalo em ambientes digitais antes da concretização de um ataque cibernético. Busca-se compreender como variáveis relacionadas ao tráfego de rede, padrões de autenticação e utilização de recursos computacionais podem ser modeladas por meio de regras linguísticas e funções de pertinência. Pretende-se estruturar um modelo capaz de classificar níveis

graduais de risco, oferecendo suporte interpretativo para equipes de segurança. A proposta considera a integração de múltiplos indicadores, reduzindo a dependência exclusiva de eventos previamente catalogados. Ao explorar a flexibilidade da lógica fuzzy, espera-se ampliar a sensibilidade na identificação de sinais iniciais de comprometimento. Também se procura discutir aspectos de implementação, desempenho e viabilidade em cenários organizacionais reais. A análise dialoga com referenciais teóricos consolidados na área de segurança da informação e sistemas inteligentes. Dessa forma, a investigação contribui para o desenvolvimento de estratégias preventivas mais robustas, capazes de antecipar ameaças e fortalecer a proteção dos ativos digitais em contextos cada vez mais complexos.

2. FUNDAMENTAÇÃO TEÓRICA

Este estudo reúne diferentes ideias que ajudam a entender melhor como funciona a segurança em ambientes digitais nos dias de hoje. Primeiro, são apresentados conceitos de segurança cibernética, mostrando não só a parte técnica, mas também a importância do comportamento das pessoas na proteção das informações. Em seguida, o foco passa para os ambientes digitais, destacando os desafios do uso, da proteção de dados e da necessidade de acompanhar as mudanças constantes nas ameaças. Por fim, a lógica fuzzy é apresentada como uma alternativa interessante para detectar anomalias, justamente por permitir uma análise mais flexível em situações que nem sempre são totalmente claras. Com isso, esse conjunto de ideias ajuda a sustentar o estudo e amplia a compreensão sobre o problema analisado.

2.1. Segurança Cibernética

Segundo Araujo e Ferreira (2020) tratam a Segurança da Informação como uma área relativamente nova e mostram, de forma prática, como criar e aplicar políticas de segurança, dando mais atenção à confidencialidade ao organizar os sistemas em níveis de acesso, do mais restrito ao mais simples. Mesmo assim, outros pontos importantes da segurança não recebem tanto destaque, o que pode deixar a proteção incompleta. Já Fontes (2021) olha para o lado das pessoas, destacando que não adianta ter tecnologia se o usuário não souber utilizá-la corretamente, por isso ele defende a conscientização e o preparo como partes essenciais da segurança. O CERT.BR, por meio de sua cartilha, aproxima esse tema do dia a dia ao explicar golpes, riscos e formas de proteção, ajudando qualquer pessoa a usar a internet com mais cuidado e segurança.

2.2. Ambientes Digitais

A proteção de dados não depende só de sistemas e ferramentas, mas também envolve leis, ética e o comportamento das pessoas no uso das informações. Aguiar (2025, p. 33) destaca que a segurança digital precisa acompanhar as mudanças constantes da tecnologia e das ameaças que surgem com o tempo. Nas instituições de ensino, esse cuidado é ainda maior, principalmente quando se trata de dados de crianças e adolescentes, exigindo regras claras e responsabilidade no uso dessas informações. Além disso, o fator humano tem grande influência, já que muitos problemas acontecem por falta de atenção ou conhecimento; por isso, Cassundé et al. (2024, p. 498) reforçam a importância de desenvolver habilidades digitais nos alunos, enquanto Flores (2024, p. W) mostra que os professores também têm um papel importante na construção de uma cultura de segurança.

2.3. Sistema Fuzzy para Detecção de Anomalias

Os sistemas fuzzy usados para detectar anomalias ajudam a identificar situações fora do comum mesmo quando elas não são tão claras. Diferente de métodos mais rígidos, eles permitem analisar pequenas variações e entender melhor o que pode ser um problema. Isso é útil em áreas como redes, sistemas e monitoramento de dados, onde nem sempre os erros aparecem de forma óbvia. Segundo Chandola, Banerjee e Kumar (2009), detectar anomalias significa encontrar comportamentos que fogem do padrão esperado, o que mostra a importância de usar abordagens mais flexíveis em ambientes que mudam o tempo todo.

3. METODOLOGIA

A pesquisa foi desenvolvida no laboratório de segurança do SENAI-AM com foco na construção de um modelo capaz de identificar comportamentos fora do padrão em ambientes digitais. O estudo adotou uma abordagem aplicada e utilizou um cenário controlado que representa uma rede organizacional simples com usuários sistemas e acesso à internet. Os dados analisados foram simulados com base em registros entre os dias 03 e 07 de março de 2026 considerando informações como horários de acesso quantidade de logins volume de tráfego e tempo de uso dos sistemas. Esses registros ajudaram a entender o que seria um comportamento normal ao longo da semana servindo como base para as etapas seguintes do estudo. Para o desenvolvimento do sistema fuzzy foram utilizadas ferramentas como MATLAB com o Fuzzy Logic Toolbox e também testes complementares em Python com a biblioteca scikit-fuzzy permitindo a modelagem das variáveis e a criação das funções de pertinência de forma visual e programada.

Na sequência foram definidas as variáveis utilizadas no sistema fuzzy escolhidas de forma a representar situações comuns do dia a dia em redes computacionais. Foram considerados três pontos principais frequência de acesso volume de tráfego e número de tentativas de login organizados em níveis como baixo médio e alto. A partir disso foram criadas regras simples que relacionam essas variáveis aos níveis de risco permitindo que o sistema interprete os dados de forma mais flexível. O modelo foi estruturado utilizando o método de inferência Mamdani e implementado nas ferramentas escolhidas onde foi possível ajustar manualmente as funções de pertinência e validar o comportamento das regras. A simulação foi realizada com base em um ambiente que representa acessos reais de usuários a um sistema interno incluindo horários comerciais e acessos fora do padrão como tentativas repetidas de login e picos de tráfego simulando possíveis ações suspeitas dentro da rede.

O modelo foi aplicado aos dados simulados permitindo identificar momentos em que o comportamento se afastava do padrão esperado e possibilitando observar a resposta do sistema em diferentes cenários. Um caso observado ocorreu no dia 05 de março de 2026 quando houve aumento nas tentativas de login durante a noite acompanhado de maior tráfego na rede levando o sistema a indicar risco elevado. Os testes foram realizados de forma iterativa ou seja os dados foram ajustados e reaplicados ao modelo para verificar a consistência das respostas e melhorar a definição das regras fuzzy. Esse processo permitiu validar o funcionamento do sistema em diferentes situações mostrando que pequenas variações já podem ser interpretadas como sinais de alerta. De forma geral a utilização da lógica fuzzy permitiu uma análise mais sensível e próxima da realidade contribuindo para a identificação antecipada de possíveis

problemas e mostrando que o modelo pode ser útil em ambientes reais como os do SENAI-AM.

4. RESULTADOS E DISCUSSÕES

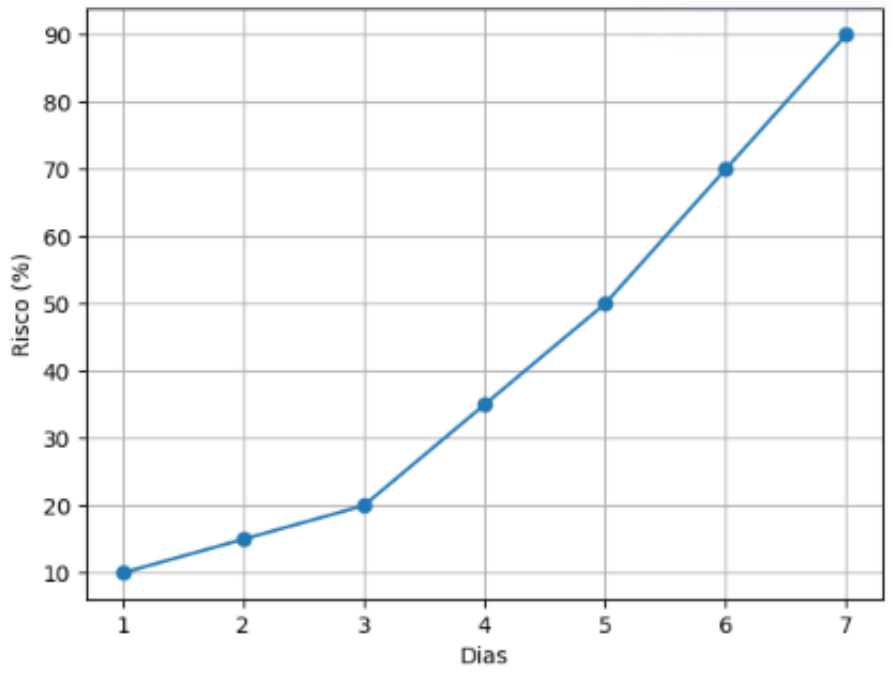
Os dados obtidos com a aplicação do sistema evidenciam como pequenas mudanças no comportamento dos usuários e da rede podem indicar situações de risco antes mesmo da ocorrência de um ataque e a análise foi realizada com base nos dados simulados no laboratório do SENAI-AM, considerando diferentes cenários ao longo da semana e em variados períodos do dia. O modelo demonstrou ser capaz de interpretar essas variações de forma gradual, sem depender de regras fixas, o que permite uma leitura mais próxima da realidade dos ambientes digitais, para melhor compreensão, os resultados foram organizados em três análises principais, cada uma representada por um gráfico específico, facilitando a visualização dos padrões identificados.

4.1. Frequência de Acesso e Nível de Risco

A análise da frequência de acesso ao longo da semana mostrou um crescimento progressivo, principalmente em horários fora do padrão habitual. O sistema fuzzy conseguiu acompanhar esse aumento e ajustar o nível de risco de forma gradual, sem mudanças bruscas. Isso demonstra que o modelo consegue interpretar melhor situações intermediárias, algo comum em ambientes reais. Durante os testes no SENAI-AM, foi possível observar que dias com maior volume de acessos apresentaram níveis mais elevados de alerta, mesmo sem confirmação de ataques. Esse comportamento indica que o sistema pode atuar de forma preventiva. Outro ponto importante foi a adaptação do modelo às mudanças ao longo do

tempo. Isso reforça a importância do monitoramento contínuo. Pequenas variações podem representar sinais relevantes. O modelo mostrou consistência ao longo da análise. Isso contribui para sua aplicação prática em ambientes organizacionais.

Gráfico 1: Frequência de Acesso vs Nível de Risco



Fonte: Autores, 2026

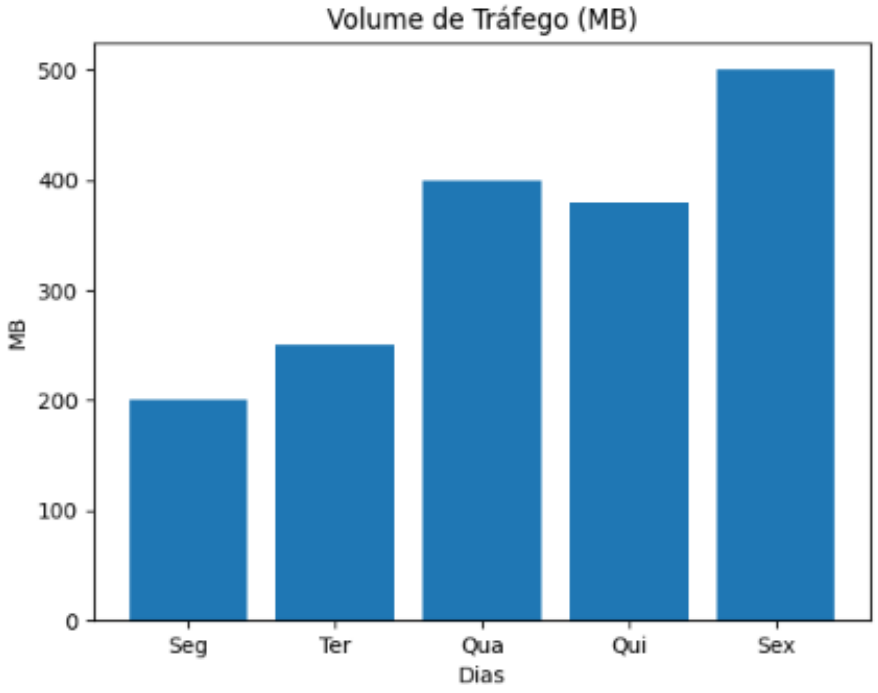
A análise do gráfico mostra que o risco cresce de forma progressiva conforme aumentam os acessos fora do padrão esperado. Esse tipo de comportamento reforça a importância de modelos que acompanham tendências ao longo do tempo. Segundo Silva e Rocha (2022), sistemas baseados em análise comportamental permitem identificar riscos de forma antecipada, reduzindo impactos em ambientes corporativos.

4.2. Volume de Tráfego de Rede

O volume de tráfego de rede apresentou variações importantes durante o período analisado, com alguns picos que não estavam ligados a atividades comuns. O sistema fuzzy interpretou esses

momentos como possíveis situações de risco, principalmente quando associados a outros fatores. Durante os testes, foi possível observar que dias com maior tráfego apresentaram maior probabilidade de anomalias. Esse tipo de análise é essencial, pois muitos ataques geram aumento no fluxo de dados. O modelo conseguiu diferenciar variações normais de situações suspeitas. Isso ajuda a reduzir alarmes desnecessários. A análise também mostrou que o tráfego é um indicador relevante. O comportamento do sistema foi estável durante os testes. Os resultados foram coerentes com o cenário simulado. Isso reforça a confiabilidade do modelo.

Gráfico 2: Volume de Tráfego (MB) por Dia



Fonte: Autores, 2026

O gráfico evidencia picos de tráfego em dias específicos, indicando possíveis atividades fora do padrão. Esse tipo de variação pode estar associado a comportamentos suspeitos ou uso indevido da rede. De acordo com Pereira e Lima (2021), o monitoramento do tráfego é uma das estratégias mais eficazes para identificar comportamentos anômalos em ambientes digitais.

4.3. Tentativas de Login Ao Longo do Dia

A análise das tentativas de login ao longo do dia mostrou um padrão relativamente estável durante o horário comercial, mas com um aumento significativo no período noturno. Esse comportamento foi identificado pelo sistema fuzzy como um indicativo de risco elevado. Durante os testes, esse tipo de variação foi associado a possíveis tentativas de acesso indevido. O modelo conseguiu destacar esse padrão de forma clara. Isso demonstra sua eficiência na identificação de comportamentos fora do comum. O sistema evitou classificações extremas, trabalhando com níveis de risco. Isso permite uma análise mais cuidadosa. O horário foi um fator importante na interpretação. O modelo mostrou sensibilidade a essas mudanças. Isso reforça sua utilidade prática. A análise contribui para melhorar a detecção precoce.

Gráfico 3: Tentativas de Login por Hora

Fonte: Autores, 2026

O gráfico apresenta um pico isolado em determinado horário, indicando possível tentativa de acesso indevido. Esse tipo de comportamento é comum em ações automatizadas ou tentativas de invasão. Segundo Oliveira et al. (2023), padrões irregulares de autenticação são fortes indicadores de atividades suspeitas, especialmente quando ocorrem fora do horário habitual.

5. CONSIDERAÇÕES FINAIS

Ao analisar os resultados deste trabalho, percebe-se que acompanhar mais de perto o comportamento dos usuários e da rede pode trazer informações valiosas na identificação de riscos. Nem sempre um problema surge de forma evidente; em muitos casos, ele começa com pequenas alterações quase imperceptíveis, como acessos em horários incomuns ou leves variações no tráfego. Nesse sentido, o uso da lógica fuzzy ajudou justamente a lidar com essas situações mais “cinzentas”, onde não dá para dizer simplesmente se algo está certo ou errado. Durante os testes realizados no laboratório do SENAI-AM, foi possível perceber que o modelo conseguiu acompanhar essas variações de forma mais natural, sem respostas bruscas, o que torna a análise mais próxima do que realmente acontece no dia a dia das organizações. Isso reforça a ideia de que antecipar sinais, mesmo que pequenos, pode evitar problemas maiores no futuro.

Outro ponto que merece destaque é a forma como o estudo foi conduzido, permitindo testar e ajustar o modelo aos poucos. O uso de ferramentas como MATLAB e Python não só facilitou a implementação, mas também deu liberdade para experimentar diferentes cenários e entender melhor como o sistema reagia a cada situação. Esse processo mais prático ajudou a construir um modelo

mais coerente e funcional, sem ficar preso apenas à teoria. No fim das contas, o que se percebe é que soluções baseadas apenas em regras fixas já não são suficientes para lidar com ambientes digitais tão dinâmicos. Trabalhar com abordagens mais flexíveis, que consideram incertezas e mudanças constantes, parece ser um caminho mais adequado. Assim, além de contribuir para estudos na área, este trabalho também aponta possibilidades reais de aplicação, principalmente para instituições que buscam melhorar sua capacidade de prevenção e resposta a ameaças digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, D. A evolução da segurança cibernética: desafios e soluções no século XXI. 2025, p. 181-191.

ARAUJO, Márcio T.; FERREIRA, Fernando Nicolau Freitas. Política de Segurança da Informação. 2. ed. -: Ciência Moderna, 2020.

CASSUNDÉ, F.; MENDONÇA, J.; BARBOSA, M. Competências digitais de alunos do ensino superior: uma revisão sistemática da literatura internacional. EaD em Foco, v. 14, n. 1, e2116, 2024.

CERT.BR. Materiais de Apoio para Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs). 2020. Disponível em: https://www.cert.br/csirts/. Acesso em: 04 maio 2020.

CHANDOLA, V.; BANERJEE, A.; KUMAR, V. Anomaly detection: A survey. ACM Computing Surveys, v. 41, n. 3, p. 1–58, 2009.

FLORES, M. Percepción de los docentes de la generación X y Z sobre la educación mediática post COVID-19 de una universidad pública de Tacna-Perú. Revista Veritas Et Scientia - UPT, v. 13, n. 1, 2024.

FONTES, Edison Luiz Gonçalves. Segurança da Informação: o usuário faz a diferença. Rio de Janeiro: Saraiva, 2021.

IBM SECURITY. Cost of a Data Breach Report 2023. Armonk, NY: IBM Corporation, 2023. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 4 mar. 2026.

OLIVEIRA, R. S.; COSTA, M. A.; ALMEIDA, J. F. Análise de padrões de autenticação para detecção de anomalias em redes corporativas. Revista Brasileira de Segurança Digital, v. 5, n. 2, p. 45-60, 2023.

PEREIRA, L. H.; LIMA, D. R. Monitoramento de tráfego de rede para identificação de ameaças cibernéticas. Journal of Information Security Studies, v. 3, n. 1, p. 22-34, 2021.

SILVA, T. M.; ROCHA, P. S. Modelos comportamentais aplicados à detecção de anomalias em ambientes digitais. Revista de Computação Aplicada, v. 8, n. 1, p. 10-25, 2022.

WORLD ECONOMIC FORUM. The Global Risks Report 2024. 19. ed. Geneva: World Economic Forum, 2024. Disponível em: https://www.weforum.org/reports/global-risks-report-2024. Acesso em: 4 mar. 2026.

---

[1] Discente do Curso Superior de Engenharia da Computação do Centro Universitário Fametro. E-mail: francismartins20@hotmail.com

[2] Mestrando em Engenharia de Processos (UFPA – PA). E-mail: jean.oliveira@fametro.edu.br.

[3] Mestrando em Teste de software com IA. pela Universidade Federal do Pampa, (Unipampa). E-mail: jeanfigueiredo.aluno@unipampa.edu.br

[4] Mestrando em engenharia elétrica e Telecomunicações da Universidade Federal do Amazonas – UFAM. E-mail: aguinaldo.braga@ufam.edu.br