ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygyno Corsetti

VOLUME 8 - Nº 2

Junho 2018

ISSN 2594-3952

O Comunicante

SUMÁRIO

Revista Científica da Escola de Comunicações
Escola Coronel Hygyno Corsetti

VOLUME 8 - Nº 2
Junho 2018

EDITORIAL

O COMUNICANTE

Revista Científica da Escola de Comunicações

Ano 8 - Nº 2
Junho 2018

ISSN 1968-6029
ISSN 2594-3952 (Digital)
Escola de Comunicações - EsCom
Escola Coronel Higyno Corsetti

O Comunicante - Revista Científica da Escola de Comunicações - Volume 8, Nº2(Jun/2018)
Brasília-DF: Escola de Comunicações. 2018 76p; 29,7 cm X 21,0 cm
Publicação Quadrimestral

ISSN 1968-6029 ISSN 2594-3952(Digital)
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Direito 7. Educação 8. História Militar 9. Informática 10. Instrução Militar 11. Gestão 12. Meio Ambiente 13. Operações Militares Conjuntas e Singulares. I. Título

O COMUNICANTE

Revista Científica da Escola de Comunicações

A Revista Científica, O Comunicante, publicada pela Escola de Comunicações, busca incentivar pesquisas científicas nas áreas afetas à Defesa e que contribuam para o desenvolvimento da Arma de Comunicações.

OBJETIVOS

Promover o viés científico em áreas do conhecimento que sejam de interesse da Arma de Comunicações e, consequentemente, do Exército Brasileiro.

Manter um canal de relacionamento entre o meio acadêmico militar e civil.

Trazer à reflexão temas que sejam de interesse da Força Terrestre e que contribuam para a Defesa.

Publicar artigos inéditos e de qualidade.

Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos Corpos de Tropa.

PÚBLICO-ALVO

A revista está voltada a um amplo espectro de pesquisadores, professores, estudantes, militares, bem como profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, História Militar, Informática, Instrução Militar, Gestão, Meio Ambiente, Operações Militares Conjuntas e Singulares.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo a outra revista, ele deverá consultá-la e cientificar-se de não estar ferindo direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

Os artigos submetidos são avaliados pela Comissão Editorial, no que se refere ao seu mérito científico e adequação às regras de apresentação de trabalhos científicos.

Em seguida, os textos são encaminhados aos pareceristas que terão o prazo de 30 dias para fazerem a avaliação. Os pareceristas não são remunerados e, caso aceitem, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista. A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos, além de sugerir mudanças eventuais de modo a adequar os textos.

Todos os textos submetidos devem vir acompanhados de carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de estar concorrendo a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta revista.

Outrossim, nenhum dos organismos editoriais, organizações de ensino e pesquisa ou pessoas físicas envolvidas nos conselhos, comitês ou processo de editoração e gestão da revista se responsabilizam pelo conteúdo dos artigos seja sob forma de ideias, opiniões ou conceitos, devendo ser de inteira responsabilidade dos autores dos respectivos textos.

PERIODICIDADE

A revista terá a periodicidade quadrimestral (fevereiro, junho e outubro) e se reserva ao direito de realizar edições especiais, além das previstas.

EXPEDIENTE

EDITORIAL

A presente edição da Revista “ O Comunicante” contém uma ampla variedade de artigos, contemplando diversas áreas de interesse das comunicações militares como gestão, informática, telecomunicações, cibernética e capacitação de recursos humanos.

Nesta publicação, é dada a devida importância à atividade logística de suprimento e manutenção do material de Comunicações Táticas do Exército Brasileiro, peça fundamental para a conservação da capacidade operativa da Força e que vem adquirindo importância pelo seu alto grau de complexidade.

As tecnologias e protocolos de comunicação são abordadas em textos de fácil leitura, contribuindo para a atualização dos conhecimentos técnicos dos leitores que lidam com o desafio de prover o suporte de comunicações ao exercício do comando e controle.

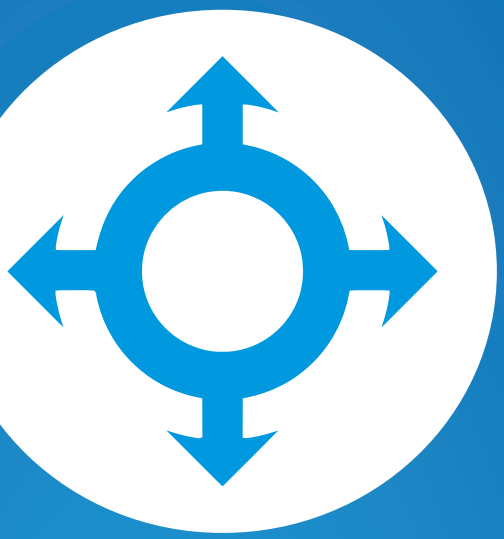
O pensar no futuro, no entanto, não impede a manutenção das tradições e da História institucional. Neste sentido, a presente edição resgata a memória do tradicional Concurso de radioamadorismo Verde Amarelo, destacando a importância da atividade até os dias de hoje.

A diversidade de temas e assuntos reflete o estágio de evolução da Força Terrestre em direção ao futuro. Neste processo de transformação, buscam-se a geração de capacidades que possibilitarão ao Exército Brasileiro atingir o estágio condizente a uma Força militar da era do conhecimento.

Uma boa leitura a todos!!

RODOLFO ROQUE SALGUERO DE LA VEGA FILHO - Cel
Comandante da Escola de Comunicações

Pareceristas Externos Convidados



ÁREA DE CONCENTRAÇÃO

GESTÃO

ESCOLA DE COMUNICAÇÕES

O PAPEL DO CENTRO LOGÍSTICO DE COMUNICAÇÕES E GUERRA ELETRÔNICA NO PROCESSO DE MANUTENÇÃO CORRETIVA DO MATERIAL CLASSE VII NO EXÉRCITO BRASILEIRO

Rodrigo Adão da Silva
Pós-graduado em Guerra Eletrônica e em Sistemas de Comunicações e Defesa

RESUMO. O Centro Logístico de Comunicações e Guerra Eletrônica é o setor pertencente ao Comando de Comunicações e Guerra Eletrônica do Exército responsável pelo assessoramento junto ao Departamento de Ciência e Tecnologia quanto à aquisição, distribuição e manutenção dos materiais de comunicações, guerra eletrônica, eletrônica e tecnologia da informação. Diante da celeridade dos combates modernos, cresce a importância dos processos de manutenção de PRODE Classe VII ocorridos no C Log Com GE, o qual como órgão gestor, deve caminhar na direção correta, retificando as assimetrias que porventura existam e otimizando ações, com a finalidade de prover uma manutenção eficaz aos seus clientes - militares das diversas organizações militares dos corpos de tropa do Exército Brasileiro.

Palavras-chave: Centro Logístico de Comunicações e Guerra Eletrônica. Manutenção. Produto de Defesa e Classe VII.

INTRODUÇÃO

No cenário difuso e não linear dos conflitos modernos, novas capacidades são exigidas para a Logística Militar desde o tempo de paz, a saber: dissuasão em nível extrarregional, prontidão logística, complementaridade, gestão integrada e ênfase na dimensão humana.

Os dias atuais caracterizam-se pela rápida evolução do espaço de batalha e estão permeados pela necessidade premente de alto grau de interoperabilidade de sistemas, elevadas taxas de transmissão de dados e ágil reparo ou reposição de itens que se encontram defeituosos.

O manual doutrinário MD 30-M-01, afirma que:

> O preparo do país para a guerra exige transformações estruturais e envolve todos os setores da nação. O planejamento, em todos os níveis, para atender a essa situação deve ser previamente elaborado, a fim de que a passagem da situação de paz para a situação de guerra transcorra da forma mais rápida e harmônica possível (BRASIL, 2011, p. 17).

Nesse mister, a manutenção do Material de Emprego Militar (MEM), doravante denominado de Produto de Defesa (PRODE) é um fator extremamente relevante na obtenção de vantagem competitiva sobre a força oponente.

Diante desse cenário e objetivando-se a reestruturação da manutenção dos materiais militares pertencentes à classe VII, foi criado e ativado o Centro Logístico de Comunicações e Guerra Eletrônica (C Log Com GE), em 19 de janeiro de 2017.

Tal fato foi realizado calcado na determinação prevista no Planejamento Estratégico do Exército (PEEX) 2016-2019, publicado no Boletim Especial do Exército no 28/14, de 22 de dezembro de 2014, relatado abaixo:

> Objetivo Estratégico do Exército Nº 8 (OEE 8): Implantar um novo e efetivo Sistema Logístico Militar Terrestre.
>
> Estratégia 8.1: Implantação da nova estrutura logística do Exército. Ação Estratégica 8.1.1: Adotar uma estrutura lógica capaz de prestar o apoio logístico na medida certa e no tempo oportuno (Prontidão Logística).

> Ano de 2016, Atividades Impostas - item 8.1.1.14: Prosseguir na implantação do Centro Logístico de Comunicações e Guerra Eletrônica (C Log Com GE) em Brasília-DF (BRASIL, 2014b, p. 20, grifo nosso).

Assim, de acordo com o Boletim Interno nº 60, de 28 de março de 2017, do Comando de Comunicações e Guerra Eletrônica do Exército (Cmdo Com GE Ex), o C Log Com GE tem por missão:

> Planejar, supervisionar e coordenar as atividades logísticas (aquisição, armazenagem, distribuição e manutenção) inerentes à Divisão Logística e à Divisão de Engenharia e Manutenção, referentes à gestão do material classe VII do Exército Brasileiro (BRASIL, 2017a, grifo nosso).

1 DESENVOLVIMENTO

1.1 GENERALIDADES

Inicialmente, reveste-se de grande importância apresentar a definição de manutenção. Balizando-se pelas literaturas militares, BRASIL (2014, p. 3-6) afirma que o Grupo Funcional Manutenção "refere-se ao conjunto de atividades que são executadas visando manter o material em condição de utilização durante todo o seu ciclo de vida e, quando houver avarias, restabelecer essa condição".

Numa perspectiva mais industrial, os experientes engenheiros mecânicos Alan Kardec e Júlio Nascif afirmam que:

> Hoje, a missão da manutenção é garantir a disponibilidade da função dos equipamentos e instalações de modo a atender a um processo de produção ou serviço, com confiabilidade, segurança, preservação do meio ambiente e custo adequados (KARDEC e NASCIF, 2003, p. 22).

Complementando o exposto, o manual doutrinário EB20-MC-10.204 - Logística indica que:

> A **manutenção** garante às forças apoiadas a disponibilidade dos equipamentos, por meio da reparação; da gestão, estocagem e distribuição de peças de reparação; da evacuação de artigos avariados ou inservíveis dos elementos apoiados (material salvado) ou do inimigo (material capturado) para recuperação ou descarte; e das aquisições de itens e/ou serviços destinados às tarefas de manutenção (BRASIL, 2014, p. 3-6, grifo nosso).

Nesse contexto, as atividades do Grupo Funcional Manutenção são identificadas nas seguintes categorias: planejamento da manutenção, manutenção preventiva, manutenção corretiva, manutenção modificadora e evacuação de material (BRASIL, 2014, p. 3-7).

Na visão de Kardec e Nascif (2003, p. 26) existem 6 tipos básicos de manutenção, a saber: corretiva não planejada, corretiva planejada, preventiva, preditiva, detectiva e engenharia de manutenção.

O presente artigo concentrou as análises no aspecto corretivo da manutenção. Nesse enfoque, BRASIL (2014, p. 3-8) atesta que "a manutenção corretiva destina-se à reparação ou recuperação do material danificado para repô-lo em condições de uso. Pode ser classificada como planejada e não planejada".

Com vistas a elucidar o tema proposto, faz-se necessário abordar as normas e diretrizes que amparam a manutenção dos PRODE CI VII no âmbito da Força Terrestre.

As Normas Administrativas Relativas ao Material de Comunicações Estratégicas, Eletrônica, Guerra Eletrônica e Informática (NARMCEI), as quais substituíram as Normas Administrativas Relativas ao Material de Telecomunicações (NARMTEL) e as Normas Administrativas Relativas ao Material de Informática (NARMINFOR-I), constituíram-se como o principal documento balizador na condução dos processos afetos à reparação de produtos de comunicações, guerra eletrônica e de tecnologia da informação.

Contudo, diante da própria dinâmica de evolução dos circuitos eletrônicos, respaldados pelo surgimento dos componentes para montagem em superfície (Surface Mounting

Device - SMD), pelo avanço da nanotecnologia e concepção dos circuitos processados digitalmente (em detrimento do desaparecimento gradual das válvulas e placas analógicas), o grupo funcional manutenção teve que se adequar às transformações em curso.

Um outro fator que contribuiu para a promoção de intensas mudanças foi a criação do Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), no ano de 2009, doravante denominado de Comando de Comunicações e Guerra Eletrônica do Exército.

É válido ressaltar que toda a incumbência sobre o controle e a gestão dos processos administrativos, incluindo os de manutenção, atinentes aos materiais classe VII, foi repassada ao CCOMGEX, que surgiu da fusão entre a antiga Diretoria de Material de Comunicações, Eletrônica e Informática (DMCEI) - que era a organização responsável pelo gerenciamento de todo material classe VII catalogado, e o Centro Integrado de Guerra Eletrônica (CIGE).

De acordo com dados obtidos do C Log Com GE, antes do estabelecimento do CCOMGEX, o cenário de gestão dos produtos Cl VII era permeado pelas seguintes características:

a. 90% de obsolescência;

b. ausência de padronização de fornecedores;

c. realização de compras de suprimentos nas oportunidades dos recursos (ausência de um planejamento prévio);

d. elevado índice de indisponibilidade do material de comunicações;

e. formação deficitária dos mecânicos, que são os militares da Qualificação Militar dos Subtenentes e Sargentos (QMS) Manutenção de Comunicações;

f. grande quantitativo de vendedores de equipamentos e não de soluções;

g. celebração de contratos sem cláusulas de garantia eficientes; e

h. deficiência no gerenciamento da manutenção.

Assim, objetivando-se minimizar esses desafios iniciou-se, dentro da CCOMGEX, um processo de reestruturação logística, por intermédio das seguintes ações:

a. estabelecimento do Suporte Logístico Integrado (SLI), também conhecido como Apoio Logístico Integrado (ALI) ou Apoio Integrado ao Produto (*Integrated Product Support* – IPS, sigla adotada pelo *Defense Acquisition University*). Resumidamente, o processo de ALI integra os requisitos de desempenho de um sistema com a otimização dos seus custos de apoio logístico ao longo do ciclo de vida projetado (GALLOWAY, 1996, p. 25);

b. acordos contemplando soluções para: distribuição de documentação técnica clara, objetiva e redigida no idioma português, treinamento de operação, treinamento de manutenção dos PRODE a serem adquiridos, obtenção de instrumental de medição de parâmetros/reparo, e de suprimentos num quantitativo capaz de viabilizar a denominada 'troca direta' para os casos que demandem maior celeridade de manutenção;

c. planejamento de transporte de material: com a abertura de processos licitatórios para a contratação de empresas de translado, utilização dos serviços aéreos prestados pela Força Aérea Brasileira e participação nos comboios organizados pelo Estabelecimento Central de Transportes (ECT) e demais organizações ilitares do Exército Brasileiro; e

d. convergência de fornecedores, visando padronizar o PRODE Cl VII

> a ser empregado nos níveis tático e operacional. Esse movimento visou dirimir os problemas existentes, oriundos da elevada gama de meios de comunicações empregados nas operações militares, como por exemplo: transceptores e soluções de RF da Motorola (empresa americana), Rohde & Schwarz (alemã), Thales (francesa), Tadiran (israelense) e Vertex Standard (*joint venture* originalmente japonesa, outrora conhecida pela denominação Yaesu).

Destarte, o comando do CCOMGEX estabeleceu parcerias com as empresas Indra, Harris Corporation e Motorola Solutions, para o fornecimento de Produtos Estratégicos de Defesa (PED), nas seguintes áreas: comunicações satelitais, radiocomunicações táticas e sistemas de rádio troncalizados.

Essa decisão, em princípio, trouxe diversos benefícios, como por exemplo, a montagem de modernas oficinas de manutenção no complexo do CCOMGEX.

Todavia, a atualização dos processos administrativos logísticos de manutenção não ocorreu em consonância com a aquisição de todos os meios necessários para a realização da atividade de manutenção no âmbito das organizações militares que possuíam tal incumbência.

Com o surgimento do CCOMGEX, fora criada a Divisão de Engenharia e Manutenção (foi fundida com a Divisão Logística, formando o atual C Log Com GE), que era o órgão responsável pelo gerenciamento da manutenção dos materiais de comunicações e guerra eletrônica do EB. Assim, a manutenção das principais soluções ficou centralizada na guarnição de Brasília. Neste ponto, destaca-se que em virtude do alto custo da montagem das oficinas de reparo e da nova concepção organizacional para a Arma do Comando, os instrumentais necessários para a realização de profícua manutenção dos novos equipamentos adquiridos, assim como as bancadas de teste (popularmente conhecidas pela alcunha “gigas de testes”) não foram distribuídos para as demais OM logísticas de manutenção dos corpos de tropa.

Isso trouxe reflexos contundentes na doutrina e no escalonamento da manutenção, pois os B Log, P R Mnt e Ars G não se encontravam com os meios adequados para a realização da manutenção dos novos MEM Cl VII.

Diante do cenário apresentado, o CCOMGEX precisou regular novos procedimentos de manutenção, o que foi feito por intermédio da publicação das Normas Provisórias de Comunicações e Guerra Eletrônica, as quais, de fato, atualizaram todos os processos de planejamento, controle e administração do suprimento Cl VII.

Tais normas receberam a titulação de provisórias até o ano de 2017, por ocasião da edição das Normas Administrativas Relativas ao Material de Comunicações e Guerra Eletrônica (NARM Com GE).

De acordo com o Aditamento nº 3 ao Boletim Interno nº 29 do CCOMGEX, de 9 FEV 17, as NARM Com GE têm a finalidade de:

> substituir a NARMCEI (Normas Administrativas Relativas ao Material de Comunicações Estratégicas, Eletrônica, Guerra Eletrônica e Informática do Exército Brasileiro), atualizar procedimentos administrativos referentes aos materiais da Classe VII, em especial ao MEM – Material de Emprego Militar – previstos na NARSUP (Normas Administrativas Relativas ao Suprimento) e NARMNT (Normas Administrativas Relativas à Manutenção), padronizar, simplificar, regular e divulgar os processos relativos aos materiais dessa classe de suprimento no Exército Brasileiro (BRASIL, 2017b, p. 5).

Ademais, as NARM Com GE indicam a correta diferenciação entre as distintas classificações do material, a saber: controlado, com controle mitigado, não controlado, em obsolescência e obsoleto. E também definem conceitualmente os termos Troca Direta e Distribuição Concentrada.

Finalizando, deve-se destacar que o capítulo VIII da norma supracitada é aquele que se destina a explicar como ocorrem os diversos processos de manutenção dos PRODE Cl VII, por meio de fluxogramas bastante elucidativos, que estão elencados de acordo com a natureza do material e o seu estado de utilização.

1.2 PRINCIPAIS SISTEMAS MANUTENIDOS NO C LOG COM GE

Atualmente, o C Log Com GE tem capacidade para realizar a manutenção dos seguintes materiais:

a. sistemas Motorola (Sistema de Rádio Digital Troncalizado – SRDT, equipamentos VHF e UHF, motobridge, repetidores, dentre outros);

b. rádios táticos da Harris (HF, VHF, UHF e enlaces de microondas);

c. intercomunicador SOTAS;

d. rádio M3TR;

e. sistemas de Guerra Eletrônica (GE); e

f. terminais do Sistema de Comunicações Militares por Satélites (SISCOMIS).

É válido ressaltar que no site do Cmdo Com GE Ex estão disponíveis os contatos telefônicos das oficinas de manutenção de cada PRODE supracitado, de modo que as OM possam realizar a retirada de dúvidas, o que proporciona maior agilidade à cadeia de manutenção.

Para as unidades detentoras de terminais terrestres do SISCOMIS, é importante destacar que o C Log Com GE é o único centro que possui capacidade de realizar a manutenção desses itens, sendo responsável pelo reparo dos terminais pertencentes às três Forças Armadas (Exército Brasileiro, Marinha do Brasil e Força Aérea Brasileira).

1.3 OPORTUNIDADES DE MELHORIA NOS CORPOS DE TROPA, COM VISTAS A CONTRIBUIR NO PROCESSO LOGÍSTICO DE MANUTENÇÃO DO PRODE CL VII

Diante do exposto, até o presente momento, algumas oportunidades de melhoria tem sido identificadas quanto ao aperfeiçoamento do processo de manutenção dos materiais classe VII, a saber:

a. maior adestramento dos operadores dos equipamentos: o desconhecimento dos usuários dos materiais quanto à operação e à falta de cuidado no manuseio tem provocado constantes danos aos PRODE Cl VII;

b. conhecimento da legislação: os procedimentos a serem seguidos para a manutenção dos materiais Cl VII estão descritos nas NARM Com GE (conforme já exposto em momento anterior). As OM devem orientar o responsável pelo material a cumprirem o previsto nas normas, a fim de evitar possíveis retardos no processo de manutenção;

c. aquisição de equipamentos não padronizados pelo Cmdo Com GE Ex: tal prática deve ser evitada, pois para tais itens não haverá apoio de manutenção no âmbito da F Ter. Tal problema geralmente acontece através da compra feita pelas OM, de produtos Motorola que não foram fornecidos pela cadeia de suprimento;

d. correta apuração de responsabilidades sobre danos ao material: as OM devem apurar corretamente, via abertura de processos administrativos (como sindicância, por exemplo) as responsabilidades quando houver indícios de má utilização de um equipamento;

e. comunicação imediata dos proble-

mas de indisponibilidade: tal situação deve ser comunicada com o máximo de celeridade (assim que for identificado) ao C Log Com GE, de modo que o Cmdo Com GE Ex possa atualizar a situação da OM considerada e realize redistribuições de material (caso haja necessidade), com vistas a manutenção do nível operativo; e

f. restituição da guia de remessa: após um PRODE retornar para a OM de origem, depois de ser reparado, o responsável pelo recebimento deverá assinar a respectiva guia de remessa – indicando a existência ou não de alterações, e enviá-la escaneada, o mais breve possível, para a Seção de Triagem do C Log Com GE, através do endereço divengmnttriagem@ccomgex.eb.mil.br. O objetivo é que o processo de quitação da referida guia não seja prejudicado.

CONCLUSÃO

A logística de manutenção corretiva dos principais PRODE Cl VII empregados na Força Terrestre, e em particular, dos Produtos Estratégicos de Defesa (PED) está concentrada nas oficinais de manutenção do C Log Com GE.

Assim, existem custos logísticos (diretos e indiretos) na questão do envio dos materiais que necessitam de manutenção corretiva para a cidade de Brasília. E no processo reverso, de envio dos materiais manutenidos para as suas respectivas OM (destino final).

Diante deste cenário, as OM de manutenção, a saber: Batalhão Logístico (B Log), Parque Regional de Manutenção (Pq R Mnt) e Arsenal de Guerra (Ars G) possuem uma reduzida capacidade de realização de manutenção corretiva nos PRODE Cl VII; em outras palavras, tais unidades estão limitadas à consecução de medidas corretivas pontuais e emergenciais.

Logo, é de grande relevância que a gestão de manutenção corretiva dos itens supracitados ocorra de forma profícua de modo a se alcançar os resultados desejáveis (baixa indisponibilidade, por exemplo), diante das diversas demandas existentes no âmbito da Força Terrestre e do cenário de flutuação econômica vigente que permeia o cotidiano do Brasil – que é um limitador no processo de novas aquisições.

Nesse contexto, as oportunidades de melhoria elencadas neste artigo devem ser implementadas, com vistas a viabilizar um maior ciclo de vida dos PED, os quais consequentemente apresentarão o mínimo de falhas admissíveis.

EL PAPEL DEL CENTRO LOGÍSTICO DE COMUNICACIONES Y GUERRA ELECTRÓNICA EN EL PROCESO DE MANTENIMIENTO CORRECTIVO DEL MATERIAL CLASE VII EN EL EJÉRCITO BRASILEÑO

RESUMEN. El Centro Logístico de Comunicaciones y Guerra Electrónica es el sector perteneciente al Mando de Comunicaciones y Guerra Electrónica del Ejército responsable por el asesoramiento junto al Departamento de Ciencia y Tecnología para la adquisición, distribución y mantenimiento de los materiales de comunicaciones, guerra electrónica, electrónica y tecnología de la información. En la rapidez de los combates modernos, crece la importancia de los procesos de mantenimiento de PRODE Clase VII ocurridos en el C Log Com GE, lo cual como órgano gestor, debe caminar en la dirección correcta, rectificando las asimetrías que puedan existir y optimi- zando acciones, con la finalidad de proveer un mantenimiento eficaz a sus clientes - militares de las diversas Organizaciones Militares de los cuerpos de tropa del Ejército Brasileño.

Palabras-clave: Centro Logístico de Comunicaciones y Guerra Electrónica, Mantenimiento, Producto del Defensa y Clase VII.

REFERÊNCIAS

BRASIL. Casa Civil. Decreto nº 98.820, de 12 de janeiro de 1990. Aprova o Regulamento de Administração do Exército. Diário Oficial da União. Brasília, DF, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/decre-

to/1990-1994/D98820.htm>. Acesso em: 10 out. 2017.

_____. Exército. Comando de Comunicações e Guerra Eletrônica do Exército. Boletim Interno nº 60/2017, de 28 de março de 2017. Brasília, DF, 2017a.

_____. _____. _____. Normas Administrativas Relativas ao Material de Comunicações e Guerra Eletrônica. Brasília, DF, 2017b. Disponível em: < http://www.ccomgex.eb.- mil.br/index.php/2015-04-10-13-35-55#>. Acesso em: 10 out. 2017.

_____. _____. Comando Logístico. Memória sobre a gestão do ciclo de vida dos materiais. Brasília, DF, [20--].

_____. _____. Departamento de Educação e Cultura do Exército. Nota de Coordenação Doutrinária no 001/2015, de 12 de janeiro de 2015. A Logística nas Operações. Brasília, DF, 2015.

_____. _____. Escola de Material Bélico. Suporte Logístico Integrado. Rio de Janeiro, RJ, 2003.

_____. _____. Estado-Maior do Exército. EB-20-MC-10.204. Logística. 3. ed. Brasília, DF, 2014a.

_____. _____. Portaria nº 1.507, de 15 de dezembro de 2014. Aprova o Plano Estratégico do Exército (PEE) 2016-2019 integrante da Sistemática de Planejamento estratégico do Exército e dá outras providências. Boletim Especial do Exército nº 28/14. Brasília, DF, 2014b. Disponível em: <http://www.infodefensa.com/archivo/files/bee%2028-14%20- %20plano%20estrat%C3%A9gico%20do%20ex%C3%A9rcito%202016-2019.pdf>. Acesso em: 10 out. 2017.

_____. _____. Portaria nº 233, de 15 de março de 2016. Aprova as Instruções Gerais para a Gestão do Ciclo de Vida dos Sistemas e Materiais de Emprego Militar (EB10-IG- 01.018), 1ª Edição, 2016, e dá outras providências. Separata ao Boletim do Exército nº 11/16. Brasília, DF, 2016. Disponível em: <http://www.dct.eb.mil.br/images/conteudo/aest/sep- be11-16_port_233-cmt_ex_eb10-ig-01.018.pdf>. Acesso em: 10 out. 2017.

_____. Ministério da Defesa. MD30-M-01. Doutrina de Operações Conjuntas – 1º Volume. Brasília, DF, 2011.

COSTA, Mariana de Almeida. **Gestão Estratégica da Manutenção**: uma oportunidade para melhorar o resultado operacional. 2013. 103 f. Trabalho monográfico (Graduação em Engenharia de Produção) – Universidade Federal de Juiz de Fora, Juiz de Fora, 2013.

DALLOSTA, Patrick Michael; SIMCIK, Thomas A. **Designing for Supportability**: driving Reliability, Availability and Maintainability In While Driving Costs Out. Defense AT&L: Product Support Issue, p. 34-38, march-april. 2012.

GALLOWAY, Iain. **Design for support and support the design**: integrated logistic support – the business case. Logistics Information Management, Vol. 9, 1996, Iss: 1 pp. 24 – 31. Disponível em: <http://dx.doi.org/10.1108/09576059610107879>. Acesso em 10 out. 2017.

JONES, James V. **Integrated Logistics Handbook**. Special Reprint Ed., McGraw-Hill: New York, 1998. Tradução: Leonardo Vilain S. João.

_____. **Integrated Logistics Handbook**. 3rd. Edition. McGraw-Hill: New York, 2006. 528 p. Livro digital.

KARDEC, Alan Pinto; NASCIF, Júlio de Aquino Xavier. **Manutenção – Função Estratégica**. 2. ed. ver. atual. Rio de Janeiro, RJ, 2003.

REVISTA VERDE-OLIVA. Logística forte é poder de combate. Brasília, Centro de Comunicação Social do Exército, ano 42, n. 228, jul. 2015.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Comunicações do Exército Brasileiro, possui especialização nas áreas de Manutenção de Comunicações e Guerra Eletrônica. Concluiu com aproveitamento o curso de Manutenção de Comunicações da Escola de Comunicações, o curso Básico de Guerra Eletrônica, no Centro de Instrução de Guerra Eletrônica (CIGE) e o curso Expedito de Guerra Eletrônica para Oficiais, no Centro de Adestramento Almirante Marques Leão da Marinha do Brasil. É pós-graduado em Guerra Eletrônica pelo CIGE e em Sistemas de Comunicações e Defesa, pela Universidade Politécnica de Madri. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email adao.silva@eb.mil.br.

ÁREA DE CONCENTRAÇÃO

INFORMÁTICA

ESCOLA DE COMUNICAÇÕES

UTILIZAÇÃO DE FRAMEWORKS NO DESENVOLVIMENTO DE SISTEMAS WEB

1º Sgt Eng Marcos Paulo Miranda de Souza
Graduado em Sistemas de Informação

RESUMO. O grande desafio na construção de sistemas, levam a constante evolução da engenharia de softwares, que tenta dimensionar quais as boas práticas a serem seguidas para que o produto final seja algo capaz de evoluir, atender as necessidades existentes e solucionar os problemas propostos inicialmente. Nesse processo de evolução surgem fatores como o gerenciamento do tempo, custos, curva de aprendizagem para a utilização de ferramentas e quais tecnologias utilizar. É nesse preâmbulo que encontra-se a utilização de frameworks como uma solução muito adotada que atinge todos esses pontos com êxito, proporcionando ganhos que possibilitam maior flexibilidade, agilidade, estabilidade, segurança, padronização de tecnologias e manutenção mais sustentável. Várias ferramentas dessa área são apresentadas todos os dias, com grandes possibilidades de utilização e tecnologias diferentes, sendo utilizadas sem uma análise a longo prazo sobre a sua capacidade de suporte às constantes evoluções dos sistemas que operam via internet (sistemas web). Dessa forma, serão apresentados alguns critérios que devem ser levados em consideração antes de uma empresa ou um programador selecionar um framework para uso.

Palavras-chave: Framework. Programação. Desenvolvimento. Engenharia de softwares.

INTRODUÇÃO

Dentre as possibilidades de escolha de frameworks, o programador PHP se depara com uma gama de opções a seu dispor. A título de exemplificação o mercado oferece o CakePHP, Symfony, Zend Framework, CodeIgniter, Yii 2, Phalcon, Prado, entre outros.

Deve-se levar em consideração, para escolha de uma ferramenta, os fatores que foram mais explorados em cada um dos frameworks e que proporcionaram vantagens em alguns aspectos, entendendo que cada um tem o seus pontos fortes e fracos, para cada tipo de projeto e objetivo.

Os fatores mais importantes que devem ser considerados num framework são estes: estabilidade, segurança, performance, curva de aprendizado, recursos técnicos disponíveis e flexibilidade.

Segundo Alvim (2010, p.12),

> O framework é um conjunto de classes que colaboram entre si, proporcionando melhores práticas de desenvolvimento e diminuição à repetição de tarefas. Além disso, evita variações de 'soluções diferentes para um mesmo tipo de problema'. O que facilita a reutilização e customização dos códigos.

A utilização dessas ferramentas tem sido largamente aplicada em grandes projetos e possuem, armazenadas dentro de suas estruturas, vários princípios da engenharia de softwares, que tem sido estudados até hoje.

1 DESENVOLVIMENTO

1.1 ESTABILIDADE

A estabilidade pode ser vista sobre dois aspectos principais: a capacidade do framework de aderir-se às novas tecnologias sem a ocorrência de erros e a capacidade de sofrer updates em relação a funcionalidades já existentes sem que ocorram erros.

Fagan (1986) relatou que mais de 60% dos erros em um programa podem ser detectados por meio de inspeções de programas. No processo *Cleanroom* (PROWELL , 1999), afirma-se que mais de 90% dos defeitos podem ser descobertos em inspeções de programas.

Quanto às inovações tecnológicas que

ocorrem constantemente e alteram o mercado de negócios, é certo afirmar que tais mudanças exigem adaptações dos recursos existentes nos frameworks para melhor atender a esse mercado. Os rumos são ditados pelas grandes empresas que escolhem uma determinada área da tecnologia a ser explorada em busca do lucro financeiro. Os analistas e programadores se deparam com a necessidade emergencial de fazer com que o seu sistema possa atingir determinada camada de clientes ou um determinado nicho deste e isso exige que o framework, que foi selecionado, seja capaz de produzir artefatos que possam ser utilizados nessa nova direção. O problema está no fato de isto não depender apenas das habilidades do programador, mas talvez de uma melhoria do framework escolhido. Esse trabalho é feito pela equipe de programadores, que são os autores da ferramenta. É nesse momento, que se identifica quais tecnologias irão sobreviver as mudanças do mercado e quais se tornarão obsoletas.

As atualizações dos frameworks não podem causar grandes impactos nos sistemas que já foram desenvolvidos para sua utilização, sob o risco de tornar inviável a aplicação dessas atualizações em projetos grandes que já foram implementados.

A nova versão do framework deve apresentar uma solução com o menor impacto possível e sem produção de erros, atingindo a performance de uma ferramenta estável.

1.2 SEGURANÇA

A segurança é uma das características mais importantes de um sistema, mas que somente é valorizada sua invasão. Normalmente, o problema remonta ao projeto estrutural, no qual os investimentos relacionados à segurança compõe parte ínfima do total investido no projeto.

O termo ‘confiança’ foi proposto por Laprie (1995) para cobrir os sistemas relacionados com atributos de disponibilidade, confiabilidade, segurança e proteção.

Um sistema deve ter, na sua lista de requisitos, os caso de segurança a serem abordados e atendidos desde a fase inicial da construção do sistema. De uma forma mais concisa, Bishop e Bloomfield (1998) definem um caso de segurança como:

> Um corpo de evidências documentado, que fornece argumentos convincentes e válidos de que um sistema é suficientemente seguro para determinada aplicação, em determinado ambiente.

Um dos erros mais comuns, na aplicação de preceitos da engenharia de softwares, é a preocupação com requisitos de segurança, somente depois da fase final de desenvolvimento. Tais requisitos devem ser planejados e previstos desde a fase da Análise de Requisitos, sendo, constantemente, monitoradas e aperfeiçoadas durante cada implementação.

A área de segurança de sistemas é muito vasta e, para uma única equipe de desenvolvimento abranger o estudo de tantas formas de ataques possíveis e vulnerabilidades descobertas a cada dia, seria realmente muito dispendioso e trabalhoso, interferindo em questões de custo final e prazos.

Dessa forma, a utilização de um framework amenizaria essa preocupação porque já tem funcionalidades voltadas para a segurança no seu escopo. Além disso, contribui para a diminuição dos gastos financeiros em pesquisas e estudos sobre segurança e de outros fatores incluídos como tempo de desenvolvimento. Portanto, ter em mãos uma ferramenta que já atende em sua estrutura aos requisitos de segurança básicos, embutidos em sua tecnologia, limita às equipes de desenvolvimento apenas o trabalho específico do tratamento de segurança do sistema.

1.3 PERFORMANCE

A performance é percebida de maneira mais abrupta, quando o framework é utilizado ao ponto de, quase, esgotar os seus recursos de hardware, podendo sobrecarregar a estrutura que o mantém, tornando inviável a sua uti-

lização.

Os requisitos de performance, quando não atendidos da maneira ideal, podem ser compensados através da utilização de mais recursos de hardware, mas essa é uma maneira mais custosa, financeiramente, para a resolução desse problema. O ideal na criação de um sistema é obter um equilíbrio entre performance e a quantidade de recursos ativos, que também são requisitos do sistema. Com esse entendimento, não podemos ter um sistema que atenda a tantos requisitos de segurança, que causem baixa performance no desempenho de funcionalidades básicas.

Essa avaliação, do equilíbrio entre a performance e os recursos concorrentes do sistema, deve ser explorada pela equipe de desenvolvimento para definir o framework a utilizar.

1.4 CURVA DE APRENDIZADO

No momento da adoção de novas tecnologias no desenvolvimento de um sistema, deve ser avaliado o tempo que leva para ter uma equipe de desenvolvimento plenamente adaptada àquela nova tecnologia. E entre os recursos necessários, o custo para treinamento dessa equipe. O gerente da equipe de desenvolvimento tem uma importante decisão: qual tecnologia deve ser utilizada no desenvolvimento para atender aos requisitos e os detalhes técnicos apontados pelo arquiteto de sistemas, cumprindo os prazos exigidos e tendo por base a curva de aprendizado registrada por equipes anteriores, que mostram o tempo médio para a obtenção de expertise num determinado framework.

Em alguns casos, mesmo que o tempo de aprendizado seja longo em relação a um determinado framework, há ganhos no desenvolvimento de outros sistemas requisitados que utilizam a mesma tecnologia. Tudo isso depende da demanda da equipe em relação ao framework, sabendo que a principal finalidade da adoção de qualquer uma dessas ferramentas está, justamente, na velocidade de produção de artefatos de sistemas.

1.5 RECURSOS TÉCNICOS DISPONÍVEIS

Os recursos técnicos disponíveis dependem da equipe de desenvolvimento, da empresa ou instituição a que pertencem. Isso também pode ser chamado de escalabilidade, visto que um sistema, na maioria das vezes, aumenta de tamanho devido as novas necessidades que aparecem durante o seu ciclo de vida.

A escalabilidade de um sistema reflete sua capacidade de oferecer um serviço de alta qualidade, uma vez que aumenta a demanda de sistema. Neuman (1994) identifica três dimensões da escalabilidade:

> 1. **tamanho**. Deve ser possível adicionar mais recursos a um sistema para lidar com um número crescente de usuários;
>
> 2. **distribuição**. Deve ser possível dispersar geograficamente os componentes de um sistema, sem comprometer seu desempenho;
>
> 3. **capacidade de gerenciamento**. É possível gerenciar um sistema à medida que ele aumenta de tamanho, mesmo que partes dele estejam localizadas em organizações independentes.

A equipe de desenvolvimento deve possuir pessoas com conhecimentos técnicos variados. É desejável que seus integrantes tenham qualificações técnicas que se complementem entre si, concomitantemente, com a experiência pessoal adquirida ao longo da carreira. Somente nesse caso, não houverá um grande investimento inicial no treinamento da equipe, haja vista a complementariedade de suas expertises, experiência pregressa.

Na análise da forma de trabalho da empresa, influenciando diretamente no aperfeiçoamento dos seus funcionários, podemos encontrar uma diretriz que prima pelo aperfeiçoamento de suas equipes através de treinamentos dentro do próprio local de trabalho. Essas são formas mais viáveis, economicamente e funcionalmente, para algumas empresas.

Com isso, a empresa deixa de iniciar a busca por um funcionário mais qualificado, evitando perda de tempo na adaptação e integração com a equipe e projetos em andamento.

1.6 FLEXIBILIDADE

A flexibilidade reflete a capacidade de um framework se adaptar mais facilmente as tecnologias existentes, sem a obrigatoriedade de mudar as formas de abordagem em relação a segurança, implementação e performance. Por exemplo, um framework robusto deve oferecer a possibilidade de trocar o tipo de banco de dados do sistema, como funcionalidade nativa da ferramenta. Um framework dessa categoria poderia mudar de MySQL para Postgres, sem fazer modificações internas além da mudança de poucos parâmetros na chamada de um objeto a ser instanciado.

A adoção de uma ferramenta com as características supracitadas redunda em ganho de tempo e custo no desenvolvimento de um sistema.

CONCLUSÃO

É inegável que a utilização de frameworks tem sido uma ferramenta muito útil na aplicação de princípios da engenharia de softwares, devido à constatação prática de ganho no tempo de desenvolvimento, economia de recursos, capacidade de adaptação, atendimento a requisitos de segurança e performance. Porém, todas essas características embutidas numa única ferramenta não descartam a interferência direta de uma equipe de desenvolvimento nos requisitos do sistema, uma vez que tais ferramentas apenas fornecem a estrutura básica que serve de alicerce às demais implementações. Essas ferramentas não devem desestimular a criatividade para a criação de novas funcionalidades em frameworks.

A utilização e o surgimento de novos frameworks têm contribuído de forma bastante positiva no desenvolvimento de programas e sistemas, mudando não só a perspectiva de agilidade dos desenvolvedores, mas também, a facilidade de acesso a novas tecnologias. A utilização desse tipo de ferramenta tornou-se essencial no mundo de hoje, desmistificando um pouco o ofício do programador e facilitando o acesso ao desenvolvimento de novas tecnologias.

USE OF FRAMEWORKS IN THE DEVELOPMENT OF WEB SYSTEMS

ABSTRACT. There are now a range of options for the PHP programmer, for example, choose between framework and among them we have: CakePHP, Symfony, Zend Framework, CodeIgniter, Yii 2, Phalcon, Prado, among others. We must take into account, at the time of choosing a tool, the factors that were most exploited in each of the most used frameworks and that provided advantages in some aspects, understanding that each has its strengths and weaknesses, depending on the type of Project and its purpose. The most important factors that should be considered in a framework are its stability, security, performance, learning curve, available technical resources and flexibility. The use of these tools has been widely applied in large projects and has stored within its structures several principles of software engineering that have been studied until today.

Keywords: Framework. Development. Programming. Software engineering.

REFERÊNCIAS

ALVIM, Paulo. Tirando o Máximo do Java EE 6 Open Source com jCompany© Developer Suite. 3. Ed. Belo Horizonte: Powerlogic Publishing, 2010. 12p.

Sommeville, Ian. Engenharia de Softwares, 9 Ed. São Paulo: Perarson Prentice Hall, 2011.

O autor é graduado em Sistemas de Informação, possui interesse em programação web, Linux e Banco de dados MySQL. Atualmente, exerce a função de monitor da Escola de Comunicações e pode ser contactado pelo email sgtmarcos@yahoo.com.br.

AVALIAÇÃO DA FERRAMENTA MINITEST NO DESENVOLVIMENTO GUIADO POR TESTES DO FRAMEWORK RUBY ON RAILS

Bruno Cezar Scopel Sarcinelli
Graduado em Análise e Desenvolvimento de Sistemas

RESUMO. Este artigo descreve o desenvolvimento de um sistema utilizando o modelo de desenvolvimento guiado por testes (TDD - *Test-Driven Development*) com as ferramentas do framework Ruby on Rails. O objetivo é demonstrar de maneira prática a aplicação dos conceitos de TDD nesse framework através da implementação de testes de modelo, funcionais e de visão. Este artigo pretende ser uma fonte esclarecida de consulta para iniciantes e profissionais já experientes que pretendem desenvolver utilizando o TDD no Ruby on Rails.

Palavra-chave: Ruby on Rails. TDD. Desenvolvimento ágil guiado por testes. Testes de Software. MVC.

INTRODUÇÃO

A atividade de teste de software tem como objetivo encontrar defeitos inseridos no decorrer do processo de desenvolvimento, constituindo um elemento crítico da garantia de qualidade de software, pois representa a revisão da especificação, projeto e geração de código (SOUZA e GASPAROTTO, 2013; PRESSMAN, 2002).

O teste é uma atividade realizada para avaliação da qualidade do produto, efetuando sua melhoria através da identificação de defeitos e problemas (SWEBOK, 2004).

O desenvolvimento guiado por testes (TDD - Test Driven Development) é uma técnica de desenvolvimento de software baseada em ciclos curtos de repetições, onde primeiramente o desenvolvedor escreve um caso de teste automatizado que define uma melhoria desejada ou uma nova funcionalidade, produz um código que possa ser validado pelo teste e, logo após, o refatora para um código sob padrões aceitáveis (BECK,2010). O princípio básico do TDD é incluir a atividade de teste de software no decorrer do processo de desenvolvimento, fornecendo feedback constante sobre o código que está sendo produzido.

O Ruby on Rails (RoR) é um framework de desenvolvimento ágil de software web criado em 2003 que permite o desenvolvimento de software na linguagem Ruby, utilizando a arquitetura MVC (BETTER EXPLAINED, 2017). O RoR foi adotado como plataforma de desenvolvimento por aplicações como Twitter (TECHTUDO, 2017), GitHub (GITHUB, 2017) e Basecamp (BASECAMP, 2017) e, por possuir diversas características que auxiliam e facilitam o desenvolvimento rápido de software, também é adotado por aplicações de pequeno e médio porte.

Segundo Ruby-doc (2017), o RoR foi projetado para dar suporte nativo ao TDD. Apesar disso, a maioria dos materiais que abordam TDD no RoR enfatizam a parte técnica do uso das ferramentas, mas não fornecem um embasamento sólido de como utilizar o TDD de maneira sistemática com as ferramentas do framework, dificultando o aprendizado correto da técnica nesse ambiente.

Os objetivos deste artigo são desenvolver um sistema baseado em demandas reais utilizando os conceitos de TDD em um ambiente RoR e, de maneira gradativa; avaliar as ferramentas de TDD disponíveis nesse ambiente, expondo suas vantagens e desvantagens, com o objetivo de fornecer um embasamento teórico e prático para desenvolvedores que tenham interesse de aplicar TDD nesse ambiente.

Este artigo está organizado da seguin-

te maneira: a Seção 1 apresenta os conceitos de desenvolvimento guiado por testes. A Seção 2 define o framework RoR e seus conceitos básicos. A Seção 3 apresenta a implementação e os resultados deste trabalho, culminando na conclusão.

1 DESENVOLVIMENTO GUIADO POR TESTES

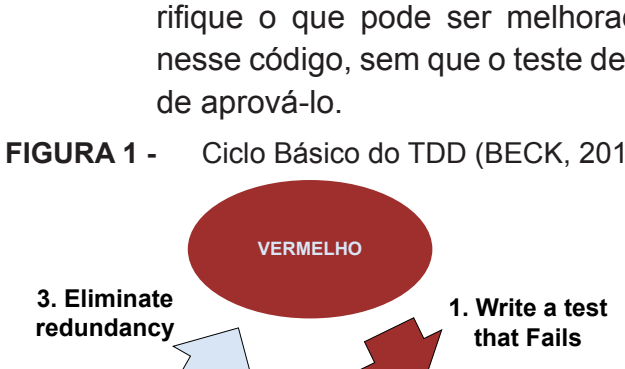
O desenvolvimento guiado por testes é uma metodologia que consiste em pequenos ciclos de desenvolvimento baseados em testes. O ciclo geral do TDD está apresentado na Figura 1 e pode ser descrito da seguinte maneira:

1) pense o que um determinado código do seu software deve implementar, descreva o contexto e defina quais as verificações por realizar. Escreva um teste para verificar a corretude desse código. Como, inicialmente, esse código não está implementado, o teste acusará que o código não foi implementado corretamente;

2) escreva o mínimo de código possível para que o teste criado, anteriormente, passe. Nesse momento, o importante é criar um código que seja aprovado pelo teste, mesmo que ele não esteja na sua forma mais completa;

3) refatore. Uma vez que o teste aprovou o código da funcionalidade, verifique o que pode ser melhorado, nesse código, sem que o teste deixe de aprová-lo.

FIGURA 1 - Ciclo Básico do TDD (BECK, 2010).



Com o TDD é possível refletir sobre a modelagem antes de escrever o código funcional, fazendo com que o sistema seja desenvolvido através de pequenos passos, até chegar a sua totalidade (SANCHEZ, 2006). Além disso, o TDD visa um código limpo, confiável, que atenda aos requisitos de forma satisfatória e cujos testes facilitem a manutenção (BAUMEISTER e WIRSING, 2017).

Alguns motivos para a adoção do TDD são: a leitura dos testes auxilia no entendimento do sistema; código desnecessário não é desenvolvido, pois só são implementados os códigos suficientes para os testes funcionarem e, consequentemente, o sistema funcionar; não existe código sem teste; os testes permitem uma refatoração segura do código, pois garantem que as mudanças não alteram o funcionamento do sistema (KAUFMANN e JANZEN, 2003).

Causevic et al. (2012) mostraram, através de experiências práticas, as vantagens que o TDD trouxe na qualidade do código a longo prazo, em conjunto com práticas de desenvolvimentos ágeis. Através de um comparativo entre o desenvolvimento convencional e o TDD, chegaram a conclusão que o TDD revela muito mais requisitos não especificados essenciais que o método convencional.

Gupta et al. (2007) demonstraram a eficácia do TDD no desenvolvimento de software de grande porte, realizando também um comparativo com o desenvolvimento sem testes. Para avaliar o processo de desenvolvimento, foram utilizadas algumas métricas como a produtividade do desenvolvedor, a qualidade do código desenvolvido e esforços gerais no desenvolvimento (manutenção, concepção, desenvolvimento e testes). Os autores concluiram que o TDD ajuda a minimizar os esforços no desenvolvimento, melhora a produtividade e a qualidade do código dos softwares, além de permitir um entendimento mais claro dos requisitos.

Como toda metodologia de desenvolvimento, há dificuldades na sua implantação.

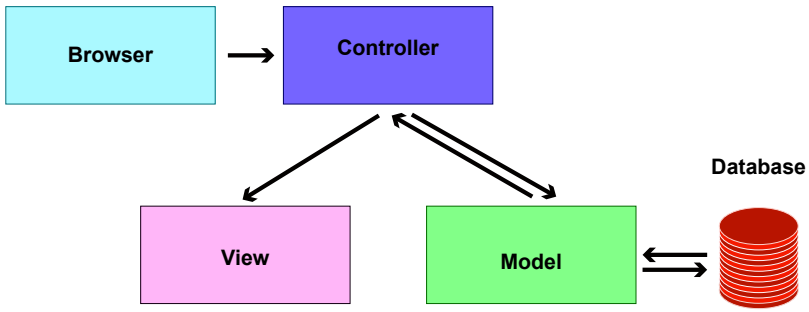
No TDD, a principal delas é a mudança cultural pela qual a equipe de desenvolvimento e a empresa precisam passar, pois o tempo gasto para a definição e o desenvolvimento dos testes precisa ser encarado pela empresa como investimento, e os desenvolvedores têm de mudar sua mentalidade na hora do desenvolvimento, dando a devida importância aos testes (ANDRADE, 2011).

2 RUBY ON RAILS (ROR)

O framework Ruby on Rails (RoR) foi desenvolvido pensando na praticidade e facilidade no desenvolvimento de aplicações Web. O framework surgiu em 2004, foi criado por David Hanson e utiliza a linguagem Ruby, que é uma linguagem orientada a objetos, interpretada, de tipagem forte e dinâmica (SOFTWARE LIVRE BRASIL, 2017).

O RoR segue o padrão de projeto MVC (*Model-View-Controller*), ilustrado na Figura 2. O MVC divide o código da aplicação em três camadas: a camada de modelos, responsável pela comunicação entre a aplicação e a base de dados; a camada de controladores, responsável por atender as requisições e preparar os dados que serão exibidos para o usuário e a camada de visões, que recebe os dados preparados pela camada de controladores e realiza a interação com o usuário (BETTER EXPLAINED, 2017).

FIGURA 2 - Padrão de projeto MVC (THOMAS, 2008)



É possível aplicar testes que cobrem todas as áreas de uma aplicação RoR, desde a entrada de dados, requisições, respostas das controladoras, visões e fluxo da aplicação (GUNDERLOY, 2017). O RoR facilita a escrita de testes pois, a medida que a aplicação é desenvolvida, arquivos de teste básicos são gerados, cabendo ao desenvolvedor estendê-los para atender às demandas da aplicação (SEA, 2009).

Segundo Thomas (2008), os possíveis testes em uma aplicação Rails são:

- teste unitário: executados continuamente durante o ciclo de desenvolvimento com o objetivo de avaliar separadamente pequenos trechos de código (unidades) de um sistema, procurando por erros de lógica e de implementação e verificando se o comportamento de classes e funções é o esperado (BARBOSA et al, 2000). Permite detectar falhas de lógica, comportamentais e de digitação, além de auxiliar na refatoração de código;
- teste funcional: avalia as requisições e respostas das controladoras. Por exemplo, avalia os métodos de um controlador com o objetivo de analisar se as requisições são bem sucedidas, se o usuário está sendo redirecionado para a página correta, se os objetos necessários para a renderização das visões foram criados corretamente, dentre outras ações. Também permite validar as respostas fornecidas pelas visões (RAILS GUIDE, 2017).
- teste de integração: analisa o fluxo da aplicação, avaliando a interação entre modelos e controladores (RAILS GUIDES TESTING, 2017).

Rappin et al. (2011) abordam o desenvolvimento guiado por testes utilizando RoR, fazendo uma correlação entre o desenvolvimento convencional e o desenvolvimento usando TDD. Entretanto, o livro não expõe as facilidades e dificuldades da técnica no RoR, focando apenas em exemplos técnicos do uso das ferramentas.

Corbucci e Aniche (2014) abordam o

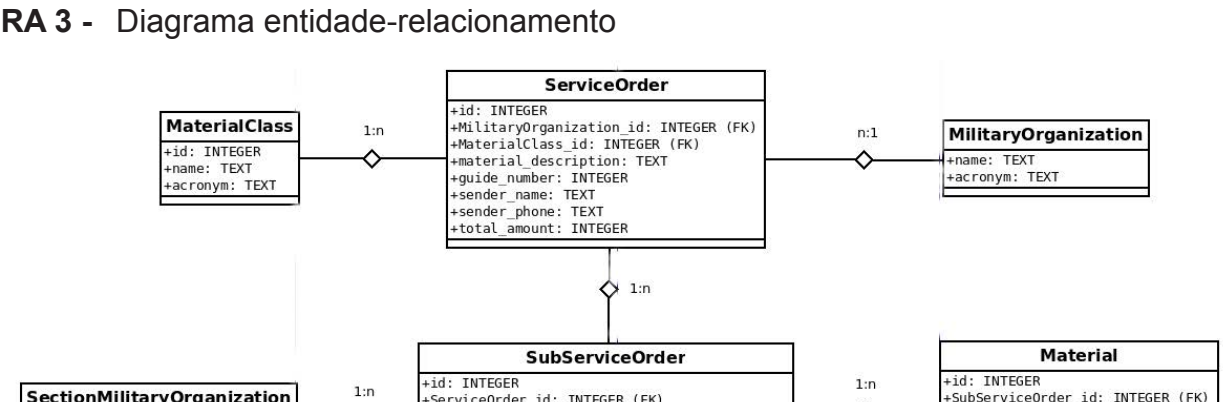
TDD através de exemplos, desde os testes mais simples até testes mais complexos. Entretanto, o livro recai no mesmo problema de outros materiais: não expõe as experiências, dificuldades e facilidades da aplicação desse método de desenvolvimento no RoR.

3 IMPLEMENTAÇÃO E RESULTADOS

Para demonstrar os conceitos de TDD na prática e avaliar as gems de TDD do RoR (AKITA ON RAILS, 2017), foi implementado um sistema de ordens de serviço para atender as necessidades de uma determinada empresa (fictícia), cujo processo de abertura e controle das ordens de serviço ainda são realizados manualmente.

O diagrama entidade-relacionamento mostrado na Figura 3 foi utilizado como ponto de partida para os primeiros testes do sistema.

FIGURA 3 - Diagrama entidade-relacionamento



O RoR permite o reaproveitamento de componentes utilizando gems (AKITA ON RAILS, 2017), que são pacotes com código Ruby gerenciados por uma aplicação do sistema operacional, chamada rubygems (AKITA ON RAILS, 2017). Utilizando gems é possível reutilizar componentes prontos que auxiliam em várias partes de uma aplicação, como por exemplo na autenticação de usuários, na renderização de imagens, e também no desenvolvimento de testes (RAILSGUIDE,2017).

Existem muitas ferramentas de testes para RoR, para comparar e exemplificar a diferença da ferramenta Minitest com outra, escolheu-se a ferramenta RSPEC. A Minitest é a biblioteca nativa do RoR para a escrita de testes de modelo, de controlador e de integração. Com a Minitest é possível testar código Ruby, utilizando uma grande variedade de asserções (RAILSGUIDE,2017).

Segundo Relish (2017) a RSpec é uma ferramenta de teste baseada na metodologia BDD (*Behaviour-Driven Development*), que permite especificar o comportamento desejado do código Ruby utilizando uma DSL (*Domain-Specific Language*) simples e expressiva, facilitando a leitura e o entendimento do código de teste. A RSPec também pode ser usada para especificar testes de modelo, controlador e integração.

O ponto de partida no desenvolvimento da nossa aplicação foi o mapeamento do diagrama entidade-relacionamento na camada de modelos do RoR. Para isso, os primeiros testes de modelo foram elaborados utilizando as gems Minitest, segundo o RAILSGUIDE (2017) e Rspec (RELISH, 2017).

3.1 TESTES DE MODELO

Com o objetivo de entender as diferenças entre a Minitest e a RSPec, os primeiros testes de modelo foram elaborados, utilizando as duas gems, e criados para atender o seguinte requisito da entidade ServiceOrder, que modela uma ordem de serviço no sistema: uma ordem de serviço não pode ter uma descrição de material vazia.

Seguindo a abordagem TDD, o primeiro passo é criar um teste que analise se é possível salvar uma ordem de serviço com um nome vazio. Caso seja possível, o teste deve acusar um erro. O código a seguir mostra o código desse teste escrito utilizando Minitest. Por questões de simplicidade, a entidade ServiceOrder passará a ser chamada de So a partir de agora.

```
1. Class Sotest < ActiveSupport:: TestCase
2.  fixtures :sos
3.  test "service order should have material description"
4.    service_order = sos(:material_description_nil
5.    assert !service_order.save,
6.    "service order saved without material description"
7.  end
8. end
```

A linha 1 declara a classe de teste do modelo So, que sempre deve estender da classe base de teste de modelos do Minitest (ActiveSupport::TestCase). Por convenção, todo nome de classe de teste escrita com Minitest deve terminar com a palavra Test, e todos os métodos que realizam testes devem começar com a palavra-chave test. Essa é a convenção adotada pelo RoR para que, quando os testes forem executados, ele possa identificar as classes e métodos que realizam testes e invocá-los.

Na maioria dos testes, há necessidade de existir uma base de testes preenchida com informações de interesse. Antes da execução de qualquer teste, o RoR carrega uma base de testes e a deixa disponível para qualquer teste em execução acessá-la. A linha 2 informa que essa classe de teste utilizará as *fixtures* de uma So. *Fixtures* são conjuntos de dados pré-definidos em um arquivo de texto YML [28], que são automaticamente carregados para a base de dados de teste antes de qualquer teste ser executado. Com *fixtures* é possível acessar linhas específicas de uma tabela utilizando rótulos, tornando-a uma ferramenta bastante atrativa para os primeiros testes de modelo.

A linha 3 declara o método de teste. A linha 4 acessa a *fixture* material_description_nil, recuperando da tabela So uma linha com o campo material_description nulo, e armazenando uma referência para essa linha na variável service_order. As linhas 5 e 6 realizam uma asserção, que é um comando que avalia um objeto de acordo com um resultado esperado. Nesse caso, espera-se que não seja possível salvar a referência service order, uma vez que ela não possui uma descrição. O método save pode ser invocado a partir da referência service_order, pois o RoR segue o padrão de projeto Active-Record (RAILS GUIDES, 2017).

O primeiro erro acusado pelo teste foi na linha 2, pois o arquivo YML com as *fixtures* não foi criado. Após a criação do arquivo de *fixtures*, o próximo erro acusado foi a ausência de uma tabela So na base de testes, pois a primeira ação do RoR ao detectar um arquivo de *fixtures* é carregá-lo na base de testes. Para solucionar esse erro, dois arquivos foram criados: um arquivo de modelo So vazio, que representará uma ordem de serviço na camada de modelos do sistema, e um arquivo de migração, responsável por criar a tabela So no banco de dados.

O próximo erro acusado foi a ausência de uma *fixture* chamada material_description_nil, uma vez que o arquivo de *fixtures* foi criado mas não foi preenchido. Após a inserção da linha material_description_nil no arquivo de *fixtures*, o próximo erro acusado foi a ausência da coluna material_description na tabela de ordens de serviço. Para corrigir esse erro, um novo arquivo de migração foi criado.

Após as alterações mencionadas anteriormente, o teste parou de informar a presença de erros e indicou uma falha: as linhas 5 e 6 acusaram que foi possível salvar uma ordem de serviço sem o campo material_description. Para corrigir essa falha, foi inserida uma validação de presença do campo material_description no arquivo de modelo So. Após essa validação, o teste foi executado sem erros e falhas.

Os pequenos ciclos de desenvolvimento utilizados para atender o requisito apresentado, também chamados de baby steps,

auxiliam no desenvolvimento gradativo de uma aplicação, levando à criação apenas de arquivos, métodos e atributos essenciais para atendê-lo, contribuindo com a limpeza de código.

Com o intuito de avaliar as diferenças entre o Minitest e o RSPec, o teste implementado anteriormente foi transcrito para o RSPec, e está apresentado no algoritmo abaixo.

```
1. RSpec.describe So, :type => :model do
2.  fixtures :sos
3.  it "must have material description"do
4.   service_order =
5.   sos(:material_description_nil).should_not be_valid
6.  end
7. end
```

As linhas 1 e 2 são semelhantes às linhas do código de teste com Minitest, informando que testes RSpec de modelo serão escritos para a entidade So e declarando as *fixtures*, respectivamente. Já as linhas 3 e 4 demonstram a principal diferença entre as duas gems: no RSPec, a descricão dos testes é feita de maneira comportamental, utilizando uma notação que se assemelha a uma descrição textual de um teste, auxiliando no entendimento do código.

Apesar do RSPec possuir uma linguagem mais informal para descrição dos testes, as duas gems analisadas atenderiam satisfatoriamente os testes desenvolvidos neste trabalho. Pelo fato de ser a gem padrão do framework, optou-se por utilizar o Minitest nos demais testes de modelos, funcionais e de visão.

Todas as entidades da aplicação foram mapeadas na camada de modelos do framework utilizando TDD com a gem Minitest, inclusive com restrições referentes à presença ou ausência de atributos, formato, tamanho mínimo, tamanho máximo e relacionamento entre as entidades, gerando uma camada de modelos coerente com as restrições impostas na modelagem de dados.

3.2 TESTES FUNCIONAIS

Testes funcionais foram criados para avaliar as requisições e respostas de todas as classes controladoras da aplicação. Para exemplificar como esses testes foram elaborados, serão apresentados os testes funcionais da controladora Material, responsável por gerenciar o acesso à entidade Material.

Requisições realizadas para um controlador RoR são feitas utilizando um dos seguintes métodos HTTP: GET, POST, PATCH, PUT ou DELETE. Dependendo do método utilizado na requisição e dos parâmetros passados, o RoR faz um roteamento automático da requisição para um método de um controlador, que será responsável por realizar todo o processamento necessário para respondê-la.

Os seguintes métodos são necessários na controladora Material:

- new: invocado através de uma requisição HTTP GET. Prepara os dados necessários para a criação de um Material e redireciona para uma visão;
- create: invocado através de uma requisição HTTP POST. Recebe um novo Material proveniente de uma visão, salva-o no banco de dados e redireciona para uma visão;
- destroy: invocado através de uma requisição HTTP DELETE. Recebe uma identificação de um Material já existente no banco de dados, remove-o e redireciona para uma visão.

Uma das restrições da modelagem de dados do sistema é que um Material só pode existir se estiver associado a uma SubServiceOrder e a uma ServiceOrder. Portanto, qualquer requisição para a controladora Material deve passar como parâmetro a identificação da SubServiceOrder e da ServiceOrder. Conforme o Rails Guides (2017), esse conceito pode ser implementado no RoR utilizando o conceito de rotas aninhadas, que força todas as requisições à controladora Material a passarem identificadores da SubServiceOrder e da ServiceOrder. Caso esses parâmetros não sejam passados, a controladora Material não

recebe a requisição.

A Tabela I mostra todas as possíveis requisições à controladora Material usando rotas aninhadas.

TABELA 1 - ROTAS ANINHADAS DA CONTROLADORA MATERIAL

Method	Routes	Controller#Action
GET	/sos/:so_id/sub_service_orders /:sub_service_order_id/materials/new	materials#new
POST	/sos/:so_id/sub_service_orders /:sub_service_order_id/materials	materials#create
DELETE	/sos/:so_id/sub_service_orders /:sub_service_order_id/materials/:material_id	materials#destroy

Para demonstrar como os testes das controladoras foram elaborados e como eles lidaram com os diferentes tipos de requisições e rotas, o próximo algoritmo descreverá três testes do controlador Material, um teste para cada tipo de requisição aceita. A controladora Material foi escolhida, pois as rotas de acesso aninhadas tornam seus testes mais complexos que os testes de outras controladoras.

```
1.  class MaterialsControllerTest < ActionController::TestCase
2.  def setup
3.   create (:material)
4.   @so= So.first
5.   @sub_service_order = SubServiceOrder.first
6.   @material = Material.first
7.  end
```

A linha 1 declara a classe de teste do controlador Material, que sempre deve estender da classe base de teste de controladoras do Minitest (ActionController::TestCase), para os testes funcionais.

A linha 2 define um setup para a entidade material. Setup é um conceito RoR que permite executar um bloco de código antes do início de cada teste (RAILSGUIDE,2017).

Uma das maneiras de utilizar fixtures nos testes é criar tuplas que rompem as restrições do banco de dados e utilizá-las nos testes. Entretanto, conforme os modelos da aplicação se tornam coerentes e testados, as tuplas inconsistentes das *fixtures* geram erros indesejados, exigindo revisão e manutenção constantes. Por essa razão, *fixtures* foram substituídas por factories em todos os testes.

Factories são modelos de registros que podem ser usados para popular uma base de testes, criando assim uma base de testes mais consistente e sem repetições. FactoryGirl é uma gem utilizada como fábrica de instâncias, mais versátil que as fixtures e cuja lógica fica isolada da implementação específica dos testes (THOUGHTBOT, 2017).

Muitos testes funcionais necessitam de uma base de testes para funcionarem. Na linha 4, a base de testes foi populada seguindo o modelo de uma factory, utilizando o método create. Esse método salva uma instância de Material na base de dados de teste para que possa ser utilizado em todos os testes.

Na linha 5, a variável global @so recebe o primeiro objeto encontrado na base de dados da entidade So, utilizando do método first da ActiveRecord. A partir dessa definição, qualquer teste da classe Material pode acessar essa variável e utilizar-se de seus atributos. O mesmo acontece nas linhas 6 e 7 com as entidades SubServiceOrder e Material.

```
10. test "action new should create an instance variable" do
11.   get :new, so_id: @so,
12.   sub_service_order_id: @sub_service_order
13.   assert_not_nil assigns (:material),
14.   "action new does not create an instance variable of
15.   type material"
16.  end
17.  test "action create redirects to action show after
18.   creating a well-formed material based on the form" do
19.   post :create, so_id: @so,
20.   sub_service_order_id: @sub_service_order,
21.   material: {name: "Name", amount: 10.0,
22.   value: 10.0, unit: "Unit",
23.   sub_service_order_id: @sub_service_order}
24.   asssert_redirected_to
```

```
25.   so_sub_service_order_paht(@so,
26.   @sub_service_order)
27.  end
28.  test "after calling the destroy action passing
29.  an invalid id, you must be redirected to the
30.  action show of the sub service order"do
31.   delete :destroy, so_id: @so,
32.   sub_service_order_id: @sub_service_order,
33.   id: -1
34.   assert_redirected_to
35.   so_sub_service_roder_paht (@so,
36.   @sub_service_order)
37.  end
38. end
```

O teste presente entre as linhas 10 e 16 analisa se, após uma requisição GET para a action new, o controlador instanciou corretamente uma variável material, que será utilizada na visão para a criação de um novo Material. Note que, devido ao aninhamento de rotas, foi necessário passar por parâmetro os identificadores da So e da SubServiceOrder.

O teste presente entre as linhas 17 e 27 verifica se a *action create* redirecionará para o local correto após ter recebido um Material preenchido do formulário, através de uma requisição POST. Já o teste presente entre as linhas 28 e 38 analisam se a *action destroy* se comporta corretamente caso o id da Material a ser removida for inválido.

Utilizando os recursos do Minitest, foi possível desenvolver utilizando TDD todos os métodos de todas as controladoras, testando de maneira exaustiva os dados por eles preparados, o processamento realizado e os seus redirecionamentos, considerando parâmetros válidos e inválidos.

3.3 TESTES DE VISÃO

Testes de visão foram criados com o objetivo de verificar se a interface com o usuário está de acordo com o que foi especificado. Ou seja, com esses testes é possível verificar se as *tags* html necessárias estão presentes na tela e se as informações nelas contidas são exatamente as informações que deveriam estar sendo exibidas.

Conforme o RailsGuide (2017), o *assert select* é um parser RoR que analisa o conteúdo HTML retornado por uma requisição feita a um controlador, e é uma poderosa ferramenta na validação de visões.

Nessa seção, apresentaremos alguns requisitos e restrições que devem ser atendidos pelas visões do controlador ServiceOrder, demonstrando como testes de visão podem ser implementados em RoR.

Como sistema elaborado é de um controle de ordens de serviço, a primeira visão apresentada deve conter uma tabela com todas as ordens de serviço já criadas. Essa visão é retornada pela *action index* do controlador ServiceOrder.

O primeiro requisito a ser validado foi que a visão *index* deve conter exatamente uma tag h2 com o conteúdo SERVICE ORDERS. O teste abaixo valida esse requisito.

```
1. test "index.html.erb must have a h2"do
2.  get :index
3.  assert_select 'h2', 1
4. end
5. test "index.html.erb h2 must have header SERVICE
6.  ORDERS" do
7.  get :index
8.  assert_select 'h2'do
9.   assert_select 'b', {count: 1,
10.   text: "SERVICE ORDERS"},
11.   "There is no header for service orders"
12.  end
13. end
```

O teste das linhas 1 até 4 está cobrando a presença de exatamente uma tag h2. Para isso, faz uma requisição GET para a *action index*, requisitando à controladora que redirecione para a visão *index*, como se fosse um usuário acessando via navegador a action index da ServiceOrder. O html é retornado e pode ser analisado pelo comando assert_select. O assert_select verifica se, nesse html retornado, possui exatamente uma tag do tipo h2. No teste das linhas 5 até 13, após selecionar a única tag existente do tipo H2, o assert_select analisa se dentro da tag h2 há exatamente uma tag b com o conteúdo dizeres SERVICE ORDERS.

Ambos os testes falham, pois a *view*

index encontra-se vazia. Para os testes passarem basta adicionar o código descrito abaixo, garantindo a existência de uma tag h2 e um cabeçalho para a *index* da ServiceOrder.

```
1.  test "index.html.erb must have a table"do
2.   get :index
3.   assert_select 'table', 1
4.  end
5.  test "index.html.erb must contain exactly one table
6.   with id sos" do
7.   get :index
8.   assert_select 'table'do
9.    assert_select "[id=?]", "sos"
10.  end
11. end
12. test "field material description of SOs is being
13.  displayed on table" do
14.  get :index
15.  @sos = So.all
16.  assert_select "table"do
17.   assert_select "[id=?]", "sos"do
18.    assert_select "tr" do
19.     @sos.each do |so|
20.      assert_select "td", {text:
21.       so.material_description} do
22.        assert_select "[id=?]",
23.        "so_material_descrption_"
24.        +so.id.to_s, {count: 1}
25.      end
26.     end
27.    end
28.   end
29.  end
30. end
```

```
<h2><b>SERVICE ORDERS</b></h2>
```

O próximo teste foi criado para validar a presença de uma tabela que lista as ordens de serviço na *index*. Essa tabela deve ter um *id* específico e, inicialmente, exibir pelo menos o campo material_description de todas as ordens de serviço presentes no banco. O código seguinte implementa esse teste.

Nas linhas 12 até 30, o teste fez uma requisição get para a controladora, recebendo de volta o conteúdo html da *index*. A variável global @sos recebeu todas as instâncias de So que estão na base de dados e, logo após, analisou se, para cada So presente no banco, há um campo td exibindo o atributo material_description.

Utilizando TDD, foi possível construir de maneira gradativa a tela inicial do sistema, validando todos os campos da tabela e todos os links que devem estar presentes. A Figura 4 mostra essa *interface*.

FIGURA 4 - *Interface INDEX* da ordem de serviço

SERVICES ORDERS

MATEIAL DESCRIPTION	GUIDE NUMBER	OPTIONS		
Viatura Blindada	2014110001	Show	Edit	Destroy
Motor de Embarcação	2014110002	Show	Edit	Destroy

Create new service order
Manage material classes
Manage military organizations
Manage section military organizations

Todas as demais telas do sistema, que envolvem criação, remoção, edição e atualização de várias entidades do sistema, incluindo entidades que possuem relacionamentos, foram criadas por meio de testes. As telas ficaram simplificadas, mas exibiram de maneira funcional todas as informações exigidas pelo cliente, buscando minimizar os problemas durante a utilização do sistema.

Testes de visão são muito importantes, pois, são através das visões que os usuários interagem com o sistema. Caso não sejam bem testados, erros graves podem acontecer durante a execução do sistema, podendo causar muito prejuizo a quem o utiliza.

É importante salientar que, apesar do layout de todas as visões estarem simplificados, os testes não levam em consideração os detalhes de estilo da aplicação. Isso significa que, caso um desenvolvedor deseje tornar a visão mais bem elaborada, os testes continuarão passando, desde que os dados sejam exibidos corretamente.

3.4 OUTRAS FERRAMENTAS PARA TESTE

Há outras gems RoR que podem ser usadas em um ou mais tipos de testes. Nesta seção duas delas serão descritas: o Cucumber e o Capybara.

Segundo o site oficial da ferramenta, o Cucumber é uma gem que cria um novo ambiente no projeto e permite a escrita de testes

de aceitação em uma linguagem muito próxima da natural. Já o Capybara, segundo Jnicklas (2012), é uma gem que ajuda a testar aplicações web, simulando como um usuário real interagiria com a aplicação.

O Cucumber foi desenvolvido para um padrão de desenvolvimento diferente do abordado neste artigo, chamado BDD (*Behavior Driven Development*). Seus testes são estabelecidos por cenários de teste onde é descrita uma ação e como o sistema deve se comportar. Um exemplo para nosso sistema de ordem de serviço é preencher todos os campos do formulário para uma nova ServiceOrder e clicar em salvar. O teste deve garantir que o usuário não ficou retido na mesma visão. O código abaixo descreve esse teste escrito com Cucumber.

```
1. Funcionalidade: Preencher o formulário da SO
2. Cenário:
3.    Deve preencher todos os campos do formulário e
salvar
4.   com sucesso
5.   Dado que eu estou na págino do formulário da SO
6.   Quando eu preencher todos  os campos
7.   E clicar em "Create SO"
8.   Então deve redirecionar para a action show da SO
```

A linha 1 descreve a funcionalidade do teste. As linhas 2 a 8 descrevem o cenário que deve ser realizado. Uma vez descrito o cenário no Cucumber, com o auxílio da *gem* Capybara, os campos do formulário serão preenchidos, como se fosse um usuário interagindo com a interface. Segue abaixo o código do Capybara para preenchimento do formulário da So.

```
1.   Dado/^que eu estou na página do formulário$/ do
2.     visit new_so_path
3.   end
4.   Quando /êu preencher todos os campos$/ do
5.     fill_in "material_description", :with=>"Blindado"
6.     fill_in "guide_number", :with=> "2014120001"
7.     fill_in "sender_name", :with=> "CB CICLANO"
8.     fill_in "sender_phone", :with=> "(67)1234-5678"
9.     fill_in "total_amount", :with=> "10"
10.    page.select "1", :from =>'material_class_id'
11.   page.select "2", :from =>'military_organization_id'
12.  end
13.  E /^clicar em "(.*?)"$/ do  |so_submit|
14.    find_button (so_submit).click
15.    save_and_open_page
16.  end
17.  Então /^deve redirecionar$/ do
18.    visit so_path(@so)
19.  end
```

Nas linhas 1 até 3, é realizada a requisição de um novo formulário para criação de uma nova So. Nas linhas 4 até 12, são realizados os preenchimentos dos campos, o código fill_in é responsável por preencher os fields do formulário. O page.select, nas linhas 10 e 11, realizam a seleção de um item do *select*.

As linhas de 13 até 16 simulam um clique no botão so_submit, salvando como o método save_and_open_page. As linhas 17 até 19 redirecionam para a *action show* da So.

CONCLUSÃO

O TDD é uma área muito ampla e relativamente recente, entretanto poucos materiais abordam por completo essa forma de desenvolvimento no ambiente RoR. Este artigo abordou o uso de desenvolvimento guiado por testes no RoR através da implementação de um sistema de ordem de serviço, mostrando como os testes unitários, funcionais e de visão podem ser feitos. Durante o desenvolvimento, foram citadas algumas dificuldades e facilidades dessa metodologia, com intuito de auxiliar aqueles que desejam utilizar essa forma de desenvolvimento no RoR.

O uso do TDD na implementação do sistema de ordens de serviço permitiu com que o sistema fosse desenvolvido de maneira gradativa, atendendo apenas os requisitos essenciais para o cliente. Por conta da mudança e adaptação com o novo paradigma, houve um atraso no desenvolvimento, mas que foi compensado pelo fato da aplicação conter um código bem testado, que facilitará futuras manutenções.

Outra vantagem dessa forma de desenvolvimento é a refatoração e a depuração de erros do código. Refatorar o código garante que ao final do desenvolvimento tem-se um código mais limpo, somente com o que interessa para que o sistema funcione, acabando com inserção de códigos desnecessários que po-

luem e dificultam a depuração.

Com os testes de modelos, funcionais e de visão o sistema será capaz de detectar alterações indevidas em qualquer uma das três camadas. Isso mostra que o TDD é muito importante em ambientes onde há alta rotatividade de desenvolvedores, pois evitará que erros cometidos por desenvolvedores em fase de adaptação com o sistema, auxiliando na estabilidade da aplicação.

O framework RoR possui ferramentas suficientes para o desenvolvimento TDD, e sua ferramenta padrão (Minitest) é suficiente para a realização de testes completos de modelo, funcionais e de visão completos. Dentre os três tipos de testes, o que mais houve dificuldade foi o teste de visão, pois a documentação da principal função utilizada (assert_select) é confusa e pouco explicativa.

Manter uma base de testes consistentes é de extrema importância para que os testes tenham efeito. Em diversos momentos, no decorrer do desenvolvimento, testes estavam aparentemente funcionando, quando na verdade nem estavam sendo executados por conta de um preenchimento equivocado da base de testes. O uso de *Factories* se mostrou mais promissor que o uso de *Fixtures*, pois facilita a criação e manutenção da base de testes.

Futuramente, pretende-se melhorar o sistema de ordem de serviço, aplicando as demais ferramentas de TDD do RoR, como os testes de integração do Minitest, e também aplicar o conceito de BDD utilizando as gems RSpec, Cucumber e Capybara.

Alguns artigos sobre TDD mencionam possíveis métricas para se avaliar, a longo prazo, os impactos do TDD. Ainda em um escopo futuro pretende-se avaliar os impactos causados por conta da implementacão desse sistema, auxiliando também na criação de novas métricas para análise da eficácia dos testes de software.

REFERÊNCIAS

AkitaonRails. Entendendo RubyGems. Disponivel em: <http://www.akitaonrails.com/2009/02/02/entendendo--rubygems#.VI4YMCvF91Y >. Acesso em: 05 setembro 2017.

AkitaonRails. Entendendo RubyGems. Disponível em <http://www.akitaonrails.com/2009/02/02/entendendo--rubygems#.VIdEsq2BvFY>. Acesso em: 09 setembro 2017.

ApiRails. Disponivel em: <http://guides.rubyonrails.org/testing.html >. Acesso em: 05 setembro 2017.

ANDRADE, Bruno Eustáquio. et al. TDD-Test Driven Development. 2011 Disponivel em: <http://pt.scribd.com/doc/53948144/Texto-Explicacao-TDD >. Acesso em: 20 outubro 2017.

Barbosa, E.F; Maldonado, J.C; Vincenzi, A.M.R.; Delamaro, M.E;Souza, S. R. S; Jino, M. **Introdução ao Teste de Software**. ICMC-USP-São Carlos, 2000.

Basecamp. The best parts of Basecamp have been turned into open-source projects. Disponível em <https://basecamp.com/open-source>. Acesso em: 09 outubro 2017.

Baumeister, H. and Wirsing, W., **Applying Test--First Programming and Iterative Development in Building an E-Business Application**. Disponível em http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.19.4707&rep=rep1&type=pdf. Acesso em: 18 outubro de 2017.

Beck, Kent, TDD - Desenvolvimento guiado por testes. Bookman, 2010.

BetterExplained. Intermediate Rails: Understanding Models, Views and Controllers. Disponível em <http://betterexplained.com/articles/intermediate-rails-understanding-models-views-and-controllers/>. Acesso em: 09 setembro 2017.

Causevic, A.; Punnecatt, S.; Sundmark, D., **Quality of Testing in Test Driven Development**, IEEE: 2012 Eighth International Conference on the Quality of Information and Communications Technology.

Corbucci, H e Aniche, M, **Test Driven Development:** Teste e design no mundo real com Ruby. Casa do Código, 2014, 207 p.

Cukes. Cucumber. Disponível em <https://cucumber.io/>. Acesso em: 19 outubro 2017.

Github. GitHub developer. Disponível em <https://developer.github.com/>. Acesso em: 09 setembro 2017.

GUNDERLOY, M.; NAIK, P.; NORIA, X. **Guia do Rails** - Um Guiapara Testar Aplicações Rails , 2011. Disponivel em: <http://guias.rubyonrails.com.br/testing.html >. Acesso em: 10 outubro 2017.

Gupta, A. and Jalote, P., **An Experimental Evaluation of the Effectiveness and Efficiency of the Test Driven Development** , IEEE: 2007 First International Symposium on Empirical Software Engineering and Measurement.

Jnicklas. Test your app with Capybara. Disponível em <http://tutorials.jumpstartlab.com/topics/capybara/capybara_with_rack_test.html>. Acesso em: 19 outubro 2017.

Kaufmann, R. and Janzen, D., **Implications of test-driven development:** a pilot study , OOPSLA '03 Companion of the 18th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications, 2003.

Pressman, R. S. **Engenharia de Software**. 5 ed. Rio de Janeiro: Mc Graw Hill, 2002, 843 p.

RailsGuides. Disponivel em: <http://guides.rubyonrails.org/routing.html>. Acesso em: 05 outubro 2017.

_____. Disponivel em: <http://guides.rubyonrails.org/ >. Acesso em: 11 outubro 2017.

Rails Guides. Active Record Basics Disponivel em: <http://edgeguides.rubyonrails.org/active_record_basics.html>. Acesso em: 05 setembro 2017.

RailsGuidesTesting. Disponivel em: <http://guides.rubyonrails.org/testing.html>. Acesso em: 11 outubro 2017.

Rappin, Noel, Rails test prescriptions - Keep Your Application Healthy, 1 ed. Pragmatic Bookshelf, 2011.

Relish. RSpec. Disponível em <https://relishapp.com/rspec>. Acesso em: 02 setembro 2017.

Ruby-Doc. Minitest. Disponível em <http://ruby-doc.org/stdlib-2.0/libdoc/minitest/rdoc/MiniTest.html>. Acesso em: 12 setembro 2017.

SANCHEZ, I., **Introdução do Desenvolvimento voltado a Testes (TDD)** ¡ Coding Dojo Floripa. Coding Dojo Floripa , 2006. Disponivel em: <http://dojofloripa.wordpress.com/2006/11/07/introducao-ao-desenvolvimento-orientado-a-testes>. Acesso em: 11 novembro 2014.

SEA, T., Minicurso de TestesOnRails. Slideshare, 10 Agosto 2009 .Disponivel em: <https://pt.slideshare.net/seatecnologia/minicurso-de-testesonrails>. Acesso em: 11 outubro 2017.

Software Livre Brasil. Disponível em <http://softwarelivre.org/ruby-on-rails>. Acesso em: 12 outubro 2017.

Souza, K. and Gasparotto, A., **A importância da atividade de teste no desenvolvimento de software**, XXXIII Encontro nacional de engenharia de produção, 11 outubro 2013 . Disponível em:<http://www.abepro.org.br/biblioteca/enegep2013_TN_STO_177_007_23030.pdf>. Acesso em: 18 outubro 2017.

Swebok 2004,Guide for the software engineering body of knowledge, 2004 version, IEEE computer society, California, EUA.

Techtudo. Guia do Twitter: descubra como fazer tudo com dicas e tutoriais. Disponível em <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2011/03/twitter-guia-completo.html>. Acesso em: 09 setembro 2017.

Thomas, D. H., **Desenvolvimento Web Ágil com Rails**. Porto Alegre: Editora Bookman, 2008.

Thoughtbot, Inc. "Factory Girl". Disponível em <https://github.com/thoughtbot/factory_girl_rails>. Acesso em: 20 outubro 2017.

O Autor é Bacharel em Análises e Desenvolvimento de Sistemas pela UFMS, Instrutor dos Cursos IT Essencial, CCNA 1, CCNA 2 da Academia Cisco e possui o curso de Guerra Cibernética para sargentos e pode ser contactado por intermédio do email scopel.bruno@eb.mil.br.

ÁREA DE CONCENTRAÇÃO

CIÊNCIA & TECNOLOGIA

ESCOLA DE COMUNICAÇÕES

AS VANTAGENS DA UTILIZAÇÃO DO POWER LINE COMMUNICATION EM OPERAÇÕES INTERAGÊNCIAS

Daniel Mateus Coelho
Pós-graduado em Engenharia de Sistemas de Radiocomunicação

RESUMO. Este trabalho busca apresentar as vantagens na utilização do Power Line Communications (PLC) em Operações Interagências, tendo em vista a dificuldade de ser disponibilizada infraestrutura de rede de dados de banda larga para todos os órgãos envolvidos nesse tipo de operação.

Palavras-chave: Vantagens. PLC. Banda larga. Interagência.

INTRODUÇÃO

A crescente necessidade de operações das Forças Armadas em conjunto com outros órgãos governamentais em seus três níveis – federal, estadual e municipal – principalmente para combater o crime organizado e o tráfico de drogas nas grandes cidades, aumenta a demanda por troca de informações através de redes de dados de grande capacidade.

A infraestrutura de redes de dados para dar suporte demanda vultosos recursos, nem sempre disponíveis, por parte dos órgãos envolvidos nas operações, e nem sempre é possível disponibilizar essa rede para todos os envolvidos, pelas características dos locais onde se desenvolvem as ações.

Para se disponibilizar uma rede de dados de banda larga para diversos usuários e com baixo investimento, utilizando infraestrutura existente, pode-se utilizar a tecnologia do *Power Line Communications* (PLC), principalmente em localidades onde não há disponibilidade de internet de alta velocidade, pois essa tecnologia permite o uso de rede elétrica para a transmissão de dados.

Dessa forma, o objetivo deste artigo é apresentar as vantagens da utilização do PLC em Operações Interagências.

A primeira seção apresenta o PLC, a segunda seção apresenta as operações interagência, a terceira seção apresenta as vantagens da utilização do PLC nas operações interagências, culminando na conclusão do presente artigo.

1 PLC

1.1 A DEFINIÇÃO

O PLC, do inglês *Power Line Communications*, é a tecnologia que utiliza a rede elétrica como meio físico para transporte de sinais de dados (BELETINNI, 2015 apud SANTOS, 2008).

O *Power Line Communication* é um sistema que permite a transmissão de sinais de internet, voz, vídeo e comunicação digital e analógica por meio da rede elétrica (BELETINI, 2015).

1.2 HISTÓRIA

A tecnologia do *Power Line Communication* (PLC) não é nova, seu primeiro uso remonta da década de 1930, quando visava monitorar o desempenho e a segurança das linhas, através do *Riple Control* (RC). Com isso era possível transmitir com alta potência e baixas taxas de velocidade.

Essa tecnologia permitia uma comunicação de modo unidirecional, sendo usada para a realização de pequenas tarefas como a ativação da iluminação pública, sistemas de telemetria, controle remoto e comunicação de voz até meados de 1980. (BELETINNI, 2015 apud SANTOS, 2008).

Na década de 1980, empresas europeias passaram a realizar pesquisas no senti-

do de analisar as características da rede elétrica e com isso chegaram a conclusão de que a faixa de 5 a 500 kHz possuía potencial de uso em relação ao sinal/ruído e a atenuação do sinal transmitido (SANTOS, 2008).

Na década de 1990, foram iniciados os testes de comunicação de alta velocidade na Inglaterra. Sendo anunciado que os problemas causados por ruídos ou interferências haviam sido solucionados e que estavam sendo realizados testes de acesso à internet com a utilização da tecnologia desenvolvida. (BELETINNI, 2015).

1.3 PRINCÍPIO DE FUNCIONAMENTO

O princípio de funcionamento da tecnologia PLC consiste em sobrepor um sinal de alta frequência (MHz) sobre os 60 Hz dispostos na rede elétrica (ROSA, 2012).

A tecnologia PLC consiste na transmissão de dados, com utilização da faixa de frequência compreendida entre 1 e 30 MHz, devido às características do meio de transmissão que introduz alta degradação fora dessa faixa. No Brasil, a Resolução 527/09, da ANATEL, define duas faixas para a utilização do serviço:

- de 1,7 a 30 MHz, destinada a aplicações com distância de até 30m;
- de 30 a 50 MHz para serviços de distâncias curtas, tipicamente 3 metros (VITAL, 2012).

O sinal transmitido com a tecnologia PLC, trafega em redes de baixa e média tensão. Com isso, existindo vários empecilhos na transmissão na rede de corrente alternada, segundo ROSA (2012), podemos evidenciar os seguintes:

- existência de ruídos e interferências que não podem ser previstos, sejam estes por abertura e fechamento dos circuitos, acoplamento de equipamento a tomadas.
- propagação das frequências em linhas abertas, sem nenhuma forma de proteção há interferências geradas por outros sistemas que atuam nas mesmas frequências de transmissão.
- as diferentes características topologias utilizadas nas redes de distribuição de energia elétrica (características não lineares, linhas abertas, existência de derivações ao longo da linha, transformadores).

Com a finalidade de permitir o perfeito funcionamento da tecnologia, empregam-se alguns tipos de modulação e multiplexação. No geral, sistemas PLC utilizam como formas de multiplexação o *Frequency Division Multiplex* (FDM) e como modulação a *Orthogonal Frequency Divison Multiplex* (OFDM) (SANTOS, 2008).

1.4 TOPOLOGIA

Segundo Rosa (2012), o emprego das redes PLC com diferentes topologias, depende da aplicação, avaliando aspectos, tais como: as necessidades, as características do local escolhido e a aplicação, além da concordância com as legislações vigentes.

De acordo com Vidal (2005), podemos classificar as tecnologias de aplicação de sistemas PLC em três grandes grupos:

1. topologia PLC *Indoor*;
2. topologia para acesso na última milha; e
3. topologia para acesso WAN.

Na topologia Indoor, a tecnologia PLC utiliza a rede de energia de baixa tensão instalada, o que permite reduzir custos com instalação de infraestrutura. Além disso, necessita apenas de adaptador chamado *Powerline Adapter*, que é ligado a tomada com o modem a ele e ao roteador. Com isso, todas as tomadas passam a ser pontos de rede.

Uma das grandes vantagens do uso da

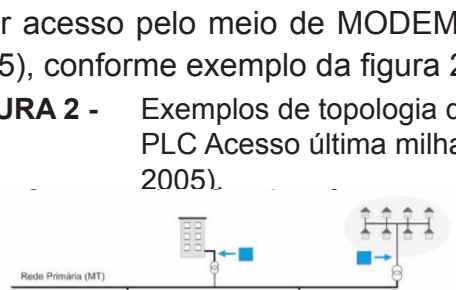
PLC é que, por utilizar a rede de energia elétrica, qualquer "ponto de energia" pode se tornar um ponto de rede, ou seja, só é preciso plugar o equipamento de conectividade (que normalmente é um modem) na tomada, e pode-se utilizar a rede de dados. Além disso, a tecnologia suporta altas taxas de transmissão, podendo chegar a 200Mbps, quando operado nas faixas de frequência de 1,7 a 30 MHz (FILIPPETTI, 2009).

A rede de dados criada com PLC pode ser interna, exemplificada pela rede de energia de apartamentos de um prédio, conforme Figura 1.

FIGURA 1 - Exemplos de uma rede PLC doméstica (VITAL, 2012).

Na topologia de acesso na última milha, a rede PLC deixar de operar apenas na rede elétrica interna de um local específico, e se expande para além dessa rede, gerando diversas sub redes de menor porte. Nessa topologia, o sinal PLC é acoplado as redes de baixa tensão após o transformador de distribuição, de modo que todos os usuários que estejam ligados a rede desse transformador passam a ter acesso pelo meio de MODEM's (VIDAL, 2005), conforme exemplo da figura 2.

FIGURA 2 - Exemplos de topologia de aplição PLC Acesso última milha (VIDAL, 2005).



A topologia de acesso WAN é utilizada quando se necessita acesso rápido a um meio, podendo este ser a internet, ou outro qualquer, onde, mediante sinal proveniente de uma portadora de serviços, o equipamento PLC servidor faz a distribuição do sinal utilizando a rede de baixa tensão, estendendo conexão a todos os usuários que estejam conectados ao transformador. O cliente recebe o sinal na tomada e com o auxílio do modem PLC faz a filtragem dos sinais de frequência. (CAVALCANTE; MENESES, 2008)

Conforme aumenta a distância entre cada cliente e o transformador, se faz necessário o uso de um repetidor.

Além disso, a rede PLC opera de modo síncrono, ou seja, as taxas de recebimento e transmissão de dados são as mesmas.

2 OPERAÇÕES INTERAGÊNCIAS

As operações interagências no âmbito do Exército Brasileiro estão fundamentadas em legislação do Ministério da Defesa que estabeleceu que são tidas como Operações Interagências aqueles que envolvam:

> interação das Forças Armadas com outras agências com a finalidade de conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes que atendam ao bem comum, evitando a duplicidade de ações, a dispersão de recursos e a divergência de soluções com eficiência, eficácia, efetividade e menores custos (BRASIL, 2012).

A Operação Ágata pode ser citada como exemplo de Operação Interagência, conforme Fig 3.

FIGURA 3 - Exemplos de agências (BRASIL, 2017).
:

Além disso, estabeleceu-se que a agência pode ser uma:

> organização ou instituição com estrutura e competência formalmente constituídas, podendo ser governamental ou não, militar ou civil, nacional ou internacional (BRASIL, 2012).

Esse tipo de operação visa reduzir redundâncias e economizar recursos, buscando a eficiência:

> capacidade de produzir o efeito desejado com economia (emprego racional) de meios; como eficácia a obtenção de um efeito desejado; e como efetividade a capacidade de manter eficácia ao longo do tempo (MD35-G-01 Glossário das Forças Armadas) (BRASIL, 2012).

Além da legislação do Ministério da Defesa, o **Manual de Operações do Exército dá** a seguinte definição para Operações de Cooperação e Coordenação com Agências:

> São operações executadas por elementos do EB em apoio aos órgãos ou instituições (governamentais ou não, militares ou civis, públicos ou privados, nacionais ou internacionais), definidos genericamente como agências (Fig. 4). Destinam-se a conciliar interesses e coordenar esforços para a consecução de objetivos ou propósitos convergentes que atendam ao bem comum. Buscam evitar a duplicidade de ações, a dispersão de recursos e a divergência de soluções, levando os envolvidos a atuarem com eficiência, eficácia, efetividade e menores custos (BRASIL, 2017).

FIGURA 4 - Exemplos de agências (BRASIL, 2017).

Ambas legislações evidenciam a preocupação com a redução de custos através da economia de meios e da redução da duplicidade de emprego de materiais.

3 VANTAGENS DA UTILIZAÇÃO DE PLC NAS OPERAÇÕES INTERAGÊNCIAS

A utilização da tecnologia PLC em operações interagências permite a redução de custos para a instalação de infraestrutura lógica. Permite, ainda, uma maior flexibilidade quando planejar as redes de dados de banda larga, necessárias para a transmissão da grande demanda de dados gerados nesse tipo de operação.

As diversas topologias apresentadas permitem que sejam disponibilizadas redes internas montadas nos centros de comando e controle, utilizando a rede de baixa tensão na topologia Indoor.

Na topologia de acesso última milha é possível disponibilizar o acesso de rede de dados nas regiões adjacentes aos centros de comando e controle através da rede de média tensão, permitindo assim que estruturas localizadas em determinada área se interliguem.

Já a topologia WAN permite a conexão, de variadas estruturas, à internet em uma área mais ampla, utilizando a rede de média

tensão disponível na região.

Com o emprego da rede de energia elétrica é possível levar a transmissão de dados em banda larga a lugares desprovidos de provedores convencionais de internet, mas que possuam ligações ao sistema de energia elétrica do país.

CONCLUSÃO

A utilização do PLC fornece às Operações Interagências grande vantagem para o sucesso desse tipo de operação, ao flexibilizar e distribuir as redes de dados, nos mesmos locais em que há o fornecimento de energia elétrica, com baixo custo.

THE ADVANTAGES OF USING POWER LINE COMMUNICATION IN INTERAGENCY OPERATIONS

ABSTRACT. This study seeks to present the advantages of using Power Line Communications (PLC) in Interagency Operations, due to the difficulty of providing broadband data network infrastructure for all the agencies involved in this type of operation.

Key Words: Advantages. PLC. Broadband. Interagency.

REFERÊNCIAS

BELETINNI, Cassiano Tramontin. **Estudo de Viabilidade da Utilização da Tecnologia Power Line Communication – PLC em Redes Locais em Comparativo com Cabo de Par Trançado**. Trabalho de Conclusão de Curso de Graduação – Curso de Tecnologias de Informação e Comunicação, Universidade Federal de Santa Catarina, Araranguá, 2015.

BRASIL. Manual MD33-M-12 OPERAÇÕES INTERAGÊNCIAS. Ministério da Defesa. 2012.

_____. Manual de Campanha EB70-MC-10.223 OPERAÇÕES. Exército Brasileiro, 5ª Ed. 2017.

CAVALCANTE, André Nascimento; MENESES, Lair Aguiar de. **Transmissão de dados via rede elétrica.** Engenharia de Telecomunicações, Instituto de Estudos Superiores da Amazônia – IESAM, 2008.

FILIPPETTI, M. **Entenda melhor o PLC** – Power Line Communications. 2009. Disponível em: <http://blog.ccna.com.br/2009/09/07/entenda-melhor-o-plc-power-linecommunications/>. Acesso em: 24/10/2017.

Reunião Interagências na 13ª Brigada de Infantaria Motorizada. Disponível na Internet. URL: http://www.eb.mil.br/noticias/-/asset_publisher/jWOqZAEImyZg/content/13-brigada-de-infantaria-motorizada-reuniao-interagenci-1/11425?inheritRedirect=false. Acesso em 24/10/2017.

ROSA, Magali da. **Monitoramento de temperatura do motor do aero gerador de pequeno porte utilizando power line communication - PLC**. 2012. 99 f. Dissertação (Mestrado) - Curso de Engenharia de Minas Metalúrgica e Minerais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012.

SANTOS, Túlio Ligneul. **Power Line Communications**. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/tulio/Fontes.htm>. Acesso em: 13/11/15.

VIDAL, Alexandre de Moura; **Estudo do estado da arte e análise de desempenho de sistemas de comunicação PLC de banda larga**. Dissertação de Mestrado em Engenharia Elétrica – Universidade Federal de Santa Catarina – UFSC, 2005.

VITAL, Richard Brandão Nogueira. VITAL, Tatiane Melo. **Comunicação de Dados em Redes de Distribuição de Energia Elétrica de Baixa Tensão.** Revista Eletrônica TECCEN, Vassouras-MG, v. 5, n. 2, p. 97-106, maio/ago., 2012.

Daniel Mateus Coelho nasceu em Cruz Alta, RS, em outubro de 1982. Recebeu os títulos de Graduação em Ciências Militares pela Academia Militar das Agulhas Negras e de Pós-Graduação Lato Sensu em Ciências Militares pela Escola de Aperfeiçoamento de Militares em 2003 e 2011, respectivamente. Recebeu ainda os títulos de Pós-Graduação Lato Sensu em Gestão de Administração Pública pela Universidade Castelo Branco em 2009 e Pós-Graduação Lato Sensu em Engenharia de Sistemas de Radiocomunicação pelo Instituto Nacional de Telecomunicações em 2017. Desde fevereiro de 2014 é instrutor nomeado da Escola de Comunicações, onde atua na Seção de Ensino a Distância, responsável por gerenciar o ensino em plataforma web da Escola de Comunicações. Tem interesse nas

áreas de Fundamentos de Telecomunicações, Comunicações Digitais Terrestres e por Satélite. Pode ser contactado pelo email daniel.coelho@eb.mil.br.

MACA: O PROTOCOLO DE CONTROLE DE ACESSO AO MEIO QUE VIABILIZA TRANSMISSÕES DE DADOS EM RÁDIOS TÁTICOS HARRIS

Antonio Anderson Silva Marques
Graduado em Ciências Militares

RESUMO. Este trabalho explora o recurso MACA (*Multiple Access with Collision Avoidance*) disponível nos equipamentos da empresa Harris, fornecedora de rádios para o Exército Brasileiro. Inicialmente foi realizada uma pesquisa bibliográfica a respeito do protocolo, seu modo de funcionamento e compreensão de suas limitações. Após, foi verificado como o protocolo é empregado no rádio, diferenças quanto a sua concepção original e a melhor forma de utilização. O trabalho conclui apontando que há diversas aplicações, sugeridas pelo próprio fabricante, onde é possível explorar o recurso com produtividade, em especial, quando se deseja a transmissão de dados e fonia. Porém o usuário deve compreender também quando não usar o protocolo, de acordo com o que pretende fazer, visto que este pode inviabilizar enlaces de longo alcance.

Palavras-chave: MACA. Enlaces. Controle de acesso.

INTRODUÇÃO

Em uma situação clássica de perda de sinal, a estação Y pode ouvir a estação X e Z, mas X e Z não podem se ouvir. X e Z portanto não conseguem evitar uma destruição mútua de seus pacotes em Y. Esta falha técnica é usualmente chamada de problema do terminal oculto.

Este manuscrito descreve um protocolo de controle de acesso para a camada 2 do modelo Open System Interconnection (OSI) chamado Acesso Múltiplo com Evitação de Colisão (MACA). O protocolo foi inspirado no método Carrier Sense Multiple Access (CSMA), porém com melhoramentos quanto à visibilidade dos terminais entre si. O método MACA soluciona o problema de terminais ocultos e ainda está apto a utilizar de forma mais racional a potência do aparelho, frente a outros protocolos testados por Karn (1990). Isso aumenta substancialmente a capacidade de tráfego do rádio, colaborando assim para o mínimo uso de potência possível para o enlace.

Em comunicações militares, uso possível de potência é um fator crítico, visto que não há possibilidade constante de reposição de baterias em rádios empregados em campanha e devido à Guerra Eletrônica inimiga, que pode utilizar esta emissão de potência em excesso para levantar informações sobre a rede ou até mesmo sobre o conteúdo transmitido, caso este seja demodulado e decodificado corretamente. De acordo com Brasil (2014),

> as MAGE oponentes são dificultadas quando as forças amigas utilizam sempre a menor potência de transmissão necessária para o estabelecimento das comunicações.

O método MACA é empregado nos rádios RF-7800V da empresa Harris, sendo utilizado quando o usuário deseja transmitir voz e também dados em uma rede local, ativando configurações de IP.

1 SUBCAMADA MAC

Dentro do modelo de camadas OSI, a camada 2 (dois) pode ser subdividida em outras duas camadas, a Controle de Ligação Lógica (LLC), que fornece uma interface para camada superior, a 3ª camada (Rede). E a subcamada Controle de Acesso ao Meio Físico (MAC), que acessa diretamente o meio físico e controla a transmissão de dados, realizando também multiplexação.

Quando há transmissão em uma rede, a subcamada MAC encapsula os dados, ou

Protocol Data Unit (PDU), de forma que eles se tornem apropriados para a rede, adicionando um preâmbulo de sincronização ou preenchimento caso necessário, também adiciona um sequência de verificação de erros e envia estes dados para a camada física de acordo com as especificações do método de acesso ao canal. De acordo com Kozierok (2005):

> *Protocol Data Unit* em telecomunicações descreve um bloco de dados que é transmitido entre duas instâncias da mesma camada. Cada camada recebe a PDU da camada superior como um bloco de dados, adiciona seus cabeçalhos (e em alguns casos, rodapés) de controle, criando a sua própria PDU, num processo chamado de encapsulamento.

Esse método de acesso ao canal será responsável por controlar os dados, evitando congestões e colisões. Adicionalmente, o método de acesso será responsável por reiniciar a transmissão caso um sinal de jamming seja detectado, ou reduzir a taxa de transmissão caso haja congestão no canal. Em síntese, de acordo com a IEEE Std 802-2001, as funções principais da subcamada MAC são:

- reconhecimento e delimitação dos dados;
- endereçamento dos dados para o seu destino;
- proteção contra erros; e
- controle de acesso para a camada física.

O método de acesso ao canal também pode ser chamado de protocolo de acesso múltiplo, pois possibilita que diversas estações se conectem ao mesmo meio físico para usá-lo em conjunto. O protocolo mais utilizado é o CSMA/CD, porém o MACA pode ser empregado com sucesso em algumas aplicações.

2 FUNCIONAMENTO DO CSMA E MACA

Ao se utilizar o CSMA, quando uma estação deseja transmitir dados para outra, ela primeiro envia um pacote chamado Pedido para Enviar, *Request to Send* (RTS). A estação receptora responde com um pacote chamado Pronto para Receber, *Clear to Send* (CTS). Se o transmissor não recebe um pacote CTS depois de um tempo estipulado, ele envia novamente um RTS e espera um tempo maior pela resposta.

Dentro do pacote RTS não há somente uma requisição para transmissão mas também que tipo de dados serão transmitidos, o que permite a estação receptora se “preparar” para o fluxo de dados, por exemplo, alocando espaço de *buffer* suficiente para armazenar o que esta por vir.

Na forma tradicional do CSMA, o protocolo exige que as demais estações permaneçam fora do canal quando uma transmissão é iniciada, o que reduz a probabilidade de colisões de pacotes.

Porém, nem sempre o CSMA detecta que o canal está pronto para uso corretamente. O componente CS do seu acrônimo, *Carrier Sense*, de acordo com Forouzan (2008), funciona da seguinte forma:

> Quando um host quer transmitir, ele primeiro “ouve” o canal (sensoriamento da portadora) para saber se existe transmissão de dados corrente. Existindo transmissão, aguardará um determinado tempo (que pode ser aleatório ou específico). Se não existir transmissão, então, dependendo da variação do CSMA implementada, ela decidirá pela transmissão ou não.

Karn (1990) aponta que em algumas situações, especialmente ao se utilizar transmissões via radiofrequência, o sensoriamento da portadora é falho. Pois nem sempre a percepção de ausência de portadora significa que o canal está livre. E, da mesma forma, o fato de detectar uma portadora de outra estação não significa que o canal está obstruído em sua totalidade, sendo mais interessante então cortar o sensor de portadoras e ampliar o mecanismo de evitamento de colisões.

Esse novo protoloco utiliza o termo

Multiple Access do CSMA, MA, e acrescenta as letras *Collision Avoidanc*e, formando MA/CA, ou MACA. A confiabilidade do MACA reside nos pacotes RTS e CTS. Quando uma estação recebe um pacote RTS que é direcionado para outro terminal, ele inibe o seu próprio transmissor tempo suficiente para este terminal responder com um CTS. Quando uma estação recebe um pacote CTS de outro terminal mas que não é direcionada a ela, há também uma inibição de seu transmissor. Em síntese, o transmissor é inibido todas as vezes que recebe um pacote CTS ou RTS que não está endereçado corretamente.

O tempo de inibição dos transmissores pode ser determinado pelo próprio protocolo, já que nos pacotes RTS também é informado o tamanho do fluxo de dados a ser enviado. O que permite a todas as estações permanecerem em silêncio durante o fluxo de dados no canal.

Enquanto houver um enlace adequado entre as estações, a recepção de um pacote CTS de uma estação que está fora de uma transmissão solicitando dados de outro terminal poderia gerar colisão no canal, porém, dentro do protocolo MACA, isso será evitado.

3 UTILIZAÇÃO DO MACA EM RÁDIOS HARRIS

O Exército Brasileiro utiliza diversos equipamentos para radiotransmissão, entre eles os rádios da empresa Harris, porém o emprego destes equipamentos em ambiente aberto traz dificuldades inerentes às comunicações.

Ao desdobrar tropas no terreno, em algumas situações, os rádios necessitam estabelecer enlaces a grandes distâncias, o que pode implicar que nem todas as estações consigam se enxergar, mesmo estando na mesma frequência, ocasionando perdas de dados, congestões no canal e colisões de pacotes.

Os rádios Harris podem ser utilizados tanto para transmissões mais simples, onde há somente fonia, como para transmissões mais sofisticadas, onde há fluxo de dados. Para as transmissões onde há somente voz, o protocolo MACA pode não ser utilizado, porém, quando há fluxo de dados, o usuário deve acionar este recurso, através do software de configuração do equipamento, o Harris *Communications Planning Application* (CPA), conforme citado no manual de operações do equipamento:

Comunicações simultâneas de voz e dados podem ocorrer em uma rede de frequência fixa, configurando o parâmetro CHANNEL ACCESS como MACA2 (*Multiple Access Collision Avoidance Generation*) e o parâmetro CIRCUIT TYPE como SIMULTANEOUS (HARRIS, 2012).

Inclusive, há uma opção disponível no equipamento que regula o tempo de espera do transmissor, característica inerente do MACA conforme já citado neste manuscrito, para evitar a colisão de pacotes entre estações que desejam utilizar o canal.

Na tentativa de uma transmissão de voz em MACA2, ocorre um tempo de espera (*hold-off*) variável ao tentar obter acesso ao canal ou ocorre quando o canal está sendo usado. Se o canal está em uso e o usuário continua transmitindo em voz durante o tom de *hold-off* (por mais de 5 segundos), ocorre a prioridade de voz. A prioridade da voz resulta em rádio transmitindo a voz como uma prioridade mais alta do que os dados que estão usando o canal no momento (HARRIS, 2012).

Conforme observado na descrição do manual, a empresa Harris modificou o parâmetro original do MACA de inibição do transmissor, visto que um canal ocupado ainda recebe transmissão porém com fluxo prioritário de voz.

Ressalta-se que o rádio RF-7800V-HH utiliza um protocolo chamado MACA2, porém possui a possibilidade de integrar-se a outros equipamentos que utilizam o MACA no seu formato original, conforme citado em:

> O protocolo MACA (*Multiple Access with Collision Avoidance*) oferece suporte à comunicação com RF-

-5800V-MP, RF-5800M-HH e RF--5800V-HH em *Wireless* IP e redes diretas. No display principal, selecione a tecla de atalho EDIT e selecione CHANNEL ACCESS > LEGACY MACA. (HARRIS, 2012)

4 PLANOS DE CONFIGURAÇÃO COM MACA

Visando auxiliar o usuário do rádio, o software CPA traz consigo alguns planos já pré-configurados chamados de *Samples Plans*, onde é possível verificar a utilização do recurso MACA conforme idealizado pelo próprio fabricante.

a) plano 25KHz AES MACA GPS (RF--7800V-HH): este é um plano voltado para transmissão de dados porém com uma banda estreita de capacidade reduzida (apenas 25 KHz), porém apresenta criptografia AES e relatórios de Situational Awareness (GPS), permitindo versatilidade ao usuário;

b) plano 75KHz AES MACA GPS (RF--7800V-HH): semelhante ao anterior, porém com uma largura de banda maior (75 KHz), apresenta criptografia e relatórios de Situational Awareness (GPS);

c) plano 75K MACA RNDIS Interface (RF-7800V-HH): este plano apresenta a largura de banda de 75 KHz e ainda a interface RNDIS ativada, pela qual o usuário poderá transmitir dados via dispositivos USB;

d) plano *Advanced Retransmission* (RF-7800V-HH): neste plano se realiza a retransmissão de dados através de uma rede LAN, onde dois conjuntos de rádios poderão estar localizados em locais distantes mas conectados via uma rede cabeada, internet ou fibra óptica.

Esses são exemplos de planos onde é possível observar o emprego do MACA, porém há outras situações nas quais os pacotes de confirmação e solicitação (CTS e RTS) não são necessários. Quando há o emprego somente de fonia o fabricante recomenda a desabilitação do MACA. Por exemplo:

a) plano *long range* MELP AES (RF--7800V-HH): neste plano, o fabricante apresenta uma configuração para enlaces a longo alcance com o equipamento, onde o MACA esta desabilitado, é empregada a potência máxima do rádio (High), a menor largura de banda (25 KHz) e o recurso MELP, um codificador de voz ideal para sinais analógicos de baixa qualidade;

b) plano Dual PTT *Voice Only* (RF--7800V-HH): semelhante ao anterior, porém com habilitação do PTT duplo.

CONCLUSÃO

O protocolo MACA pode ser utilizado para redução da taxa de erros em equipamentos rádio, fornecendo uma solução para redução da congestão e colisão de pacotes através do seu mecanismo de confirmação e requisição. Porém cabe ao usuário decidir quando aplicar este recurso, priorizando dados ou fonia. A fabricante HARRIS fornece alguns exemplos de planos onde o usuário pode verificar o melhor uso do protocolo.

MACA: THE ACCESS CONTROL PROTOCOL THAT ALLOWS DATA TRANSMISSIONS IN HARRIS TACTICAL RADIOS

ABSTRACT. This work explores the MACA (Multiple Access with Collision Avoidance) feature available on Harris equipment, a provider of radios for the Brazilian Army. Initially a bibliographical research was done regarding the protocol, its mode of operation and its limitations. After, it was verified how the protocol is used in the radio, its differences as to its original design and the best form of use. The paper concludes by pointing out that there are several applications, suggested by

THE MANUFACTURER ITSELF, WHERE IT IS POSSIBLE TO EXPLOIT THE RESOURCE WITH PRODUCTIVITY, ESPECIALLY WHEN DATA TRANSMISSION AND PHONICS ARE DESIRED. HOWEVER, THE USER MUST UNDERSTAND WHEN TO ALSO GIVE UP THE PROTOCOL, ACCORDING TO THE USE THAT INTENDS TO MAKE OF THE EQUIPMENT, SINCE THIS CAN MAKE UNFEASIBLE LONG-RANGE LINKS.

KEYWORDS: MACA, LINKS. ACCESS CONTROL.

REFERÊNCIAS

BRASIL. Exército Brasileiro. Comandante de Operações Terrestres. Caderno de Instrução EB70-CI-11.403. Brasília, DF, 2014.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4ª ed. São Paulo: McGraw-Hill, 2008.

HARRIS. Manual de Operação RF-7800V-HH: RÁDIO VHF PORTÁTIL. Rochester: Harris Corporation, 2012.

KARN, Phil. **MACA:** A New Channel Access Method for Packet Radio. 1990. 9th ARRL Computer Networking Conference, Ontario, Canada. 1990.

KOZIEROK, Charles M. **Data Encapsulation, Protocol Data Units (PDUs) and Service Data Units (SDUs)**. Disponível em < http://www.tcpipguide.com/free/t_DataEncapsulationProtocolDataUnitsPDUsandServiceDa-2.htm> Acesso em: 16 de outubro de 2017.

KUROSE, James F.; Ross, Keith W. **Redes de computadores e a internet:** uma abordagem top-down. 6ª ed. São Paulo: Pearson Education do Brasil, 2003.

PINHEIRO, José Mauricio Santos. **Frames, Pacotes e Datagramas**. Disponível em <www.projetoderedes.com.br> Acesso em: 22 de maio de 2017.

EFEITO COLATERAL CAUSADO PELO EMPREGO DO INTERFERIDOR ANTI-DRONE SCE 0100 (IACIT) EM REDES WI-FI OUTDOOR

Daniel Roberto Resende[1], Marcelo Carneiro de Paiva[2].

Pós-graduado em Engenharia de Sistemas de Radiocomunicação[1], Mestrado em Engenharia Elétrica[2]

RESUMO: O uso de drones em ações terroristas, visando atingir aglomerações de pessoas, principalmente em grandes eventos, tornou-se uma preocupação das autoridades públicas. No Brasil, para garantir a segurança da população em eventos como as olimpíadas, o Exército Brasileiro utiliza bloqueadores de sinais (jammers) de radiofrequência capazes de atuar no sistema de controle da maioria dos drones disponíveis no mercado com o intuito de produzir um "escudo de proteção" nas áreas com maior concentração de pessoas. Este trabalho propõe analisar, por meio de teste de campo e modelos de propagação, qual o impacto do uso desses bloqueadores, dentro de um cenário urbano, em redes Wi-Fi outdoor, tendo em vista que a frequência da maioria dos canais de controle dos modelos atuais de drones trabalham na mesma faixa de frequência que roteadores usados em redes Wi-Fi.

Palavras-chave: Bloqueador Anti-Drone. Interferência em redes Wi-Fi outdoor. Padrão 802.11. SCE 0100 – IACIT.

INTRODUÇÃO

O uso de drones como atividade recreativa ou mesmo profissional se tornou bastante comum nos dias atuais. Porém, a popularidade desse dispositivo traz a possibilidade de se implementar uma arma que pode ser encarada como uma ameaça terrorista em eventos internacionais de grande porte (OLIVEIRA, 2015). Um ataque terrorista, em um grande evento como a copa do mundo ou as olimpíadas, utilizando um drone, pode ter grandes proporções e expor o despreparo das forças de segurança envolvidas (OLIVEIRA, 2015).

Para este problema existem soluções no mercado. A empresa americana Liteye System, por exemplo, desenvolveu um sistema composto por câmeras de alta definição, radares e bloqueadores direcionados de ondas de rádio que são capazes de detectar, monitorar e impedir o voo de Drones. Esse sistema ficou conhecido como "Raio da Morte" (DEFESANET, 2016).

Nas olimpíadas de 2014 e na copa do mundo de 2016, eventos internacionais sediados pelo Brasil, as forças armadas brasileiras foram as responsáveis pela segurança destes eventos. Com a finalidade de combater ações terroristas que envolvam o uso de drones o exército brasileiro adquiriu um equipamento Interferidor (Jammer), especificadamente desenvolvido para atuar no canal de controle dos principais modelos de drones disponíveis no mercado. Este interferidor é capaz de bloquear o sinal de rádio que controla o drone, fazendo com que o aparelho cesse voo ou simplesmente fique desorientado (DEFESANET, 2016).

Grande parte dos drones utiliza como canal de controle às faixas de frequências não licenciadas destinadas a transmissão de sinais Wi-Fi. Portanto, o uso de interferidores de radiofrequência pode causar interferência em dispositivos Wi-Fi localizados dentro de sua área de atuação (ARAUJO, 2017).

O uso de interferidores foi autorizado pela ANATEL devendo ser restrito em operações específicas, episódicas, urgentes e temporárias em situações de risco potencial ou iminente de ações necessárias à preservação da ordem pública e da segurança das pessoas e do patrimônio (DEFESANET, 2016).

O objetivo desse artigo é mostrar, por meio de testes de campo e modelos de propagação, a atuação de um sinal interferente gerado pelo equipamento SCE 0100, da empresa

IACIT e seu efeito indesejável para uma rede Wi-Fi, causando transtornos para o cidadão comum que está conectado em um roteador Wi-Fi outdoor, ou até mesmo em redes do tipo ponto a ponto que atendem a grandes empresas.

O trabalho encontra-se estruturado em cinco seções. A seção II apresenta uma discussão sobre o uso de drones em ações terroristas evidenciando o uso de interferidores como contra medidas a essas ações. A seção III apresenta um estudo sobre o padrão de redes sem fio IEEE 802.11. O equipamento SCE 0100-D, utilizado como interferidor neste estudo, é apresentado em termos de características técnicas na seção IV. O teste de campo, análise e discussão dos resultados obtidos são apresentados na seção V. Na seção VI, são apresentadas as principais conclusões sobre o trabalho realizado e perspectivas de trabalhos futuros.

1 A AMEAÇA DRONE

Os drones ou VANT's (Veículo Aéreo Não Tripulado) podem ser definidos como qualquer objeto que se desprenda do chão e seja capaz de se sustentar na atmosfera com propósito diferente de diversão (OLIVEIRA, 2015). De pequeno porte são capazes de suportar cargas próximas de 8 kg e voar com uma velocidade de 30 km/h, a uma distância de 2000 metros do seu ponto de controle e com uma autonomia de até 25 minutos (OLIVEIRA, 2015). Um aparelho assim, carregando algum componente químico, como um ácido ou até mesmo um explosivo, se usado em locais com grande aglomeração de pessoas, pode causar um grande estrago.

É fácil encontrar exemplos reais do quanto é difícil identificar e interceptar um drone. Em 2015, um drone conseguiu invadir acidentalmente a casa branca, nos EUA, sem que nenhum alarme fosse acionado. Durante o ocorrido, cogitou-se a possibilidade de um ataque terrorista, sendo descartada após a localização do proprietário do aparelho que relatou ter perdido o controle do mesmo (LEONNIG, 2015). Em abril de 2015, no Japão, um drone, carregando material radioativo, conseguiu pousar no telhado do escritório oficial do primeiro ministro japonês. O responsável pelo aparelho era um ativista japonês que queria protestar contra o uso de energia nuclear (SHANKER, 2015).

Devido à grande parte das pessoas usarem seus drones como hobby e com o intuito de baratear e simplificar o sistema, a maioria desses aparelhos utiliza, em seu canal de controle, as faixas de frequências ISM (Industrial Sientific and Medical). Trata-se de bandas reservadas internacionalmente para o desenvolvimento industrial, científico e médico. Essas bandas foram definidas em 1985 pelo FCC (Federal Communications Commission), órgão regulador da área de telecomunicações e radiodifusão. Este órgão reservou uma parte do espectro de frequência para desenvolvimentos livres, sem a necessidade de licenciamento, definindo somente normas para limitação de potência de transmissão e técnicas de modulação dentro destas faixas (TELECO, 2017). No Brasil, a ANATEL (Agência Nacional de Telecomunicações) regulamenta sobre o uso de equipamentos de radiocomunicação de radiação restrita por meio da resolução n º 506 de 1º de julho de 2008, onde são definidas as faixas de frequências ISM, bem como a potência máxima permitida para equipamentos que usem essas frequências.

Alguns drones mais sofisticados dispõem de recursos de navegação por meio de GPS (Global Positioning System, Sistema de Posicionamento Global) onde seu trajeto pode ser pré-estabelecido e o voo ser executado sem a necessidade de um operador. Esse sistema também é usado em caso de perda do sinal de controle fazendo com que o aparelho possa pousar em local pré-definido. Esse tipo de controle de drones não será alvo de avaliação nesse artigo.

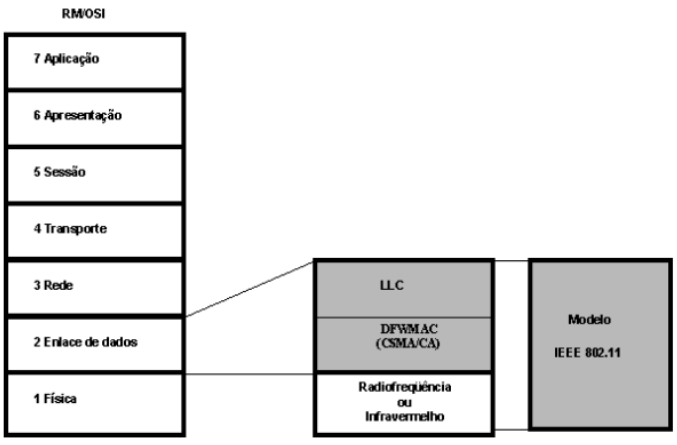
2 PADRÃO DAS REDES SEM FIO IEEE 802.11

Devido à implementação de várias tecnologias que permitiram uma maior taxa de transferência de dados por meio de ondas eletromagnéticas, técnicas de segurança mais robustas e a diminuição de custos, as redes sem fio ou Wi-Fi passaram a fazer cada vez mais parte do nosso cotidiano. Além de serem flexíveis e de fácil instalação, é cada vez mais perceptível à substituição das redes cabeadas pelas redes sem fio (NARDIN, 2008).

O IEEE (Institute of Electrical and Electronics Engineers) é o órgão responsável pela definição do padrão usado para redes locais sem fio, denominado WLAN (Wi-fi Local Area Network), padrão 802.11. Esse padrão deveria atender a algumas premissas básicas, como suportar diversos canais; sobrepor diversas redes na mesma área de canal; apresentar robustez com relação à interferência; possuir mecanismos para evitar nós escondidos; oferecer privacidade e controle de acesso ao meio (BARIZON, 2005).

O padrão 802.11 especifica a camada de nível físico e seu controle de acesso e pode ser comparado com o modelo OSI conforme ilustrado na Figura 1. Os padrões de redes locais sem fio, WLAN, foram definidos pelo IEEE especificando somente a camada física e a camada de enlace. Esse estudo ficará restrito a nível da camada física das redes sem fio.

FIGURA 1 - Comparação do padrão 802.11 com o RM-OSI (BARIZON, 2005).



A camada física está relacionada ao serviço de transmissão do rádio. É nela que são definidos os parâmetros do tipo do sinal transmitido, tais como a frequência, a largura de banda do canal, a modulação, a filtragem entre outros (BARIZON, 2005). Basicamente, ela é responsável por transmitir os bits por meio do canal de comunicações, definindo todas as especificações elétricas e mecânicas. Tem como principal função a modulação do sinal para ser transmitido pela onda eletromagnética. Além disso, também realiza a técnica de espalhamento espectral (Spread Spectrum) com o intuito de proteger o sinal contra interferências (SIRUFO, 2004).

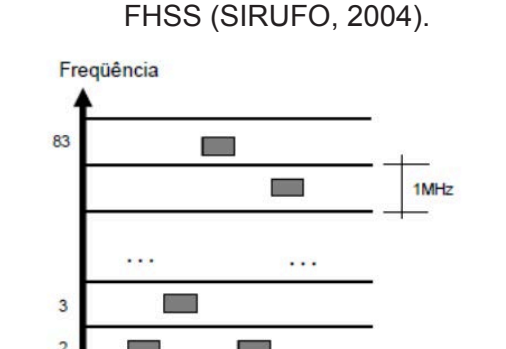
O nível físico pode ser empregado de três formas, sendo duas de radiofrequência baseadas na técnica de espalhamento espectral chamadas de FHSS (Frequency Hopping Spread Spectrum – espalhamento espectral por salto de frequência) e DSSS (Direct Sequence Spread Spectrum – espalhamento espectral por sequência direta) e uma por transmissão de infravermelha difusa (SIRUFO, 2004).

Apesar de permitir uma maior taxa de transferência de dados a transmissão infravermelha possui um comprimento de onda muito pequena o que acaba refletindo em pouco poder de penetração, restringindo seu alcance a cerca de 10 metros em visada direta. Essas características tornam seu uso inviável para redes sem fio fazendo que a transmissão por radiofrequência se torne o padrão adotado em redes sem fio.

A técnica de espalhamento FHSS, ilustrado na Figura 2, consiste na divisão da banda disponível em vários subcanais. A transmissão ocorrerá em curtos intervalos de tempo, onde a estação transmissora e a receptora são sincronizadas para saltar entre os subcanais em uma sequência pseudo-aleatória pré-determinada. No Brasil a largura de banda disponível na faixa de frequência ISM de 2,4 GHz (83,5 MHz) foi dividida em 83 subcanais, nos quais pelo menos 75 desses devem ser utilizados. No caso de um canal estar sobre interferência, os dados são retransmitidos somente no próximo salto ou quando for encontrado um

subcanal limpo. Devido à faixa de frequência utilizada ser bastante poluída pelo uso de aparelho microondas, telefones sem fios e outros equipamentos essa técnica possui baixa taxa de transmissão de dados que podem chegar a no máximo a 2 Mbps (BARIZON, 2005;SIRUFO, 2004).

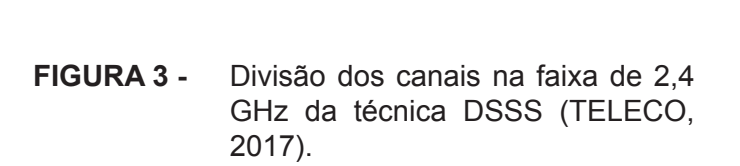
FIGURA 2 - Diagrama frequência vs. tempo em FHSS (SIRUFO, 2004).



Na técnica de espalhamento DSSS cada bit recebe um código padrão chamado CHIP antes de ser transmitido. Esse código é conhecido somente pela estação transmissora e receptora o que torna a transmissão mais difícil de ser interceptada. A adição do código torna mais eficiente a correção de erros sem a necessidade de retransmissão e também distribui o sinal ao longo de toda a faixa disponível, tornando-o mais robusto e confiável.

A técnica DSSS também opera na faixa de frequência ISM de 2,4 MHz divididos em 14 canais de 22 MHz de largura de banda com intervalos de 5MHz entre eles. Desse modo as frequências acabam sendo compartilhadas fazendo com que as redes operando em canais muito próximos acabam se interferindo mutuamente (BARIZON, 2005;SIRUFO, 2004).

FIGURA 3 - Divisão dos canais na faixa de 2,4 GHz da técnica DSSS (TELECO, 2017).



É importante destacar que essas técnicas de transmissão foram previstas no padrão 802.11 original. Ao longo do tempo, por meio de novas técnicas ou de combinações das já existentes, mudanças na faixa de frequência de operação e dos códigos empregados, vários sub-padrões foram criados pelo próprio IEEE, com a finalidade de se aumentar a velocidade de transmissão, a confiabilidade e a robustez contra interferências do sistema. Entre padrões desenvolvidos, destacam-se como os mais usados os seguintes:

802.11a: trabalha na faixa de frequência ISM de 5 GHz em 8 canais de rádio e permite uma taxa de transferência de dados de até 54 Mbps por canal. Utiliza a técnica OFDM (Orthogonal Frequency Division Multiplexing) onde a largura de banda disponível é dividida em 52 diferentes frequências, sendo 48 para dados e 4 para sincronização. Como vantagem apresenta melhor imunidade por trabalhar a faixa dos 5 GHz (menos sinais interferentes), porém é incompatível com outros padrões 802.11 já existentes além de ter um alcance menor e maior custo dos equipamentos (STANGARLIN, 2012).

802.11b: foi o primeiro padrão utilizado em grande escala (chegou ao mercado antes do 11a) e trabalha na faixa de frequência ISM de 2,4 GHz. Permite uma taxa de até 11 Mbps utilizando a técnica de transmissão DSSS com um alcance máximo estimado em 300 metros. Tem custo dos equipamentos baixo e compatibilidade com outros padrões 802.11 disponíveis. Como desvantagem trabalha em uma faixa de frequência mais poluída sendo assim mais suscetível a interferências (STANGARLIN, 2012).

802.11g: opera na faixa de frequência ISM de 2,4 GHz, associando duas técnicas de modulação, a DSSS e a OFDM (é o que difere do padrão 11b). Permite uma taxa máxima de 54 Mbps adaptativa, onde, ao aumentar a distância de transmissão, a taxa de dados tende a cair mantendo-se a estabilidade do sinal. O emprego da modulação OFDM (melhor eficiência na utilização da banda passante) permitiu velocidades iguais ao padrão 11a mesmo ope-

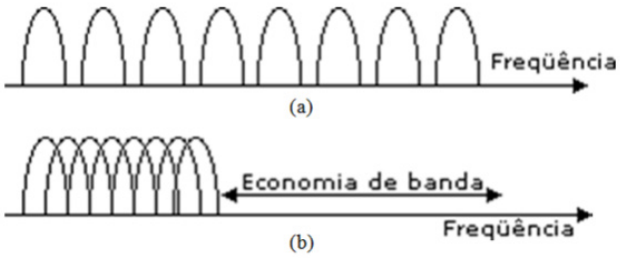
rando na frequência de 2,4 GHz e o mesmo alcance do padrão 11b, o qual é compatível (STANGARLIN, 2012).

802.11n: esse padrão foi criado com o objetivo de atingir velocidades de transmissão maiores do que as redes cabeadas (100 Mbps), além de melhorar o alcance e a confiabilidade. Para isso foi implementado melhorias nos algoritmos de transmissão e a técnica MIMO (Multiple-Input, Multiple-Output) permitindo o uso de vários fluxos de transmissão e recepção de forma paralela (várias antenas para transmitir e receber). Tudo isso aumentou a velocidade de transmissão para 300 Mbps e ainda dobrou o alcance. No padrão 11n pode se operar com canais com largura de banda de 40 ou de 20 MHz (nesse caso com redução da velocidade), e com frequências de 2,4 e 5 GHz, o que o torna compatível com os demais (STANGARLIN, 2012).

Percebe-se que a introdução da técnica de modulação OFDM melhorou substancialmente a velocidade nas transmissões de dados nas redes sem fio.

Ao contrário do que se vê em várias literaturas, o OFDM não se trata de uma técnica de multiplexação como a FDM (Frequence Division Multiplexing) e a TDM (Time Division Multiplexing) que agregam sinais distintos para serem transmitidos por um único meio. Trata-se de uma evolução do FDM. Na multiplexação FDM as frequências das subportadoras necessitam de serem afastadas uma das outras (bandas de guarda), impedindo que os sinais enviados sofram interferência mútua. No OFDM, esse espaçamento não é necessário, uma vez que as frequências das subportadoras se sobrepõem umas nas outras ortogonalmente, tornando-as independentes e possibilitando a identificação de cada subportadora pelo receptor de modo seguro. Na prática, ocorre uma racionalização do uso do espectro, o que permite aumentar a taxa de transmissão de dados com a mesma banda disponível, conforme ilustrado na Figura 4 (CAVALCANTI, 2009). Entre as principais vantagens do uso do OFDM se destacam a maior capacidade de transmissão e a robustez aos ambientes com desvanecimento seletivo em frequência. Como desvantagem apresenta dificuldade de sincronismo das subportadora e sensibilidade aos desvios de frequência (TELECO, 2017).

FIGURA 4 - (a) Espectro com oito subportadoras associadas em FDM e (b) Espectro com oito subportadoras associadas em OFDM (TELECO, 2017).



3 O INTERFERIDOR SCE 0100 – IACIT

O produto SCE 0100, ilustrado na Figura 5, da fabricante IACIT é apresentado em quatro diferentes modelos. O modelo SCE 0100-D utilizado em aplicações contra drones, SCE 0100-C usado em aplicações contra comunicação celular, SCE 0100-R voltado para aplicações contra RCIED (Remote Controlled Improvised Explosive Device) e o SCE 0100-M empregado em aplicações portáteis contra RCIED e comunicação. Como o foco deste trabalho são aplicações voltadas à interferência de drones o modelo SCE0100-D tem suas características discutidas nesta seção.

O SCE0100–D (DroneBlocker) possui capacidade de bloquear e/ou interferir através dos 6 (seis) canais independentes, Tabela I, e com capacidade de operar simultaneamente, disponíveis ao longo das faixas de frequência comumente utilizada em controles remotos de drones. A ação de bloqueio é realizada por meio de um sinal interferente que realiza uma varredura em toda a faixa de frequência do canal em que estiver operando. A taxa de varredura por cada canal é prevista em manual e também apresentada na Tabela I.

FIGURA 5 - Interferidor SCE 0100 (IACIT, 2017)

TABELA 1 - Canais de interferência do modelo SCE 0100-D (IACIT, 2016).

Canal	Faixa de Freq [MHz]	Potência de saída [W]	Taxa de varredura [µs]
1	27-75	1/10/100	100
2	433-470	1/10/100	100
3	902-928	1/10/50	100
4	GPS L1/L2/L5	1/10	20
5	2400-2500	1/5/10/25/50	150
6	5700-5900	1/15	50

Devido às altas velocidades de varredura a visualização no analisador de espectro mostra uma interferência de barragem em toda a banda do canal em operação, conforme a Figura 6. É importante destacar que, segundo o manual do fabricante, 95% dos drones mais comuns operam nas faixas de frequência de 2,4 e 5,8 GHz (canais 5 e 6). Essas faixas de frequência são as mesmas usadas nas redes sem fios no Brasil e por isso se tornaram alvo desse estudo.

FIGURA 6 - Visualização da realização de uma interferência no Canal 1 (IACIT, 2016).

Quanto à antena utilizada para transmissão do sinal interferidor, o equipamento possui dois tipos: uma antena direcional, que atende os dois canais (5 e 6) e duas antenas omnidirecionais, nesse caso uma para cada canal, conforme Figura 7. A antena direcional permite que o operador do interferidor minimize os efeitos colaterais indesejados apontando-a para alvo (drone), poupando dessa forma possíveis redes sem fio que estejam ao redor da antena de transmissão do jammer. Por esse motivo, as análises realizadas nesse estudo serão feitas utilizando antenas omnidirecionais, onde não é possível ter o controle da emissão do sinal interferente. A antena omnidirecional utilizada para o canal 5, conforme Figura 7(a) também atende os canais 2, 3 e 4. Já a antena vista na Figura 7(b) atende somente ao canal 6. Suas características elétricas estão apresentadas na Tabela 2.

FIGURA 7 - (a) Antena omnidirecional para a frequência de 2,4 GHz (Canal 5) e (b) Antena omnidirecional para a frequência de 5,8 GHz (Canal 6).

(a)

(b)

TABELA 2 - Características elétricas das antenas utilizadas pelo SCE 0100-D (IACIT, 2016).

Antena omnidirecional para os canais 2,3,4 e 5	
Faixas de frequência	452-468 MHz (Canal 2) 790-960 MHz (Canal 3) 1710-2170 MHz (Canal 4) 2300-2700 MHz (Canal 5)
Ganho	3 a 6 dBi
Polarização	Vertical
VSWR	≤ 2,5:1
Ângulo de meia potência (horizontal)	360°

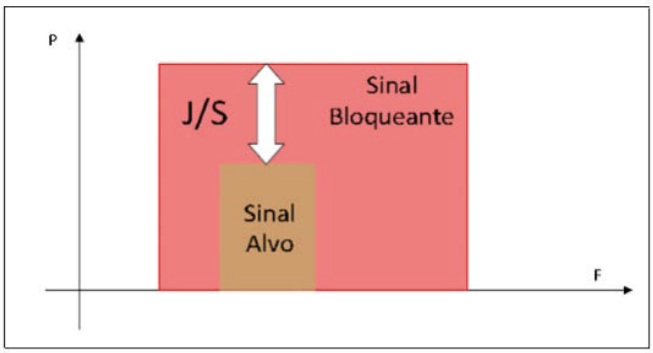
Antena omnidirecional para os canais 2,3,4 e 5	
Ângulo de meia potência (vertical):	25°
Antena omnidirecional para o canal 6	
Padrão de irradiação	Omnidirecional
Faixa de frequência	5700-5900 MHz
Ganho	6 dBi
Polarização	Vertical
VSWR	≤ 1,5:1
Ângulo de meia potência (horizontal)	360°
Ângulo de meia potência (vertical)	25°

4 TESTE DE CAMPO

A.Relação Jammer/Signal (J/S)

A relação J/S (Jammer/Signal) determina quantas vezes a potência do sinal interferidor é maior que o sinal alvo, conforme ilustra a Figura 8. Essa relação é comumente expressa em dB. Para ser eficiente em uma interferência sobre um sinal digital, necessita-se que a relação J/S seja igual a 0 dB e que seja realizada pelo menos durante 1/3 do tempo em que o sinal a ser bloqueado esteja transmitindo. Nessas condições, as informações que vão chegar ao demodulador já estarão degradadas o suficiente para que seja interrompida a comunicação de um sinal digital (BRASIL, 2012).

FIGURA 8 - Relação J/S (BRASIL, 2012).



B. Setup de Teste

O teste realizado tem como objetivo verificar a possibilidade do equipamento SCE 0100-D interferir em uma comunicação entre dois dispositivos que se comunicam através de uma rede Wi-Fi. Sendo assim, realizou-se a montagem de um setup de teste conforme ilustrado na Figura 9. O equipamento SCE 0100-D foi posicionado a 200 metros de um notebook e um roteador, sendo estes posicionados próximos um do outro uma distância de 1,5 metros. O roteador utilizado foi o modelo D-Link DIR-600, cujas características técnicas são apresentadas na Tabela 3. Em relação ao interferidor, a antena utilizada foi ilustrada na Figura 7 (a). Imagens do Setup de teste podem ser observadas na Figura 10.

FIGURA 9 - Esquema de teste de campo.

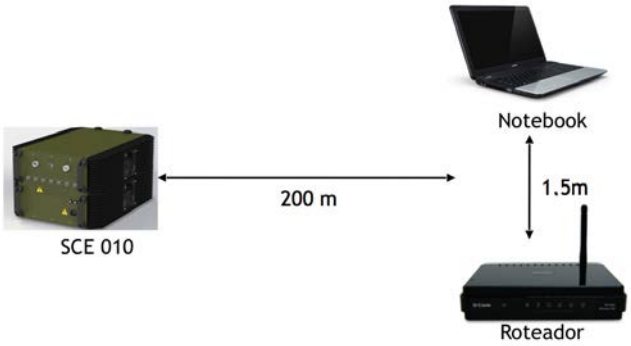


TABELA 3 - Características técnicas do roteador D-Link, modelo DIR – 600 (DIR-600, 2010).

Fabricante	D-Link
Modelo	DIR - 600
Padrões Wi-Fi	802.11b/g/n
Frequência de funcionamento	2.4 GHz a 2.497 GHz
Potência nominal	14 dBm +/-2 dB
Quantidade de antenas	1 (não removível)
Ganho de antena	5 dBi

Antes do início do emprego do interferidor realizou-se o teste de conectividade entre o roteador e o notebook, o qual apresentou o resultado esperado de perda nula de pacote de dados, conforme ilustrado na Figura 11.

FIGURA 10 - Detalhe antena omnidirecional interferidor SCE 0100 – IACIT e interferidor SCE 0100 – IACIT.

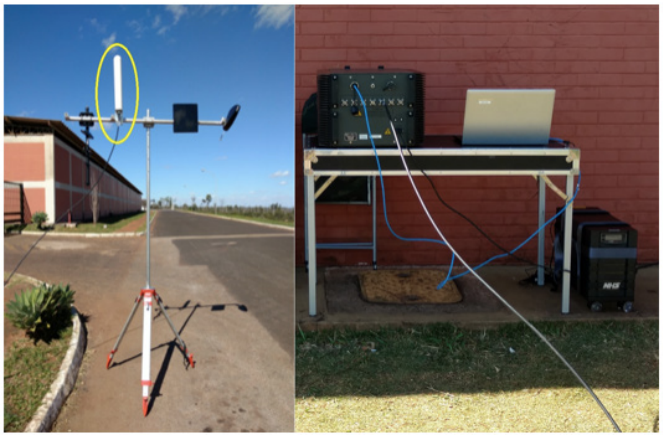
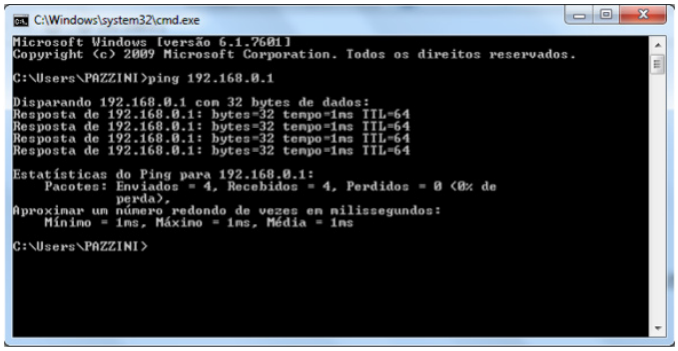


FIGURA 11 - Status conexão Wi-Fi com interferidor desligado.



C.Resultados e discussões

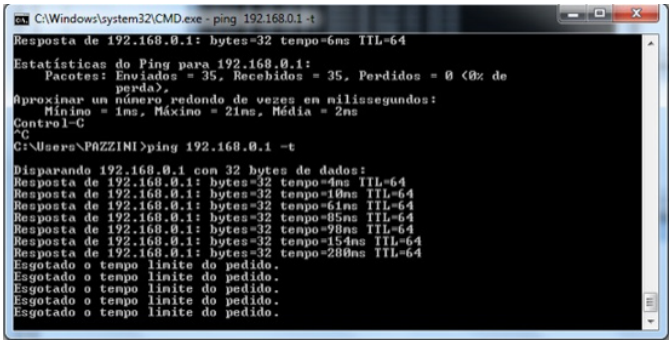
O teste consistiu em observar o status da rede com o interferidor ligado, inicialmente com 1Watt de potência. Em sequência a potência do sinal interferidor, cuja banda foi de 100MHz (2,4 a 2,5 GHz), foi aumentada gradativamente para 5, 10, 25 e 50 Watts. Para cada valor de potência do sinal interferidor um novo teste de conectividade da rede Wi-Fi era realizado entre o roteador e o notebook. Os resultados observados são apresentados na Tabela IV. Observa-se que a comunicação de dados entre o roteador e notebook, sob as condições de setup, sofre interferência para um sinal interferidor com nível de potência maior ou igual a 40dBm. A Figura 12 apresenta o status do teste de conectividade entre o roteador é o notebook para sinal interferidor com nível de potência de 40 dBm.

TABELA 4 - Resultados de teste de campo.

Potência [W]	Potência [dBm]	Distância [m]	Interferência
1	30	200	Não
5	37		Não
10	40		Sim
25	44		Sim
50	47		Sim

O teste de campo comprovou que o equipamento SCE 0100 realmente causa interferências em redes Wi-Fi. Percebeu-se ainda que, nem mesmo a técnica de espalhamento espectral utilizada pelos dispositivos Wi-Fi, que oferece certa robustez diante de interferências, foi capaz de permanecer imune ao sinal interferente.

FIGURA 12 - Status conexão Wi-Fi sendo interferida.



No manual de operação do software planejador de missões do equipamento SCE 0100, em sua base teórica, encontra-se um modelo de atenuação no espaço livre para distâncias de até 200 metros entre o interferidor e seu alvo, com visada direta, dado por

$$L = 32{,}45 + 20 \cdot \log_{10}[d(\text{km})] + 20 \cdot \log_{10}[f(\text{MHz})], \quad (1)$$

onde d é a distância em km entre o transmissor e o receptor e f a frequência do sinal transmitido em MHz. O manual também apresenta um modelo de propagação dado por

$$P_r = P_t + (G_t + G_r - L_t - L_r) - L, \quad (2)$$

onde Pr é a potência de recepção, Pt é a potência de transmissão Gt e Gr são os ganhos das antenas de transmissão e recepção, respectivamente, e Lt e Lr são as perdas em cabos e conectores dos sistemas de transmissão e recepção, respectivamente (IACIT,

2016).

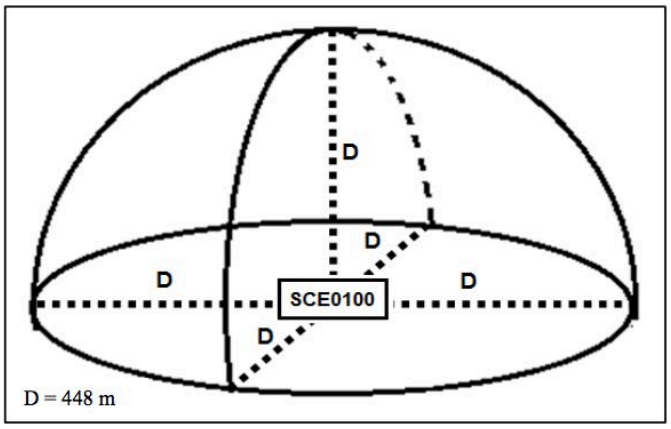
Definida a distância e frequência do sinal pode-se por meio de (1) obter a atenuação no espaço livre para o setup de teste, sendo este valor de 86,254 dB. Em seguida é possível obter a potência recebida pelo roteador por meio de (2). Considerando os valores de ganho, perdas e potência de transmissão apresentados na Tabela V e a atenuação calculada anteriormente, obtém-se como potência de recepção -39,854 dBm. Em tese, de acordo com o teste realizado, essa é a potência necessária no alvo para interromper a comunicação entre o roteador e o notebook. Esse nível de sinal passa a ser o valor de referência para que haja interferência.

TABELA 5 - Dados práticos dos equipamentos.

Antena Omnidirecional do SCE 0100	
Ganho	4,5 dBi (valor médio)
Antena roteador	
Ganho	5 dBi (data sheet)
Cabo de transmissão do SCE 0100	
Atenuação	0,5 dB/m (5 metros)
Conector SCE 0100	
Atenuação	0,3 dB/conector (2 conectores)
Interferidor SCE 0100	
Potência de TX	10W (40 dBm)
Frequência de Operação	
SCE 0100 (2,4 a 2,5 GHz)	Roteador (2,45 GHz) Freq. Média

Após a realização do teste, constatou-se que o equipamento SCE 0100 realmente é capaz de provocar um efeito colateral indesejável em redes Wi-Fi durante o seu uso normal (atuar tendo como alvo os drones). Com a finalidade de se obter a distância máxima que a interferência causada pelo SCE 0100-D pode alcançar, dentro das condições colocadas em teste, por meio de (1) e (2) e com os dados disponíveis é possível encontrar tal distância. Para isso, adota-se o valor de potência recebida que permite causar interferência no alvo, neste caso Pr = -39,854 dBm. Para determinar o máximo alcance utiliza-se a potência máxima fornecida pelo equipamento SCE 0100-D em sua saída, ou seja, 50 W/47 dBm. Logo, obtém-se uma distância de 448 metros o que supostamente seria capaz de gerar uma região de interferência conforme ilustrado na Figura 13.

FIGURA 13 - Região de interferência efetiva com 50 W de potência (BARBOSA, 2017).



É importante observar que esses dados, em tese, só teriam validade nas mesmas condições em que foi realizado o teste de campo, no caso, a visada direta entre o interferidor e o roteador, sendo esse com características semelhantes ao D-Link DIR 600.

CONCLUSÕES

O presente trabalho apresenta um estudo prático sobre a interferência do equipamento SCE 0100- D, utilizado em aplicações contra drones, em redes Wi-Fi próximas. Neste contexto, foram apresentadas algumas situações que demonstram como os drones podem ser utilizados em atividades terroristas. Estudou-se o padrão das redes sem fio IEEE 802.11 e alguns aspectos da camada física deste padrão. O equipamento interferidor SCE 0100-D também teve suas características estudadas. Em sequência foi realizada a configuração de um setup de testes que permitiu obter o nível de potência mínima do sinal interferidor capaz de impedir a comunicação de dados entre um roteador e um notebook.

Durante a realização do teste verificou-se que o equipamento realmente causa interferências em conexões Wi-Fi. O referido teste também trouxe, em tese, uma distância máxima de referência para que haja interferência

quando reproduzidas as condições definidas no teste executado (visada direta e roteador D-Link DIR-600). Essa distância foi definida em aproximadamente 448 metros e pode ser considerada pelos planejadores e operadores quando o equipamento for empregado em um cenário urbano, onde o efeito indesejável de interferências em redes Wi-Fi comerciais e domésticas é mais provável.

O teste de campo levou em consideração a interrupção total da conexão Wi-Fi entre um roteador e um notebook. Porém, em uma interferência externa em uma conexão Wi-Fi que não seja forte o suficiente para causar a interrupção do sinal, pode levar a uma perda considerável na qualidade do canal, causando lentidão para o usuário. Dentro dessa ótica, é válido considerar que os efeitos colaterais podem ser muito superiores aos 448 metros levantados.

Como trabalhos futuros propõe-se a realização de um estudo de interferência acidental em redes Wi-Fi indoor pelo uso do interferidor SCE 0100-D, simulação da área de interferência causada pelo interferidor e o estudo e obtenção da distância máxima de atuação do interferidor com o uso de antena direcional.

REFERÊNCIAS

ARAUJO Luiz Albert, et al – **Desafios da defesa e segurança frente à nova ameaça do uso ilícito de VANTs**. Disponível em: <http://www. defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xii_cadn/desafios_da_defesa_segurana_vants.pdf> Acesso em: 29 de abril 2017.

BARBOSA, Ricardo Luís; MARINS, Carlos Nazareth Motta – **Análise do campo de ação de um interferidor de RF sobre um receptor GPS de drone**. VI SRST – Seminário de Redes e Sistemas de Telecomunicações, INATEL, Julho 2017.

BARIZON, Ben-Hur Monteiro. PONTIFÍCIA UNIVERSIDADE CATÓLICA, Rio de Janeiro-RJ, 3-Redes locais sem fio IEEE 802.11, Certificação Digital nº 0124845/CA. Disponível em: <https://www.maxwell.vrac.puc-rio.br/5688/5688 _4.PDF> Acesso em: 26 de abril de 2017.

Brasil. Ministério da Defesa. Exército Brasileiro. Centro de Instrução de Guerra Eletrônica – Manual de Ensino de Guerra Eletrônica, Brasília – DF, 2012.

CAVALCANTI Arthur Barreto de Rangel Moreira. **Uma avaliação da interferência entre redes 802.11g**, Recife - PE, 2009.

DEFESANET. DRONES, Novo sistema promete derrubar Drones invasores em até 15 segundos. Agosto de 2016. Disponível em: <http://www.defesanet.com.br/vant/noticia/23362/Novo-sistema-promete-de rrubar--drones-invasores-em-ate-15-segundos/> Acesso em: 22 de dezembro de 2016.

_____. DRONES, Drones assassinos: a maior ameaça terrorista à segurança dos jogos Olímpicos e Para olímpicos. Julho de 2016. Disponível em: <http://www.defesanet.com.br/vant/noticia/22944/Drones-as-sassinos--a-maior-ameaca-terrorista-a-seguranca-dos--Jogos-Olimpicos-e-Paraolimpicos-/> Acesso em: 22 dezembro de 2016.

_____, Forças Armadas: Autorizadas a usar bloqueadores de celular nas Olimpíadas e GLO. Janeiro 2016. Disponível em: <http://www.defesanet.com.br/eventos/noticia/21411/Forcas-Armadas--Autori zadas--a-usar-bloqueadores-de-celular-nas-Olimpiadas-e--GLO/> Acesso em: 20 de abril de 2017.

IACIT Soluções Tecnológicas S/A - Manual Técnico do Produto equipamento SCE 0100.

_____. Manual de Operação do Software IHM SCE 0100.

_____. Manual de Antenas do equipamento SCE 0100.

_____. Manual Técnico do software planejador de missões para o equipamento SCE 0100.

LEONNIG, Carol D.; WHITLOCK, Craig. Drone incident at White House highlights long-studied, still-unsolved security gap. The Washington Post, 26 jan. 2015. Disponível em: <http://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied--still-unsolved-security-gap/20 15/01/26/e d2e7f9e-a-594-11e4-a7c2-03d37af98440_story.html>. Acesso em: 26 de abril de 2017.

OLIVEIRA, Gilberto de Jesus. **O Drone como fator de risco decorrente de condições não previstas na segurança radiológica em Grandes Eventos**, Rio de Janeiro, 2015.

NARDIN, Marcelo de. **Análise comparativa entre redes sem fio locais e metropolitanas**, camada física, Porto Alegre, 2008.

SHANKAR, Sneha. Japan Arrests Yasuo Yamamoto For Landing Radioactive Sand-Laced Drone On Shinzo Abe's Office Roof. International Business Times, 25 abr. 2015. Disponível em: <http://www.ibtimes.com /japan--arrests-yasuo-yamamoto-landing-radioactive-sand-laced-drone-shinzo-abes-office-1896688>. Acesso em: 26 de abril 2017.

SIRUFO, Sergio Henrique. PONTIFÍCIA UNIVERSIDADE CATÓLICA, Rio de Janeiro-RJ, 2-Padrão IEEE 802.11, Certificação Digital nº 0210420/CA. Disponível em: <https://www.maxwell.vrac.puc-rio.br/7589/7589_3.PDF> Acesso em: 26 de abril de 2017.

STANGARLIN Douglas Pegoraro. Análise de desempenho de redes sem fio com diferentes protocolos de criptografia: um estudo de caso, Santa Maria – RS, 2012.

TELECO. Seção Tutoriais Regulamentação – Regulação do Espectro: Uso Não-Licenciado. Disponível em: <http://www.teleco.com.br /tutoriais/tutorialespecradio/pagina_2.asp > Acesso em: 29 de abril de 2017.

_____. Seção Tutoriais Banda Larga. Redes WiFi II: Tecnologias RF para 802.11 Disponível em: <http://www.teleco.com.br/tutoriais /tutori alwifimanaus2/pagina_3.asp> Acesso em: 29 de abril de 2017.

_____._____. Redes WiFi: Espectro de Frequências ISM. Disponível em: <http://www.teleco.com.br/tutoriais/ tutorialredeswifi1/pagina_5.asp> Acesso em: 25 de abril de 2017.

ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

DEEPWEB: ANONIMATO?

Cap Luiz Paulo Lopes dos Santos
Pós-graduado em Guerra Cibernética

RESUMO. O uso da Internet possibilitou o surgimento de "seções" que não são acessados por sites de busca como o Google e Bing, hospedando assim sites de forma anônima, sem registro algum, dando origem a *Deep* Web. Motores de busca como o Google contam com programas chamados de rastreadores que reúnem informações seguindo trilhas de hiperlinks que ligam tudo que está na internet, isso é chamado de indexação. Essa abordagem funciona adequadamente às páginas que compõem a Surface Web, que seria composta por todo conteúdo visivel da internet (sites e conteúdo em geral), que pode ser visitado e indexado por rastreadores nos mecanismos de busca; porém esses programas têm dificuldades em penetrar bancos de dados que não são configurados para responder a consultas digitadas pelos usuários que realizam esta busca. A *Deep* Web (também chamada de *Deepnet*, Web Invisível, *Undernet* ou Web oculta) é composta por todo conteúdo que não está na *Surface* Web, ou seja, é tudo que não está indexado por ferramentas de busca padrão, trazendo um novo modo de utilizarmos a rede.

Palavras-Chave: Segurança cibernética. Comportamento humano. Engenharia social.

INTRODUÇÃO

Segundo Paganini(2012), o Deep Dark WEB é um lugar misterioso, onde se faz o anonimato, chamado pelo autor de hacker's Paradise, sendo a porção do ciberespaço inacessível por muitos aspectos.

As regras e os procedimentos válidos para a Surface Web, que corresponde a parte da internet que é indexada, ou seja, todos os sites e bancos de dados que são reconhecidos por sites de busca como o Google, o Yahoo, Bing, são muitas das vezes alterados, e onde os mecanismos de busca através de seus rastreadores não conseguem identificar o que é site e o que não é na Deep Web.

Para um melhor entendimento, pode-se fazer analogia a um Iceberg, figura 1, como é mostrado pelo site Brandpowder, onde os buscadores são navios sob a superfície do mar com todo o conhecimento indexado à sua disposição, e a *Deep* Web é a zona profunda do mar, pela qual navegam os hackers anonimamente.

Como fala Bergma, (2001), CEO da Structured Dynamics LLC, um dos fundadores, diretor de tecnologia e presidente da Corporação Bright Planet, os mecanismos de busca utilizam numa página na internet uma espécie de scanner, varrendo todo o site com seus computadores até achar outros sites no qual o primeiro site faz referência, ou possui links relacionados.

FIGURA 1 - CONCEITO DA DEEP WEB

Fonte: www.brandpowder.com

Novamente, é feito outro vasculhamento que parte destes novos sites encontrados, analisando as páginas da Web e seguindo os links contidos nelas, como um usuário faz ao navegar na Internet. Eles avançam de link em link e transmitem, aos servidores do Google, os dados destas páginas da Web, relacionando todos os sites que são encontrados e registrados.

Esses sites são registrados nos buscadores a fim de tornar visível o site aos mecanismos de busca. Outra forma dos motores de busca obterem estes sites, ocorre quando o autor do site apresenta as suas próprias páginas da Web para serem listadas diretamente por um motor de busca.

Na *Deep* Web, os sites não seguem obrigatoriamente a mesma métrica de registro. Sites simplesmente são criados e ativados sem nenhuma espécie de registro. Sem informações, os buscadores não tem como saber de onde são os sites, muito menos como achá-los a fim de indexá-los e torná-los visíveis.

Páginas que não possuem referências ou links que as identifiquem, e apresentam conteúdo textual codificado em arquivos multimídia (imagem ou vídeo) ou formatos de arquivo específicos, acabam atuando como verdadeiros mecanismos de bloqueio de acesso ao seu conteúdo. Estas páginas tornam-se invisíveis aos scanners de rede, chamados de web crawlers, e não são manipulados pelos motores de busca.

Os motores de busca não conseguem encontrar ou recuperar o conteúdo da *Deep* Web porque muitas das fontes da *Deep* Web necessitam de consulta direta aos seus bancos de dados, e esses motores não são construídos para fazer isso.

1 UTILIZAÇÃO DA DEEP WEB

Segundo os criadores da tecnologia, pessoas usam o Tor (um navegador da internet de software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online) para acessar a Deep Web, a fim de impedir que sites rastreiem seus familiares, evitar a identificação ao se conectar a sites de notícias, serviços de mensagens instantâneas ou similares, quando se encontram bloqueados pelos seus provedores de Internet. Jornalistas usam o Tor para se comunicarem de forma mais segura com contatos, como afirmado por Quintin (2014).

As organizações não-governamentais (ONGs) usam o Tor para que os seus trabalhadores possam se conectar ao seu site, enquanto estão em um país estrangeiro, sem notificarem que estão trabalhando com essa organização.

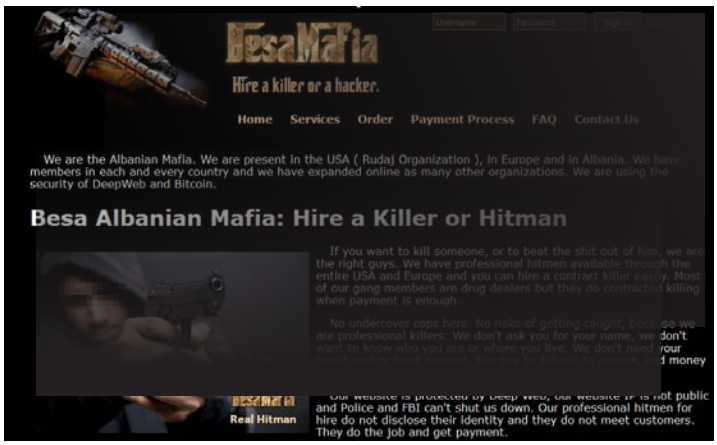
Serviços ocultos do Tor permitem aos usuários publicar web sites e outros serviços sem a necessidade de revelar a localização do site. Um ramo da marinha americana usa Tor para recolher informação de fonte aberta, e uma de suas unidades usou Tor enquanto operava no Oriente Médio recentemente como afirma Levine (2014).

Parte da população, usa o anonimato para quebrar a censura, e usufruir do livre acesso à internet e a privacidade de conversa, usufluindo do meio sem quebrar conceitos legais e/ou morais.

No entanto, existe também o uso que é ilegal, conforme apresentado no começo do trabalho. O usuário que navega na Deep WEB está mais propenso, mesmo que acidentalmente, a ser direcionado a sites de conteúdo ilegal ou impróprio. Na Deep WEB todo cuidado é pouco.

O uso ilegal da Deep Web é o que causa preocupação aos governos e o cidadão comum. Mesmo quem a conhece evita usá-la, com vistas a evitar a vinculação de seus nomes as atividades ilegais associadas a este meio, como mosta a Figura 2.

Figura 2 Site de contratação de assassinatos na Deep Web



Na Deep Web, como os sites podem

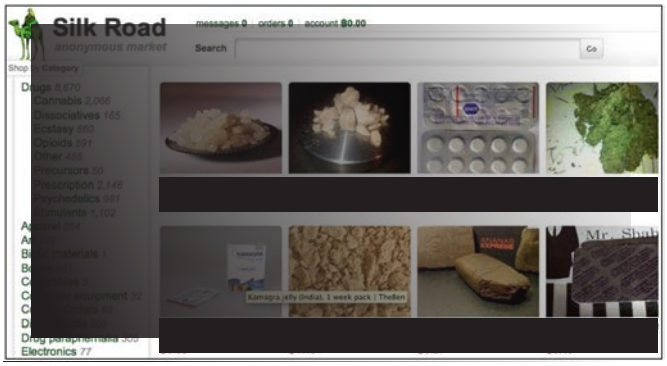
ser criados dentro de total anonimato, sem saber onde está o servidor ou quem é o dono, muitas pessoas usam essa oportunidade para realizarem atividades ilícitas, como afirma Gomes (2017), que vão desde a venda de drogas até contratação de assassinatos.

Em 2 de outubro de 2013, o FBI (Federal Bureau of Investigation) fechou um famoso site de venda de drogas da Deep Web chamado Silk Road o qual teria vendido drogas, movimentando mais de 1,2 bilhões de dólares. A existência do site foi revelada em 2011 e não podia ser acessado sem a intervenção do navegador Tor como disse Greenberg (2013).

Segundo Altieres Rohr (2013), quando um serviço na rede Tor é criado, ele é cadastrado na rede e o site não registra o endereço real de seus visitantes. A Bitcoin (moeda virtual anônima irrastreável), fazendo uso desse anonimato, tornou o site Silk Road popular, como afirma o site “buybitcoinworldwide”.

Se o anonimato era tão importante para um dos sites mais famosos de venda de drogas da Deep Web, como o FBI chegou ao dono do site? Simples, por intermédio da engenharia social! Dois clientes do site ameaçaram divulgar informações sobre seus usuários. Aliás, um deles era ex-funcionário do Silk Road.

Figura 3 Site Silk Road de venda de drogas na Deep Web



O dono do site, Ross William Ulbricht, teria contratado um assassino de aluguel, serviço que também pode ser achado na Deep Web, para matá-los e acabar com as ameaças. Porém, o assassino de aluguel era na verdade um agente secreto do FBI, que falsificou a realização do homicídio, e chegou até o local onde o ex-funcionário do site estaria.

Outros erros foram cometidos por Ulbricht, tal como participar de fóruns on-line não anônimos, publicando endereços com o nome de seu site Silk Road, usando inclusive seu e-mail pessoal para que interessados entrassem em contato para colaborar com seu “projeto”.

Ulbricht usou seu e-mail pessoal no fórum, também se cadastrou em sites para programadores e pediu ajuda para criar códigos relacionados ao uso de serviços ocultos na rede Tor. Em redes sociais divulgou por conta própria o Silk Road, o que facilitou ainda mais sua identificação pelas autoridades.

O relato exposto caracteriza bem o maléfico uso da deep web e, como o site DailyMail (2011) apresentou, não se trata de mau uso isolado do ambiente anônimo. Em dada ocasião, o grupo de hackers Anonymous publicou 190 IPs de usuários acusados de prática de atividades ligadas à pedofilia, exemplos que reforçam o mau uso da Deep Web.

Verificou-se, que, embora tenha havido esforços de autoridades americanas em prender o dono e fechar o site Silk Road na Deep Web em 2011, o site voltou à ativa, verificado no mês de setembro de 2014, com o nome de Silk Road 2.0, e que mantém todas as atividades normalmente, incluindo também a venda de materiais eletrônicos, livros, quadros, álcool, jóias, entre outros. Consegue-se achar diferentes tipos de sites na Deep Web, pode-se até encontrar uma réplica do site Facebook, que na Deep Web se chama “Torbook”, e até mesmo uma réplica do Twitter, “Twitter Clone”.

2 ANONIMATO SEGURO?

Percebe-se que, quer sejam agentes governamentais ligados à atividade de inteligência ou agentes macomunados em práticas ilegais, o anonimato é um fator extremamente relevante na deep web, mas é apenas uma das preocupações de seus usuários.

Segundo Mitnik (2018), a eficiência

de qualquer sistema de segurança está diretamente relacionada aos usuários do sistema. O fator humano sempre será o elo fraco na cadeia e, portanto, o mais explorado. Segundo essa lógica, e conforme comprovações supracitadas, mesmo o ambiente hermeticamente criado para produzir anônimato é incapaz de fazê-lo, porquanto seus usuários sempre deixam rastros que os identificam.

Por exemplo, não adianta se preocupar com o anonimato da rede se forem cometidos erros de se expor na Surface Web, como utilizar e-mails particulares em blogs na Deep Web, utilizar nomes verdadeiros, divulgando assim a sua identidade dentro de uma rede criptografada.

A criptografia da rede Tor só funciona dentro da rede junto com os nós de entrada ou os nós intermediários. O grande problema da criptografia da rede Tor são os nós de saída. Esses nós de saída decriptografam o conteúdo para fazer a integração com o site no qual se faz a comunicação.

Ou seja, um provável usuário que esteja tentando ver o conteúdo que está trafegado na rede, tem apenas que ficar no nó de saída do Tor, cuja lista está disponível publicamente, e ver o conteúdo dos dados que está trafegando com um analisador de tráfego.

Para corrigir isso, é necessário usar uma criptografia fim a fim, como o SSL. Como no próprio site do ToR-Project fala, o navegador Tor é uma solução parcial à anonimidade.

Acredita-se que grande parte desses nós de saída são vigiados por governos para saber o que está tramitando na rede, a fim de verificar o conteúdo do tráfego, como cita Altieres Rohr (2014), editor do site de segurança Linha Defensiva, quando fala que a internet inteira nasceu de um projeto das forças armadas norte-americanas e que a intenção não é “colocar uma pedra no próprio sapato”.

Rohr ainda fala que a NSA (National Security Agency) tem uma missão conflitante, pois precisa possuir a capacidade de espionar as comunicações, e caso a tenha em larga escala, provavelmente agentes adversários também a terão, o que colocará a segurança nacional dos Estados Unidos em risco.

Em prol disso, Altieres Rohr afirma que os chamados “nós de saída” são controlados pela NSA e outras agências de espionagem. Tais agências têm acesso a todo o conteúdo que sai e entra na rede, funcionando para ocultar a origem das comunicações, mas não protege conteúdo algum.

Em seu artigo para a Wired Magazine, Zetter (2007) expõe que um consultor de segurança de computadores sueco Dan Segerstad revelou nomes de usuário e senhas de mais de 100 contas de e-mails usados por vítimas, através da informação do acolhimento de cinco nós Tor de saída colocados em locais diferentes na internet.

Segundo Zefter (2007) Dan Segerstad, disse em entrevista que:

> É aprovado pelo EFF (Electronic Frontier Foundation), organização sem fins lucrativos sediada em San Francisco, Califórnia, cujo objetivo declarado é proteger os direitos de liberdade de expressão, e outros grupos de defesa das liberdades civis como método de denunciantes e os trabalhadores de direitos humanos para se comunicar com os jornalistas, entre outros usos.

Porém, como já foi dito aqui, o Tor somente promove a anonimidade não sabendo de onde vem a informação, mas para o seu conteúdo também ser anônimo, precisa da criptografia SSL.

No dia 30 de Julho de 2014, a rede Tor sofreu um ataque que tentou expor seus usuários. No post de seu blog oficial em 2014, a equipe do ToR-Project afirma ter identificado alguns computadores, que voluntariamente aderiram ao sistema (os chamados “relays”), tentando identificar seus usuários.

Segundo TOR *Security Advisory* (2014):

> Parece que eles estão mirando em

> pessoas que operam ou acessam os serviços anônimos do Tor. O ataque envolveu em modificações em protocolos, exigindo 'ataques de confirmação de tráfego'.

Esse ataque foi uma tentativa de localizar a origem do tráfego através dos nós que compõem a rede, a equipe do ToR-Project descobriu que os "relays" entraram na rede em 30 de janeiro de 2014 e foram removidos no dia 4 de julho de 2014. O post no blog oficial diz:

> como não sabemos quando começou o ataque, os usuários que usaram serviços anônimos nesse período devem presumir que foram afetados.

Como resposta, ToR-Project avisa que removeu os "relays" dos quais tomou conhecimento, atualizou o software de seu navegador (e aconselha seus usuários a realizarem o mesmo procedimento).

CONCLUSÃO

Para navegar na rede oculta de computadores, concluiu-se que o mais importante é incorporar procedimentos de salvaguarda e segurança, tais como:

- não instalar addons, (recursos adicionais que complementam um programa), pois podem ter falhas ou vulnerabilidades;
- acessar somente sites que tenham criptografia HTTPS (protocolo HTTP com Security) o qual fornece criptografia dos dados tramitados entre a máquina e o site no qual está se fazendo o acesso; e
- não abrir documentos através do navegador, prática comum em alguns e-mails, como, por exemplo, o Gmail e o Hotmail, que o usuário pode visualizar e editar arquivos no próprio Browser, sem fazer o download para a máquina.

Acessar a Deep Web, é utilizar um SO chamado Tails, que foi desenvolvido para que seus usuários acessem a rede Tor, e se mantenham anônimos na internet, com algumas características que favorecem esse anonimato.

Caso a navegação seja realizada sem seguir esses cuidados, pode ocorrer a quebra do anonimato ou causar contaminação na máquina, fortalecendo o acúmulo de rastros da navegação.

Também pode haver a danificação da máquina por algum malware que tenha se obtido durante a navegação da Deep Web, caso isso ocorra, é recomendado a formatação.

A Deep Web ainda é um território digital pouco estudado e por demais mistificado. O advento da guerra cibernética e a crescente preocupação dos governos com a segurança virtual de suas infraestruturas críticas, certamente, promoverão, maiores e diversificados estudos, a respeito desse espaço, ainda, pouco explorado.

DEEP WEB: ANONYMITY?

ABSTRACT. The use of the Internet allowed the appearance of "places" that are not accessed by search engines such as Google and Bing, thus hosting anonymous sites without any registration giving rise to Deep Web. Search engines like Google rely on programs called crawlers that gather information by following trails of hyperlinks that link everything that is on the Internet, it's called indexing. This approach works properly to the pages that make up the Surface Web, which is formed by all the content of the Internet, sites, content in general, that can be visited and indexed by crawlers in the search engines; But these programs have difficulties in penetrating databases that are configured to respond to queries typed by users who perform this search. The Deep Web (also called Deepnet, Invisible Web, Undernet or Web Hiding), is composed of all content that is not on the Web surface, that is, it is anything that is not indexed by standard search tools, bringing a new How to use the network.

Keywords: Cyber security. Human behavior. Social Engineering.

REFERÊNCIAS

GOMES, HELTON. **Da Dark Web a pen-drives engolidos:**

como a PF investiga pornografia infantil na internet, 07 agosto 2017. Disponivel em: <https://g1.globo.com/tecnologia/noticia/da-dark-web-a-pen-drives-engolidos-como-a-pf-investiga-pornografia-infantil-na-internet.ghtml>. Acesso em: 21 Fevereiro 2018.

GREENBERG, ANDY. **End Of The Silk Road:** FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market, 02 outubro 2013. Disponivel em: < https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#12ce49325b4f>. Acesso em: 21 Fevereiro 2018.

_____. **Bitcoin Anonymity** - Is Bitcoin Anonymous?. Disponivel em: <https://www.buybitcoinworldwide.com/anonymity/>. Acesso em: 21 fevereiro 2018.

BBC. G1. Internet oculta: os segredos de um universo paralelo, 19 Julho 2014. Disponivel em: <http://g1.globo.com/tecnologia/noticia/2014/07/internet-oculta-os-segredos-de-um-universo-paralelo.html>. Acesso em: 19 Julho 2017.

BECKETT, A. **The Guardian.** The dark side of the internet, 26 Novembro 2009. Disponivel em: <http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet>. Acesso em: 26 Agosto 2017.

BERGMA, M. K. **White Paper: The Deep Web**: Surfacing Hidden Value, Agosto 2001. Disponivel em: <http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104>. Acesso em: 28 Setembro 2017.

BREWSTER, T. F. Forbes. **Can You Completely Trust Tor To Protect Your Privacy?**, 10 Julho 2014. Disponivel em: <http://www.forbes.com/sites/thomasbrewster/2014/07/30/can-you-completely-trust-tor-to-protect-your-privacy-fresh-attacks-would-suggest-not>. Acesso em: 06 Agosto 2017.

BRIGHT PLANET, D. W. I. **DEEP WEB:** A PRIMER, 2014. Disponivel em: <http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/>. Acesso em: 28 Julho 2017.

CARDOSO, C. **Putin oferece US$ 111 mil pra quem quebrar o Tor**, 26 julho 2014. Disponivel em: <http://meiobit.com/293647/russia-kgb-oferecera-111-mil-dolares-para-quem-quebrar-o-tor/>. Acesso em: 26 Julho 2017.

DIGITAL, R. O. V**eja 4 cuidados na hora de usar o Tor**, navegador da Deep Web, 21 Agosto 2014. Disponivel em: <http://m.olhardigital.uol.com.br/noticia/veja-4-cuidados-na-hora-de-usar-o-tor-navegador-da-deep-web/43682>. Acesso em: 28 Agosto 2017.

DREDGE, S. The Guardian. **What is Tor?** A beginner's guide to the privacy tool, 05 Novembro 2013. Disponivel em: <http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser>. Acesso em: 09 Setembro 2017.

ESTES, A. C. Gizmodo. **Rússia abre concurso caça-níquel para quem quiser tentar quebrar o Tor**, 28 Julho 2014. Disponivel em: <http://gizmodo.uol.com.br/russia-concurso-tor/>. Acesso em: 30 Julho 2017.

GLENNY, M. The New York Times. **Cyber Subterfuge,** 27 Novembro 2013. Disponivel em: <http://www.nytimes.com/2013/11/28/opinion/cyber-subterfuge.html?pagewanted=all&module=Search&mabReward=relbias%3As%2C%7B%222%22%3A%22RI%3A18%22%7D>. Acesso em: 21 Agosto 2017.

GUERNESY, L. The New York Times. **Mining the 'Deep Web' With Sharper Shovels**, 25 Janeiro 2001. Disponivel em: <http://www.nytimes.com/2001/01/25/technology/mining-the-deep-web-with-sharper-shovels.html?module=Search&mabReward=relbias%3As%2C%7B%222%22%3A%22RI%3A18%22%7D>. Acesso em: 21 Agosto 2017.

HERN, A. The Guardian. **US government increases funding for Tor**, giving $1.8m in 2013, 29 Julho 2014. Disponivel em: <http://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router>. Acesso em: 26 Agosto 2017.

KAUFMAN, L. Media Decoder. Book by 2 From Google Takes a Deep Look at the Web, 2 Dezembro 2012. Disponível em: <http://mediadecoder.blogs.nytimes.com/2012/12/02/a-book-by-two-from-google-takes-a-deep-look-at-the-web/?_r=0>. Acesso em: 21 Agosto 2017.

KISS, J. The Guardian. **Tor 'deep web' servers go offline as Irish man held over child abuse images**, 06 Agosto 2013. Disponível em: <http://www.theguardian.com/technology/2013/aug/05/tor-deep-web-servers-offline-freedom-hosting>. Acesso em: 06 Agosto 2017.

MACDIARMID, P. Exame. Computadores do governo alteraram Wikipedia, 28 Agosto 2014. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/computadores-do-governo-alteraram-wikipedia-diz-folha>. Acesso em: 30 Agosto 2017.

PAGANINI, P. **The Deep Dark Web**. 212 Providence St: Paganini-Amores, 2012.

QUINTIN, C. **7 coisas que você precisa saber sobre o Tor**, 04 Julho 2014. Disponível em: <http://gizmodo.uol.com.br/7-coisas-que-voce-precisa-saber-sobre-o-tor/>. Acesso em: 07 Julho 2017.

ROHR, A. G1. **Conheça a Deep Web e a 'internet invisível', 06 janeiro 2012**. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-a-deep-web-e-a-internet-invisivel.html>. Acesso em: 26 agosto 2017.

_____. **É possível combater a censura sem ajudar o crime na internet?**, 29 Outubro 2013. Disponivel em:

<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/e-possivel-combater-a-censura-sem-ajudar-o-crime-na-internet.html>. Acesso em: 01 Agosto 2017.

_____. **Se a rede Tor foi desenvolvida pelos EUA, ela é confiável?**, 13 fevereiro 2014. Disponivel em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao-se-rede-tor-foi-desenvolvida-pelos-eua-ela-e-confiavel.html>. Acesso em: 26 Agosto 2017.

STATCOUNTER. Stat Counter Global Stats. [S.l.]: [s.n.]. Disponivel em: <http://gs.statcounter.com/#desktop+console-os-ww-monthly-201406-201408>. Acesso em: 26 Setembro 2017.

TOR security advisory. “relay early” traffic confirmation attack, 30 Julho 2014. Disponivel em: <https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack>. Acesso em: 05 setembro 2017.

WILLIAMS, A. C. **Russia Declares War On Bloggers With Sweeping New Censorship Law**, 07 Maio 2014. Disponivel em: <http://thinkprogress.org/world/2014/05/07/3435292/what-its-like-to-use-the-internet-in-russia/>. Acesso em: 28 Julho 2017.

WRIGHT, A. **Exploring a ‘Deep Web’ That Google Can’t Grasp**, 22 Fevereiro 2009. Disponivel em: <http://www.nytimes.com/2009/02/23/technology/internet/23search.html?pagewanted=1&_r=0&th&emc=th>. Acesso em: 21 Agosto 2017.

ZETTER, K. **Rogue Nodes Turn Tor Anonymizer Into Eavesdropper’s Paradise**, 09 outubro 2007. Disponivel em: <http://archive.wired.com/politics/security/news/2007/09/embassy_hacks>. Acesso em: 01 Setembro 2017.

LEVINE, YASHA. **Almost everyone involved in developing tor was (or is) funded by the us government**, 14 julho 2014. Disponivel em: < https://www.infowars.com/almost-everyone-involved-in-developing-tor-was-or-is-funded-by-the-us-government/>. Acesso em: 21 Fevereiro 2018.

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras (2011). Tem experiência na área de Defesa, com ênfase em Defesa Cibernética. Carreira desenvolvida nas áreas de TI, Redes, Infraestrutura e Segurança da Informação e Telecomunicações. Dentro da área de segurança da informação, possui possui expertise em Forense computacional, Tratamento de incidentes de segurança da informação, Políticas de segurança da informação, Auditoria, Hardening Linux, Segurança física e Firewall. Possui proficiência em Inglês nível intermediário e pode ser contactado pelo email luizpaulo.santos@eb.mil.br.

ÁREA DE CONCENTRAÇÃO

EDUCAÇÃO

ESCOLA DE COMUNICAÇÕES

PROCESSO DE AVALIAÇÃO EM CURSOS E ESTÁGIOS GERAIS DAS LINHAS DE ENSINO MILITAR BÉLICO, COMPLEMENTAR E DE SAÚDE, NO EXÉRCITO

José Erlan Nunes Matias
Graduado em Matemática

RESUMO. Este trabalho consiste em analisar a concepção dos monitores e instrutores com relação ao processo de avaliação na aprendizagem em sala de aula, assim como confrontar seus conceitos e ideias com as dos autores - pesquisadores do assunto em questão. A experiência dos cursos e estágios realizados, bem como a literatura pesquisada, foram as principais ferramentas utilizadas para a análise. Para conhecer as opiniões dos instrutores e monitores – do Sistema de Ensino do Exército no que tange os cursos e estágios gerais das Linhas de Ensino Militar Bélico, Complementar e de Saúde – foi realizado um questionário com cinco perguntas. Este tema é extremamente importante, pois muitas vezes excluímos alguns alunos que apresentam potencialidades ainda não descobertas por causa de distorções no processo ensino-aprendizagem, cuja avaliação faz parte. Foi observado que boa parte dos instrutores e monitores utilizam a avaliação apenas para dar notas aos seus alunos, bem como guardar as informações obtidas como um simples documento de comprovação de capacidades dos alunos. A ideia distorcida da avaliação é ainda uma realidade em nosso sistema educacional, mas é verdade também que o instrutor tem ainda poder dentro da sala de aula, o mesmo pode mudar o papel coercitivo da avaliação e tornar esse instrumento mais eficaz.

Palavras-Chaves: Avaliação. Professor. Aprendizagem.

INTRODUÇÃO

A ideia de que a nota abaixo da média em uma avaliação (exame) é fruto da incapacidade ou ignorância do aluno ainda é uma realidade presente em nossos Estabelecimentos de Ensino (Estb Ens). Não se leva em consideração outros fatores que podem interferir no processo de aprendizagem do discente, que muitas vezes desiste de aprender por diversos motivos. Um deles é a ênfase exagerada na avaliação, como se fosse o principal objetivo do processo ensino-aprendizagem, tornando o sentido de avaliar distante do real objetivo. Segundo Vasconcellos:

> Avaliação é um processo abrangente da existência humana, que implica uma reflexão crítica sobre a prática, no sentido de captar seus avanços, suas resistências, suas dificuldades e possibilitar uma tomada de decisões sobre o que fazer para superar os obstáculos. (2007, p.53)

Diante dessa problemática, há uma vasta pesquisa sobre o assunto. Para esse trabalho foram consultadas literaturas de pensadores da educação como: Vasconcellos (2007), Méndez (2002) e Romão (1998) com intuito de contribuir, não só na quantidade, mas também qualitativamente na análise do processo avaliativo. Vale destacar a pesquisa realizada na legislação e nas normas utilizadas pelos Estb Ens em seus cursos e estágios.

O tema escolhido para análise foi o seguinte: processo de avaliação em cursos e estágios gerais das linhas de ensino militar bélico, complementar e de saúde, no Exército Brasileiro. O instrumento de avaliação utilizado pelo docente tem uma importância significativa no processo ensino-aprendizagem, quando utilizado com objetividade e conhecimento, pois além de mostrar qual o real entendimento dos alunos com relação a um determinado assunto, pode mostrar falhas quanto aos métodos educacionais utilizados em sala de aula. Para Méndez (2002, p.36), sob o ponto de vista construtivista com relação ao ensino-aprendizagem, concordamos que o bom trabalho realizado em sala de aula irá refletir positivamente na avaliação.

A pesquisa foi realizada através de ferramenta de pesquisa online (google drive), cujos sujeitos da pesquisa foram os monitores e instrutores que lecionam em Estabelecimentos de Ensino do Exército. Os estabelecimentos assim como os nomes dos docentes não serão divulgados.

Para a coleta de informações foi utilizado um questionário de pesquisa com questões abertas, como também uma pesquisa bibliográfica. As questões tinham por objetivo analisar as concepções dos docentes no processo de avaliação da aprendizagem e confrontá-las com as dos autores pesquisados.

1 PROFESSOR X AVALIAÇÃO

Para iniciar o nosso estudo, devemos destacar a avaliação formativa que tem como papel principal trabalhar a serviço do conhecimento, diferente daquela avaliação que apenas promove a competição e o individualismo. Como afirma Méndez (2002, p.29):

> Conforme se entenda o conhecimento, a avaliação vai - deve ir - por uns caminhos ou por outros. E, quando a desligamos do conhecimento, nós a transformamos em uma ferramenta meramente instrumental que serve para tudo, embora realmente valha para muito pouco no campo da formação integral... .

A avaliação não dever ser um instrumento apenas para atribuir nota e guardá-la como registro, mas sim para superar os erros tanto do docente quanto do discente e buscar eliminar o paradigma da exclusão e não-conhecimento. No quadro 1 podemos observar as respostas dadas pelos docentes para a primeira pergunta formulada.

QUADRO 1 - Legislações e normas

O senhor conhece as legislações e normas utilizadas no processo de Avaliação da Aprendizagem no Sistema do Exército?	
Instrutor nº 1	Sim
Instrutor nº 2	Sim
Instrutor nº 3	Sim
Instrutor nº 4	Não
Instrutor nº 5	Sim

Fonte: o autor, 2017.

Essa pergunta teria como objetivo saber qual parcela dos docentes conhece as normas utilizadas no processo de avaliação. É de extrema importância entender e conhecer os métodos utilizados nas avaliações, pois todos eles têm uma finalidade. Dependendo do elemento atitudinal, ficaria difícil utilizar determinado instrumento avaliativo, tornando-o ineficaz. Para melhoria continua desse aspecto, seria interessante os Estb Ens seguirem o que consta no artigo 41, do Regulamento de Preceitos Comuns aos Estabelecimentos de Ensino do Exército (R-126): “O Corpo Docente frequentará, anualmente, estágios de atualização pedagógica e administração escolar”. É de grande valia manter o quadro de docentes atualizado quanto aos preceitos e ferramentas pedagógicas utilizados nos cursos e estágios, com isso deixando mais claro o sentido da avaliação. Os docentes muitas vezes desconhecem as modalidades da avaliação, bem como seus instrumentos, mesmo conhecendo as normas presentes nas legislações. Propiciar momentos de discussão entre os docentes e mediadores, facilitará a compreensão dos elementos do processo ensino-aprendizagem.

QUADRO 2 - Avaliação da aprendizagem

O que significa avaliar a aprendizagem em sala de aula?	
Professor nº 1	Quantificar o conhecimento adquirido pelos instruendos
Professor nº 2	Serve como um feedback que ajuda a nortear os próprios métodos de ensino
Professor nº 3	Verificar se o aluno consegue realizar a atividade ao nível de competência a que a instrução foi proposta
Professor nº 4	Verificar se os discentes estão assimilando o conteúdo

O que significa avaliar a aprendizagem em sala de aula?	
Professor nº 5	É um meio pelo qual a instituição tende melhorar o processo ensino-aprendizagem

Fonte: o autor, 2017.

Segundo Romão (1998, p.34),

> se tentarmos levantar os diversos conceitos de avaliação da aprendizagem, certamente encontraremos tanto quantos são seus formuladores (ROMÃO, 1998).

Pode-se verificar nas respostas obtidas, mas o que é notável também em algumas respostas é a definição da avaliação da aprendizagem através dos seus objetivos: comparar, acompanhar, observar, quantificar, mostrando que o conceito do assunto abordado é ainda muito vago por boa parte dos docentes.

Esse trabalho não pretende de forma alguma definir genuinamente o conceito de avaliação, mas sim mostrar as diversas concepções que há a respeito do tema.

Como as definições para a avaliação são diversas, estamos expondo as concepções de pesquisadores renomados nessa área de pesquisa, para que possamos entender melhor e com respostas mais densas, o assunto abordado.

Observa-se nas respostas que boa parte dos docentes acredita que a avaliação não tem relação alguma com o professor, como se ela não reproduzisse falhas no processo de ensino. Verifica-se que avaliar está muito mais para medidas do que análises pedagógicas. De acordo com Méndez (2002, p.13),

> em termos precisos, deve-se entender que avaliar com intenção formativa não é o mesmo que medir, nem qualificar e nem sequer corrigir; avaliar tampouco é classificar, examinar, aplicar testes (MÉNDEZ, 2002).

A avaliação deverá ser uma troca, onde poderíamos analisar a realidade dos discentes e verificar suas necessidades profissionais e pessoais, bem como reorientar para uma aprendizagem melhor e para a melhoria do sistema de ensino. Aqui entra o papel do envolvimento de todo corpo docente do Estb Ens, formado, de acordo com o artigo 37 do Regulamento de Preceitos Comuns aos Estabelecimentos de Ensino do Exército (R-126), pelo comandante, subcomandante, instrutores e monitores. O quadro 3 apresenta as respostas da terceira pergunta feita aos docentes.

QUADRO 3 - Instrumentos de avaliação

Qual(is) instrumento(s) que o senhor utiliza para avaliar os instruendos? Por quê?	
Objetivo: analisar quais os instrumentos de avaliação os docentes utilizam e por que os utilizam. A intenção da pergunta era também verificar se tinha algum objetivo ou finalidade a utilização desses instrumentos.	
Professor nº 1	Prova escrita ou prática. Avalia com alto grau a meritocracia.
Professor nº 2	Palestra, demonstração, exercícios individuais e avaliação. Entendo que são as melhores maneiras de se obter um bom resultado
Professor nº 3	Atividade prática por permitir ao instrutor visualizar se houve a compreensão do conteúdo transmitido
Professor nº 4	Provas
Professor nº 5	Exercício individual para avaliar o militar em si, e exercícios em grupo para avaliar os instruendos de maneira geral

Fonte: o autor, 2017.

Após análise das respostas dos professores, nos quadros, pode-se deduzir que, para avaliar, os docentes utilizam diversos instrumentos, variando assim a forma de analisar, onde contribui para uma avaliação mais democrática e qualificada. A utilização somente de apresentação oral pode ser muito proveitosa para “João”, mas existem diversas competências que devem ser analisadas em João, isso

quando o principal objetivo da avaliação é analisar, acompanhar e verificar a aprendizagem do aluno. Esse mesmo instrumento utilizado com João pode não ser adequado para "José". Claro que a sua deficiência tem que ser trabalhada pelo professor, mas há qualidades neste que tem de ser descobertas e desenvolvidas, pois, só assim, é possível empreender o respeito pelo ser em crescimento. Por isso, é interessante a diversidade e finalidade dos instrumentos de avaliação. Quem é o responsável, em sala de aula, pelo desenvolvimento do aluno na área afetiva, na criação, na argumentação etc., é o professor. Ele tem em mãos diversos instrumentos para possibilitar esse processo de construção. Podemos citar como exemplo a entrevista que ocorre através do diálogo e segundo Méndez (2002, p.107) permite comprovar e valorizar, com base em uma sólida formação por parte do docente, a consistência do raciocínio, das aquisições e das capacidades cognitivas do aluno.

Nas respostas dos docentes, são poucos aqueles que apontaram objetivos na utilização dos instrumentos de avaliação, ficando obscura a finalidade do processo.

Tornar independente o papel do docente com relação à avaliação do conhecimento em sala de aula é de grande valia por contribuir, não só pela valorização do profissional, pois é ele quem está analisando e contribuindo para o desenvolvimento do aluno. É o docente quem sabe a real necessidade do aluno; é ele que, quando compreende suas atribuições, ajuda na mediação aluno-conhecimento. Por isso, é imprescindível que ele esteja diretamente ligado ao processo ensino-aprendizagem em sala de aula, para saber qual o instrumento mais adequado para avaliar o aluno. No quadro 4, observa-se algumas respostas em relação a esse tema.

QUADRO 4 - Responsabilidade pela seleção dos instrumentos de avaliação

Em relação aos instrumentos de avaliação utilizados em sala de aula, responda: Quem os determina em seu Estb Ens? Você concorda? Justifique.	
Professor nº 1	O monitor da matéria. Sim. Dá liberdade ao monitor para verificar qual é a melhor ferramenta a utilizar
Professor nº 2	Vem determinado no PlaDis. Na maioria das vezes, discordo
Professor nº 3	Os formais, são determinados conforme Plano de Disciplinas, ainda assim, o como será feito é proposto pelo instrutor, mediante aprovação da Divisão de Ensino (STE).
Professor nº 4	Seção de Ensino. Sim
Professor nº 5	O instrutor tem liberdade na escolha dos instrumentos a serem utilizados, sendo, porém, fiscalizado e também avaliado pela seção técnica de ensino

Fonte: o autor, 2017.

O Estb Ens não perde suas responsabilidades e atribuições no processo de aprendizagem, mas o principal responsável por utilizar e escolher os instrumentos de avaliação deveria ser o professor. A escola tem o papel no processo avaliativo buscando ferramentas de acordo com as necessidades dos docentes, como também, analisar juntamente com o docente se esse instrumento é de fato a ferramenta mais adequada para acompanhar o aprendizado do aluno. Os instrumentos utilizados na avaliação só fazem sentido quando propicia o desenvolvimento do educando e do corpo docente, refutando quaisquer correlações como instrumentos de dominação e exclusão.

Nota-se, de acordo com as respostas dos docentes, que alguns Estb Ens participam na escolha, independentemente da aprovação do instrutor e dos instrumentos avaliativos. É comum escutar dos próprios docentes que o Estb Ens cobra muito o conteúdo programático, deixando de lado a qualidade do aprendizado, pois o que importa realmente é a quantidade de informações que aquele aluno detém.

> Devemos descartar a ideia de que o fracasso é uma questão que só atinge o professor que se depara com essa situação e o aluno. O fracasso escolar é um assunto da escola. Aí está o saber e o saber fazer reflexivo do professor, que implicam tomar as decisões adequadas no momento oportuno, em função das neces-

> sidades do sujeito que aprende e em virtude dos contextos nos quais ocorre a aprendizagem, saber científico de especialidade e saber didático de decisão e de aplicação, ambos constitutivos do caráter próprio e pertinente da profissionalização docente. Nesse sentido, a avaliação é um ponto importante da prática do conhecimento e da implementação e do desenvolvimento do professor em seu exercício profissional. (MÉNDEZ, 2002, p. 87)

No quadro 5 estão as respostas dos docentes em relação ao seu papel e do discente no processo avaliativo.

QUADRO 5 - Papéis pedagógicos

Qual é o papel do professor e do aluno no processo de avaliação em sala de aula?	
Professor nº 1	Docente: verificar a qualidade de seu ensino. Discente: verificar a qualidade de seus estudos
Professor nº 2	Um tem a responsabilidade de adequar a instrução ao objetivo da mesma e preparar o outro para que obtenha o conhecimento mínimo necessário para alcançar tal objetivo que será refletido nas avaliações
Professor nº 3	Do docente: propor atividades que permitam ao aluno demonstrar a aquisição da competência desejada/proposta. Do aluno: preparar-se para adquirir tal competência, buscando conteúdo não apenas nas fontes propostas pelos instrutores e demonstrar seu domínio durante as avaliações
Professor nº 4	O professor tem a missão de passar o que sabe ao aluno e testá-lo com o intuito de verificar se esta assimilando tudo. O aluno tem a obrigação de apresentar o retorno esperado pelo instrutor
Professor nº 5	O papel do professor é avaliar e assessorar o instruendo, o qual terá o papel de demonstrar, através dos meios utilizados na avaliação, o conhecimento adquirido ou não

Fonte: o autor, 2017.

O papel do professor no processo de avaliação não é usar esse instrumento para pressionar os alunos, muito menos utilizar para impor a sua autoridade, o docente tem um papel a cumprir e numa avaliação formativa esse papel é importantíssimo para vencer a barreira da incapacidade profissional, onde se seleciona os mais capazes e exclui os problemáticos.

> [...] compromisso com a aprendizagem efetiva de todos os alunos. Ser professor não é ser mero transmissor de informações; é garantir que o aluno aprenda, é ser capaz de favorecer as condições para a efetiva aprendizagem por parte de todos os alunos. Portanto, é fundamental o aluno em suas dificuldades. (VASCONCELOS, 2007. p. 126)

A concepção de educação está diretamente ligada à avaliação e ambas são praticadas e entendidas, segundo Méndez (2002, p.121) como um continuum. Podemos verificar essa concepção no artigo 4º das Normas para a Avaliação da Aprendizagem – 3ª Edição (NAA – EB60-N- 06.004) que descreve a Avaliação Formativa como contínua e como está se processando a aprendizagem, propiciando mudanças de rumos para o discente e para o docente quando o resultado esperado não for atingido;

Verifica-se, nas respostas dos docentes, que cada um tem a sua opinião e concepção epistemológica com relação à aprendizagem em sala de aula e essas concepções caminham muitas vezes em paralelo ao processo de avaliação. De acordo com o que os docentes afirmam, é fácil entender que eles conhecem, em parte, sua missão em sala de aula, basta saber se aplicam no seu cotidiano escolar aquilo que teoricamente defendem e conhecem.

Como defende Vasconcelos (2007, p.126), o aluno tem de assumir um papel ativo na construção de seus destinos e se comprometer com sua mudança, e não apenas “conseguir nota para passar”. Analisando as ideias de alguns docentes, podemos notar que o papel do aluno, no processo de avaliação, con-

funde-se com o seu papel no processo ensino-aprendizagem. Um dos professores citou a autoavaliação e essa só é possível se o aluno entender seu papel no processo de avaliação da aprendizagem e contribuir assim para que o ambiente em sala de aula se torne mais propício ao aprendizado.

É muito proveitoso negociar com os alunos a elaboração da avaliação, pois assim o professor vence a barreira da imposição e da arrogância, fazendo assim que tudo aquilo que aconteceu no processo de aprendizagem não venha a quebrar a interação e as expectativas do aluno (ROMÃO, 1998, p. 76).

CONCLUSÃO

Essa pesquisa teve a intenção de buscar informações sobre as concepções de docentes a respeito da avaliação em sala de aula. Percebeu-se o quanto é difícil o entendimento de avaliação e a escolha de ferramentas apropriadas para cada finalidade. Foi observado durante a pesquisa o quanto se confunde o conceito de avaliação com seus objetivos. Esse tema ainda é muito complexo no sistema de ensino, avaliar muitas vezes exclui ao invés de corrigir os erros. Vencer o fracasso pode trazer o equilíbrio e muitas vezes motivar os alunos a buscarem respostas até então desconhecidas ou não assimiladas.

Usar caneta vermelha para mostrar os erros é a melhor forma de correção? Essa forma de avaliação apenas reforça mais o papel do professor e aluno a simples expectadores do processo ensino-aprendizagem. Nosso sistema de avaliação está favorecendo o ser individual em detrimento do ser social. Excluir ao invés de incluir. Classificar a analisar. De fato a avaliação está muitas vezes distante do real objetivo, mas se pensarmos nos processos de seleção no mercado de trabalho, bem como no processo para ingressar em uma universidade podemos verificar que essa mudança é muito mais ampla e externa à sala de aula. Fica como ideia para pesquisa posterior, entender as modalidades da avaliação da aprendizagem, bem como das ferramentas utilizadas nos cursos e estágios gerais das Linhas de Ensino Militar Bélico, Complementar e de Saúde, como consta na portaria Nº 202 - DECEx, DE 23 DE NOVEMBRO DE 2016 que aprova as Normas Para a Avaliação da Aprendizagem – 3ª Edição (NAA – EB60-N-06.004), confrontando com as ideias dos pesquisadores mencionados neste documento.

EVALUATION PROCESS IN COURSES AND GENERAL STAGES OF THE BELIEVING, COMPLEMENTARY AND HEALTH MILITARY TEACHING LINES IN THE BRAZILIAN ARMY

ABSTRACT: This work consists of analyzing the conception of monitors and instructors regarding the evaluation process in classroom learning, as well as confront their concepts and ideas with as authors of products - researchers of the subject in question. An experiment of courses and internships conducted, as well as a researched research, were as main tools for an analysis. To analyze the ideas of instructors and instructors - from the Army Teaching System in what is a teaching course and general stages of Military, Complementary and Health Military Education - a questionnaire with five questions was carried out. At the same time there were questions such as: 1) Do you know about legislation and standards in the process of Learning Assessment in the Army? 2) What does it mean to evaluate learning in the classroom? 3) Which instrument do you use to evaluate the instructors? Because? 4) In relation to the evaluation instruments used in the classroom, answer: who determines your educational institution? Do you agree? Justify. 5) What is the role of the teacher and the student in the evaluation process in the classroom? This topic is extremely important because we often exclude some students who have already been discovered because of distortions in the teaching-learning process. It was observed that a good part of the instructors an assessment only to give notes to their students as well as save as information obtained as a document to prove at the end of a course or internship, a disability of the students. The distorted idea of evaluation is still a reality in our educational system, but it's true, it also exists in your education system, but it's also true that you're looking for it.

Keywords: Evaluation. Learning. Teacher.

REFERÊNCIAS

BRASIL. Portaria nº 202 - DECEx, de 23 de novembro de 2016. Aprova as Normas para a Avaliação da Aprendizagem – 3ª Edição (NAA – EB60-N-06.004) e dá outras providências.

_____. Portaria nº 549, de 6 de outubro de 2000. Aprova o Regulamento de Preceitos Comuns aos Estabelecimentos de Ensino do Exército (R-126)

_____. Portaria nº 143- DECEx, de 25 de novembro de 2014. Aprova as Normas para Desenvolvimento e Avaliação dos Conteúdos Atitudinais (NDACAEB-60-N-05.013).

MÉNDEZ, Juan Manuel Álvarez. Avaliar para conhecer, examinar para excluir. Porto Alegre: Artmed Editora, 2002.

ROMÃO, José Eustáquio. Avaliação dialógica: desafios e perspectivas. São Paulo: Instituto Paulo freire, 1998.

VASCONCELOS, Celso dos santos. Construção do conhecimento em sala de aula. 16. ed. São Paulo: Libertad, 2005.

_____. Avaliação: concepção dialética-libertadora do processo de avaliação escolar. 17. ed. São Paulo: Libertad,2007.

O autor é formado pela Escola de Sargentos das Armas e graduado pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul em Licenciatura em matemática. Atualmente, é instrutor deste estabelecimento de ensino e integra a Seção de Ensino B. Pode ser contactado por intermédio do email erlanpe@gmail.com

ÁREA DE CONCENTRAÇÃO

HISTÓRIA MILITAR

ESCOLA DE COMUNICAÇÕES

O CONCURSO VERDE AMARELO E A REDE NACIONAL DE EMERGÊNCIA DE RADIOAMADORES

Daniel Moura Felix Cardoso
Pós-graduado em Operações Militares

RESUMO. Este trabalho apresenta o radioamadorismo, o Concurso Verde Amarelo (CVA) e a Rede Nacional de Emergência (RENER), dispondo sobre a preparação física, técnica e mental dos radioamadores, bem como a preparação de suas estações, em apoio às ações de calamidade pública no Brasil. Ao reunir estudos acerca do radioamadorismo e seu emprego em calamidades, podemos identificar as possibilidades e limitações do serviço de radioamadorismo, bem como suas necessidades e embasamento jurídico para o seu correto emprego. A intenção desse artigo foi a de consolidar os conhecimentos e identificar a validade dos ensaios práticos no estabelecimento de uma rede nacional (por intermédio de um concurso de radioamadores) com a finalidade de manutenir o pronto emprego em situações de emergência. A regularidade dos contatos apresentados pelos radioamadores nas diversas edições do Concurso Verde Amarelo, torna possível identificar estações de rádio fixas próxima a àreas de calamidade, objetivando o estabelecimento de uma rede rádio emergencial.

Palavras-Chave: Radioamador. Concurso verde amarelo. Rede nacional de emergência de radioamadores. Calamidade pública.

INTRODUÇÃO

Até os anos 80, a viabilidade de se possuir uma linha telefônica em casa era quase nenhuma, pelo valor dispendioso de adquiri-la. Comumente, os mais afortunados cediam as suas linhas residenciais para os vizinhos efetuarem ou receberem ligações.

Com o aumento exponencial da troca de informação, as pessoas sentiram a necessidade de possuir uma forma mais econômica e de confirmada eficácia para comunicar-se à distância. Dessa forma, a atividade de radioamadorismo teve largo emprego até o surgimento e disponibilização de tecnologias mais favoráveis.

Em um momento de crise, na defesa civil, considerando uma inundação ou um deslizamento de terra, alguns dos serviços básicos são suprimidos pela calamidade. Normalmente, o serviço de energia elétrica e de comunicações são interrompidos por causa do mau tempo, destruição das linhas de transmissão de energia elétrica e de telefonia por fio e, até mesmo, de telefonia celular por falha nas antenas retransmissoras. Uma alternativa muito utilizada e comprovadamente eficaz é o emprego do radioamadorismo para a imediata implantação de uma rede de telecomunicação emergencial nesses momentos.

No ambiente militar, a grande capilaridade das Forças Armadas espalhadas pelo território nacional e a necessidade destas em realocar seus recursos humanos, fez com que os militares procurassem meios, para solucionar o problema comunicação com seus familiares deixados em suas cidades de origem. Muitas dessas cidades, sedes de Organizações Militares, não possuíam cabeamento telefônico ou centrais telefônicas que comportassem a distribuição de linhas pelas residências. Dessa forma, a atividade de radioamadorismo passou a ser amplamente utilizada nesse momento de pré-evolução da telefonia, por esta classe que a cada dois, três anos seguia destino pelos diversos rincões deste país. Por vezes, as estações eram utilizadas por vizinhos, em substituição ao serviço telefônico. Essa mesma realidade foi vivenciada por funcionários de bancos federais e estaduais até a ampliação dos meios de comunicações públicos.

1 DESENVOLVIMENTO

O Radioamadorismo é uma atividade voltada para o estabelecimento e o desenvol-

vimento de novas formas de telecomunicações via rádio e o estudo da propagação das ondas eletromagnéticas, na qual podem ser favorecidas quaisquer pessoas envolvidas no processo. Ao longo do tempo, o radioamadorismo atuou como solução alternativa ao alto custo da telefonia pública, até a década de 80, até assumir o viés emergencial, característico do estabelecimento das comunicações críticas em momentos emergenciais como crises e calamidades.

Pode-se identificar o caráter humanitário que permeia a atividade de radioamadorismo, no apoio aos órgãos de defesa civil e a sociedade afligida pelas calamidades.

Nesse ínterim, a Rede Nacional de Emergência de Radioamadores foi estabelecida para facilitar a organização e permitir o exercício do comando e controle, em situações de crise, calamidade ou emergência.

Nesse sentido, o estabelecimento de concursos de radioamadores contribuem para o treinamento dos operadores, integração entre os participantes e manutenção da própria rede nacional de emergencial de radioamadorismo.

1.1 RADIOAMADORISMO

A preparação para o ingresso na atividade de radioamadorismo exigia algum conhecimento técnico e expertise na preparação da estação. Portanto, o candidato procurava aprender com companheiros que já utilizavam o serviço de radioamadorismo, realizando cursos e buscando orientações em seus quartéis com companheiros da área de comunicações. Alguns militares iniciaram a atividade de radioamadorismo por intermédio da faixa do Cidadão, reconhecido oficialmente como Serviço Rádio do Cidadão. Tratava-se de um serviço de telecomunicações de interesse restrito, explorado no regime privado, para comunicações de uso compartilhado entre estações fixas ou móveis, utilizava a faixa de radiofrequência de 27 MHz, por meio da canalização de frequências com modo de operação único (a fonia). Sua principal finalidade era proporcionar comunicações, atendendo situações de emergência e transmitindo sinais de telecomando para dispositivos elétricos. Seu acesso não dependia de comprovação de conhecimentos técnicos, pois o objetivo maior desse Serviço é permitir a existência autônoma e privada de meios de telecomunicações, onde o Estado ainda não podia oferecer. Portanto, algo relativamente embrionário e significativamente menor em relação à capacitação técnica dos radioamadores, diversidade de frequências e modos de operação que estes utilizam.

As provas de capacidade para o exercício da atividade de radioamadorismo envolvem questões de ética e técnica operacional, legislação de radioamadorismo e, dependendo da classe, quantidade de frequências, modo de operação e nível de potência que se pretenda utilizar, adicionam-se as provas de recepção e transmissão em código morse e radioeletricidade.

No Brasil, o radioamadorismo é dividido em três classes: A, B e C. Os radioamadores classe C possuem autorização para o uso de determinadas faixas para operação e um limite de 100w de potência. Os radioamadores classe B tem um acréscimo de faixas para uso, além de um incremento na potência dos equipamentos alcançando 1000w. Os radioamadores de classe A gozam dos mesmos direitos dos radioamadores de classe B, podendo, ainda, gerir estações rádio de entidades, instituições escolares e estações repetidoras.

Muitos Radioamadores optaram em começar pela banda de PX ou logo após a aprovação na prova de habilitação ao serviço, adquiriram um equipamento de menor custo, uma vez que os equipamentos de radioamadorismo possuem um valor considerável. O gradual aprofundamento do radioamador com a atividade faz com que se busque melhores rádios e antenas de maior desempenho, visando diversificar contatos, de melhor qualidade, maior distância, incluindo contatos internacionais (DX), construindo marcos colecionáveis de estabelecimento de enlace, catalogando os

contatos por intermédio dos cartões QSL ou meios eletrônicos (internet) de confirmação.

Um dos fatores que faz surgir a paixão pela atividade de radioamadorismo está no êxito do enlace estabelecido. Ao ver o resultado do esforço empreendido, estudando os detalhes técnicos do rádio, calibrando sua estação, preparando sua antena, buscando a menor onda refletida e sendo recompensado pelo estabelecimento do contato rádio, sem depender de estações repetidoras. Dessa forma, o radioamador sabe que consegue colocar no espectro eletromagnético o sinal adequado à realização de um contato, sem depender de fatores diversos aos seus equipamentos, apto à se comunicar com qualquer radioamador que possua um equipamento rádio em condições similares ou não. O conhecimento adquirido pode ser tão vasto que o radioamador busca a otimização da transmissão e reduz perdas sem ter que trocar o seu equipamento. Diversos são os fatores que influenciam na transmissão otimizada, como direcionar antenas para o local da outra estação com precisão, utilizar antenas polarizadas corretamente e conectadas ao rádio com linhas de baixa perda, via de regra coaxiais.

1.2 O EXÉRCITO, AS COMUNICAÇÕES E O RADIOAMADORISMO

A Escola de Comunicações (EsCom) do Exército é uma instituição de ensino militar voltada para a capacitação técnica e tática de oficiais e sargentos para o combate moderno, aliando a competência do ensino militar bélico à modernidade da era do conhecimento. A EsCom é uma escola de tradições, com desenvolvimento do ensino na área de informática, cibernética, manutenção de equipamentos e comunicações. Nesta última, muito do que é estudado é fruto do que fora desenvolvido pelos radioamadores ao longo dos mais de cem anos de história.

O Clube de Radioamadores da Escola de Comunicações (CRAEC) é uma entidade civil que estabeleceu (e até hoje promove) o Concurso Verde Amarelo (CVA) de Radioamadores, que consiste em classificar aqueles radioamadores que fizerem contatos entre si em um prazo de 24 horas nas modalidades de Single Side Band e Telegrafia com a finalidade de congraçar os participantes e identificar suas habilidades. Da mesma forma, o CVA é um meio de atestar capacidade de transmissão das estações rádio, e resistência física e mental dos radioamadores, submetendo-os a um longo e contínuo período de operação, fazendo-os procurar pela melhor hora de propagação e realizando o máximo de contatos.

A audição apurada do radioamador aliada à sua vontade de garantir maior variedade de contatos faz com que o mesmo busque, inclusive, aquele contato interferido por alto ruído e menor clareza, empenhando-se para receber a informação de forma completa e precisa. O CRAEC, utilizando-se dos resultados do CVA pode fornecer ao Comando da Força Terrestre um relatório das possibilidades e limitações do radioamadorismo, dos diversos radioamadores em cada classe e suas estações, catalogando os voluntários e adeptos das atividades militares podendo trabalhar de forma a auxiliar o comando e controle.

Essa é a forma que o Exército Brasileiro tem de aferir a agregação dos radioamadores à sua capacidade laboral, bem como estimular a melhoria desses na atuação consigo. Nos concursos de radioamadores, seus relatórios (chamados de LOG) indicam os contatos realizados e, com base nas informações neles constante, os organizadores das competições tem todas as condições de saber quais são as estações que poderiam compor uma rede de emergência ou redundante de operações.

1.3 CALAMIDADES PÚBLICAS

Conforme observa-se anualmente nos diversos jornais e telejornais, as calamidades públicas são realidade em várias localidades do nosso país. Elas se apresentam de várias formas, mas aquelas mais ocorrentes são os deslizamentos de terra e inundações.

Os deslizamentos de terra normalmen-

te se dão em momentos de grande pluviosidade, afetando localidades que se apoiam em serras ou elevações normalmente com pouca ou nenhuma vegetação para evitar ou reduzi-los. Essas localidades, dentre outras consequências, sofrem com os soterramentos e desmoronamentos de instalações que podem suprimir os citados serviços públicos, e nesse caso, as telecomunicações.

1.4 REDE NACIONAL DE EMERGÊNCIA DE RADIOAMADORES

Vendo grande potencial nessa classe seleta de operadores de telecomunicações e seguindo exemplo de outros países que fazem uso desse serviço, o Ministério da Integração, por intermédio da Portaria Ministerial MI-302, de 24 de outubro de 2001, criou a Rede Nacional de Emergência de Radioamadores (RENER). Essa rede, que é formada por radioamadores voluntários e coordenada pela Liga de Amadores Brasileiros de Rádio Emissão (LABRE) Nacional, encontra-se em condições de ser operada em momento de crise ou de calamidade pública, adicionando assim mais meios de comunicações para as forças de segurança pública, guarda costeira ou defesa civil.

> O voluntariado exerce extrema importância para o sucesso de uma Defesa Civil. É com o auxílio de trabalhos voluntários que o Estado presta serviços concernentes às atividades de defesa civil com maior facilidade. O profissional, de qualquer área, que é voluntário da Defesa Civil, além de estar exercendo a cidadania, está contribuindo para que os problemas existentes em sua comunidade sejam resolvidos. (CERRI NETO, 2007).

Segundo MOURA, podemos relacionar o emprego da Rede Nacional de Emergência de Radioamadores, que é regulada por legislação específica, com a preservação do bem-estar dos cidadãos e a proteção da sociedade (MOURA, 2015). O Radioamador mostrou-se valioso em momentos como o atentado terrorista de 11 de setembro de 2001 contra o World Trade Center em Nova Iorque-Estados Unidos, terremoto no Haiti em janeiro de 2010 e tantos outros.

A RENER foi acionada e empregada em eventos ocorridos no Brasil, sendo algumas dessas atuações mais recentes e de conhecimento público em Santa Catarina, em 2008; em São Luiz do Paraitinga e Cunha, São Paulo, em 2010; e na região serrana do estado do Rio de Janeiro, em 2011. (VEIGA JÚNIOR, 2014) Todas essas atuações em apoio à defesa civil por ocasião de deslizamentos de terra, inundações e outras calamidades públicas.

CONCLUSÃO

Com o mesmo vigor que o Padre Roberto Landell de Moura, brasileiro, precursor das transmissões voz via rádio no mundo, o radioamador é peça fundamental para a exploração e manutenção das telecomunicações via rádio, principalmente em momentos de crise. Com o mesmo espírito de inovação, o radioamador emprega nos equipamentos atuais os mesmos princípios fundamentais de Landell.

> Antes da modernização do rádio, as estações amadoras já eram largamente empregadas por serem o meio mais eficaz para se comunicar. Entretanto tratavam-se de equipamentos grandes que ocupavam muito espaço, devido ao sistema valvulado que era empregado. A evolução tecnológica substituiu as válvulas por transistores, circuitos integrados e outros componentes que foram responsáveis por difundir o emprego do rádio como hobby, pois o barateamento dos equipamentos acabou por popularizar a radiodifusão. (MOURA, 2015, p. 49)

Radioamador, que de amador só tem o nome e a paixão pela atividade de radiotransmissão, pois o caráter de profissionalismo apresentado pelos integrantes dessa seleta classe de estudiosos e cientistas da área técnica de telecomunicações é impressionantemente usada em qualquer momento, de qualquer maneira e a qualquer hora para estabelecer os enlaces rádio em proveito de qualquer ajuda humanitária ou apoio aos órgãos governamentais nas ações de defesa civil ou operações militares das Forças Armadas

THE GREEN YELLOW CONTEST AND THE NATIONAL AMATEUR RADIO EMERGENCY NETWORK

ABSTRACT: This work presents a study about the participation of amateur radio in the National Amateur Radio Emergency Network (RENER) in the Green Yellow Contest (CVA) for their physical, technical and mental preparation, as well as their stations for the support of this network in actions of public calamity in Brazil.

Keywords: Amateur Radio. Yellow Green Contest. National Amateur Radio Emergency Network. Public Calamity.

REFERÊNCIAS

BRASIL. Ministério da Integração Nacional. Portaria Ministerial nº 302, de 24 de outubro de 2001. Cria a Rede Nacional de Emergência de Radioamadores – RENER, como parte integrante do Sistema Nacional de Defesa Civil – SINDEC. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 26 out. 2001. Seção 1, p. 131.

BRASIL. Agência Nacional de Telecomunicações. Resolução nº 578, de 30 de novembro de 2011. Aprova o Regulamento do Serviço Rádio do Cidadão. Brasília, 06 de dezembro de 2011. Disponível em < http://www.anatel.gov.br/legislacao/resolucoes/2011/77-resolucao-578>. Acesso em: 14 nov 2017.

BRASIL. Ministério da Integração Nacional. Portaria Ministerial nº 307, de 22 de julho de 2009. Aprova a Norma de Ativação e Execução dos Serviços a serem prestados pela Rede Nacional de Emergência de Radioamadores - RENER. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 23 jul. 2009. Seção 1, p. 139.

CERRI NETO, Mauro. **Aspectos Jurídicos das Atividades de Defesa Civil**. Brasília: Secretaria Nacional de Defesa Civil, 2007.

MOURA, Marcelo Reis de. **Vantagens e Desvantagens da mobilização da Rede Nacional de Radioamadores em apoio às Operações Militares nas Olimpíadas de 2016 na cidade do Rio de Janeiro**. 2015. 65 f. Trabalho de Conclusão de Curso (Pós-Graduação em Ciências Militares) – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2015.

VEIGA JUNIOR, João Carlos Valentim. **Rede Nacional de Emergência de Radioamadores:** evolução, procedimentos e aspectos legais. Revista Jus Navigandi, Teresina, ano 19, n. 3965, 10 maio 2014. Disponível em: <https://jus.com.br/artigos/28110>. Acesso em: 30 out. 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Infantaria do Exército Brasileiro, Radioamador Classe B, licenciado pela ANATEL. É pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais. Atualmente, exerce a função de Presidente do Clube de Radioamadores da Escola de Comunicações, onde também desempenha a função de Instrutor e pode ser contactado pelo email felix.daniel@eb.mil.br.

Endereço

Estrada Parque do Contorno, Rodovia DF - 001, KM 5
Setor Habitacional Taquari - Lago Norte - Brasília - DF
CEP: 71559-902
Telefone: (0xx61) 3415-3532
(PABX) 3415-3502 (Voz/Fax)
Sitio: www.escom.eb.mil.br