INSERÇÃO DE CONCEITOS DE CRIPTOGRAFIA NO CURSO TÉCNICO EM INFORMÁTICA VIA RELAÇÃO COM A FÍSICA QUÂNTICA

Érica de Araujo Castro [1]
Marina Silva de Medeiros [2]
Stephanie Pereira de Medeiros[3]
Messias Vilbert Souza Santos [4]
Rafael Peixoto de Morais Pereira [5]

RESUMO

A formação de técnicos em informática dos Institutos Federais está baseada em: manutenção, programação e redes. Tal formatação deixa de lado a segurança da informação, relevante em qualquer transferência de dados. Esse artigo traz uma forma de inserir o estudo da criptografia através da interdisciplinaridade com a física quântica, dada a sua conexão com as perspectivas de uma nova criptografia. Uma palestra, que abordou tal relação, foi realizada e a percepção dos discentes sobre o tema, antes e depois, foi analisada. Os resultados evidenciam o êxito em conhecimento adquirido por parte dos alunos e a importância dessa temática como motivadora de engajamento na área.

Palavras-chave: Criptografia, Física quântica, Formação de técnicos, Interdisciplinaridade.

INTRODUÇÃO

O século XX foi marcado pelo avanço da tecnologia e por construções teóricas inovadoras. A física, por exemplo, impulsionou o avanço da ciência em áreas distintas e, consequentemente, gerou um grande impacto na sociedade (ZANOTTA et al.,2011). Esse contexto de inovação técnica/teórica continua presente nos dias atuais, principalmente no ramo da informática, motivo pelo qual atrai o interesse da população em geral, mais ainda dos jovens que veem nessa área uma boa oportunidade de trabalho e realizações.

Do ponto de vista das oportunidades, o Curso Técnico Integrado em Informática, oferecido nos campus do Instituto Federal, onde a modalidade integrada diz respeito ao ensino médio, torna-se a porta de entrada de muitos estudantes e é, por vezes, o primeiro contato com a informática em nível acadêmico. Dessa forma, a abrangência dos conteúdos, mesmo que de forma superficial, é crucial como norteador das possibilidades do técnico formado. Em

[1] Discentes do Curso Técnico em Informática do Instituto Federal - IFRN, ericacastro1011@gmail.com;
[2] Discentes do Curso Técnico em Informática do Instituto Federal - IFRN, marina.mdrsjs@gmail.com;
[3] Discentes do Curso Técnico em Informática do Instituto Federal - IFRN, stepmedeiros7@gmail.com;
[4] Doutor em física pela Universidade Federal de Pernambuco - UFPE, messias.vilbert@ifrn.edu.br;
[5] Mestre em ensino pela Universidade Estadual do Rio Grande do Norte - UERN, rafael.moraes@ifrn.edu.br

consonância com a ideia de uma formação mais abrangente, torna-se importante que as disciplinas regulares do ensino médio aportem, sempre que possível, conhecimentos que remetam a sua relação com a informática, dando base para o desenvolvimento integral, mas também específico, do aluno.

Uma das disciplinas em que a relação citada é natural é a Física, que é dividida em três subáreas: a clássica, a moderna e a contemporânea. Por isso, o presente trabalho pautou-se dessa compreensão interdisciplinar e, exemplos reais da conexão entre Informática e Física foram utilizados como forma inserir o estudo da segurança da informação e criptografia no curso técnico, o que foi feito através de questionários (norteadores da atividade e avaliativo) e palestra. Um dos grandes exemplos da relação entre Física moderna e Computação tornou-se realidade prática em 2007 com o anúncio do primeiro computador quântico (Orion, Empresa Canadense D-Ware) (FAPESP,2007). Os conceitos físicos associados à sua concepção e a tecnologia aplicada prometem, por exemplo, superar a criptografia atual e impor um novo paradigma à área.

Dentro do contexto acima, a percepção da relação entre a Segurança da Informação e a Física Moderna torna-se importante para uma construção mais ampla do conhecimento da própria área e do cenário tecnológico por parte do aluno no que diz respeito às perspectivas, inclusive no sentido de seguir na área de Informática em cursos de graduação.

Mediante a aplicação de questionários e de uma palestra, este trabalho forneceu a possibilidade do vislumbre de que, como sociedade, estamos na era da informação, o que traz a necessidade da preservação e aprimoramento do sigilo das informações, acarretando na busca da evolução do conhecimento da física e dos métodos de criptografia que, embora proporcionem em nossos dias um bom nível de segurança (UNO;FALEIROS, s.d), podem, com a aplicação da física quântica, tornar-se obsoletos.

METODOLOGIA

A atividade foi realizada em um Instituto Federal de Educação, Ciência e Tecnologia e teve como público alvo alunos do 1° ao 4° ano dos turnos matutino e vespertino do Curso Técnico Integrado em Informática. A prática foi organizada em 3 fases, apontadas e detalhadas abaixo:

Fase I – Procurou-se investigar, por meio de um questionário, o conhecimento dos alunos sobre a temática e sobre a possível familiaridade a respeito da correlação entre a física e a criptografia, além das suas dificuldades de acesso a esse tipo de informação.

Fase II – A coleta e análise das informações do primeiro questionário auxiliou na constituição da aula em modelo de palestra e de um questionário avaliativo da mesma.

Fase III – Aplicação da palestra para os alunos; análise sobre o impacto que a mesma trouxe para os discentes via respostas do questionário avaliativo.

Inicialmente, a coleta de dados foi realizada através de um questionário eletrônico estruturado por questões abertas e fechadas, com nove perguntas. Obteve-se 70 respostas, sendo 19 do 1º ano, 25 do 2º ano, 18 do 3º ano matutino e vespertino e 8 do 4º ano. A partir do resultado, foi possível avaliar os conhecimentos prévios dos discentes com relação à segurança da informação e da sua correlação com a física.

Após essa etapa, houve a construção do modelo de aula em forma de palestra com duração de aproximadamente 90 minutos. Na palestra, foram abordados inicialmente os seguintes conteúdos: o conceito de criptografia, seu histórico e evolução ao longo do tempo, o conceito de chaves simétricas e assimétricas, a criptografia de chave pública do tipo RSA e sua confiabilidade em relação ao tempo computacional. Essa primeira parte da palestra foi ministrada por três discentes do Curso Técnico em Informática. Tais discentes são coautoras deste trabalho e foram acompanhadas pelos dois professores (um de física e outro de informática) responsáveis pelo estudo.

A segunda parte da palestra trouxe as novas ideias e inovações que remetem ao estudo da física quântica. Nessa parte, que ficou a cargo do professor de Física participante do estudo, foram discutidos os conceitos físicos sobre a dualidade onda partícula, a sobreposição de estados quânticos e o colapso da função de onda de um sistema quântico, por serem esses os assuntos relevantes no que diz respeito à transferência de informação quântica. Após a introdução desses conceitos fundamentais, foi possível demonstrar, por meio de exemplos simples, que o tipo de criptografia atual estaria vulnerável a um computador quântico, mas, em contrapartida, o mesmo pode gerar uma criptografia a priori inquebrável. Com isso, direcionou-se a palestra para a relação e a importância da criptografia quântica para a segurança futura. Assuntos como o interferômetro de Mach-Zehnder, a interpretação do paradoxo EPR por Artur Ekert e as ideias decorrentes, a polarização da luz, o entrelaçamento quântico e a desigualdade de Bell foram explicitados de forma geral, assim como foi abordado, a título de conhecimento, a construção de um computador quântico compatível com as necessidades atuais, os algoritmos já existentes e os desafios para uma evolução nessa área, como, por exemplo, a decoerência quântica e ruído térmico.

A palestra foi ministrada no dia 23 de novembro de 2018 no auditório do Instituto, na presença de 112 alunos do curso de informática e de professores, tanto da área técnica quanto da propedêutica. No fim da palestra, os alunos ficaram à vontade para fazer perguntas e foram expostos a um questionário de múltipla escolha composto por três perguntas:

- Pergunta 1: A palestra lhe trouxe informação relevante para seu curso?
- Pergunta 2: Você achou o conteúdo abordado na palestra interessante?
- Pergunta 3: Após a palestra você conseguiu compreender a relação que existe entre a criptografia atual, seus limites e o que a física quântica pode trazer para esse cenário?

O questionário foi idealizado com objetivo de saber se o conhecimento exposto na palestra sobre a criptografia, segurança da informação e da física trouxeram benefícios para os alunos em relação ao curso e se os estudantes conseguiram ou não construir esse elo entre as duas áreas numa perspectiva motivacional em relação ao prosseguimento num curso de informática.

DESENVOLVIMENTO

A Física moderna, que surgiu no início do século XX com a explicação da radiação de corpo negro por Max Planck, do efeito fotoelétrico e a teoria da relatividade por Albert Einstein, e, logo depois, com a introdução das bases da Mecânica Quântica por Erwin Schrödinger, Niels Bohr, etc., possui excepcional importância e aplicabilidade em nossa sociedade tão tecnológica, mas, apesar disso, vem sendo pouco abordada em nível médio (SOUZA; Eduardo, 2016), mesmo constando na ementa do Curso Técnico Integrado em Informática. Ostermann e Moreira [1] e Oliveira e Viana [2], ao argumentarem sobre a necessidade da abordagem da Física moderna em nível médio, insistem que esse conhecimento fornece a explicação científica para utensílios tecnológicos usados no cotidiano, principalmente os de comunicação (RICARDO et al., 2014).

A partir da década de 90, a inserção da Física moderna no ensino médio passou a ter uma importância especial para pesquisadores da área de educação em ciências, visto ser ela a responsável pelo atendimento das novas necessidades cotidianas, sendo essencial para o homem contemporâneo, abrangendo um conjunto de conhecimentos que extrapola os limites da ciência e da tecnologia (PINTO; ZANETIC,1999).

A Física moderna está completamente correlacionada com o avanço da criptografia, visto que, no contexto atual, muitos centros de pesquisa vêm buscando, com computadores

quânticos, métodos alternativos que possam, futuramente, promover um nível de segurança bem mais elevado que os da atualidade (UNO; FALEIROS, 2018).

> Baseando-se nos princípios da Mecânica Quântica, a grande vantagem da criptografia quântica em relação aos outros reside em sua segurança incondicional, ou seja, não apresenta falhas como os métodos criptográficos atuais e não pode ser quebrado, mesmo com poderosos computadores (UNO; FALEIROS, 2018).

Criptografia é um termo utilizado como "sinônimo" para a codificação de informações. Segundo O'Brien e Marakas (2007, p. 436), "a criptografia envolve o uso de algoritmos matemáticos especiais, ou chaves, para transformar dados digitais em códigos antes de serem transmitidos e para decodificar os dados quando são recebidos". Ela é uma ciência de grande importância para segurança da informação, pois é responsável por proteger todos os dados que depositamos nos computadores e nas redes.

> O grande objetivo da criptografia é transferir uma mensagem ou arquivo, chamado de texto claro, que pode ser entendido pelo usuário, e criptografá-lo em um texto cifrado de modo que somente as pessoas autorizadas saibam como transformá-lo em sua forma original novamente (TANENBAUN, 2009).

Pelo prisma da física, a criptografia atual está baseada em sistemas clássicos, logo, seus algoritmos podem ser chamados de clássicos. A segurança nesse tipo de criptografia não aponta para a impossibilidade da quebra do código, pelo contrário, concentra-se na variável denominada tempo computacional, que é o tempo para que um computador aplique todas as possibilidades de combinações de algarismos e, nesse caso, decodifique uma mensagem. Vê-se então que a segurança da informação está associada à quantidade de algarismos de uma chave. Atualmente, as chaves utilizadas para relações comerciais, bancos, etc., possuem mais que cem (100) algarismos, o que exigiria um tempo computacional da ordem de décadas nos casos mais simples, tornando a própria tentativa de quebra inviável. (CASSINELLO; GÓMEZ, 2017).

Na contramão dessa segurança baseada em quantidade de algarismos, a física quântica entra nesse cenário trazendo consigo ferramentas e conceitos para mostrar que "tamanho não é documento" e propõe que a direção é adentrar na era da informação quântica. Os conceitos fundamentais que tornam isso tecnologicamente aplicável são: a dualidade onda-partícula, introduzida por De Broglie em 1924; O colapso da função de onda e o princípio da sobreposição de sistemas quânticos, estes dois últimos tomaram forma através da interpretação mais comum da mecânica quântica (A interpretação de Copenhague - 1927) cujos ícones são os físicos Niels Bohr e Werner Heisenberg. (RESNICK, Eisberg,1979). Em resumo, a dualidade onda-partícula nos diz que, em escalas subatômicas, os constituintes fundamentais da matéria apresentam tanto características de onda, quanto de partícula, e que a emergência de uma ou outra propriedade

está relacionada com o tipo de experimento e com o objetivo da medição do mesmo. Tratando-se da sobreposição e do colapso pode-se dizer que:

> Se for possível descobrir, de alguma maneira, se uma partícula quântica, que pode passar por dois caminhos, passou por um ou pelo outro, a partícula deixa de passar pelos dois (colapsa sua função de onda). Caso contrário, a partícula passa pelos dois (sua função de onda é a sobreposição dos dois caminhos). (CASSINELLO; GÓMEZ, 2017)

O contexto acima descrito está experimentalmente comprovado e teoricamente fundamentado, inclusive com evidências razoavelmente atuais, como o experimento do interferômetro de Mach-Zehnder. (PONTES, Rafael; 2016).

Os conceitos da mecânica quântica, embora pouco intuitivos, levam a ideias de fato inovadoras, como a utilização do princípio da sobreposição de estados quânticos para criação de bits quânticos (qubits). Visto que partículas quânticas têm seus estados sobrepostos, ao invés da informática se limitar aos bits clássicos identificados por 0 ou 1, pode ir além e ter, com o qubit, 0 e 1 ao mesmo tempo, enquanto não houver medição no sistema (CASSINELLO; GÓMEZ, 2017). Em situações de vantagem computacional, que pode ser medida em termos de tempo computacional, vê-se que 300 qubits = 〖10〗^90 bits. Dessa forma, um computador quântico, com a capacidade de bits atuais, seria capaz de reduzir o tempo de quebra de uma mensagem criptografada de dezenas de anos para minutos. Ao mesmo tempo, um código, ou chave gerada quanticamente não pode ser quebrado sem que se perceba que houve interferência no sistema, dado o conceito de colapso da função de onda, pois, tal tentativa de quebra seria interpretada como uma medição do sistema quântico. (CASSINELLO; GÓMEZ, 2017)

RESULTADOS E DISCUSSÃO

Através do recolhimento das informações pré-palestra, percebeu-se que, dos 52 entrevistados, 31 (59,6%) que possuem familiaridade com a física clássica ensinada em sala, já conheciam o conceito de criptografia, sendo a maioria jovens com idade entre 17 e 18 anos.

Ainda, conforme os resultados do formulário eletrônico, ficou explícito que os jovens possuem algumas dificuldades na disciplina de Física, no qual foram mencionados obstáculos como: cálculos abstratos sem a compreensão do que foi exposto (55,8%), dificuldade de concentração durante a aula (34,6%) e dificuldade para relacionar o que foi dito em sala de aula com a realidade (9,6%).

Mais da metade dos entrevistados (61,5%) afirmaram que não dispunham de conhecimento sobre qualquer tópico de física moderna, o que é natural, visto que, dificilmente, esses assuntos são abordados em nível médio e, mesmo quando são, não é fácil de ser associado

com o cotidiano, pois, além de conter fenomenologia pouco intuitiva, também está implicado com operações matemáticas muitas vezes de nível superior, permitindo apenas uma abordagem superficial de muitos fenômenos, o que diminui o entusiasmo dos alunos no âmbito acadêmico para o entendimento da temática, por conseguinte, influencia na segurança para afirmar sobre a apreensão desse tipo de conhecimento.

Além disso, o resultado sobre a compreensão dos alunos a respeito da relação entre as perspectivas da criptografia e a física quântica é crítico, porém, esperado. Apenas 3,8% dos entrevistados afirmaram ter uma noção a respeito do tema antes da aplicação da palestra e 96,2% não conseguem fazer a ligação dos fenômenos quânticos mais básicos, como o efeito fotoelétrico, com alguma utilização prática. O fato de existirem discentes que afirmaram ter esse conhecimento prévio pode estar associado ao interesse pessoal dos mesmos e a facilidade atual de se encontrar informação em canais de comunicação que atuam em divulgação científica.

Um total de 112 discentes compareceram a palestra e foram expostos a um questionário pós-palestra, com o qual observou-se um sucesso quase que unânime para com os objetivos do trabalho. Desses 112 discentes (representados no gráfico 1), aproximadamente 94,7% consideraram que a palestra trouxe alguma informação relevante em relação ao curso de informática, 4,5% indicaram que talvez ela tenha sido relevante e apenas 0,8% acharam que ela não teve relevância alguma. Além disso, 107 alunos, equivalente à 95,5%, acharam o conteúdo da palestra interessante, enquanto 5 alunos (4,5% aproximadamente) acharam o conteúdo pouco atrativo. Por fim, 99,1% dos discentes alegaram que ao fim da palestra conseguiam relacionar a criptografia com a física quântica.

Vale frisar que, embora o último percentual aponte para uma homogeneidade na compreensão da temática, as turmas que participaram são bastante heterogêneas em vários aspectos, até mesmo em nível de conhecimento prévio. De fato, isto denota que, mesmo conteúdos complexos, como os apresentados na palestra, tornam-se mais claros
quando as aplicações práticas ficam evidentes. É importante dizer também que houve um grande esforço para apresentar apenas um núcleo necessário de conceitos e postulados, os quais foram esclarecidos a partir de exemplos, contraexemplos e aplicações.

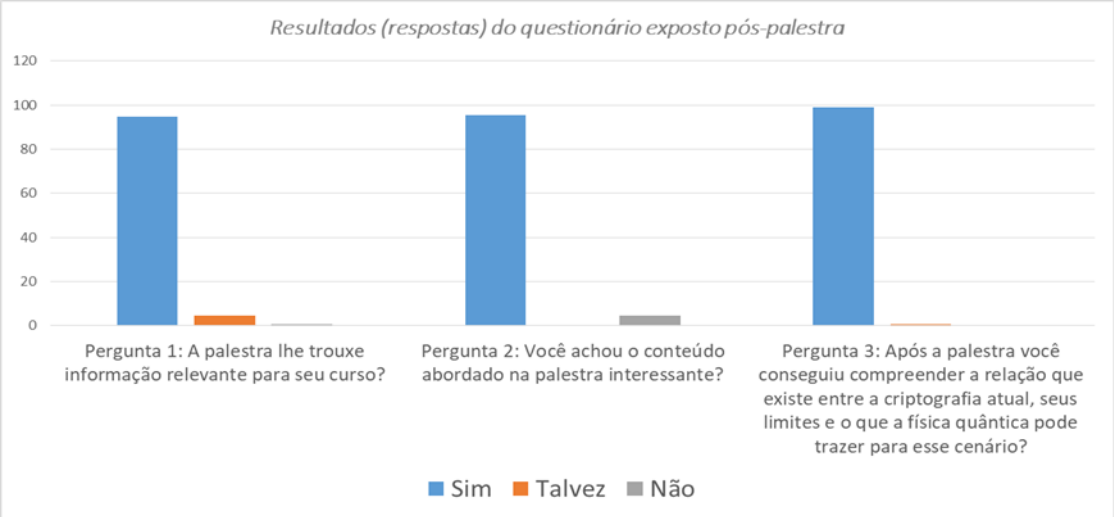

Gráfico 1: Resultado do questionário exposto pós-palestra.

Ao separar os resultados por turma observou-se que: na turma do 1º ano Matutino, representada por 34 alunos presentes à palestra, o resultado foi positivo. Apesar da turma ainda não ter visto conceitos importantes das ementas de Física e de Informática necessários para a compreensão do tema. De acordo com os dados, eles tiveram discernimento suficiente para fazerem a correlação dessas duas áreas após a palestra.

Na turma do 2º ano Vespertino, representada por 2 alunos, os mesmos alegaram que a palestra foi significativa para o curso. A pouca participação dessa turma está associada com o horário da palestra que ocorreu no período matutino. Mesmo assim, foi possível perceber a evolução nas respostas dos alunos presentes, o que está em concordância com o fato de que no 2º ano os alunos já viram os conceitos fundamentais de física e informática e conseguem, portanto, fazer uma melhor avaliação sobre essas duas áreas.

Nas duas turmas de terceiro ano, representadas por 31 alunos (matutino) e 21 alunos (vespertino), a palestra teve impacto bem parecido. Certa dificuldade perceptível na última pergunta era esperada, levando em consideração que no 3º ano os discentes não possuem mais física na grade e acabam esquecendo de alguns conceitos que foram mencionados na palestra.

Na turma do 4º ano Matutino, representada por 6 alunos, a palestra teve total relevância no aprendizado dos alunos, eles compreenderam totalmente o foco da apresentação. Embora eles não tenham mais física na grade, esse resultado pode ser explicado tendo em vista que estudantes no último ano normalmente se dedicam para a prova do ENEM e assim, precisam voltar a estudar todos os conceitos de física, somado a isso, no último ano eles já estão habituados com os conceitos de informática, o que ajuda ainda mais na hora da compreensão da relação da física com a informática.

CONSIDERAÇÕES FINAIS

A experiência desenvolvida e apresentada nesse estudo é resultado de uma pesquisa realizada no Curso Técnico de Nível Médio Integrado em Informática do Instituto Federal, com o objetivo de analisar formas de inserir o estudo teórico-histórico da criptografia e apresentar sua relação com a física moderna, mais especificamente com os princípios da física quântica, de modo a proporcionar maior abrangência de conhecimento. Tal abordagem pode ser realizada sem a apresentação dos meandros matemáticos associados ao tema, dado que, em princípio, a forma de inserção foi pensada como um motivador para o prosseguimento dos discentes na área de informática e como uma forma de divulgação científica, e não como um curso formal sobre o assunto.

A partir dos resultados obtidos mediante questionário pré-palestra sobre a física moderna, criptografia e suas possibilidades, foi possível detectar, dentro do nosso espaço amostral, que os alunos do Curso de Informática não conseguem, em sua grande maioria, fazer a correlação entre a física moderna e a criptografia, o que apontou para a importância de sua discussão e para a forma de inserção implementada. Além disso, ao avaliar os dados do questionário pós-palestra, constatou-se que a abordagem dessa temática foi, na percepção dos alunos, de considerável relevância para os futuros técnicos do instituto, pois, permitiu o acesso a esse conhecimento mesmo não estando na grade do curso, proporcionando, por consequência, uma melhor preparação profissional dos discentes.

Uma das perspectivas do trabalho realizado, dado o seu nível de aceitação pelos discentes, é tornar a palestra anual, absorvendo sempre melhorias e abordando as recentes inovações que surgirem. Dessa forma, é possível atingir novos alunos a cada ano. Também existe a perspectiva de levar a palestra para os outros campus do Instituto e, a partir daí, construir um modelo de curso que trate da temática exposta por este trabalho.

REFERÊNCIAS

CASSINELLO, Andrés; GÓMEZ, J.L.Sánchez. **O mistério quântico: Uma expedição às fronteiras da física.** São Paulo: Editora Planeta do Brasil,2017

FALEIROS, Antonio; UNO, Daniel**. Princípios de Criptografia Quântica.** Disponível em: <http://www.bibl.ita.br/ixencita/artigos/FundDanielNobuo.pdf>. Acesso em 23 de setembro de 2018.

FAPESP.**Computador quântico em ação**.Disponível em <http://revistapesquisa.fapesp.br/2007/03/01/computador-quanticoemacao/#prettyPhoto>. Acesso em 24 de março de 2019.

MARAKAS, George E.; O'BRIEN James A. **Administração de Sistemas de Informação – Uma Introdução**. São Paulo: Mc Grawn-Hill, 2007

MARQUES, V. Thiago; RIBEIRO, H.C. Bruno. **Criptografia: abordagem histórica, protocolo DIffie-Hellman e aplicações em sala de aula.** João Pessoa- PB, 2013.

NASCIMENTO, M. Patricio. **Criptografia Quântica Novas Tecnologias na Segurança de Dados e Telecomunicações.** Fundação Educacional do Município de Assis, 2014.

[2] OLIVEIRA F.; VIANNA M. in **Anais IX Encontro Nacional de Pesquisa em Ensino de Física**. Jabodicatubas , MG. 2004.

[1] OSTERMANN F; MOREIRA M.A. **Investigações em Ensino de Ciências**. 2000.

PINTO, A. Custódio; ZANETIC. **É POSSÍVEL LEVAR A FÍSICA QUÂNTICA PARA O ENSINO MÉDIO?** . São Paulo, 1999.

PONTES, Rafael. **Simulação Computacional do Interferômetro de Mach-Zehnder.** Disponível em: <https://www.if.ufrj.br/~carlos/trablicen/raphael/monografiaRaphaelFinal.pdf > Acesso em 24 de março de 2019.

RESNICK, Eisberg. **Física quântica: Átomos, moléculas, sólidos, núcleos e partículas.** Editora Campus: Rio de Janeiro, 1979.

SINGH, Simon. **O Livro dos Códigos.** Brasil: Record, 2014.

SOUZA, Claudio Eduardo de. **A Física Quântica no Ensino Médio: o uso de TDICS como instrumentos de Ensino-aprendizagem.** Disponível em: < https://repositorio.ufsc.br/handle/123456789/167276 > Acesso em: 22 mar.2019

TANENBAUM, Andrew S. **Sistemas operacionais modernos.** 3. ed. São Paulo: Pearson Prentice Hall, 2009.

ZANOTTA et.al. **O GPS: unindo ciência e tecnologia em aulas de física**. Universidade Federal o Rio Grande do Sul: Porto Alegre- RS, 2011.