ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações
Escola Coronel Hygino Corsetti

VOLUME 7 - Nº 3
Outubro 2017

ISSN 2594-3952

O Comunicante

SUMÁRIO

Artigos

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 7 - Nº 3

Outubro 2017

EXPEDIENTE

O COMUNICANTE

Revista Científica da Escola de Comunicações

Ano 7 - Nº 3
Outubro 2017

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

O Comunicante Revista Científica - Escola de Comunicações Volume 7, Nº3(Out/2017)
Brasília-DF: Escola de Comunicações. 2017 65p; 29,7 cm X 21,0 cm

Publicação Quadrimestral
ISSN 1968-6029
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina
6. Direito 7. Educação 8. Informática 9. Instrução Militar 10. Gestão 11. Meio Ambiente
12. Operações Militares Conjuntas e Singulares.11

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 a 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, todos profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, 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 consultar a mesma a respeito da submissão do artigo a esta Revista Científica, cientificando-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 e os mesmos terão o prazo de 30 dias para fazerem a sua 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

O QUE O FUTURO NOS RESERVA?

Não há necessidade de recorrer às pesquisas globais para entender que vivemos num diuturno turbilhão de avanços tecnológicos, mas fazê-lo nos ajuda a entender qual é a perspectiva intuitiva do avanço tecnológico. Por exemplo, estima-se que, nos próximos 30 anos, o mundo estará um bilhão de vezes mais avançado tecnologicamente.

Em outras palavras, estaremos vivendo numa realidade completamente diferente da cotidiana; surreal se comparada à realidade de 50 anos atrás, quando nem ao menos se vislumbrava a viabilidade da telefonia celular.

O conhecimento adquirido, esforço e empreendimento nos levaram a exercer certo domínio sobre a tecnologia vigente, em cada campo do conhecimento, segundo as especializações e competências almejadas. Isso nos foi útil para alcançar a alvorada dos acontecimentos, mas é ineficiente para nos projetar ao horizonte vindouro.

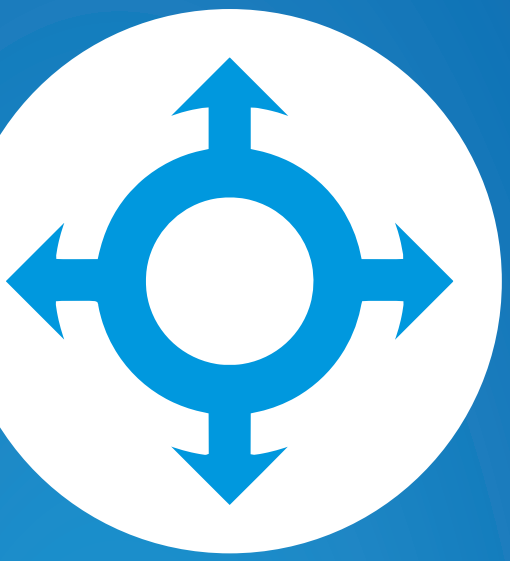
É necessária uma mente irrequieta, que não se acomoda, que não se contenta com os primeiros passos, que vislumbra o horizonte distante e não se deixa esmorecer diante do planejamento necessário para alcançá-lo. É capaz de firmar com solidez os pés no chão, enquanto ruma em direção ao futuro.

Buscando veementemente esse horizonte, a Revista O Comunicante convida seus leitores a conhecerem o universo tecnológico e científico contemporâneo, suas indagações, questionamentos, problemas e possíveis soluções, com vistas a nos projetar rumo àquilo que nos aguarda.

Boa leitura a todos.

ÂNDREI CLAUHS – Cel
Comandante da Escola de Comunicações

Pareceristas Externos Convidados



Márcio Denis Pessanha Gonçalves

- Assessor Jurídico e Chefe da Seção de Inovação Tecnológica do Comando de Comunicações e Guerra Eletrônica do Exército.
- Bacharel em Direito e Doutor em Ciência da Informação.
- Área de Atuação: Direito.

ETHICAL HACKING E LEGÍTIMA DEFESA ELETRÔNICA

Isaac Rodrigues Ramos Neto
Pós-graduando pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas)

RESUMO. Estudo sobre a possibilidade de configuração de legítima defesa eletrônica diante da atuação dos Times de Resposta a Incidentes de Segurança Computacional (CSIRT), na observância da prática do delito de invasão de dispositivo informático na modalidade qualificada, previsto no artigo 154-A, §§ 3º e 4º, do Código Penal Brasileiro. Debate acerca da prática do ethical hacking e se tal conduta amoldar-se-ia à excludente da legítima defesa. Utiliza o método dedutivo, bem como a pesquisa doutrinária, legislativa e jurisprudencial. Recorre à internet como forma de complementação dos assuntos estudados. Espera demonstrar, ao final, que o ethical hacking poderá configurar hipótese de legítima defesa eletrônica, desde que obedecidos todos os requisitos desta, sendo o caminho mais adequado para reduzir os danos gerados pela invasão, pois, uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet, causando à vítima danos de improvável reparação.

Palavras chave: Legítima defesa. Crimes eletrônicos. Invasão de dispositivo informático.

1 INTRODUÇÃO

A Revolução Informacional, iniciada nas duas últimas décadas do século XX, caracteriza-se pela introdução da geração, do processamento e da transmissão de informações como fontes fundamentais de produtividade e poder por causa das novas condições tecnológicas surgidas nesse período (CASTELLS, 2005, p. 65), criando-se, assim, um novo paradigma.

Uma das diferenças entre a Revolução Informacional e as Revoluções Industriais dos séculos XVIII e XIX é a amplitude dos seus efeitos. Com os meios de comunicação bem mais avançados do que naquela época em razão da própria revolução, pode-se afirmar que, hoje, um grande número de países já adentrou a era da informação.

Não obstante tenha trazido grandes benefícios para as mais diversas áreas do conhecimento, por exemplo, a bioengenharia, a engenharia genética, a microeletrônica e as telecomunicações, a Revolução Informacional também acarretou um crescimento na ocorrência de crimes eletrônicos. Isso se deu, especialmente, pela alteração do perfil do agente que comete tais tipos de delitos.

O criminoso eletrônico ostentava a qualidade de “exímio perito na operação de computadores e sistemas computacionais” (MONTEIRO NETO, 2003, p. 41), todavia, hoje, qualquer curioso usuário da internet pode aprender, por meio de diversos tutoriais disponibilizados na web, como realizar uma invasão. Assim, considerando que há meios técnicos e jurídicos para identificar o infrator e puni-lo devidamente e que uma vez de posse da informação subtraída, o invasor poderia facilmente espraiá-la pela internet, nascem alguns questionamentos: seria possível reconhecer a legítima defesa, amparada pelo Direito Penal como causa excludente de ilicitude, diante da observância da prática desse delito? Em que situações específicas? Quais seriam seus limites?

O objetivo aqui trazido é o de analisar, à luz do direito penal brasileiro, a possibilidade de configuração de legítima defesa diante da observância da prática do delito de invasão de dispositivo informático em sua modalidade qualificada. Perceber-se-á que toda a análise realizada é interdisciplinar, porque, se não o fosse, seria incompleta. Valer-se apenas do Direito para entender esse fenômeno seria uma atitude

falha.

A pesquisa tem especial aspecto acadêmico, pois a discussão acerca da legítima defesa eletrônica é incipiente, necessitando de análises aprofundadas. Possui, ainda, relevante aspecto social no intuito de esclarecer se determinada conduta de proteção da informação poderá ser considerada legítima defesa ou não, extravasando seus limites.

2 DESENVOLVIMENTO

Com a sanção da Lei nº 12.737/2012, o ordenamento jurídico brasileiro foi presenteado com a tipificação do primeiro delito eminentemente eletrônico: a invasão de dispositivo informático (artigo 154-A do Código Penal). Essa tipificação representa o primeiro grande passo no sentido de combater os crimes eletrônicos no Brasil, que, paulatinamente, só aumentam o seu número de incidências.

Deve-se atentar, contudo, que, em alguns casos, o Poder Judiciário não conseguirá agir de forma efetiva e eficaz para recuperar os danos sofridos em razão desse novo tipo penal, especialmente, na sua modalidade qualificada, em que há subtração de informações e eventual compartilhamento. Sabe-se que uma vez obtida a informação, se esta não for imediatamente recuperada, o agente criminoso poderá difundi-la rapidamente por toda a internet, impossibilitando, assim, qualquer justa reparação pelos prejuízos sofridos. O direito ao esquecimento, por exemplo, não passa de uma mera fantasia, visto ser impossível relegar ao oblívio dados dispersados na rede mundial de computadores.

Assim, como meio de enfrentar tais delitos, levanta-se a possibilidade de configuração da legítima defesa em meio ambiente eletrônico.

2.1 DEFINIÇÃO DE ETHICAL HACKING

O ethical hacking pode ser entendido sob dois aspectos.

De um lado, pode ser definido como uma forma de prevenção, consistindo numa série de testes de segurança, a fim de identificar as possíveis falhas nos sistemas e, assim, fortalecê-los (KNIGHT, 2009).

Por outro lado, também pode ser visto como a ação de recuperação dos dados subtraídos, agindo o profissional de segurança com a mesma técnica do agente criminoso (hacking back). É esta faceta que interessará ao presente trabalho.

O hacking back é um meio de resposta ativa contra invasões. São duas as suas principais modalidades (DENNING, 2008, p. 422). A primeira trata-se de uma invasão com a finalidade de localizar o sistema computacional que originou os ataques e, consequentemente, os agentes envolvidos. A segunda envolve contra-atacar a máquina de origem dos ataques, com a finalidade de suspender a ação invasiva, bem como, eventualmente, recuperar informações obtidas de modo indevido.

Dois acontecimentos tornaram-se famosos nos Estados Unidos pela utilização desta técnica para combater delitos eletrônicos: o primeiro, um ataque eletrônico contra o Pentágono; e o segundo, contra o site da Organização Mundial do Comércio (OMC).

Em setembro de 1998, foi documentada, pela primeira vez, a utilização da técnica do hacking back. O Pentágono reagiu a um ataque de negação de serviço, iniciado pela Eletronic Disruption Theater, uma organização hacktivista, utilizando-se de uma técnica ofensiva para interromper o funcionamento daqueles dispositivos de onde partiam as invasões (JAYASWAL; YURCIK; DOSS, 2002, p. 381).

A segunda reação documentada ocorreu em janeiro de 2000, durante uma reunião da OMC. O grupo The Electrohippies Collective, também conhecido por e-Hippies, invadiram o site da OMC, utilizando também ataques de negação de serviço (DENNING, 2008, p. 423).

Na ocorrência de uma invasão, devem ser seguidos três passos na utilização do hacking back (PINHEIRO, 2013, i. 8.37). O primei-

ro passo é identificar o causador da invasão por meio de sistemas de detecção (intrusion detection systems – IDS), como o firewall. O segundo passo é chegar ao dispositivo informático responsável pelos ataques (traceback). Atenta-se que a invasão de um dispositivo informático também poderá resultar no controle remoto deste. Um possível ataque ao computador que está apenas sendo manipulado, apesar de não configurar o delito do artigo 154-A, por ausência de dolo, não impossibilita a reparação civil pelos eventuais danos causados. O terceiro e último passo é contra-atacar, seja para interromper o funcionamento daquele sistema, cessando a invasão, ou para recuperar informações obtidas ilegalmente (KESAN; HAYES, 2012, p. 461-467).

O tempo para a tomada dessas decisões deve ser o mais curto possível, facilitando a identificação do invasor e diminuindo as perdas econômicas (JAYASWAL; YURCIK; DOSS, 2002, p. 380).

2.2 TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL (COMPUTER SECURITY INCIDENT RESPONSE TEAMS – CSIRT)

Com o grande número de incidentes computacionais, conforme informações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) e do Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov), surge a necessidade de aprimorar a segurança das empresas, bem como dos órgãos públicos, agora, com o fim de proteger as suas informações e o bom desenvolvimento de suas atividades. Tal proteção é feita pelo CSIRT.

O primeiro CSIRT surgiu em 1988, após um fato conhecido por The Morris Worm Incident (PEIXOTO, 2008, p. 2).

O CSIRT tem, como objetivo primordial, o monitoramento, "para que se possa pegar o infrator literalmente com a 'mão na máquina', quer ele seja de dentro, algum funcionário ou colaborador, quer seja de fora" (PINHEIRO, 2013, i. 8.37). É, assim, necessário um funcionamento incessante, sendo o CSIRT um verdadeiro guardião da rede. Os times também poderão ser um grupo ad hoc, formado exclusivamente para responder e avaliar incidentes específicos (CRESPO, 2011, p. 113), desvirtuando-se, nesses casos, de sua natureza de monitoramento.

A atuação do CSIRT no combate a incidentes pode ser resumida em seis grandes etapas (PEIXOTO, 2008, p. 36 et seq.):

a) Preparação: momento de prevenção, conscientização dos usuários e realização de auditorias;

b) Identificação, contenção e erradicação: coincidem com as três fases do hacking back anteriormente expostas;

c) Recuperação e aprendizado: essa etapa nada tem que ver com a recuperação de informações subtraídas. É um momento de evolução, em que o CSIRT irá recuperar-se dos danos eventualmente sofridos, ampliará e aperfeiçoará suas defesas, verificará se o sistema está operando corretamente e, finalmente, aprenderá com seus erros, tentando evitar novas falhas em situações futuras.

2.3 ETHICAL HACKING E LEGÍTIMA DEFESA ELETRÔNICA

A legítima defesa está prevista no Direito Penal Brasileiro, no CP, art. 23, II, como uma causa de excludente de ilicitude. Historicamente, a legítima defesa surgiu após a vingança particular cair em desuso (FIORETTI, 2002, p. 21). Pode ser definida como o uso moderado dos meios necessários, a fim de repelir injusta agressão, atual ou iminente, a direito seu ou de terceiro(s).

Pode-se afirmar que a expressão "legítima defesa" trata-se de uma redundância, um pleonasmo. Na realidade, o termo "legítima" foi acrescentado pelo Direito Romano, pois as palavras "defesa" e "agressão" eram designadas

pelo mesmo termo: o verbo fendo (FIORETTI, 2002, p. 21).

O conceito de legítima defesa sofreu abalos apenas durante a Idade Média, período no qual predominou os impérios da Igreja Católica. Segundo FIORETTI (2002, p. 39), "o exercício da legítima defesa parecia um ato lesivo da caridade para com o próximo".

A partir do conceito anteriormente descrito, infere-se seus requisitos.

O primeiro é a injusta agressão a um bem jurídico. O termo agressão deve ser entendido como toda ação que tenha a finalidade de por em perigo ou gerar dano a um bem jurídico, podendo ser violenta ou não (PRADO, 2009, p. 351; BITENCOURT, 2012, cap. XXI, i. 6.3.1). O conceito de injusto coincide com o de ilícito. Se houver afronta a um bem tutelado pelo ordenamento jurídico, mesmo não havendo um tipo penal específico, a legítima defesa poderá ser invocada, desde que a conduta obedeça aos requisitos necessários para sua configuração. Portanto, observe-se que a injustiça da agressão deverá estar relacionada a aspectos objetivos, nunca podendo estar relacionada com o seu autor.

O segundo é um requisito temporal, qual seja agressão deverá ser atual ou iminente. Iminente é a conduta que está prestes a acontecer, não admitindo, portanto, delongas na repulsa (BITENCOURT, 2012, cap. XXI, i. 6.3.1). Atual é a agressão presente, que, já iniciada, ainda não se concluiu (PRADO, 2009, p. 352) ou, simplesmente, aquela que está acontecendo (GRECO, 2015, p. 404). Portanto, é pouco provável a configuração de legítima defesa em relação ao tipo penal ora estudado quando a vítima for um usuário comum, pois este não possui, em regra, aparatos e conhecimentos técnicos para repelir a agressão no tempo adequado.

O terceiro é o uso moderado dos meios necessários. Meios necessários são os "eficazes e suficientes para repelir a agressão" (RODRIGUES, 2008, p. 68). A valoração acerca de quais meios serão os necessários para a repulsa "deve ser sempre [...] ex ante, isto é, do ponto de vista do sujeito no momento em que se defende" (ZAFFARONI; PIERANGELI, 2013, p. 523). O conceito de uso moderado leva em consideração o dano causado na ação. Assim, em nenhuma hipótese, a agressão infligida pela legítima defesa poderá ser maior que a própria agressão a qual ela combate (BITENCOURT, 2012, cap. XXI, i. 6.3.3), visto que, se assim o for, dará margem à ocorrência de legítima defesa sucessiva.

O quarto e último requisito é o animus defendendi. Ao contrário dos demais requisitos de ordem objetiva, este possui caráter subjetivo. Como assevera PRADO (2009, p. 353), o "agente deve ser portador do elemento subjetivo, consistente na ciência da agressão e no ânimo ou vontade (animus defendi) de atuar em defesa de direito seu ou de outrem".

2.4 LEGÍTIMA DEFESA ELETRÔNICA: NOVO CONCEITO OU APENAS UM NOVO CASO?

No Brasil, a legítima defesa eletrônica surgiu, primeiramente, no Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo, que definia "defesa digital", no art. 154-C, como a

> manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação.

Todavia, essa definição foi duramente criticada, pois criava uma figura específica de defesa que muito se distanciava daquela respaldada no artigo 25 do Código Penal. Deixava claro, ainda, que o instituto só poderia ser utilizado por "agente técnico ou profissional habilitado". Foi finalmente retirada após avaliação feita pela

Comissão de Constituição, Justiça e Cidadania (CCJC) do Senado Federal.

A prática do ethical hacking, em sua modalidade hacking back, pelo CSIRT quando está diante da prática do delito de invasão a dispositivos informáticos em sua forma qualificada, conforme o art. 154-A, § 3º, CP, deverá ser considerada legítima defesa nos termos estabelecidos no próprio art. 25, CP.

A injusta agressão a um bem jurídico, o primeiro requisito, está configurada, pois o tipo penal previsto no CP, art. 154-A, § 3º, protege, em especial, o "conteúdo das comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas, assim definidas em lei".

A resposta atual ou iminente à agressão, o segundo requisito, está relacionada à própria atuação dos CSIRTs, visto que atuam monitorando incessantemente todas as atividades nas redes de computadores de determinada empresa ou órgão, protegendo, assim, todo o fluxo de informações.

O uso moderado dos meios necessários, o terceiro requisito, também está presente, pois a técnica do hacking back foca-se na cessação da invasão, bem como na recuperação das informações subtraídas.

O animus defendendi, o quarto requisito, deverá ser avaliado caso a caso. Todavia, aqui, presumir-se-á presente, pois se está analisando a conduta de um time formado por profissionais que atuam na área de segurança da informação.

Diante do exposto, não se pode afirmar que a legítima defesa eletrônica se trata de um novo conceito. Ela é apenas um novo caso dentro da clássica previsão do Código Penal, nascida diante da necessidade de proteção das informações contra os novos agentes criminosos que se utilizam do meio ambiente eletrônico em suas empreitadas delituosas.

2.5 EXCESSOS NA PRÁTICA DO ETHICAL HACKING

O CP, art. 23, parágrafo único, prevê que "o agente, em qualquer das hipóteses deste artigo, responderá pelo excesso doloso ou culposo".

Configura o excesso quando há "flagrante desproporção entre a ofensa e a agressão, quando o agente responde com um tiro a um tapa desferido pelo agressor e quando o agente mata uma criança porque esta adentrou ao seu pomar e apanhou algumas frutas" (RODRIGUES, 2008, p. 69).

O excesso na prática do ethical hacking como legítima defesa pode ser verificado quando, por exemplo, na tentativa de recuperar os arquivos, informações além daquelas subtraídas também são obtidas, podendo ser do próprio agressor ou de um usuário diverso que tenha seu dispositivo controlado. Verifica-se nessas duas hipóteses, respectivamente, um uso imoderado e uma agressão contra terceiros.

É difícil dizer se tais excessos seriam puníveis na esfera penal, visto que tanto o delito de invasão de dispositivo informático quanto o crime de exercício arbitrário das próprias razões não preveem a modalidade culposa. Assim, para que houvesse a sanção penal nesses casos, o excesso deveria ser doloso, além de a conduta dever amoldar-se a todos os demais elementos previstos no art. 154-A, caput, do Código Penal.

2.6 JURISPRUDÊNCIA BRASILEIRA ACERCA DO TEMA

Em consulta aos sítios eletrônicos do Supremo Tribunal Federal, do Superior Tribunal de Justiça, dos cinco Tribunais Regionais Federais e dos vinte e sete Tribunais de Justiça, não foi encontrada nenhuma decisão acerca do tema desenvolvido.

As decisões, em sua maioria, são referentes a habeas corpus ou a conflito de competência. Não tratam, em nenhum caso, sobre a possibilidade de legítima defesa contra o crime de invasão de dispositivo informático.

Trata-se de uma discussão incipiente no Direito Penal e que ainda não teve a oportunida-

de de chegar aos tribunais.

3 CONCLUSÃO

Os efeitos de reconhecer ou não o ethical hacking como hipótese de legítima podem ser representados por dois extremos, respectivamente: um caminho para a devida proteção das informações ou uma trilha para um caótico cenário no melhor estilo “velho oeste”.

Na visão otimista, o ethical hacking, aqui considerado como meio de legítima defesa, representaria uma opção para a contenção dos efeitos das práticas criminosas em meio eletrônico, visto a redução dos danos sofridos pelas invasões ser seu principal objetivo.

Apesar de existirem outros recursos jurídicos capazes de punir o invasor, estes se mostram lentos devido à instantaneidade dos ataques eletrônicos, sendo uma resposta imediata no momento da invasão mais adequada para a devida proteção das informações. Lembrando, novamente, que uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet.

No contexto pessimista, o ethical hacking, aqui não considerado em nenhuma hipótese meio de legítima defesa, encorajaria a prática do vigilantismo em vez do uso de recursos jurídicos, criando-se, assim, um cenário de faroeste. As empresas contratariam outras que prestassem serviços de segurança de informação, fazendo estas o papel de verdadeiros pistoleiros.

Tais empresas praticariam o ethical hacking sem limites, pois o Poder Judiciário e a legislação penal apresentar-se-iam lentos, incapazes de solucionar plenamente os problemas advindos das invasões. O ethical hacking, longe dos parâmetros estabelecidos pela legítima defesa, seria, portanto, a medida mais eficaz para a contenção desses delitos. Sistemas invadidos e controlados remotamente por um sistema principal capaz de executar ações por meio daqueles poderiam ser considerados alvos, pois não haveria limites para o contra-ataque. As ferramentas de ethical hacking continuariam a se desenvolver e seriam utilizadas secretamente até que medidas legais e judiciais fossem implementadas. Com a ausência de fiscalização na realização do ethical hacking e o desenfreado número de ataques e contra-ataques, a integridade da internet restar-se-ia prejudicada.

É certo que alguns casos chegariam ao Poder Judiciário, mas seria uma quantidade mínima. Em outros, a própria vítima contrataria uma empresa de segurança capaz de rastrear o invasor e buscar fazer justiça com as próprias mãos, passando, agora, à verdadeira condição de criminosa, podendo sua conduta ser tipificada, a depender do caso, no crime de exercício arbitrária das próprias razões ou no próprio crime de invasão de dispositivo informático, agindo, assim, em concurso de agentes. Outra implicação desse péssimo cenário seria a proliferação de seguros contra invasões eletrônicas.

Diante do exposto, qual seria a solução mais adequada para a sociedade brasileira? Os futuros cenários de uso do ethical hacking variam da paz ao caos. Este trabalho posiciona-se no sentido de se construir uma postura ofensiva. Não se fará nenhuma propositura de inovação legislativa, pois se entende que o conceito de legítima defesa delineado no Código Penal Brasileiro, em seu art. 25, é preciso e suficiente para constatar o uso regular do ethical hacking. Sendo hipótese de legítima defesa, a indústria iria desenvolver aplicativos capazes de interromper tais ataques, chegando-se, talvez, ao ponto de os usuários domésticos serem capazes de evitar tais invasões. Verifica-se, por fim, que os obstáculos mais difíceis de serem transpostos e que envolvem diretamente o tema são aqueles de cunho social, em especial, a responsabilidade legal do invasor e daquele que age em excesso de legítima defesa.

ETHICAL HACKING AND ELECTRONIC SELF-DEFENSE

ABSTRACT. Research on the possibility of

setting up electronic self-defense in the face of Computer Security Incident Response Teams' action against a computing device invasion in the qualified form under Article 154-A, §§ 3º and 4º, of the Brazilian Criminal Code. Debates about the practice of ethical hacking and if such conduct would conform to the legal definition of self-defense. Uses deductive method and the doctrinal, legislative and judicial researches. Uses the internet as a way to complement the studied subjects. Hopes to demonstrate that the ethical hacking can configure hypothesis of electronic self-defense, since obeyed the imposed restrictions, and being the most adequate way to reduce the damage caused by the invasion, because the invader can quickly and easily generate multiple copies of the archives and spread them over the internet once in possession of the information, causing a damage difficult to repair.

Keywords: Self-defense. Electronic crimes. Computing device invasion.

REFERÊNCIAS

BRASIL. Decreto-Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 25 julho 2017.

_____. Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei n. 9.296, de 24 de julho de 1996, o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei n. 10.446, de 8 de maio de 2002, e a Lei n. 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e da outras providencias. Disponível em: <http://www.oab.org.br/pdf/substitutivoazeredo.pdf>. Acesso em: 25 julho 2017.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte Geral, vol. 1. 14. ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011 – São Paulo : Saraiva, 2012, epub.

CASTELLS, Manuel. A Sociedade em Rede. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. Brasil, 2016. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 24 setembro 2017.

CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO. Estatísticas de incidentes de rede no governo – 2° trimestre/2017. Brasil, 2017. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_2Trimestre_2017.pdf>. Acesso em: 24 setembro 2017.

_____. Estatísticas de incidentes de rede no governo – 1° trimestre/2017. Brasil, 2017. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_1Trimestre_2017.pdf>. Acesso em: 24 setembro 2017.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. – São Paulo : Saraiva, 2011.

DENNING, Dorothy E. The Ethics of Cyber Conflict. In: HIMMA, Kenneth Einar; TAVANI, Herman T. The Handbook of Information and Computer Ethics. Hoboken, New Jersey : Wiley, 2008. p. 407-428. Disponível em: <http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handbook_of_Information_and_Computer_Ethics.pdf>. Acesso em: 24 setembro 2017.

FIORETTI, Julio. Legítima Defesa: Estudo de Criminologia. Traduzido por Fernando Bragança. – Belo Horizonte : Líder, 2002.

GRECO, Rogério. Curso de Direito Penal (parte geral). 17 ed. Rio de Janeiro : Impetus, 2015.

JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: IEEE 2002 International Symposium on Technology and Society (ISTAS'02): Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 24 setembro 2017.

KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: Harvard Journal of Law & Technology, Cambridge, Massachusetts, vol. 25, nº 2, Spring 2012. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 24 setembro 2017.

KNIGHT, William. License to hack? - Ethical hacking. In-

fosecurity, 16 OCT 2009. Disponível em: <http://www.info-security-magazine.com/view/4611/license-to-hack-ethical--hacking/>. Acesso em: 24 setembro 2017.

MONTEIRO NETO, João Araújo. Crimes Informáticos: uma abordagem dinâmica ao direito penal informático. Pensar (UNIFOR), v. 8, p. 39-54, 2003. Disponível em: <http://hp.unifor.br/pdfs_notitia/1690.pdf>. Acesso em: 24 setembro 2017.

PEIXOTO, Mário César Pintaudi. Criando um CSIRT: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008, p. 2.

PINHEIRO, Patrícia Peck. Direito Digital. 3ª ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 – São Paulo : Saraiva, 2013, epub.

PRADO, Luiz Régis. Curso de direito penal brasileiro, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1.

RODRIGUES, Arlindo Peixoto Gomes. A legítima defesa como causa excludente da responsabilidade civil. – São Paulo : Ícone, 2008.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. Manual de Direito Penal Brasileiro: parte geral. 10ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2013.

O Autor é pós-graduando em Ciências Criminais pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Graduado em Direito pela Universidade Federal do Ceará (UFC). Ex-bolsista de extensão do Núcleo de Estudos em Ciências Criminais da Faculdade de Direito da UFC. Ex-estagiário da Defensoria Pública do Estado do Ceará, da Procuradoria da União, do Ministério Público junto ao Tribunal de Contas dos Municípios do Estado do Ceará e da Justiça Federal. Atualmente, é advogado em Fortaleza/CE. E pode ser contactado por intermédio do email isaacrrneto@gmail.com

DESCARTE SEGURO DE MÍDIAS DE ARMAZENAMENTO: COMO PRESERVAR SUA PRIVACIDADE E ECONOMIZAR RECURSOS

Raphael Leonardo Bernardo de Souza
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: Este trabalho está inserido na área de estudo da gestão, na linha de pesquisa da manutenção dos materiais de comunicações e eletrônica. Tem por principal objetivo analisar os procedimentos utilizados no 4° Batalhão de Comunicações (4°BCom), bem como propor melhorias no processo do descarte seguro das mídias informáticas que armazenam informações corporativas. Embora haja orientação para utilização de software que elimine os dados definitivamente, falta indicação de aplicativo padrão para esta finalidade. Assim, este estudo analisa as opções, na busca por um programa confiável para sanitização dessas mídias, considerada a possibilidade de reutilização das mesmas. Para isso, realiza uma pesquisa exploratória, que aborda os tipos de dispositivos de armazenamento, o funcionamento do sistema de arquivos e a sanitização das mídias informáticas. Em seguida, por meio de um questionário, coleta informações sobre os processos executados no 4°BCom. Por fim, realiza experimentos no sistema operacional Linux para exclusão de arquivos de texto em dispositivos magnéticos e eletrônicos. Então, aponta a ferramenta Shred como a mais adequada em comparação a BleachBit e Wipe. Além disso, verifica que os procedimentos executados no 4°BCom garantem o descarte seguro dos materiais que armazenam informações corporativas. Conclui-se que este trabalho contribui para a gestão da informação, ao disponibilizar um método para a efetiva eliminação de documentos, e para a gestão do material, ao possibilitar a reutilização dos dispositivos de armazenamento.

Palavra-Chave: Gestão da informação. Gestão do material. Informações corporativas. Descarte de mídias informáticas. Sobrescrita de dados.

1 INTRODUÇÃO

A gestão está no centro do funcionamento das instituições, pois atua em áreas fundamentais para o alcance dos objetivos organizacionais, como a gestão do material e da informação, que influenciam diretamente na disponibilidade e na racionalização de recursos.

Essas áreas estão intrinsecamente associadas ao tratar-se dos materiais de informática, cuja utilização aumentou a partir da década de 1980, o que ocasionou a gradativa migração dos documentos para o formato digital.

Nesse panorama, os meios tecnológicos destacaram-se ao possibilitarem o armazenamento de grandes volumes de informações em suporte digital e a recuperação ágil de conteúdos. (SILVA, 2015).

Contudo, o uso crescente de documentos digitais requer uma atenção especial ao descarte das mídias de armazenamento, para não comprometer a confidencialidade das informações sigilosas.

A cartilha emergencial de segurança de tecnologia da informação e comunicações do Exército Brasileiro instrui que os discos rígidos sejam formatados com software que elimine os dados definitivamente, mas não indica um aplicativo padrão para essa finalidade. Dessa lacuna na padronização dos procedimentos, surge a necessidade de apontar um utilitário confiável, razão que justifica este estudo.

Este trabalho trata sobre o descarte seguro dos materiais que armazenam informações corporativas, com foco nas ferramentas de limpeza definitiva de seus conteúdos.

O ambiente de referência para este trabalho foi o 4° Batalhão de Comunicações (4°BCom) e o estudo limita-se ao sistema

operacional Linux Ubuntu, homologado para uso nas estações de trabalho do Exército Brasileiro. Limita-se ainda à sanitização de mídias magnéticas e eletrônicas, por meio dos aplicativos BleachBit, Shred e Wipe para excluir arquivos de texto .odt.

Assim, formulou-se o problema: as ferramentas de limpeza de conteúdo utilizadas no 4°BCom garantem o descarte seguro dos materiais que armazenam informações corporativas?

Com suas análises, este trabalho contribui para o aprimoramento dos procedimentos empregados pelo 4°BCom no descarte seguro das mídias de armazenamento. Pode servir de estudo para a elaboração de normas de ação para eliminação de dados armazenados em mídias informáticas, no Exército Brasileiro. Pode ainda conscientizar os usuários quanto à segurança das informações particulares.

Este trabalho tem como objetivo geral analisar os procedimentos utilizados no 4°BCom e propor melhorias no descarte seguro das mídias que armazenam informações.

Os objetivos específicos são:

Identificar os tipos de mídias que armazenam informações.

Descrever três ferramentas gratuitas e seus métodos de limpeza de conteúdo de mídias informáticas.

Apontar as vantagens e desvantagens metodológicas dos aplicativos avaliados, demonstrar sua confiabilidade e indicar o mais seguro.

1.1 PROCEDIMENTOS METODOLÓGICOS

Trata-se de pesquisa exploratória, com objetivo de descrever os tipos de mídias de armazenamento de informação e as ferramentas apropriadas para a limpeza de seu conteúdo, indicando o procedimento mais seguro, considerando a possibilidade de reutilização do equipamento.

A revisão da literatura possibilitou o embasamento teórico necessário para responder as questões de estudo, abordando os tipos de dispositivos de armazenamento, o funcionamento do sistema de arquivos e a sanitização das mídias informáticas.

Em seguida, foi elaborado um questionário, que foi aplicado à Seção de Informática do 4°BCom, a fim de colher informações concretas a respeito dos processos executados naquela Organização Militar (OM).

A partir dessa base, seguiram-se os experimentos de laboratório, nos quais utilizou-se uma máquina virtual Linux Ubuntu 16.04 LTS, com 10 *Gigabytes* de disco rígido, 1 *Gigabyte* de memória RAM e processador Intel Core i3 64 bits. Os dispositivos de armazenamento utilizados foram um HD externo de 500GB e um pendrive de 4GB de capacidade, ambos com o sistema de arquivos Ext4. O tipo de arquivo utilizado nos testes foi o .odt, por ser o formato padrão para documentos criados no LibreOffice Writer, ferramenta de processamento de texto do Linux.

A pesquisa foi realizada entre os meses de fevereiro e junho de 2017, possibilitando a comparação de diferentes ferramentas de limpeza de conteúdo e a verificação de sua confiabilidade, na busca por resultados práticos para o descarte seguro de mídias informáticas no 4°BCom.

2 DESENVOLVIMENTO

2.1 DISPOSITIVOS DE ARMAZENAMENTO

A utilização dos materiais informáticos no armazenamento da informação, em substituição ao papel, trouxe vantagens como diminuição do espaço físico e agilidade na recuperação da informação.

Silva (2015) comunica que o registro da informação em suporte digital é realizado em diversos tipos de dispositivos, que são classificados em magnéticos, ópticos e eletrônicos.

2.1.1 Armazenamento magnético

Sobre os meios magnéticos, representados pelas fitas magnéticas, disquetes e discos rígidos, Marçula e Benini Filho explicam que:

> Os dados são armazenados magnetizando-se determinados pontos do material magnético, permitindo que os dados sejam mantidos mesmo quando o campo magnético de gravação for retirado. Com isso, a leitura posterior dos dados pode ser realizada detectando-se as correntes induzidas pelos campos magnéticos armazenados. (2008, p. 123).

2.1.2 Armazenamento óptico

Quanto ao armazenamento óptico, onde estão incluídos os CDs, DVDs e discos Blu-ray, para a gravação e leitura dos dados, são necessários drives que utilizam o raio laser, conforme destaca Englander:

> Os dados são armazenados no disco na forma de reentrâncias (lands) e saliências (pits) em sequência. Essas são gravadas na superfície do disco máster (mestre) com um laser de alta potência. [...] Um feixe laser é refletido para fora da superfície em relevo do disco à medida que este é girado por um motor. O reflexo é utilizado para diferenciar reentrâncias e saliências, e estas são convertidas em bits. (2011, p. 257 e 258).

2.1.3 Armazenamento eletrônico

Acerca dessa tecnologia, que inclui os cartões de memória, *pendrives* e SSDs, Marçula e Benini Filho (2008) destacam suas características de não volatilidade, possibilidade de gravar ou apagar dados por meio de sinais elétricos, baixo consumo de energia e pouco espaço físico ocupado.

2.2 SISTEMAS DE ARQUIVOS OU FILESYSTEMS

De acordo com Englander (2011), um arquivo constitui uma unidade lógica de armazenamento e pode ser definido como uma coleção organizada de informações.

Ainda segundo Englander (2011), o gerenciamento de arquivos é realizado pelo sistema de arquivos, que os identifica e manipula pelos nomes, determina seus requisitos físicos, aloca espaço para armazená-los e mantém informações sobre eles, possibilitando sua recuperação.

Para complementar o entendimento, Mota Filho explica:

> Os *filesystems* possuem duas porções básicas: a área de controle e a área de dados. É na área de controle que encontraremos as informações sobre os diversos arquivos espalhados pela partição de disco que contém o *filesystem*. Na área de dados encontraremos o conteúdo dos arquivos. (MOTA FILHO, 2012, p. 153)

É importante destacar que, embora os arquivos sejam armazenados fisicamente nos dispositivos, sua visualização pelo usuário ocorre de forma lógica, conforme o sistema de arquivos, que cria uma estrutura semelhante a uma tabela de conteúdos, localizando os arquivos com facilidade.

Além disso, o *filesystem* mantém uma lista de espaço livre, indicando a disponibilidade para alocação de novos itens, e remaneja o espaço de um arquivo excluído, devolvendo-o à lista de espaço livre.

Mota Filho (2012) informa que os sistemas de arquivos mais conhecidos são FAT16, FAT32 e NTFS para o sistema operacional Windows e Ext2, Ext3, Ext4, ReiserFS, JFS e XFS para o Linux.

2.3 SANITIZAÇÃO DE MÍDIAS DE ARMAZENAMENTO

Ao tratar sobre mídias de armazenamento de informações, é importante abordar a correta eliminação dos documentos digitais, para impossibilitar a recuperação dos dados.

A simples exclusão de um arquivo não

atende aos requisitos de segurança, pois segundo Englander (2011, p. 458):

> "[...] os dados em arquivos excluídos não são de fato apagados do disco, a menos que se faça um esforço especial para limpar ou misturar todos os bits nos blocos utilizados pelo arquivo. Trata-se de um risco potencial à segurança".

Na verdade, a deleção tradicional e a formatação simples alteram apenas a área de controle do sistema de arquivos, devolvendo o espaço liberado para a lista de espaço livre, mas mantendo a área de dados inalterada.

Portanto, devem ser consideradas as possibilidades de recuperação de dados, conforme afirmam Farmer e Venema (2007, p. 131): "uma grande quantidade de informações excluídas podem ser recuperadas [...], mesmo quando essas informações foram excluídas há muito tempo".

Isso constitui ameaça à confidencialidade das informações corporativas, o que remete à busca por formas adequadas de eliminação definitiva dos documentos sigilosos, conforme destaca Beal (2008, p. 7):

> No que tange à confidencialidade, o descarte de documentos e mídias que contenham dados de caráter sigiloso precisa ser realizado com observância de critérios rígidos de destruição segura (por exemplo, [...] softwares destinados a apagar com segurança arquivos de um microcomputador que, se simplesmente excluídos do sistema, poderiam ser facilmente recuperados com o uso de ferramentas de restauração de dados).

Entre as ferramentas que se propõem a recuperar arquivos deletados, Mota Filho (2012) indica Foremost, programa que lê a superfície do disco, independentemente de *filesystem*, para regenerar arquivos através de suas propriedades.

A fim de garantir a eliminação segura de documentos digitais, a National Security Agency (NSA) aprova as seguintes técnicas de sanitização: desmagnetização, desintegração, incineração, fragmentação etc, que resultam na destruição total ou inutilização do próprio dispositivo. De acordo com a NSA (2014, p. 10, tradução nossa), sanitização é definida como "a remoção de informação do dispositivo de armazenamento de tal modo a evitar a recuperação de dados usando qualquer técnica conhecida".

Como o final do ciclo de vida de um documento digital não implica na inoperabilidade da mídia que o contém, é necessário estudar ferramentas que eliminem o conteúdo, sem danificar o dispositivo de armazenamento. Isso possibilita o reaproveitamento dos meios informáticos, como ocorre no Exército Brasileiro, para redistribuição interna ou transferência para outros órgãos governamentais, contribuindo para a racionalização dos recursos públicos e o aparelhamento computacional de outras instituições.

Para remover os dados sem comprometer o dispositivo, pode-se utilizar a técnica de wipe, que consiste na sobrescrita das informações. Segundo Diesburg e Wang (2010, tradução nossa), uma forma de remover os dados confidenciais é sobrescrevê-los.

Os métodos mais famosos utilizados pelos programas de sobrescrita de dados são DoD 5220.22 e Gutmann.

O manual DoD 5220.22-M, publicado em 1995 pelo Departamento de Defesa dos Estados Unidos, indica que, para realizar o descarte seguro, é necessário sobrescrever a informação três vezes. Já o método Gutmann, criado em 1996, consiste em sobrescrever a informação 35 vezes com dados aleatórios, objetivando eliminá-la.

Embora esses métodos sejam bastante referenciados, não existe consenso acerca da quantidade de sobrescritas necessárias para garantir a exclusão segura.

Confirmando essa controvérsia, Diesburg e Wang (2010, tradução nossa) afirmam que quanto mais vezes o dado é sobrescrito, mais segura é sua exclusão. Já Ivascu (2011, tradução nossa) declara que, nos dispositivos

atuais, múltiplas sobrescritas não são mais efetivas que uma única, alertando que a execução de três sobrescritas pode demorar mais de um dia para apagar um disco rígido de grande capacidade.

O Exército Brasileiro, por meio da Portaria n° 011-DCT, de 29 de março de 2010, aprovou o Plano de Migração para Software Livre, estabelecendo a migração de 100% dos sistemas operacionais das estações de trabalho para Linux até 2011.

Para o Linux, Silva (2015) indica o aplicativo gráfico BleachBit, que se propõe a eliminar definitivamente documentos e pastas, além de sobrescrever o espaço livre do disco, utilizando o método de sobrescrita única com zeros.

Outro aplicativo apontado por Silva (2015) é o Shred, utilitário de linha de comando nativo do Linux, que, por padrão, realiza três sobrescritas dos dados, mas permite ao usuário escolher quantas sobrescritas deseja executar.

Outra opção é a ferramenta Wipe, aplicativo de linha de comando, que apaga arquivos, diretórios ou o conteúdo dos dispositivos, sobrescrevendo a área de dados, com dados aleatórios. Por padrão, Wipe realiza 34 sobrescritas, entretanto, opcionalmente executa apenas quatro passagens. (MOTA FILHO, 2012).

2.4 PROCEDIMENTOS REALIZADOS NO 4° B COM

Após aplicação do questionário, respondido pela Seção de Informática do 4°BCom, foram coletadas as seguintes informações sobre as práticas daquela OM:

a) os tipos de mídias utilizadas são HD externo, DVD e pendrive;

b) antes da doação de dispositivos de armazenamento, realiza-se a limpeza dos conteúdos, por meio da ferramenta Shred com cinco sobrescritas;

c) a ausência de dados é verificada através do aplicativo Foremost;

d) no descarte final, além dos procedimentos anteriores, é feita a desmontagem das peças do HD;

e) na redistribuição interna de computadores, é executada a formatação simples do HD;

f) não há divulgação dos procedimentos ao público geral.

2.5 TESTES REALIZADOS

As ferramentas empregadas para a eliminação dos documentos foram BleachBit, Shred e Wipe, que se diferenciam pelos métodos de sobrescrita (única e múltiplas) e formas de funcionamento (gráfico e linha de comando).

Para finalizar os testes e verificar a confiabilidade das técnicas de sanitização executadas, foi utilizado o aplicativo de recuperação de dados Foremost, citado por Mota Filho (2012).

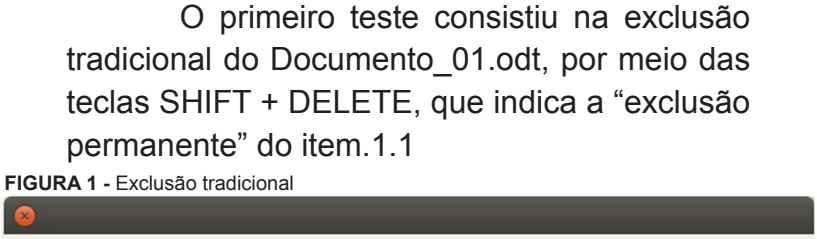
2.5.1 Exclusão de dados em meio magnético

Nos testes em meio magnético foi utilizado um HD externo de 500GB, denominado HD_teste.

Inicialmente foram criados os seguintes arquivos e salvos no HD_teste: Documento_01.odt, Documento_02.odt, Documento_03.odt, Documento_04.odt e Documento_05.odt.

O primeiro teste consistiu na exclusão tradicional do Documento_01.odt, por meio das teclas SHIFT + DELETE, que indica a “exclusão permanente” do item.1.1

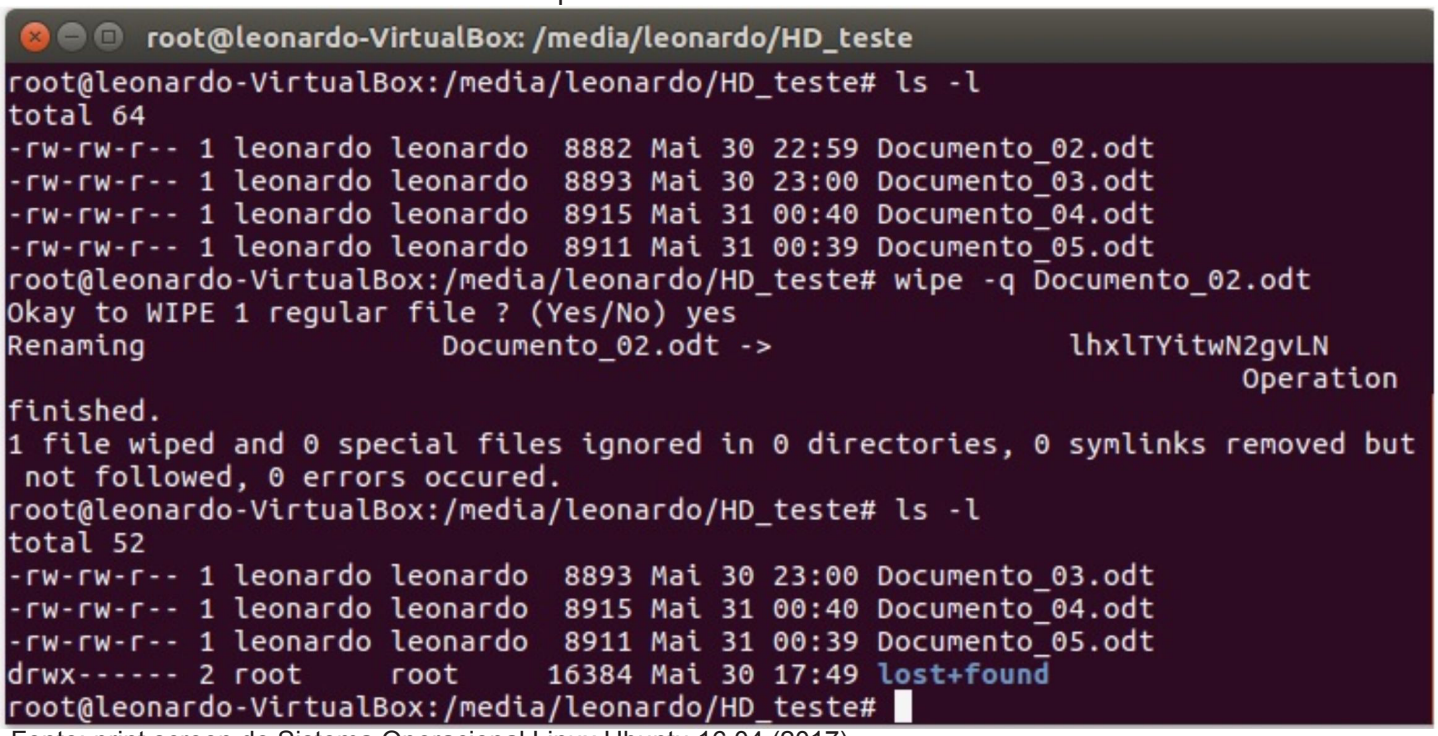
FIGURA 1 - Exclusão tradicional



Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Em seguida, procedeu-se a aplicação da ferramenta Wipe, através do comando wipe -q Documento_02.odt, realizando quatro passagens de sobrescrita do arquivo.

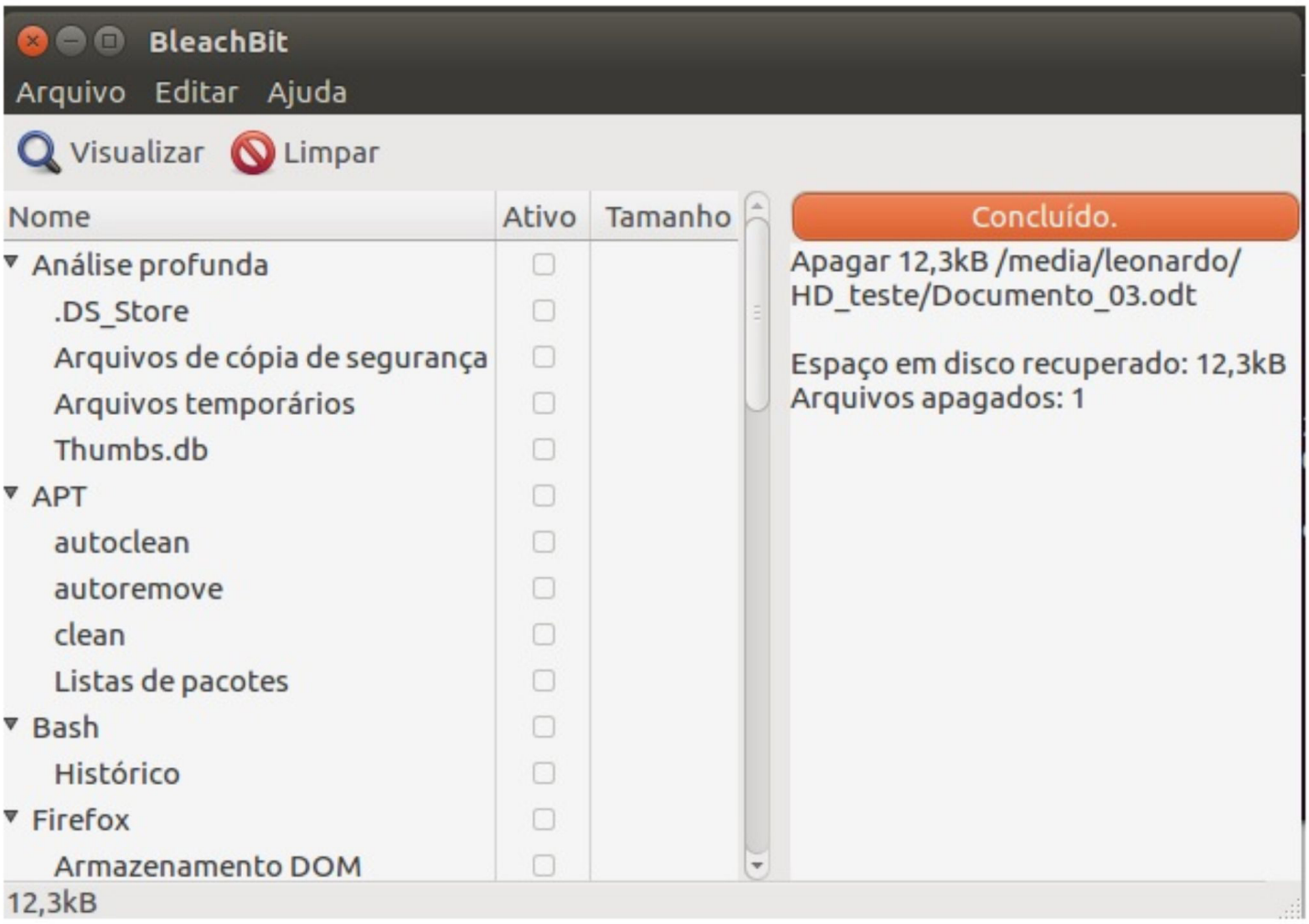
FIGURA 2 - Exclusão documental com Wipe.



Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Logo após, foi utilizado o aplicativo BleachBit para realizar a sobrescrita do Documento_03.odt.

FIGURA 3 - Exclusão documental com BleachBit



Fonte: print screen do aplicativo BleachBit (2017).

No teste seguinte, foi empregado o utilitário Shred, por meio do comando shred -un 1 Documento_04.odt, realizando uma sobrescrita do arquivo.

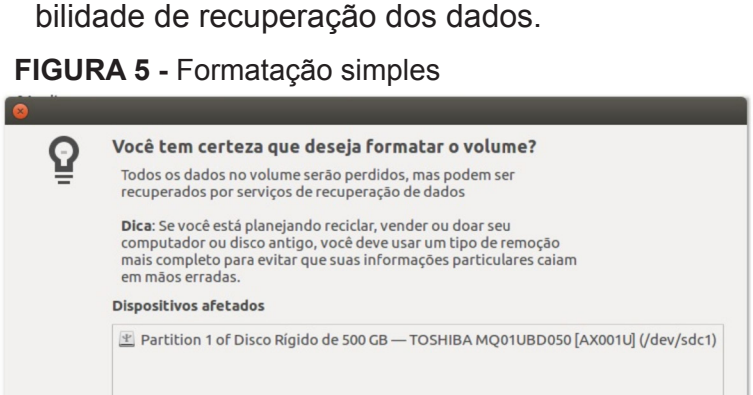
FIGURA 4 - Exclusão documental com Shred

```
root@leonardo-VirtualBox:/media/leonardo/HD_teste# ls -l
total 40
-rw-rw-r-- 1 leonardo leonardo  8915 Mai 31 00:40 Documento_04.odt
-rw-rw-r-- 1 leonardo leonardo  8911 Mai 31 00:39 Documento_05.odt
drwx------ 2 root     root     16384 Mai 31 19:14 lost+found
root@leonardo-VirtualBox:/media/leonardo/HD_teste# shred -un 1 Documento_04.odt
root@leonardo-VirtualBox:/media/leonardo/HD_teste# ls -l
total 28
-rw-rw-r-- 1 leonardo leonardo  8911 Mai 31 00:39 Documento_05.odt
drwx------ 2 root     root     16384 Mai 31 19:14 lost+found
root@leonardo-VirtualBox:/media/leonardo/HD_teste#
```

Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Para a eliminação do Documento_05.odt, foi realizada a formatação simples do HD_teste, opção que adverte o usuário para a possibilidade de recuperação dos dados.

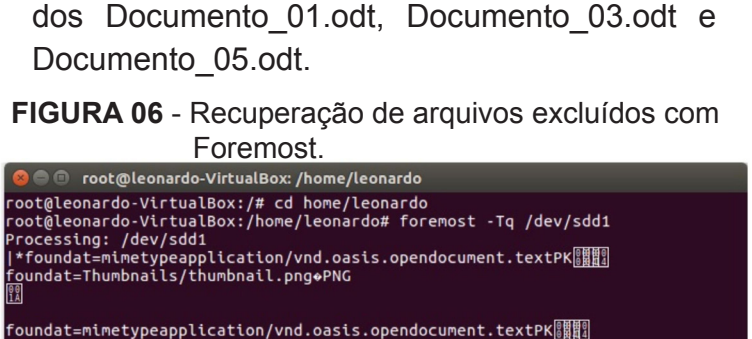
FIGURA 5 - Formatação simples



Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Então, foi executado o aplicativo Foremost, na tentativa de recuperar os arquivos supracitados, sendo verificada a existência dos Documento_01.odt, Documento_03.odt e Documento_05.odt.

FIGURA 06 - Recuperação de arquivos excluídos com Foremost.

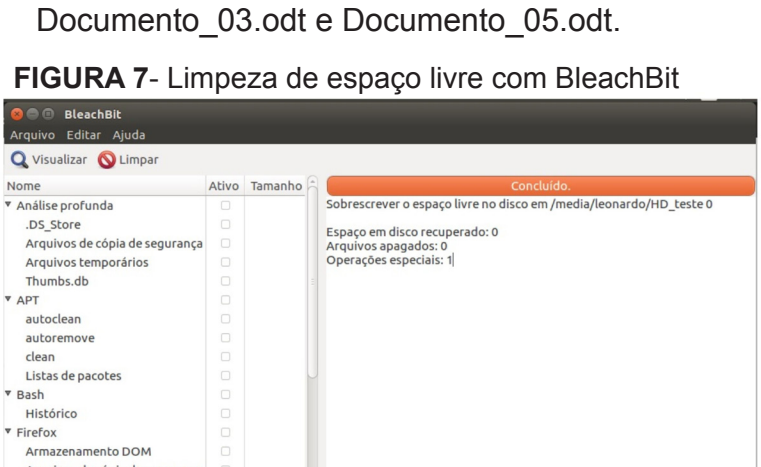


Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Como foi constatada a permanência de arquivos no dispositivo, procedeu-se a sobrescrita do espaço livre, realizando-se três experimentos isolados e nas mesmas condições de execução.

No primeiro teste, foi empregado o BleachBit, que demorou seis horas para concluir o procedimento. Então, utilizou-se o Foremost e verificou-se a possibilidade de regeneração dos Documento_03.odt e Documento_05.odt.

FIGURA 7- Limpeza de espaço livre com BleachBit



Fonte: print screen do aplicativo BleachBit (2017).

Em seguida, realizou-se a sobrescrita do HD_teste, por meio do Wipe, com quatro passagens, o que levou mais de 62 horas para ser concluído, seguido de uma busca com Foremost, que não encontrou nenhum dado.

Finalizando, executou-se o aplicativo Shred para sobrescrever uma única vez o HD_teste, levando cerca de 14 horas para conclusão. Enfim, com o Foremost, verificou-se a inexistência de dados.

2.5.2 Exclusão de dados em meio eletrônico

Nos testes em meio eletrônico utilizou-

-se um Pendrive de 4GB, denominado Pendrive_teste.

Inicialmente foram criados os seguintes arquivos e salvos no Pendrive_teste: Documento_06.odt, Documento_07.odt, Documentoe_08.odt, Documentoe_09.odt e Documentoe_10.odt.

No primeiro experimento, realizou-se a exclusão tradicional do Documento_06.odt, por meio das teclas SHIFT + DELETE, que indica a "exclusão permanente" do item.

Em seguida, aplicou-se o Wipe, através do comando wipe -q Documento_07.odt, no Pendrive_teste, realizando quatro passagens de sobrescrita do arquivo.

Logo após, utilizou-se o BleachBit para executar a sobrescrita do Documento_08.odt.

Na sequência, foi empregado o Shred, por meio do comando shred -un 1 Documento_09.odt, realizando uma sobrescrita do referido arquivo.

Para a eliminação do Documento_09.odt, foi realizada a formatação simples do Pendrive_teste. No entanto, essa opção alerta para a possibilidade de recuperação dos dados.

Da mesma forma que o experimento no HD_teste, a execução do aplicativo Foremost, na tentativa de recuperar os arquivos apagados, constatou a existência de três arquivos, sendo os Documento_06.odt, Documento_08.odt e Documento_10.odt.

Em consequência da permanência desses dados no dispositivo, procedeu-se a sobrescrita do espaço livre, realizando-se três experimentos isolados e nas mesmas condições de execução.

No primeiro teste, foi empregado o BleachBit, que levou cerca de 12 minutos para concluir o procedimento. Então, utilizou-se o Foremost e verificou-se a impossibilidade de restauração dos arquivos.

Em seguida, utilizou-se o Wipe para sobrescrever quatro vezes o Pendrive_teste, demorando 1 hora e 15 minutos para conclusão. Logo após, foi procedida uma busca com Foremost, constatando-se a inexistência de dados.

No terceiro teste, executou-se o Shred para sobrescrever uma única vez o Pendrive_teste, levando 22 minutos para ser concluído. Enfim, por meio do Foremost, verificou-se a inexistência de dados.

2.6 ANÁLISE DOS RESULTADOS E COMPARAÇÃO DAS FERRAMENTAS

Após todos os testes, observou-se que os resultados foram muito semelhantes, conforme descrito a seguir:

QUADRO 01 - Resultados dos testes de exclusão de arquivos

Dispositivo de armazenamento	Arquivo escluído	Forma de exclusão	Recuperado com Foremost	Integridade do conteúdo recuperado
HD_Teste	Documento_01.odt	Deleção tradicional	Sim	100%
HD_Teste	Documento_02.odt	Wipe	Não	-
HD_Teste	Documento_03.odt	BleachBit	Sim	100%
HD_Teste	Documento_04.odt	Shred	Não	-
HD_Teste	Documento_05.odt	Formatação Simples	Sim	100%
Pendrive_teste	Documento_06.odt	Deleção tradicional	Sim	100%
Pendrive_teste	Documento_07.odt	Wipe	Não	-
Pendrive_teste	Documento_08.odt	BleachBit	Sim	100%
Pendrive_teste	Documento_09.odt	Shred	Não	-
Pendrive_teste	Documento_10.odt	Formatação Simples	Sim	100%

Fonte: Elaborado pelo autor (2017).

a) os arquivos Documento_01.odt e Documento_05.odt, respectivamente apagados pela deleção tradicional e formatação simples do HD_teste, bem como os Documento_06.odt e Documento_10.odt, apagados pela deleção tradicional e formatação simples do Pendrive_teste, foram totalmente recuperados, confirmando a teoria da preservação da área de dados;

b) o aplicativo Foremost não foi capaz de encontrar os Documento_02.odt e Documento_07.odt, concomitantemente eliminados do HD_teste e do Pendrive_teste, pela ferramenta Wipe, o que comprova a eficiência desta na exclusão definitiva de documentos;

c) os arquivos Documento_03.odt e Documento_08.odt, eliminados respectivamente do HD_teste e do Pendrive_teste, através do BleachBit, foram plenamente restaurados, evidenciando que este utilitário não cumpre a proposta de eliminação definitiva de arquivos;

d) o Foremost não encontrou qualquer vestígio dos Documento_04.odt e Documento_09.odt, respectivamente apagados do HD_teste e do Pendrive_teste, com a utilização do Shred, comprovando a confiabilidade dessa ferramenta na exclusão definitiva de documentos;

- A fim de eliminar os três arquivos ainda remanescentes em cada dispositivo, realizou-se a limpeza de espaço livre dessas mídias. Os resultados são expostos abaixo:

QUADRO 2 - Resultados dos testes de limpeza de espaço livre

Ferramenta utilizada	Método de sanitização	Tempo de limpeza do HD_teste	Nº de arquivos eliminados no HD_teste	Tempo de limpeza do Pendrive_teste	Nº de arquivos eliminados no Pendrive_teste
BleachBit	Sobrescrita única com zeros	6 h	01	12 min	03
Wipe	quatro sobrescritas com dados aleatórios	62 h	03	1h 15min	03
Shred	Sobrescrita única com dados aleatórios	14 h	03	22 min	03

Fonte: Elaborado pelo autor (2017).

e) a limpeza realizada pelo BleachBit foi eficaz no Pendrive_teste, eliminando definitivamente os arquivos remanescentes. No entanto, foi insatisfatória no HD_teste, uma vez que o Foremost encontrou dois daqueles arquivos ainda intactos na mídia magnética (Documento_03.odt e Documento_05.odt). Embora os tempos de execução desse método (6h no HD e 12min no Pendrive) sejam menores que os tempos das demais ferramentas, seus resultados foram comprometedores no HD;

f) no segundo teste, foi executada a sanitização do HD_teste e do Pendrive_teste, pelo Wipe, na opção de quatro sobrescritas, que eliminou completamente os arquivos remanescentes, impossibilitando a recuperação dos dados em ambos os dispositivos;

g) o último teste consistiu na utilização do Shred, na opção de sobrescrita única, para limpeza do HD_teste e do Pendrive_teste, que se mostrou efetivo, pois nenhum dado foi recuperado pelo Foremost.

A análise dos resultados esclarece que

o aplicativo BleachBit não é confiável para a exclusão definitiva de arquivos e limpeza de espaço livre. Já as ferramentas Wipe e Shred foram aprovadas em todos os testes.

Destacam-se também os tempos gastos para realizar a sobrescrita de dispositivos de maior capacidade, como o HD_teste de 500GB. Enquanto Wipe demorou 62h, Shred gastou 14h nesse processo.

3 CONCLUSÃO

O presente trabalho teve por objetivo geral analisar os procedimentos utilizados no 4° B Com e propor melhorias no processo do descarte seguro das mídias informáticas capazes de armazenar informações corporativas.

Assim, verificou-se que os procedimentos executados naquela OM garantem o descarte seguro dos materiais capazes de armazenar informações corporativas, uma vez que utilizam a ferramenta Shred com cinco sobrescritas. No entanto, para aprimorar seus processos e torná-los mais eficientes, passo a listar procedimentos passíveis de melhorias, resultante dos estudos desta pesquisa científica, a saber:

a) alterar a quantidade de sobrescritas de cinco para uma única, pois é suficiente para alcançar o objetivo da sanitização, conforme proposta de Ivascu, comprovada neste trabalho científico;

b) utilizar o aplicativo Shred, o qual os experimentos científicos comprovaram eficiência, para limpeza de HD antes da redistribuição interna de computadores, nos casos em que o destinatário não deva ter acesso a documentos do antigo detentor;

c) divulgar as técnicas de sanitização ao público geral da OM, a fim de contribuir para a conscientização individual relativa à segurança das informações corporativas e particulares do pessoal.

Ficou demonstrado, de forma empírica, como os arquivos apagados de um dispositivo informático por métodos convencionais podem ser facilmente recuperados por programas de recuperação de dados, a exemplo do Foremost. Isso confirmou a necessidade de aplicar um método de exclusão segura.

A análise dos aplicativos selecionados possibilitou a comparação de diferentes métodos, confirmando a declaração de Ivascu (2011) de que múltiplas sobrescritas não são mais efetivas que uma única sobrescrita. Pode-se afirmar também que quanto maiores a capacidade do dispositivo a ser sanitizado e o número de sobrescritas a serem realizadas, maior será o tempo gasto no processo.

Dentre as ferramentas testadas, o Shred apresentou-se como a mais eficiente, por atingir o mesmo grau de segurança na eliminação definitiva dos documentos, com menos sobrescritas de dados e, consequentemente, menor tempo de execução.

Além de contribuir para a melhoria do processo de sanitização das mídias do 4° B Com, este estudo poderá contribuir para a formulação de procedimentos de sanitização citados nas Normas Gerais de Ação (NGA) de cada OM segundo suas peculiaridades.

Pode contribuir também para a conscientização dos usuários, alertando-os para as formas de eliminação segura das informações particulares, evitando exposições desnecessárias.

Como sugestão para trabalhos futuros, apontam-se a análise de outros aplicativos de eliminação segura de dados, como DBAN, secure-delete e os comandos dd e dcfldd, além de testes com outros tipos de arquivos, como imagem, áudio e vídeo.

Enfim, esse trabalho contribui para duas áreas importantes da gestão: a gestão da informação e a gestão do material.

Na primeira, ao disponibilizar um método para a efetiva eliminação de documentos,

evitam-se problemas oriundos da divulgação indevida de informações sigilosas ou informações pessoais.

Na segunda, ao eliminar o conteúdo sem danificar os dispositivos de armazenamento, possibilita-se a reutilização dos mesmos, o que aumenta a disponibilidade e racionalização de recursos.

SAFE DISPOSAL OF STORAGE MEDIA: HOW TO PRESERVE YOUR PRIVACY AND SAVE RESOURCES

ABSTRACT: This work is inserted in the area of study of the management, in the line of research of communication and electronic equipment maintenance. Its main goal is to analyze the procedures used in 4th Signal Battalion (4thBCom), as well as to propose improvements in the safe disposal process of computer media that stores corporate information. Although there is guidance for using software that permanently deletes data, there isn't indication of a standard application for this purpose. Thus, this study analyzes the options, in order to find a reliable program for the sanitization of these media, considering the possibility of reusing them. To do this, it performs an exploratory research, which addresses the types of storage devices, the operation of the file system and the sanitization of computer media. Then, through a questionnaire, it collects information about the processes performed in 4thBCom. Finally, it performs experiments in the Linux operating system to exclude text files on magnetic and electronic devices. So it points to Shred tool as the most appropriate in comparison to BleachBit and Wipe. In addition, it verifies that the procedures performed in the 4thBCom guarantee the safe disposal of materials that store corporate information. It's concluded that this work contributes to the information management - providing a method for the effective elimination of documents, and to the material management - by enabling reuse of storage devices.

Keywords: Information management. Material management. Corporate Information. Disposal of Computer media. Overwriting data.

REFERÊNCIAS

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BRASIL. Portaria nº 011-DCT, de 29 de março de 2010. Aprova o plano de migração para Software Livre no Exército Brasileiro, versão 2010. **Boletim do Exército**, Brasília, DF, Separata ao Boletim do Exército nº17, 30 de abril de 2010.

BRASIL. Portaria nº 720, de 21 de novembro de 2011. Aprova a cartilha emergencial de segurança de tecnologia da informação e comunicações. **Boletim do Exército**, Brasília, DF, Separata ao Boletim do Exército nº47, 25 de novembro de 2011.

DIESBURG, S. M; WANG, A. A. **A survey of confidential data storage and deletion methods**. ACM Computing Surveys, Vol. 43, n. 1, Article 2, 2010.

ENGLANDER, Irv; tradução e revisão técnica TANAKA, Edson. **A Arquitetura de Hardware Computacional, Software de Sistema e Comunicação em Rede**: Uma Abordagem da Tecnologia da Informação. Rio de Janeiro: LTC, 2011.

FARMER, D.; VENEMA, W. **Perícia Forense Computacional**: Teoria aplicada à prática. São Paulo: Pearson Prentice Hall, 2007.

IVASCU, Mihaita. **Data Erasure on Magnetic Storage**. International Conference of Scientific Paper. Brasov: AFASES, 2011.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. **Informática:** Conceitos e Aplicações. São Paulo: Érica, 2008.

MOTA FILHO, João Eriberto. **Descobrindo o Linux:** entenda o sistema operacional GNU/Linux. São Paulo: Novatec, 2012.

NATIONAL SECURITY AGENCY. **NSA/CSS Storage Device Sanitization Manual**. Disponível em: <https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf>. Acesso em 25 abr. 2017, 20:12:32.

SILVA, Silvio Lucas. **O descarte seguro de documentos arquivísticos em suporte digital**. Paraíba: UFPB, 2015. Disponível em: <http://tede.biblioteca.ufpb.br-/bitstream/tede/4968/2/arquivototal.pdf>. Acesso em: 18 fev. 2017, 15:48:24.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). 1° Tenente do Serviço de Intendência do Exército Brasileiro. É pós-graduado pela Escola de Comunicações, *Lato Sensu*, de Especialização em Comunicações. Atualmente, exerce a função de Chefe da Seção de Planejamento e Gestão do 4° Batlahão de Comunicações e pode ser contactado pelo email rapha.leo08@gmail.com.

A IMPORTÂNCIA DE UM PROGRAMA DE CONSCIENTIZAÇÃO NO ÂMBITO DO EXÉRCITO BRASILEIRO

Felipe Pereira Cyrino
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: Diante do cenário tecnológico moderno, no qual há um processo contínuo de inovação e integração de novos conceitos e capacidades, se percebe o que a informação se tornou o maior patrimônio da sociedade. O valor da informação no contexto moderno é tão grande, que ela se faz vital para qualquer instituição que se queira manter viva e competitiva. De tal maneira percebe-se que as instituições possuem um alto grau de dependência da informação. Essa dependência nos faz perceber que a Segurança da Informação é um pré requisito para qualquer instituição, inclusive para o Exército Brasileiro. Em contrapartida observa-se, no contexto atual, que a Engenharia Social é um dos fatores que mais comprometem não só a Segurança da Informação, mas também a segurança organizacional. A engenharia Social trata-se de uma técnica de intrusão que explora as fraquezas do ser humano, fazendo ou não o uso de tecnologias para a obtenção da informação. O presente estudo trata-se de uma revisão bibliográfica e documental que tem o objetivo geral verificar e compreender a Engenharia Social e destacar a importância de conscientização do tema no âmbito do Exército onde serão abordadas técnicas utilizadas pela Engenharia Social e medidas para combatê-la. Nesse contexto será observado, como resultado do estudo, a importância de um programa de conscientização para combater a Engenharia Social.

Palavras-Chave: Informação. Engenharia Social. Segurança da Informação.

1 INTRODUÇÃO

O presente estudo está inserido no campo da cibernética. De acordo com Morais (2006), cibernética pode ser definida como a “ciência da comunicação e do controle, seja do animal (homens, seres vivos), seja da máquina”.

Fazendo uma imersão no campo da cibernética, o presente trabalho tem como objetivo explorar o campo da engenharia social. O tema visou apontar a importância da conscientização e do treinamento para combater os ataques dos engenheiros sociais.

Atualmente o mundo é fortemente articulado por redes, devido aos grandes benefícios que são oferecidos pela alta tecnologia que está em constante desenvolvimento.

Nesse contexto, é possível perceber o valor que a informação adquiriu nos dias atuais; sendo ela de vital importância a qualquer instituição. Por esse motivo, a informação passou a merecer uma gestão mais específica que, entre outras coisas, contemplasse a garantia da segurança da informação.

Com relação à segurança da informação, se pode dizer que as instituições têm ciência e adquirem tecnologias de última geração para manterem a Informação segura. As intuições, ao investirem nessas tecnologias para segurança da informação, acabam esquecendo-se de um fator tão importante quanto à tecnologia, que é o fator humano.

O fator humano destaca-se como um importante elo para que exista a segurança da informação, já que é fato que grande parte dos vazamentos de informações das instituições ocorre por técnicas que conhecemos por Engenharia Social. (PEIXOTO, 2006)

Pode-se definir engenharia social como o conjunto de práticas que são utilizadas para a obtenção de informações valiosas e sigilosas das instituições por meio da vulnerabilidade humana, geralmente se utiliza da falta de conhecimento dos indivíduos ou do excesso de segurança dos mesmos.

A partir destes assuntos foi levantado o

seguinte questionamento com base no estudo dos conceitos de segurança da informação e engenharia social: Qual a importância da conscientização e do uso de medidas de defesa contra a engenharia social?

Assim sendo, o presente estudo apresenta ao efetivo do Exército Brasileiro embasamento teórico para entenderem como a engenharia social ataca e quais são os principais métodos utilizados pela mesma. O trabalho apresenta também as principais medidas de proteção da informação que podem ser utilizadas, a fim de que os militares possuam alguns artifícios para identificarem um ataque da engenharia social e tenham embasamento para se defenderem.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O presente estudo pretende integrar os conceitos básicos e a informação científica relevante e atualizada, a fim de fornecer subsídios suficientes para analisar, verificar e compreender a engenharia social e destacar a importância de conscientização do tema no âmbito do Exército.

1.1.2 Objetivos Específicos

A fim de viabilizar a consecução do objetivo geral de estudo, foram formulados objetivos específicos, de forma a desencadear logicamente o raciocínio descritivo apresentado neste estudo. Os seguintes objetivos específicos foram elencados:

a. compreender de que maneira o comportamento do homem afetam a proteção da informação;

b. conhecer conceitos e características da segurança da informação;

c. estudar conceitos e características da engenharia social;

d. identificar as principais ferramentas e técnicas utilizadas pela engenharia social;

e. Identificar as principais medidas que podem ser utilizadas para a proteção da informação.

1.2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa é um estudo descritivo e bibliográfico, no qual através da leitura e revisão bibliográfica, responsáveis por fornecer a base teórica do trabalho, os elementos tidos como importantes serão expostos e analisados. Cabe ressaltar também que serão destacados alguns autores visando alcançar os objetivos propostos.

Ao término da revisão, por se tratar de um campo de investigação com produção de conhecimento já estudada antes, foram encontrados várias fontes de pesquisa de qualidade, visto que se trata de documentos importantes e autores renomados.

Amparados nessas fontes, iniciou-se a coleta de dados, baseada em leituras de livros, revistas e endereços eletrônicos. Na realização da pesquisa foi realizado um fichamento, devido ao grande número de informações levantadas, pois é um modo de armazenar essas informações que se faz muito útil quando existe a necessidade de recuperar um dado. Para isso, serão utilizadas fichas-resumo, nas quais vão se apresentar de maneira rápida e concisa as idéias do autor; e fichas de citação, onde serão transcritos fragmentos relevantes ao estudo.

O levantamento e a seleção da bibliografia, a coleta de dados, a análise dos dados, a leitura analítica, e a argumentação compõem o delineamento da pesquisa.

Para a realização da pesquisa bibliográfica, os trabalhos citados abaixo serviram como fonte de busca:

a. livros específicos focados em engenharia social e segurança da informação;

b. revistas;

c. artigos;

d. consulta a endereços eletrônicos es-

pecializadas no assunto.

2 FATOR HUMANO NO MANUSEIO DA INFORMAÇÃO

Em qualquer instituição, onde exista a preocupação com o manuseio e a segurança da informação, sempre existirá um fator que se destaca como um fator de desequilíbrio, o conhecido "fator humano". (MARCELO; PEREIRA, 2005).

De tal forma, é necessário que se reconheça a importância do elemento humano no trato com as informações, levando em consideração que o ser humano é o elo mais fraco da cadeia de segurança. Assim sendo, sobre o ser humano devem recair os principais cuidados durante as fases de especificação, implantação e gestão da segurança da informação. (PINHEIRO, 2008).

Como define Mitnick; Simon :

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003 apud ALVES, 2010, p. 14).

O fator humano está diretamente relacionado a uma grande parte de ataques promovidos contra a informação. A exploração das vulnerabilidades do ser humano é um ponto que deve ser levado em consideração em qualquer política de segurança da informação.

2.1 VULNERABILIDADES DO SER HUMANO

Como já foi dito, o ser humano é o elemento mais vulnerável de qualquer sistema de segurança da informação. São exatamente os traços comportamentais e psicológicos apresentados pelo ser humano que são explorados pela engenharia social.

Dentre essas características tornam o ser humano vulnerável, é possível destacar (JUNIOR, 2006):

- **vontade de ser útil**: Geralmente, o ser humano procura agir com cortesia e busca ajudar os outros quando se faz necessário;
- **busca de novas amizades**: Quando são elogiados, o ser humano costuma sentir-se bem, ficando assim mais vulnerável para fornecer informações;
- **prorrogação da responsabilidade**: Muitas vezes o ser humano considera que ele não é o único responsável por um conjunto de atividades ou responsabilidades;
- **persuasão**: É compreendida como a arte de persuadir pessoas, onde se busca respostas específicas para determinado objetivo; e
- **autoconfiança**: Como próprio nome diz, é o fato que a maioria das pessoas não se consideram ingênuas a ponto de serem enganadas e utilizadas de alguma maneira.

Existem inúmeros outros fatores que ainda podem ser considerados vulnerabilidades do ser humano. Em razão destes fatores, é possível entender que sempre haverá brechas de segurança da informação, uma vez que a manipulação das informações é feita por indivíduos.

3 SEGURANÇA DA INFORMAÇÃO

De acordo com Peixoto (2006, apud ALVES, 2010, p. 17), "O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos,

modificações não autorizadas ou até mesmo sua não disponibilidade".

A segurança da informação é dividida em três pilares ou princípios básicos, que são definidos por Peixoto (2006) da seguinte maneira:

- **confidencialidade**: É a garantia que as informações chegarão ao seu destino sem que se dissipem para outros meios ou lugares onde não deveriam passar;
- **integridade**:É a garantida de que as informações não sofreram nenhuma alteração durante o trajeto entre o remetente e o destinatário; e
- **disponibilidade**: A informação deve estar sempre disponível aos seus usuários no momento em que estes necessitarem. Peixoto (2006) entende que nada adianta ter confidencialidade e integridade se a informação não estiver disponível.

Em resumo, segurança da informação pode ser compreendida como as políticas, procedimentos e medidas técnicas usadas para impedir o acesso não autorizado a um sistema de informação.

3.1 VULNERABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Podemos compreender vulnerabilidade da segurança da informação como uma fragilidade da segurança da informação, ou simplesmente como pontos mais suscetíveis a serem expostos a danos.

Os principais tipos de vulnerabilidades existentes na segurança da informação, de acordo com Peixoto (2006) são classificadas da seguinte forma:

- **físicas**: São constituídas por instalações com estruturas de segurança fora dos padrões mínimos, como exemplo uma sala de CPD mal planejada;
- **naturais**: São as causadas por fenômenos naturais, como tempestades, incêndios, desabamentos, além da falta de energia;
- **hardware**: São os desgastes causados nos equipamentos por obsolescência ou má utilização;
- **software**: São constituídos pela má instalação, pelo vazamento de informações, pela perda de dados ou pela indisponibilidade de recursos;
- **mídias**: Fontes de armazenamento de mídias podem ser perdidas ou danificadas;
- **comunicação**: Constituídos por acessos não autorizados ou pela perda de comunicação; e
- **humanas**: São as vulnerabilidades que se referem ao fator humano que são exploradas pelas técnicas da engenharia social.

Ainda sobre o tema, Peixoto (2006) diz que geralmente as empresas ou instituições não adotam potencial investimento em segurança digital mais especificamente na segurança das informações.

4 ENGENHARIA SOCIAL

Campos (2007) define a engenharia social como de uma técnica utilizada para que se obtenha acesso a informações, onde ,substancialmente, um indivíduo se utiliza de métodos para induzir uma pessoa a quebrar protocolos e procedimentos de segurança.

Nakamura e Geus (2003) definem engenharia social da seguinte forma:

> A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem

> senhas ou outras informações que possam comprometer a segurança da organização. (NAKAMURA,GEUS, 2003, p.70).

Pode-se definir engenharia social como o conjunto de práticas que são utilizadas para a obtenção de informações valiosas e sigilosas das instituições por meio da vulnerabilidade humana, geralmente se utiliza da falta de conhecimento dos indivíduos ou do excesso de segurança dos mesmos.

Mostrando a importância que deve ser dada a engenharia social, Peixoto (2006) afirma que a dentre as vulnerabilidades encontradas na segurança da informação a engenharia social está inserida como um dos desafios (senão o maior) mais complexos e que merecem total atenção.

4.1 FERRAMENTAS UTILIZADAS PELO ENGENHEIRO SOCIAL

O engenheiro social realiza seus ataques fazendo uso de ferramentas comuns presentes no nosso dia a dia e que muitas vezes passam despercebidas por todos.

Dentre as principais ferramentas que são utilizadas pelos engenheiros sociais podemos destacar: (PEIXOTO, 2006)

- **telefone ou Voip**: Se passar por alguém que não é seria um dos típicos ataques de engenharia social;
- **internet**: através de sites que forneçam informações sobre a pessoa (facebook);
- **intranet**: Por exemplo, por acesso remoto, capturando-se o micro de determinado usuário da rede e se passando por alguém que na verdade não é;
- **e-mail** (Fakemail, e-mails falsos, os famosos phishing scan);
- **pessoalmente**: Fazer uso do poder de persuasão, da habilidade de saber conversar;
- **fax**: É necessário obter o número do fax antes para depois iniciar o ataque;
- **cartas/correspondência**: Embora não seja muito utilizado atualmente, esse recurso funciona muito bem com pessoas mais velhas;
- **spyware**: Software “espião” usado para monitorar de modo oculto as atividades do computador de um alvo;
- **mergulho no lixo**: Muitas vezes aquilo que é descartado no lixo de maneira indevida, pode possuir informações que serão usadas pelo engenheiro social contra a vítima; e
- **surfar sobre os ombros**: Nada mais é que observar as pessoas digitando no computador informações como senhas e usuários e assim conseguir roubá-las.

Existem várias ferramentas que podem ser usadas para os ataques dos engenheiros sociais. No uso destas ferramentas o Engenheiro Social se utiliza de algumas técnicas simples, que serão exploradas adiante.

4.2 TÉCNICAS UTILIZADAS PELO ENGENHEIRO SOCIAL

Aliadas ou uso das ferramentas, mostradas anteriormente, os engenheiros sociais se utilizam de técnicas onde procuram explorar a vulnerabilidade humana, sempre possuindo uma resposta ao possível comportamento humano apresentado pela vítima.

De acordo com Peixoto (2006), os engenheiros sociais sempre se utilizam de técnicas clássicas. A seguir serão mostradas algumas dessas técnicas.

4.2.1 Informações Inofensivas x Valiosas

Basicamente funciona como um quebra-cabeça. As informações são obtidas em pedaços e quando juntados resultarão na “figura completa”. Sendo assim informações que em

uma primeira impressão parecem irrelevantes, quando reunidas com outras informações também consideradas irrelevantes, podem dar origem a uma informação de grande valia.

Ainda, concordando com Peixoto (2006), é necessário avaliar todo repasse de informação, levando em consideração quem está solicitando e a real necessidade desta pessoa saber da informação.

4.2.2 Criando Confiança

Essa técnica utilizada pela engenharia social trata-se basicamente de adquirir primeiramente a confiança, reforçar esse vínculo de amizade aumentando ainda mais a confiança, para então começar a atacar e conseguir as informações julgadas necessárias.

De acordo com Peixoto (2006), o engenheiro social se prepara para responder todas as perguntas e indagações que podem acontecer, sem demonstrar nervosismo, sem gaguejar ou sem demonstrar insegurança de forma que a vítima não desconfie de nada.

4.2.3 Simplesmente Pedindo

A referida técnica é considerada a mais simples utilizada para se obter uma informação. Quando existe uma dúvida o natural é perguntar, ou seja, pedir a resposta.

De acordo com Peixoto (2006), para que a técnica tenha sucesso é necessário que o engenheiro social tenha conhecimento da linguagem e da estrutura do ambiente onde pretende fazer o ataque.

Em uma entrevista para a Information Week Brasil, Kevin Mitnick (2003) afirma que as duas características que são mais utilizadas nessa técnica são a autoridade e o medo. A autoridade transmite segurança no momento em que o engenheiro social demonstra que sabe o que está falando, o que faz a vítima se sentir sufocada e fornecer a informação desejada. Isso também acontece pelo fator do medo.

4.2.4 Engenharia Social Inversa

Essa técnica se baseia, basicamente, na criação de um problema pelo engenheiro social que somente ele conseguirá resolver. Dessa forma, o engenheiro social ganha confiança do alvo conseguindo convencer que existe um problema ou que o problema esta prestes a acontecer. Em seguida o atacante se apresenta como a pessoa certa que pode resolver problema. (MITNICK e SIMON, 2003 apud PEIXOTO, 2006).

Essa técnica é muito eficiente, pois o engenheiro social ganha a confiança da vítima, facilitando a obtenção das informações que realmente o atacante deseja.

5 MEDIDAS DE DEFESA CONTRA ENGENHARIA SOCIAL

Um dos maiores especialistas nesse assunto, Kevin Mitnick, é citado por Peixoto (2006) e afirma que: “A verdade é que não existe tecnologia no mundo que evite o ataque de um Engenheiro Social.” (MITNICK e SIMON, 2003 apud PEIXOTO, 2006, p. 56)

Em seu artigo, Filho (2004) considera que a medida que a o papel da informação na sociedade aumenta e ganha importância, a engenharia social se torna uma das principais ameaças de segurança das organizações. Com isso existem algumas medidas simples que podem ser tomadas para se defender ou evitar um ataque de engenharia social em uma organização. São elas:

- **educação e treinamento**: As pessoas devem ter consciência sobre o valor da informação que elas manipulam. Devem ser apresentados conceitos e as ferramentas e os métodos utilizados pela engenharia social;
- **segurança física**: Somente pessoas autorizadas devem ter acesso a determinadas dependências de uma organização e sempre que possível devem ser usados o monitoramento por câmeras das entradas da depen-

dência;

- **política de segurança**: São instruções claras que fornecem uma orientação para preservar informações; e
- **controle de acesso**: Os mecanismos de controle e acesso têm como objetivo evitar que usuários sem permissão possam ter acesso a informações ou a equipamentos.

O sucesso dos ataques da engenharia social pode acontecer em qualquer nível de comando das organizações, independentemente do investimento em realizado em segurança. O engenheiro social visa o atacara o fator humano e é um grande erro supor que qualquer um está imune. (GARTNER, 2002).

6 TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA

Ao se falar sobre o desenvolvimento de um programa de conscientização é pensado em tecnologias e estruturas físicas, porém não se pode deixar de lado o fator mais importante de todos que é o fator humano.

Um programa de conscientização sobre segurança da informação tem o objetivo principal influenciar os integrantes de uma organização a mudarem seus hábitos e atentarem para a importância da segurança da informação. (FONSECA, 2009)

Aliados ao programa deverão ter as políticas de segurança, e principalmente o treinamento do pessoal, que é um fator essencial para se alcançar sucesso em questão de segurança. (PEIXOTO, 2006)

Os treinamentos dos integrantes devem levá-los a criarem a percepção automática de quais informações devem ser protegidas e como adotar medidas simples para protegê-las e também devem fazer com que os integrantes consigam perceber ou identificar um ataque de engenharia social. (FONSECA, 2009)

Vale ressaltar, de acordo com Gartner (2002), afirma que uma política de segurança desatualizada ou surrealista leva os integrantes a negligenciá-las, o que dificulta o reconhecimento de um ataque de engenharia social.

Um bom e objetivo programa de treinamento e conscientização sobre segurança da informação, levando em consideração os aspectos do comportamento humano, devem levar em consideração alguns tópicos como os descritos por Mitnick e Simon (2003, apud PEIXOTO, 2006) e por Fonseca (2009). São eles:

- descrever a forma com que engenheiros sociais utilizam suas habilidades para enganar as pessoas;
- como reconhecer um possível ataque de Engenharia Social, identificando ferramentas e métodos utilizados pelos atacantes;
- o procedimento quando se desconfiar de alguma solicitação suspeita;
- a importância de questionar solicitações, independente do cargo, função ou importância que o solicitante possui;
- o fato de não confiar em pessoas que fazem solicitações de informações, sem antes fazer uma verificação adequada da identidade e autoridade da pessoa que deseja a informação;
- como proceder para a proteção de informações sigilosas;
- sintetizar e explicar cada ação da política de segurança, como exemplo, as mediadas de defesa quanto com o lixo ou a criação de senhas;
- a obrigação de cada integrante atender as políticas e as consequências do não atendimento;
- melhores práticas no uso do correio eletrônico, alertando para os vírus e armadilhas em geral;
- questões físicas de segurança;

- eliminação de documentos que contenham informações sigilosas independentemente se sua natureza é física ou eletrônica; e
- fornecer periodicamente material informativo, como por exemplo, lembretes (de preferência curtos e que chamem atenção).

Ainda sobre a conscientização e treinamento, Mitnick (2003) afirma que é interessante que se realizem testes com o objetivo de encontrar falhas ou descumprimento de alguma norma. Deve ser avisado aos integrantes da instituição que os testes serão realizados periodicamente.

Um programa de treinamento e conscientização se resume, basicamente, em uma reeducação de todos os integrantes da instituição, inserindo cada vez mais a cultura de segurança da informação. (FONSECA, 2009)

Todos os integrantes de uma instituição devem ser treinados e tem a consciência da importância da segurança da informação. A defesa mais forte contra os ataques de engenharia social é o fator humano estar bem treinado.

A conscientização e o treinamento devem existir sempre. Os integrantes devem sempre ser lembrados da possibilidade de sofrer ataque e de como evitá-los ou de como reagir diante de um.

7 CONCLUSÃO

O presente trabalho teve como objetivo geral aprofundar o tema Engenharia Social e alertar para a importância da conscientização do tema no âmbito do Exército.

Como objetivos específicos foram buscados um melhor entendimento sobre o que é Engenharia Social e Segurança da Informação, de forma que fossem enumeradas algumas medidas para a prevenção de ataques de engenheiros sociais.

Na conjuntura atual, é possível percebermos que o trâmite de informações se tornou muito mais veloz e que houve um grande aumento no fluxo da informação transitada. Sendo assim, a informação ganhou cada vez mais importância e é fundamental saber proteger as informações, principalmente aquelas restritas que o Exército possui.

À medida que o avanço da tecnologia permitiu um ganho de tempo e uma maior eficiência para a tomada de decisões por parte das instituições, como no caso do Exército Brasileiro, percebemos que tal avanço, também permitiu que fossem abertas novas portas para ações externas contra as informações. Observamos então, a importância que deve ser dada a segurança da informação.

O fator humano está diretamente relacionado com a segurança da informação, isto porque o manuseio da informação passa pelas mãos das pessoas da instituição. A segurança da informação começa e termina nas pessoas. Investir em tecnologia e deixar de lado o fator humano é um erro grave. É justamente nesse ponto que atua a Engenharia Social, explorando as vulnerabilidades humanas para adquirirem informações que julguem interessantes.

A engenharia social é definida basicamente como a exploração das vulnerabilidades humanas, através de métodos e ferramentas, para a obtenção de informações. Como disse Peixoto (2006), a engenharia social está inserida como um dos desafios (senão o maior deles) mais complexos no âmbito da segurança da informação.

Para inibir os ataques dos engenheiros sociais ou diminuir a efetividade dos mesmos, o Exército Brasileiro assim como qualquer instituição deve adotar estratégias tanto no nível físico (nos meios pelos quais o engenheiro social atua) quanto no nível psicológico (manipulando emoções).

A criação de um programa de conscientização em segurança, aliado as normas de segurança e da sua divulgação, faz com que os integrantes da instituição compreendam a importância da segurança da informação; quais

devem ser os cuidados no manuseio na informação; quais informações são sigilosas e quais são de caráter ostensivo; e quais medidas devem ser tomadas em caso de suspeita de ataque de um engenheiro social.

Aliados a esse programa de conscientização, deve estar algo que sem sombra de dúvidas é fundamental para combater ataques de engenharia social: o treinamento. Todas as pessoas que tem contato ou trabalham diretamente no manuseio de informações, principalmente sigilosas, devem passar por um treinamento para aprender a identificar os métodos e ferramentas utilizados no ataque de um engenheiro social e como irá reagir diante de um possível ataque.

Observamos também que uso de medidas simples de proteção já dificulta e muito o trabalho realizado pelo engenheiro social. O controle e acesso das áreas que manipulam informações sigilosas; a preocupação com a segurança física; a criação de uma política de segurança; a preocupação com o lixo; o simples uso de antivírus; e a preocupação em estabelecer uma senha segura, são exemplos de algumas medidas que defende uma instituição de um possível ataque.

Mas o principal inibidor de ataques de engenheiros sociais é sem dúvida a conscientização e o treinamento. O treinamento deve fazer a pessoa aprender a identificar os tipos de ataque e como reagir a cada um deles. Concordamos com Kevin Mitinick (2003) em que não existe tecnologia que evite um ataque de engenheiro social, portanto o treinamento contínuo é essencial para que as pessoas possam conhecer e estejam sempre preparadas para lidar com possíveis ataques.

O estudo do assunto não se esgotou totalmente neste trabalho, uma vez que este não era nosso objetivo. Este trabalho serve como um estudo preliminar para que novos trabalhos possam ser feitos a fim de aprofundar, discutir e padronizar processos e controles para inibir os ataques dos engenheiros sociais.

No final da pesquisa podemos observar a importância da conscientização dos militares do Exército, assim como em qualquer instituição, sobre a engenharia social, abordando técnicas e ferramentas utilizadas. Observamos também a importância de existir o treinamento do pessoal para evitar ataques.

O trabalho atingiu o objetivo estabelecido, que era colaborar como um meio de conscientização a respeito do tema proposto. Inserido no campo da cibernética, o trabalho apresentou conceitos sobre a Engenharia Social e mostrou que por mais tecnologia que exista na segurança da informação, continua sendo o ser humano o fator mais crítico e vulnerável. Foram abordadas também algumas medidas de simples adoção para o combate da Engenharia Social.

Conclui-se então que para proteger as informações das ações da Engenharia Social, é interessante que o Exército incentive uma cultura de conscientização sobre o tema, e que mantenha sempre atualizada, além de realizar treinamentos com as pessoas que manipulam as informações sigilosas, para que não exista perda ou vazamento de informações.

Não existe uma fórmula mágica para tornar um ambiente que manipula informação totalmente seguro. O conhecimento das técnicas da Engenharia Social, através de um programa de conscientização; e de medidas para evitar ataques de engenheiros sociais, ensinadas e reforçadas através dos treinamentos, são fundamentais para que o Exército Brasileiro consiga inibir vazamentos ou perdas de informações, obtidas através da Engenharia Social.

SOCIAL ENGINEERING:THE IMPORTANCE OF A CONSCIENTIZATION PROGRAM IN THE FRAMEWORK OF THE BRAZILIAN ARMY

ABSTRACT: Faced with the modern technological scenario, in which there is a continuous process of innovation and integration of new concepts and capacities, one realizes what information has become the greatest patrimony of society. The value of information in the modern context is so great that it becomes

vital to any institution that wants to stay alive and competitive. In such a way it is perceived that the institutions possess a high degree of dependence of the information. This dependence makes us realize that Information Security is a prerequisite for any institution, including for the Brazilian Army. On the other hand, it is observed in the current context that Social Engineering is one of the factors that most compromise not only Information Security, but also organizational security. Social engineering is an intrusion technique that exploits the weaknesses of the human being, whether or not the use of technologies to obtain information. The present study is a bibliographical and documentary review that has the general objective to verify and to understand the Social Engineering and to emphasize the importance of raising awareness of the subject within the scope of the Army where the techniques used by Social Engineering will be approached and measures to combat it. In this context, it will be observed, as a result of the study, the importance of an awareness program to combat Social Engineering.

Keywords: Information, Social Engineering, Information Security.

REFERÊNCIAS

ALVES, Cássio Bastos. **Segurança da Informação VS. Engenharia Social**: Como se proteger para não ser mais uma vítima. 63f. Brasília, 2010. Disponível em: < http://www.administradores.com.br/_resources/files/_modules/academics/academics_3635_20101207234707794d.pdf > Acesso em: 05 abril de 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências - elaboração. Rio de Janeiro, 2002.

_____. **NBR 10520**: citação em documentos. Rio de Janeiro, 2002.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. 4ª edição rev. e ampl. Florianópolis: Visual Books, 2011.

ESCOLA DE COMUNICAÇÕES. Seção de Pós-Graduação e Doutrina. **Extrato do Manual de Metodologia da Pesquisa, confeccionada pelo Centro de Estudos de Pessoal (CEP) ao Curso de Psicopedagogia e Orientação Educacional pela Professora Maria Christina Zentgraf**. Brasília, 2017.

FERREIRA, Aurélio B. de Holanda. **O mini dicionário da língua portuguesa**. 4ª edição revista e ampliada do mini dicionário Aurélio. 7ª impressão – Rio de Janeiro, 2002.

FILHO, Antônio Mendes da Silva. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistema de Informações in Revista Espaço Acadêmico nº42 – novembro de 2004; Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm> Acesso em: 02 maio de 2017.

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf > Acesso em: 12 abr. 2017.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**: o usuário faz a diferença. 1. ed. São Paulo: Saraiva, 2006.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. **A segurança dos documentos digitais**. Revista Jurídica: Órgão Nacional de Doutrina, Jurisprudência, Legislação e Crítica Judiciária, Porto Alegre, Ano 53, v. 50, n. 295, p. 59-71, mai. 2002.

GARTNER, INC. **Protect Against Social Engineering Attacks**. Gartner's Information Security Strategies Research, Volume 1, Issue 1, February 2002; Disponível em: <http://www.gartner.com/gc/webletter/security/issue1/article2.html> Acesso em 10 maio. 2017

GONÇALVES, L. R. O. **Um modelo para verificação, homologação e certificação de aderência a norma nacional de segurança da informação – NBR-ISSO / IEC- 17799**. 189f. Tese (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, COPPE – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Rio de Janeiro, 2005.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social.** [S.l.: s.n.], 2006, Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 17 abr. 2017.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia, Paraná, v. 8, n. 3, p. 38-44, jan./mar. 2005.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de In-**

formação Gerenciais: administrando a empresa digital. 5ª ed. São Paulo: Person Pretice Hall, 2004.

MARCELO, Antônio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MITNICK, Kevin D.; SIMON, Willian L. **A arte de enganar: Ataques de Hackers**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MORAIS, Catiane Pimentel De. **Cibernética, Teoria Matemática e Teoria dos Sistemas**. 2006. Disponível em <http://www.zemoleza.com.br/trabalho-academico/humanas/contabilidade/cibernetica-teoria-matematica-e-teorias-dos-sistemas> Acesso em: 23 Mai 17.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em ambientes Cooperativos**. Editora Futura; 2003

PEIXOTO, Márcio C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**.1ª ed. Rio de Janeiro: Brasport, 2006.

PINHEIRO, José Maurício. **Biometria nos Sistemas Computacionais – Você é a Senha**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação. 9ª reimpressão. Rio de Janeiro: Elsevier, 2003

SILVA FILHO, Antonio Mendes Da. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. Revista Espaço Acadêmico Nº42/2004. Disponível em: <http://www.espacoacademico.com.br/042/42amsf.htm> Acesso em: 10 Fev. 2017.

SIQUEIRA, Marcelo Costa. **Gestão Estratégica da Informação**. Rio de Janeiro: Brasport, 2005.

YAMAGISHI, T. **Trust and social intelligence**: the evolutionary game of mind and society. Tóquio: Tokyo University Press, 1998.

ZAPATER, Márcio; SUZUKI, Rodrigo. **Segurança da Informação**: Um diferencial determinante na competitividade das corporações. São Paulo: Promon, 2005.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). 1° Tenente da Arma de Artilharia do Exército Brasileiro da turma de 2013. Concluiu com aproveitamento o curso de Operação do Sistema de Mísseis e Foguetes no Centro de Instrução de Mísseis e Foguetes. É pós-graduado pela Escola de Comunicações, *Lato Sensu*, em Oficial de Comunicações. Atualmente, exerce a função de Chefe do Centro de Operações de Apoio Logístico do Centro de Logística de Mísseis e Foguetes e pode ser contactado pelo email felipereira.art@gmail.com.

A PROTEÇÃO DO FLUXO DA INFORMAÇÃO NO SISTEMA DE COMANDO E CONTROLE DA FORÇA TERRESTRE COMPONENTE

Gustavo Ovídio Ribeiro de Castro
Pós-graduado, Lato Sensu, em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: A Força Terrestre Componente é o comando singular responsável pelo planejamento e execução das operações terrestres no contexto de uma operação conjunta. Nas Operações, será instalado um Sistema de Comando e Controle que possuirá um Conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrina, procedimentos e pessoal essenciais para o comandante planejar, dirigir e controlar as ações de sua organização para que se atinja uma determinada finalidade. A obtenção e a proteção da informação constituem-se em um dos principiais elementos do combate moderno. A Guerra da Informação é exercida desde os tempos de paz e contra diferentes tipos de ameaça. Nesse contexto, o Sistema de Comando e Controle está diretamente relacionado ao novo cenário dos combates modernos que tem por objetivo principal obter a Superioridade da Informação por meio da Guerra Centrada em Redes. Cresce, assim, a importância da Segurança da Informação, ou seja, torna-se necessário entender quais são as atividades e as tarefas necessárias para garantir a proteção e a segurança das informações geradas.

Palavras-chave: Comando e Controle. Guerra da Informação . Segurança de Informação.

1 INTRODUÇÃO

O presente artigo tratou sobre os aspectos relativos ao gerenciamento do fluxo da informação operativo no Sistema Comando e Controle da Força Terrestre quando do emprego do Exército Brasileiro nas operações.

A palavra informação conforme o Manual de Fundamentos Operações (BRASIL, 2014, p. 3-8) é o elemento fundamental da Era do Conhecimento, e que, produzir, obter, utilizar e disseminar informações oportunas, objetivas e com credibilidade têm relação direta com a qualidade do processo decisório.

O Exército Brasileiro apresentou, em 2014, sua doutrina relativa as Operações de Informação por meio do Manual de Campanha EB-20-MC-10.213 Operações de Informação. Essas operações visam a evitar, impedir ou neutralizar os efeitos das ações adversas na Dimensão Informacional.

Desse conceito de Operações de Informações, abordagens relativas a Guerra da Informação podem ser observadas nas Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro:

> XVI - Guerra da Informação: conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (BRASIL, 2014, p. 12).

Com a crescente importância da informação precisamos entender como é o gerenciamento da informação nos sistemas de informação empregados no Exército Brasileiro. O Manual Comando e Controle (BRASIL, 2015, p 5-3) apresenta que com o aumento do volume e do fluxo de informações, o plano de gerenciamento de informação deve ser elemento primário do plano de operações.

Nessa linha de entendimento, referente a importância do gerenciamento da informação no Sistema de Comando e Controle, o Exército Brasileiro elaborou um manual para delegar as atribuições relativas a proteção. O Manual Proteção (BRASIL, 2015, p 3-2) cita que a célula de proteção coordena as atividades e sistemas

destinados a preservar a força por intermédio de uma sistemática de gerenciamento de risco, incluindo tarefas relacionadas as informações.

Portanto, para compreender o gerenciamento da informação, torna-se indispensável o entendimento sobre quais são as atividades e tarefas necessárias para garantir a proteção do fluxo da informação.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

O artigo teve como objetivo geral compreender as atividades e as tarefas funcionais inerentes à proteção da informação no fluxo da informação no Sistema Militar de Comando e Controle da Força Terrestre Componente.

Como justificativa para o artigo pode-se verificar que na Doutrina de Operações Conjuntas do Ministério da Defesa consta uma estrutura de Comando e Controle com aspectos e procedimentos diferentes da existente no Exército Brasileiro. Tais procedimentos e estruturas podem ser adotados visando otimizar os procedimentos de proteção da informação nas operações.

Foi realizada uma pesquisa descritiva de cunho documental, sendo que a forma de abordagem utilizada foi a quantitativa. O delineamento de pesquisa contemplou as fases de coleta dos dados, comparação com a Doutrina Militar Terrestre, análise dos dados coletados e a discussão dos resultados.

Os assuntos do referencial teórico visam apresentar desde o entendimento macro das operações, envolvendo seu ambiente operacional, passando posteriormente pelo entendimento do Sistema de Comando e Controle e, por fim, compreendendo as atividades e tarefas dos elementos do Estado-Maior do Centro de Coordenação de Operações.

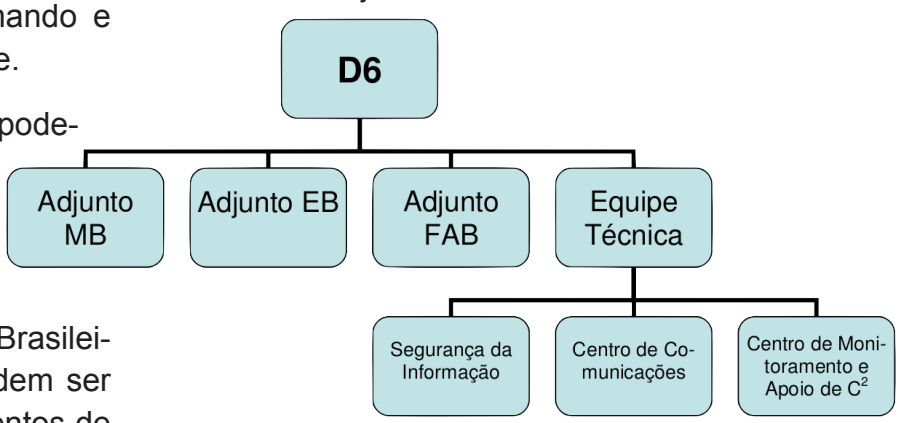
Por fim, os procedimentos adotados para o presente estudo foi a pesquisa doutrinária dos assuntos relativos a proteção da informação e as fontes de pesquisa foram manuais doutrinários do Ministério da Defesa e do Exército Brasileiro.

2.2 REFERENCIAL TEÓRICO

2.2.1 Comando e Controle na Doutrina de Operações Conjuntas

Na Doutrina de Operações Conjuntas do Ministério da Defesa pode-se verificar uma estrutura de Comando e Controle com aspectos e procedimentos que poderiam ser adotados pelo Exército Brasileiro, visando otimizar os procedimentos de proteção e segurança da informação nas operações.

FIGURA 1 - Estrutura da D6 no Estado-Maior Conjunto



Fonte: MD30-M-01, 2011, p 141

As atribuições inerentes a proteção da informação, que são de competência do setor de Segurança da Informação na Seção de Comando e Controle do Estado- Maior Conjunto, podem ser destacadas em: Instrução de Segurança da Informação, Plano de Adestramento de Segurança da Informação, assessorar no Plano de Segurança Orgânica e Gestão dos Sistemas de Informação.

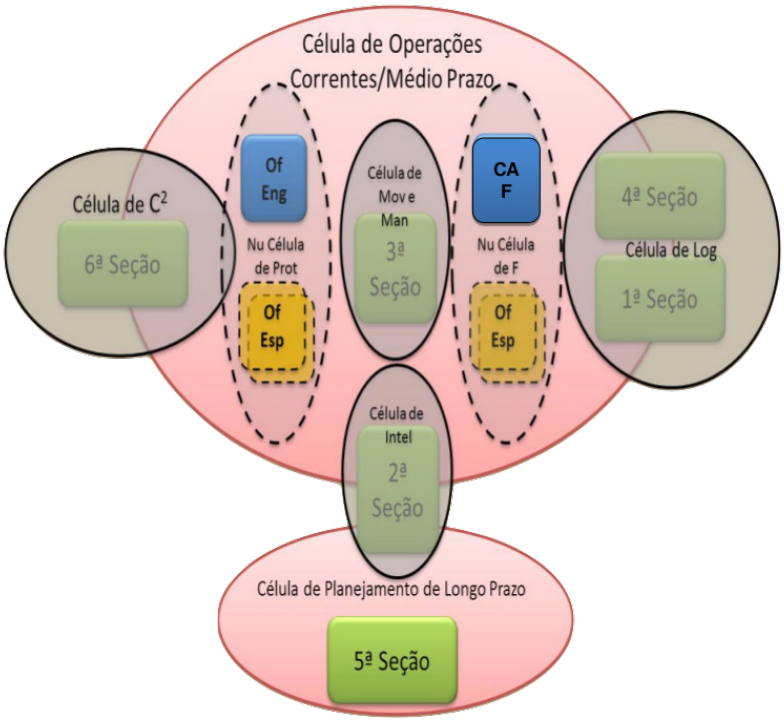
Portanto, pode-se constatar que no Estado-Maior Conjunto já está normatizado os procedimentos relativos a proteção da informação.

2.2.2 Comando e Controle na Força Terrestre Componente

O Estado-Maior da Força Terrestre Componente foi dividido em células funcionais e agora trabalha em um ambiente de interação e

integração das diversas especialidades, competências e capacitações existentes na Força Terrestre.

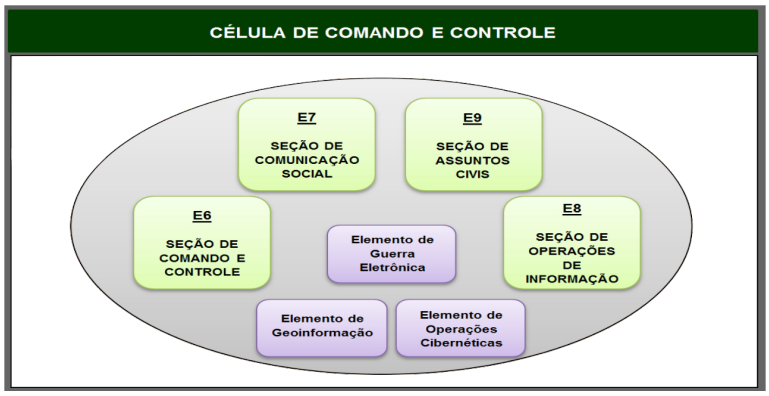
FIGURA 2 - Centro de Coordenação de Operações (CC Op) de um FTC



Fonte: BRASIL, 2014, p B-1

No esquema representado na figura acima, pode-se verificar uma área de interseção entre a Célula de Comando e Controle e a Célula de Proteção. Ou seja, existem atribuições e responsabilidades comuns no que se refere a proteção.

FIGURA 3 - Célular de Comando e Controle



Fonte: BRASIL, 2014, p 4-3

Na figura acima pode-se observar a existência de um Elemento de Operações Cibernéticas integrante da Célula de Comando e Controle do Centro de Coordenação de Operações da Força Terrestre Componente.

2.2.3 Atividades e Tarefas

2.2.3.1 Comando e Controle (C2)

Conforme Manual de Campanha EB-70-MC-10.341 Lista de Tarefas

Funcionais temos a seguinte atividade: realizar a gestão do conhecimento e da informação. Dentre outras, as tarefas podem ser verificadas a seguir:

> a) Estabelecer redes e sistemas de informações: compreende ampliar e defenderas redes de informação para garantir o fluxo das ordens e dos relatórios.
> c) Gerenciar informações e dados: compreende assegurar o acesso à informação com segurança e em níveis escalonáveis de usuários.
> e) Avaliar a informação coletada: compreende verificar a relevância da informação, realizando uma triagem inicial.
> f) Processar informações relevantes: compreende considerar imediatamente as informações críticas nas simulações e projeções para ajustar a operação constantemente. (BRASIL, 2016, p. 2-2)

2.2.3.2 Inteligência (Intlg)

Conforme Manual de Campanha EB-70-MC-10.341 Lista de Tarefas

Funcionais temos a atividade de apoio à obtenção da consciência situacional na qual apresenta, dentre outras, a tarefa a seguir:

> Apoiar constantemente as atividades de ptç (C Intlg): esta tarefa tem como objetivos: impedir que ações hostis de qualquer natureza comprometam dados, informações, conhecimentos e sistemas a eles relacionados; impedir a realização de atividades de espionagem, sabotagem, propaganda hostil, terrorismo, desinformação; e induzir o centro de decisão do adversário a posicionar-se de forma equivocada. (BRASIL, 2016, p. 4-3)

2.2.3.3 Proteção (Ptç)

Conforme o EB70-MC-10.341 Lista de Tarefas Funcionais temos as atividades e tarefas, abaixo listadas, que tratam sobre informação:

QUADRO 1 - Atividades inerentes à função de combate proteção e suas tarefas

7.2 ADOTAR MEDIDAS DE CONTRAINTELIGÊNCIA	
7.2.1 Tarefas:	a) Adotar medidas de segurança orgânica: visa a obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes do Sistema de Defesa. b) Adotar medidas de segurança ativa: destina-se a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza, dirigidas contra os interesses da sociedade e do Estado.
7.7 REALIZAR MEDIDAS DE GUERRA CIBERNÉTICA	
7.7.1 Tarefas:	b) Adotar medidas de segurança de sistemas operacionais e serviços de rede em uso: consiste em estabelecer políticas de segurança da informação, acompanhadas de normas e procedimentos que possam ser implementados em quaisquer ambientes, independente do nível de conhecimento técnico dos usuários destes serviços. ... e) Estabelecer estrutura de segurança ofensiva: consiste em manter equipes multidisciplinares em condições de fazer frente a ameaças identificadas e com a finalidade de manter a iniciativa nas ações cibernéticas.

Fonte: BRASIL, 2016, p. 7-1 e 7-4 – adaptado pelo autor

Nesse contexto de proteção, o Manual de Campanha EB70-MC-10.232 Guerra Cibernética apresenta o seguinte conceito para Proteção Cibernética:

> Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente. (BRASIL, 2017, p. 3-4)

2.2.4 Células Funcionais

2.2.4.1 Célula de Inteligência

As atribuições da Célula de Inteligência, com foco na segurança da informação, podem ser verificadas no Manual de Campanha EB-20-MC-10.202 FTC.

> d) produzir informações e conhecimentos, visando ao apoio à decisão do Cmt FTC e, quando pertinente, aos demais níveis decisórios;
> n) supervisionar a execução das medidas de contra inteligência;
> o) estabelecer, em coordenação com a Seção de Comando e Controle, a arquitetura da rede de inteligência para troca de informações dentro do EM e com os elementos subordinados nos diferentes níveis;
> t) fiscalizar e coordenar o acesso de militares ou representantes de governos ou de organizações estrangeiras a informações ou documentos sigilosos ou sensíveis; (BRASIL, 2014, p. 3-7 e 3-8)

2.2.4.2 Célula de Comando e Controle

O Manual de Campanha Força Terrestre Componente determina que o responsável pela estruturação do sistema de Comando e Controle da FTC, bem como por coordenar e disciplinar o seu funcionamento é o Chefe da Seção de Comando e Controle.

Dentre as atribuições listadas no manual acima referenciado, as que são diretamente relacionadas a gestão da informação podem ser verificadas na tabela.

QUADRO 2 - Atribuições inerentes ao Chefe da Célula de Comando e Controle

Atribuições	c) planejar e coordenar à instalação, operação, manutenção e desmobilização de todos os sistemas de C2 da FTC, em coordenação com as demais seções do EM FTC; f) orientar o estabelecimento e o gerenciamento do banco de dados da FTC, contando com a contribuição das demais seções do EM para a sua atualização; h) planejar, coordenar e executar as medidas necessárias ao adestramento do pessoal necessário à operação do sistema de C2; i) coordenar com as seções de Operações e de Inteligência as atividades afetas à exploração do espectro eletromagnético e do ambiente cibernético, com vistas à obtenção de informações e à proteção de dados de interesse; j) estabelecer medidas de controle e segurança dos sistemas eletrônicos operados pelo comando da FTC; m) realizar a gestão das informações, em coordenação com outros membros do EM;

Fonte: BRASIL, 2014, p. 3-10 e 3-11 – adaptado pelo autor

2.2.4.3 Célula de Proteção

O Manual de Campanha EB-20-MC-10.202 FTC determina que a Célula de Proteção coordena as atividades e sistemas destinados a preservar a força por intermédio de uma sistemática de gerenciamento de risco, a qual inclui tarefas relacionadas com a proteção do pessoal, dos meios físicos e das informações.

A célula é chefiada pelo Chefe da Seç Ptç e possui, dentre outras, as seguintes atribuições: analisar, planejar e coordenar as missões e atividades de proteção e propor diretrizes quanto ao emprego dos sistemas e execução das tarefas de proteção.

Da mesma forma, o EB20-MC-10.202 cita que a Célula de Proteção coordena com a Seção de Comando e Controle (6a Seção) na Célula de Comando e Controle os aspectos relativos à tarefa de proteção da informação.

2.2.5 Oficiais / Elementos Especialistas

2.2.5.1 Elemento de Guerra Cibernética

Quanto aos aspectos de proteção cibernética, o Catálogo de Capacidades de Exército Brasileiro prevê que o Elemento de Guerra Cibernética deve conduzir ações para garantir o funcionamento dos nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e G Ciber para neutralizar ataques e exploração cibernética em nossos meios.

2.2.5.2 Oficial de Proteção das Operações

O EB20-MC-10.202 FTC apresenta o Oficial de Segurança das Operações como o responsável por desenvolver os procedimentos de segurança das operações. Além disso, suas atribuições incluem: revisar os documentos do EM FTC, os acessos aos sistemas de informação e as interações com a mídia.

O Manual de Campanha EB-20-MC-10.213 Operações de Informação cita, que o representante da Segurança das Operações, em coordenação com as outras Seções, é o responsável pela identificação das vulnerabilidades das nossas Capacidades Relacionadas à Informação e segurança das informações das nossas forças.

2.2.5.3 Oficial de Gestão do Conhecimento

O Oficial de Gestão do Conhecimento agrega ao EM FTC maior capacidade no que se refere à integração e ao gerenciamento de sistemas de informações. As suas principais atribuições são apresentadas no EB20-MC-10.202 FTC.

> g) coordenar o apoio do E6 quanto à manutenção de redes, bancos de dados, armazenamento e assistência técnica; e (BRASIL, 2014, p. 3-18 e 3-19)

2.2.5.4 Oficial de Segurança da Informação (EM Cj)

Conforme a Doutrina de Operações

Conjuntas do Ministério da Defesa,

MD30-M-01, o Centro de Operações deve ter, em sua estrutura, um Oficial de Segurança da Informação, subordinado à D6 e trabalhando em estreita coordenação com a D2 do EMCj.

Da mesma forma, a doutrina cita que cada F Cte deve indicar um Oficial de Segurança da Informação, responsável pelos seus respectivos sistemas.

QUADRO 3 - Atribuições inerentes ao Oficial de Segurança da Informação

Atribuições	a) elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação; b) elaborar e cumprir o Plano de Adestramento de Segurança da Informação do C Op; c) assessorar o Cmt Op nos assuntos de Segurança da Informação; d) propor, analisar e verificar se os requisitos de Segurança da Informação estão sendo cumpridos; e) identificar os integrantes do sistema que necessitem de proteção, de acordo com o grau de sigilo da informação por eles processada ou armazenada; f) assessorar a D2 na elaboração do Plano de Segurança Orgânico; g) reportar ao Cmt Op e aos demais Oficiais de Segurança da Informação do SISMC2, após uma avaliação preliminar, os incidentes de Segurança da Informação; h) controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2; i) supervisionar a elaboração, o controle e a manutenção do histórico dos sistemas utilizados; j) analisar o impacto da descontinuidade dos serviços e suas consequências para o C Op, elaborando e testando um Plano de Contingência; k) exigir do pessoal externo ao C Op, autorizado a executar serviços no SISMC2, a assinatura de um Termo de Responsabilidade e o cumprimento das regras estabelecidas para guarda e proteção do sigilo das informações que possa ter acesso; l) empenhar-se para que os serviços (instalações, manutenções ou correções), sejam feitos sem afetar a Segurança da Informação; e m) fazer o possível para que todos os usuários estejam cientes das instruções em vigor para a Segurança da Informação, por meio da assinatura do Termo de Responsabilidade.

Fonte: BRASIL, 2011, p. 121 – adaptado pelo autor

2.3 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

2.3.1 Na atividade de Comando e Controle

Tratando sobre como deve ser a atividade de proteção na gestão do Conhecimento e da Informação, pode-se constatar que as tarefas deverão primar pela manutenção fidedigna dos seguintes aspectos da informação: disponibilidade, integridade, confiabilidade, autenticidade e não repúdio.

Para estabelecer a Gestão da Informação nas redes e sistemas de Informações, constata-se a necessidade da elaboração de uma Política de Segurança da Informação, pela Célula de Comando e Controle, que contemple normas quanto à segurança física, lógica, de dados, de usuários e de redes.

2.3.2 Na integração e interação entre as Células

Na revisão doutrinária, foi apresentado que o E6 identifica as vulnerabilidades e desenvolve procedimentos para proteger o Comando e Controle e a gestão de Sistemas de Informação e Comunicações. Da mesma forma, o E6 deverá colaborar com a confecção de planos relacionados à segurança das operações, particularmente vinculados à segurança das informações.

Com a criação da Seção de Segurança da Informação, subordinada a Seção de Comando e Controle, da Célula de Comando e Controle, seria possível realizar as atribuições pertinentes a proteção da informação haja vista a peculiaridade dos assuntos relativos a Segurança da Informação e Comunicações.

Dentre outras atribuições realizadas pela Seção de Segurança da Informação, podem ser destacadas: assessorar o Cmt Op nos assuntos de Segurança da Informação, assessorar a D2 na elaboração do Plano de Segurança Orgânica, controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2 e empenhar-se para que os serviços (instalações, manutenções ou correções) sejam feitos sem afetar a Segurança da Informação.

Da mesma forma, em proveito da Função de Combate Proteção, a Seção de Segurança da Informação teria condições de realizar a tarefa de manter equipes multidisciplinares em condições de fazer frente a ameaças identificadas e com a finalidade de manter a iniciativa nas ações cibernéticas.

2.3.3 Nas responsabilidades funcionais

Primeiramente, uma tarefa ora atribuída ao Oficial de Gestão do Conhecimento é a de coordenar o apoio do E6 quanto à manutenção de redes, bancos de dados, armazenamento e assistência técnica. Tal tarefa de coordenação poderia ser realizada diretamente pelo Chefe da Célula de C2, pois é o responsável pela instalação do Sistema de C2, por intermédio da Seção de Comando e Controle.

Da mesma forma, não seria desejável que as responsabilidades inerentes a sistemas de informação fossem acumuladas pelo Oficial de Segurança das Operações, da Célula de Ptç. Tais motivos visam a segregação das informações que tramitam nos sistemas e o acumulo demasiado de atribuições em um mesmo Oficial.

Quanto a documentação operacional empregada pela Força Terrestre Componente, poderia ser adotado o documento previsto para as Operações Conjuntas do Ministério da Defesa. O referido documento é o Apêndice Instrução de Segurança da Informação ao Anexo de C2 ao Plano Operacional, que seria confeccionado pelo Oficial de Segurança da Informação.

O Elemento de Operações Cibernéticas, integrante da Célula de Comando e Controle, poderia ser o Oficial de Segurança da Informação e, consequentemente, o Chefe da Seção de Segurança da Informação.

Dentre as principais atribuições da seção podem ser destacadas: elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação, controlar as autorizações para o acesso de usuários aos sistemas de informação do SISMC2 e fazer o possível para que todos os usuários estejam cientes das instruções para a Segurança da Informação.

3 CONCLUSÕES E RECOMENDAÇÕES

Neste artigo pode-se constatar um estudo sobre as atividades e tarefas necessárias para garantir a proteção do fluxo da informação no SISMC2 da FFTC para compreender os aspectos relativos ao gerenciamento da informação.

Tendo em vista a crescente importância da informação, foi necessário entender quais são as responsabilidades no gerenciamento da informação nos sistemas de informação empregados pelo Exército Brasileiro para verificar eventuais possibilidades de melhoria no emprego do referido Sistema de Comando e Controle.

O Sistema de C2 apresenta uma estrutura complexa, diversa e abrangente e, durante a pesquisa realizada, foi possível constatar que a Doutrina de Operações Conjuntas do Ministério da Defesa apresenta uma estrutura de Comando e Controle com aspectos e procedimentos diferentes dos preconizados pelo Exército Brasileiro

Para garantir um efetivo procedimento de controle sobre a segurança e a proteção do fluxo da informação no Sistema de C2, torna-se fundamental integrar e interagir as Células Funcionais de Inteligência, Comando e Controle e Proteção.

Primeiramente, verificou-se a viabilidade em adotar parcialmente a estrutura de C2 conforme a Doutrina de Operações Conjuntas no que se refere a criação da Seção de Segurança da Informação subordinada a Seção de C2, cuja

atribuição principal seria a de assessorar o Cmt Op nos assuntos de Segurança da Informação.

No segundo momento, teríamos a vinculação do cargo de Oficial de Segurança da Informação ao Elemento de Operações Cibernéticas, com a responsabilidade de elaborar, divulgar e fiscalizar o cumprimento da Instrução de Segurança da Informação por ocasião da exploração do Sistema de C2.

Por fim, verificou-se a possibilidade da adoção do Apêndice Instrução de Segurança da Informação ao Anexo de C2 ao Plano Operacional contento os procedimentos e as atribuições necessárias às Seções do EM da FTC e as responsabilidades dos elementos integrantes do EM da FTC. Tal documento seria elaborado pelo Oficial de Segurança da Informação.

Portanto, o trabalho poderá servir para direcionar novas propostas de estudo sobre o assunto para que o resultado final seja a contribuição com o desenvolvimento doutrinário do Exército Brasileiro, visando ampliar os aspectos de proteção do fluxo da informação no Sistema de C2 da Força Terrestre.

THE PROTECTION OF THE INFORMATION FLOW IN THE COMMAND AND CONTROL SYSTEM OF THE GROUND FORCE COMPONENT

ABSTRACT: The Component Ground Force is the only command responsible for planning and executing ground operations in the context of a joint operation. In Operations a Command and Control System will be installed which will have a set of essential facilities, equipment, information systems, communications, doctrines, procedures and personnel for the commander to plan and control the actions of his organization to achieve a purpose. Obtaining and protecting information is one of the main elements of modern combat. Information Warfare has been carried out since times of peace and against different types of threats. In this context, the Command and Control System is directly related to the new scenario of modern combats whose main objective is to obtain Information Superiority through Network Warfare. Thus, the importance of information security is increased, that is, it becomes necessary to understand what activities and tasks are necessary to ensure the protection and security of the information generated.

Keywords: Command and Control, Information Warfare and Information Security.

REFERÊNCIAS

BRASIL. Estado-Maior do Exército Brasileiro. Manual de Campanha E20-MC-10.202 Força Terrestre Componente. 1. ed. Brasília, 2014.

_____. _____. Manual de Campanha EB20-MC-10.205 Comando e Controle. 1. ed. Brasília, 2015.

_____. _____. Manual de Campanha EB20-MC-10.208 Proteção. 1. ed. Brasília, 2015.

_____. _____. Manual de Campanha EB20-MC-10.213 Operações de Informação. 1. ed. Brasília, 2014.

_____. _____. Manual de Campanha EB70-MC-10.232 Guerra Cibernética. 1. ed. Brasília, 2017.

_____. _____. Manual de Campanha EB70-MC-10.341 Lista de Tarefas Funcionais. 1. ed. Brasília, 2016.

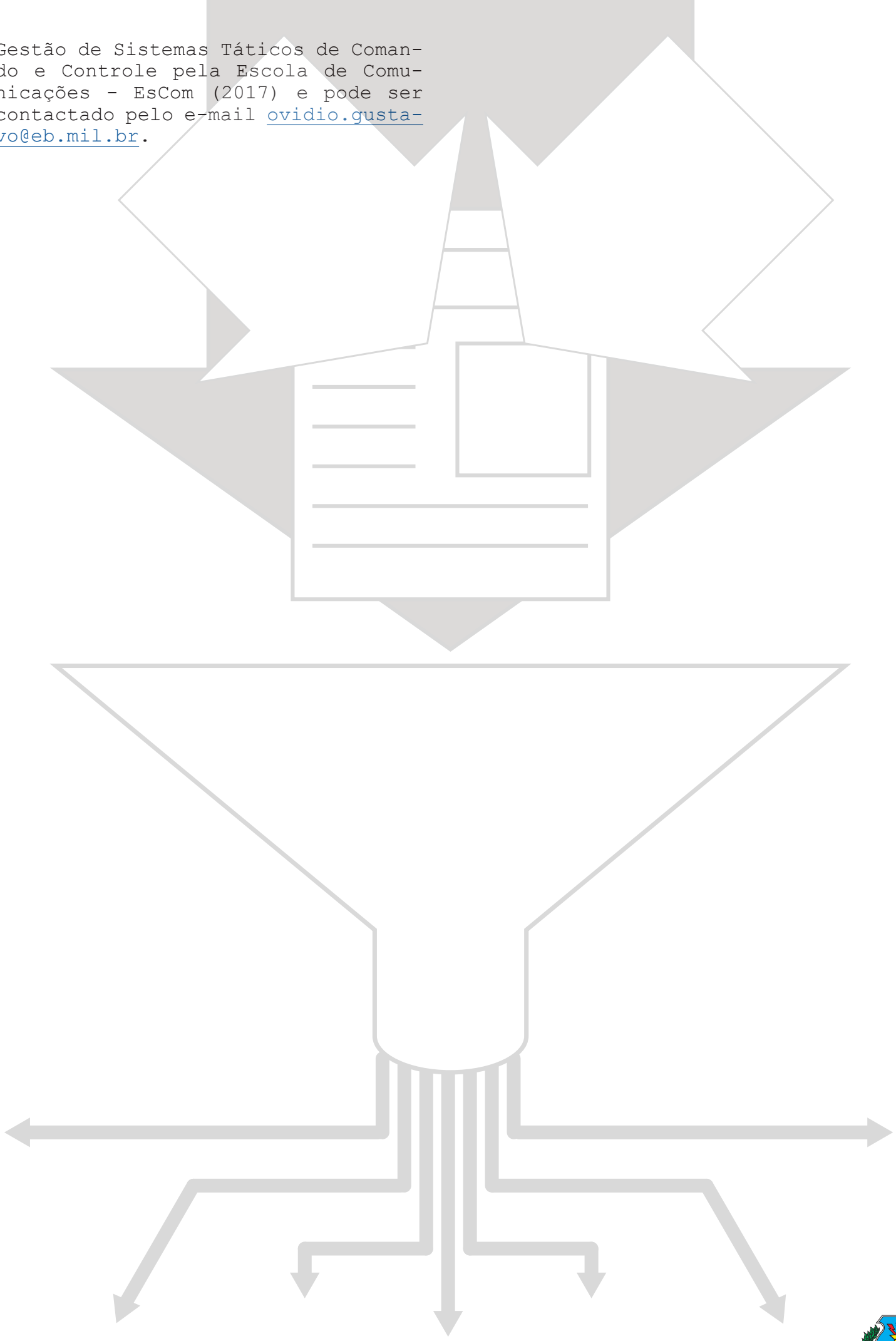
_____. _____. Manual de Fundamentos EB20-MF-10.103 Operações. 4. ed. Brasília, 2014.

_____. _____. Portaria nº 803-Cmt Ex, de 30 de julho de 2014: Aprova as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro - EB10-IG-01.014. Brasília, 2014.

_____. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas – 3º Volume. 1. Ed. Brasília, 2011.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras - AMAN (2006), pós graduado em Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica - CIGE (2011), em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais - EsAO (2015) e em

Gestão de Sistemas Táticos de Comando e Controle pela Escola de Comunicações - EsCom (2017) e pode ser contactado pelo e-mail ovidio.gustavo@eb.mil.br.



O CURRÍCULO REFERENTE ÀS COMUNICAÇÕES NO CURSO DE ARTILHARIA DA AMAN E SUA APLICABILIDADE NA TROPA

Douglas Maya Flores
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: A presente pesquisa trata do currículo referente às comunicações no curso de artilharia da Academia Militar das Agulhas Negras (AMAN) e sua aplicabilidade na tropa. O subsistema comunicações na artilharia é essencial para interligar todos os postos envolvidos na preparação e na condução dos tiros e na coordenação com os elementos apoiados. Com o objetivo de obter um conhecimento prévio mais concreto, foi procedida a análise da educação por competências e o levantamento das possibilidades de utilização do equipamento Harris RF-7800V-HH (da família Falcon III), usado como parâmetro por ter sido recentemente adquirido pelo Exército Brasileiro e por mobiliar a grande maioria dos GAC. Posteriormente, a pesquisa relacionou a teoria com os resultados obtidos através da opinião dos oficiais recém formados pela AMAN, tratando de sua formação, do preparo na parte de comunicações e do conhecimento do material analisado. Constatou-se, assim, que os métodos utilizados necessitam de reformulação e, para isso, foram levantados subsídios que, além de melhorar o aprendizado dos futuros líderes do Exército Brasileiro, aumentarão a operacionalidade e a segurança no emprego dos equipamentos rádios durante as missões da Artilharia.

Palavras chave: Comunicações na Artilharia. Rádio Falcon 3. Ensino por Competências. AMAN.

1 INTRODUÇÃO

O presente artigo está relacionado ao campo de pesquisa inserido na área de Educação e na linha de pesquisa Currículo por Competências, conforme definido pela Lista de Assuntos de Trabalhos Acadêmicos disponibilizada pela Escola de Comunicações.

O escopo do trabalho ficou restrito à análise da educação por competências, visando adequar os métodos de ensino-aprendizagem e de avaliação ao perfil ideal do concludente do curso de formação da AMAN. Foi procedido o levantamento das possibilidades de utilização do equipamento Harris RF-7800V-HH Rádio Portátil VHF (da família Falcon III), da maneira como elas são ministradas as instruções no Curso de Artilharia da AMAN e da forma que são empregadas pelas frações responsáveis pelas Comunicações nos Grupos de Artilharia de Campanha (GAC). Tal pesquisa fornece subsídios que, além de, possivelmente, melhorar as instruções em um futuro próximo, aumentarão a operacionalidade e a segurança no emprego dos equipamentos rádios durante as diversas missões da Artilharia Brasileira.

O objetivo geral do estudo consiste em obter um conhecimento mais concreto acerca de como o Curso de Artilharia da AMAN, particularmente na parte de comunicações, vem preparando os cadetes, à luz do ensino por competências, para desempenhar a função de Adjunto do Oficial de Comunicações, prevista para oficial subalterno da subunidade.

O fato de que a Instituição deve estar preocupada com o auto-aperfeiçoamento de seus profissionais e deve disponibilizar meios para que eles desenvolvam suas atividades da melhor forma é irrefutável. Este trabalho visa, justamente, fornecer idéias concretas acerca das condições da formação dos futuros oficias, de modo que melhore ainda mais a capacidade destes militares no planejamento e na execução das missões.

2 DESENVOLVIMENTO

2.1 O ENSINO POR COMPETÊNCIAS

O Dicionário Larousse define competência como a "capacidade decorrente do conhecimento que alguém tem sobre um assunto. É a soma de conhecimentos ou habilidades". As competências, segundo RUAS (1998), são formadas por três elementos:

O **conhecimento** - refere-se ao saber. Implica questionamentos e esforços voltados à informação que possa agregar valor ao trabalho. O conhecimento é o que se deve saber para desenvolver com qualidade aquilo que lhe é atribuído (RUAS, 1998).

As **habilidades** - referem-se ao saber fazer. Centraliza-se no desenvolvimento de práticas e consciência da ação tomada. As habilidades são o que se deve saber para obter um bom desempenho (RUAS, 1998).

As **atitudes** - referem-se ao saber agir. Busca um comportamento mais condizente com a realidade desejada. Deve-se saber agir para poder empregar adequadamente os conhecimentos e habilidades (RUAS, 1998). A noção de competência pode ser relacionada a verbos como: mobilizar recursos, integrar saberes múltiplos e complexos, saber aprender, ter visão estratégica, além do mais as competências devem agregar valor econômico para a organização e social para o individuo. (FLEURY E FLEURY, 2006).

A definição de competência abrange diversas idéias, dentre elas o conceito de habilidade, que pode causar certa confusão durante o estudo em questão. Por exemplo, competência é resolver problemas matemáticos, sendo as habilidades para isso saber ler, calcular, interpretar, tomar decisões e registrar por escrito.

As competências englobam uma maior complexidade, pois comportam antecipações, generalizações, inferências, transposições analógicas, além de outras capacidades humanas. Em outras palavras, a competência pode ser entendida como um armazenamento de recursos que, oportunamente são mobilizados de acordo com a situação-problema.

2.1.1 Práticas pedagógicas e os papéis do docente e do discente

O conceito de aprendizagem pode ser simplificado a um grande processo de crescimento (influenciado pelas emoções e afetos) e de intercâmbio com o ambiente, vindo a gerar uma mudança de atitude no indivíduo. Para Fleury e Fleury, (2006: 40), os modelos de aprendizagem estão fundamentados em duas correntes teóricas, o behaviorista e o cognitivista.

Behaviorista – têm como base principal o comportamento, este pode ser observável e mensurável. Pois parte do principio que a análise do comportamento significa o estudo das relações entre eventos estimuladores e respostas, planejar o processo de aprendizagem implica estruturar esse processo passível de observação mensuração e réplica cientifica.

Cognitivista – busca ser mais abrangente do que o modelo anterior, tentando explicar os fenômenos mais complexos, também procura utilizar dados objetivos e subjetivos, levando também em consideração as crenças e as percepções.

Segundo Swieringa e Wierdsma (1992) o processo de aprendizagem organizacional pode ser divida em natural e induzida. A primeira, a forma mais primitiva de aprendizagem, ocorre de maneira informal, tendo como principais técnicas a observação, imitação e repetidas tentativas. Já a segunda, mais conhecida atualmente como treinamento, necessita de uma estrutura formalizada para induzir as pessoas a adquirir, acumular e transferir informações e conhecimentos.

Pode existir uma confusão entre a construção do conhecimento e a adaptação do indivíduo ao meio, sendo talvez a razão da comum associação da noção de competências com o princípio do "aprender a aprender" sem a devida compreensão. Valorizando, assim, indivídu-

os autodidatas em detrimento da aprendizagem pela apreensão dos saberes escolares.

O aluno aparece como o centro do processo de aprendizagem, construtor do conhecimento, sendo o sujeito que questiona, pesquisa, cria e aprende. Ao professor cabe a incumbência de ser o facilitador, orientador e mediador do conhecimento, que fornecerá ao aluno ferramentas para solucionar novas situações-problema.

Segundo o Professor Doutor Gilberto Teixeira (USP), o conteúdo a ser ensinado depende dos conhecimentos do docente, mas a maneira de ensinar dependerá da forma como os discentes aprendem. Ele ainda cita que uma das características mais marcantes do homem, distinguindo-o dos outros animais, é a sua capacidade de educar-se, que é muito mais do que repetir experiência ou conhecimentos.

O problema maior não reside no acúmulo de conhecimentos em si, mas na falta de estratégias e situações que levem os aprendizes a utilizarem esses conceitos em suas vidas. As competências, portanto, não se opõem aos saberes, mas ao mero acúmulo de informações e de pré-requisitos como fim.

2.1.2 Avaliando competências

Propor trabalhos em grupo, como forma de avaliação, desenvolve a capacidade argumentativa e exercitam valores como tolerância e respeito às diferentes opiniões, ou melhor, às diferenças como um todo. A importância de saber ouvir é igual ou até mesmo maior do que a capacidade de argumentar; para ter propriedade para falar de um determinado assunto, é preciso ver, lendo no caso, e ouvir sobre ele (é a maneira como a criança aprende, por exemplo, ao ver e ouvir os adultos a seu redor).

Três tipos de avaliação foram identificados durante a pesquisa:

a) A **avaliação diagnóstica** visa identificar os conhecimentos prévios do aprendiz. Requer que o avaliador saiba observar, analisar, as dificuldades dos alunos, permitindo, assim, a (re) construção da aprendizagem.

b) A **avaliação formativa** visa à inclusão do aluno no processo, resgatando-o se for o caso, respeitando às diferenças e construindo o conhecimento coletivamente.

c) A **avaliação somativa** (cumulativa ou somatória). É aquela que serve para verificar se o conteúdo transmitido realmente foi assimilado.

O processo como um todo deve ser mais formativo, buscando avaliar as competências propostas no perfil do curso e envidando todos os esforços para que todos atinjam as competências almejadas. Para que haja fidedignidade neste processo, é muito importante o professor criar o hábito de registrar fatos, observando nos alunos suas habilidades e atitudes.

2.2 IMPLEMENTAÇÃO DAS COMPETÊNCIAS NO EXÉRCITO BRASILEIRO

Os documentos que respaldam o processo de transformação no ensino do Exército Brasileiro são a Diretriz Geral do Comando do Exército 2011-2014; a Diretriz para o Projeto de Implantação do Ensino por Competências no Exército Brasileiro (Portaria nº 137, de 28FEV12), a Diretriz do Processo de Transformação do Exército Brasileiro (DPTEB), e o Projeto de Implantação do Ensino por Competências a cargo do DECEx.

O objetivo fundamental da formação do novo profissional militar é capacitá-lo para atuar no âmbito das transformações sociais, econômicas, políticas e culturais do século XXI, como constante na Estratégia Nacional de Defesa (END).

O Exército Brasileiro atenta para formação acadêmica e profissional de seus oficias, pois, além de coordenarem ações em situação de guerra, eles representam a Força Terrestre na área social. Embora continue bélico, o conteúdo atenta para o gerenciamento de conflitos e

para a priorização de esforços para a paz.

Inicialmente, as dúvidas emergentes da ordem de adotar a Educação por Competências ficam centradas, com equívoco, nas mudanças a serem realizadas na formatação dos consagrados “currículos por objetivos”.

Uma característica marcante da educação por objetivos é o conhecimento voltado para a prova, que levava o cadete a decorar o conteúdo, ao invés de tentar superar limites. Assim, possuíam tendência ao imediatismo e ao pensamento medíocre de somente enfatizar o que seria cobrado. Eis um paradigma a ser quebrado na sociedade meritocrática.

O Exército Brasileiro é moldado em valores, sendo extremamente dependente deles, fato que também impede a total adoção da sistemática de ensino-aprendizagem baseada nas competências, pois quando o espírito crítico do universitário entrar totalmente na Força, o soldado questionará tudo. A instituição precisa ser opressora em certo ponto e carece de pessoas com valores bem arraigados. A hierarquia deve preceder ao pensamento crítico e, para isso, o tenente deve transparecer confiança para que os subordinados sigam suas ordens com disciplina.

A metodologia de ensino utilizada está relacionada com a Taxonomia dos Objetivos Educacionais, popularmente conhecida como “Taxonomia de Bloom”, que divide as possibilidades da aprendizagem em três grandes domínios: cognitivo, afetivo e psicomotor. Paralelamente a isso, o Departamento Geral de Pessoal (DGP) reúne as diversas competências militares em 03 grupos: Competências Profissionais, Competências Interpessoais e Competências do Espírito Militar.

As Competências Profissionais estão voltadas para a arte da guerra onde, embora também esteja ligada à teoria das estratégias e planejamentos, prevalece o desenvolvimento psicomotor. O modelo mais adequado a ser utilizado nessa situação é o behavorista (teoria comportamental), pois internaliza no militar os movimentos necessários numa situação de combate a serem acionados através do estímulo-resposta.

As Competências Interpessoais, por outro lado, estão voltaram para a interação do militar com os companheiros e, principalmente, com a sociedade. Por ter maior ligação com área cognitiva, elas se desenvolvem de maneira mais eficiente com o modelo cognitivista (teoria cognitiva).

A idéia geral de educação por competências é mais aliada à TEORIA COGNITIVA e, diante do cenário projetado para os militares em 2020 e 2030, complexo e imprevisível, é pertinente priorizar este processo de ensino-aprendizagem. Afinal, ela confere ao discente, além da construção efetiva do conhecimento, o domínio de ferramentas para a solução de problemas diversos.

As competências do Espírito Militar estão estritamente ligadas aos valores a serem desenvolvidos pelos cadetes e, consequentemente, relacionadas também ao domínio afetivo do conhecimento. Dentro dessa perspectiva foram criados os Atributos da Área Afetiva (AAA), que devem ser desenvolvidos nos cadetes e acionados dependendo da atividade.

2.2.1 Práticas pedagógicas e avaliações no ensino militar

Por ser um espaço meritocrático, onde naturalmente existe uma disputa entre os cadetes, o docente militar utiliza atividades com teor competitivo, incluindo premiações, que podem motivar os discentes ao aprendizado.

Elas podem ser analisadas através do conceito do condicionamento operante, onde o reforço visa garantir que o comportamento desejado ocorra novamente, podendo ser positivo, quando há a adição de um estímulo no ambiente que resulte no aumento da freqüência da resposta que o gerou; ou negativo, quando a resposta emitida remove algum estímulo aversivo (elemento punitivo). A punição é muitas vezes confundida com o reforço negativo, pois o ele-

mento punitivo encontra-se inserido neste. Porém, ao contrário do reforço negativo, o objetivo da punição é levar à extinção do comportamento.

Uma idéia extremamente interessante, verificada nos relatos dos instrutores, foi adotada no Curso Básico da AMAN. Consiste no uso dos cadetes do terceiro ou quarto ano como monitores, possibilitando uma maior divisão da quantidade de alunos e conferindo atendimento mais individualizado. Assim, dividindo as instruções para os monitores, todos os discentes terão contato com o material, serão supervisionados mais facilmente e suas dúvidas serão dirimidas.

Além de motivar o cadete mais moderno, que enxerga seu futuro imediato no monitor, é conferida a oportunidade proporcionada ao cadete mais antigo, ainda em formação, de transmitir conhecimento, treinando sua postura e liderança perante os subordinados e, caso necessário, retirar as eventuais dúvidas com o oficial instrutor da matéria.

Observou-se também como boa prática o uso de trechos de filmes ou até mesmo gravações (recursos audiovisuais) para exemplificar a matéria de forma mais elucidativa e contextualizada. Dessa forma, é possível atingir diversos sentidos do instruendo, inclusive o fator emocional, e incutir mais realidade para a instrução. Além disso, o som ajuda a despertar, evitando que o cadete durma.

No ambiente militar persiste, erroneamente, a “cultura do erro zero”, tratada inclusive na página 35 da DPTEB, que incentiva ações metodológicas que encarem o erro como parte da reconstrução do conhecimento, dando espaço para a criatividade e para a persistência.

Geralmente o instruendo aprende mais com os erros do que com os acertos, pois ele fica remoendo a situação para entender o porquê daquela falha. Portanto, é preciso colocar na formação militar o aluno em situações em que ele possa cometer erros sem medo de ser punido.

Na Força Terrestre também são utilizadas como ferramentas as avaliações diagnósticas, formativas e somativas para mensurar o desempenho do cadete, principalmente na parte cognitiva.

Como forma de avaliar a área afetiva, são analisados os diversos registros realizados ao longo do período sobre as atitudes do aluno nas instruções, sua apresentação individual e sua personalidade em geral. Tudo isso irá compor o “conceito” do discente, sendo o formativo divulgado no meio do ano e o somativo, que entra no cálculo da nota final, ao final do ano letivo. Na parte psicomotora temos os Testes de Avaliação Física (TAF) e os Testes da Aptidão de Tiro (TAT).

2.3 COMUNICAÇÕES NA ARTILHARIA: O ADJ O COM, O RÁDIO RF 7800V-HH – FALCON 3 E A APLICABILIDADE DO PLADIS NA TROPA

A Artilharia é uma arma que proporciona o apoio de fogo a grande distância. Para cumprir sua missão, utiliza obuses, canhões, foguetes e mísseis, ocupando posições no terreno a fim de disponibilizar o fogo, destruindo ou neutralizando os alvos que ameacem o êxito da operação.

Os materiais de artilharia de tubo do Brasil possuem um alcance pequeno - em média 10km - comparado com os materiais mais atuais, como os lançadores múltiplos de foguetes, que atingem 40km no sistema Astros II e atingirá 300km com o sistema Astros 2020. Assim, os meios de comunicação precisam acompanhar esse desenvolvimento, tanto em alcance como em defesa contra a guerra eletrônica.

Pela sua versatilidade e rapidez de instalação, o sistema rádio oferece grande flexibilidade para o exercício do comando e controle nas operações. A sua utilização é indispensável nas comunicações entre elementos separados por grandes massas de água, territórios controlados pelo inimigo ou terrenos onde a construção de circuitos fio é impossível ou impraticável.

2.3.2 Adj O Com

A principal função ligada às comunicações que pode ser exercida pelos discentes formados na AMAN é a de Adjunto do Oficial de Comunicações (Adj O Com), sendo o Oficial de Comunicações (O Com) o comandante da Bateria Comando, capitão mais antigo dentre os comandantes de SU. O Adj O Com, também oficial, acaba desencadeando as missões relacionadas às comunicações do GAC sob orientação do capitão.

O Oficial de Comunicações prepara os planos e ordens de comunicações, aciona e supervisiona a instalação, operação e manutenção do sistema de comunicações do GAC, sendo os sargentos da Arma de Comunicações os especialistas do grupo nessa parte. Ele também é o responsável pela segurança desse sistema no âmbito de sua Unidade.

Nas operações, o Adj O Com auxilia o comandante do GAC no estabelecimento e na exploração das comunicações, bem como deverá participar dos reconhecimentos para a montagem do Centro de Comunicações (C Com).

2.3.3 Equipamento Rádio RF 7800V-HH – Falcon 3

O rádio Falcon III (RF-7800V-HH) é um equipamento militar que possui grande resistência às intempéries climáticas e a impactos, desenvolvido para conferir uma transmissão eficaz e, simultaneamente, proteger a informação em questão. Opera entre as freqüências de 30 e 108 MHz (predominantemente na faixa VHF). Os enlaces nessa faixa de freqüência envolvem propagação através da troposfera e das ondas terrestres, necessitando da visada direta. É possível o uso das ondas ionosféricas, até 50 MHz, dependendo do nível de ionização da camada.

Possui os seguintes modos de transmissão: FSK 2,4 kbps FM Analógico, MELP, FSK 16 kbps, FSK/TCM, CVSD e TDMA opcional. A sua potência pode ser ajustada em 0,25W; 2W; 5,0W e 10W. Seu alcance varia entre 8 e 15 km. Na base veicular a potência atinge 50W e o alcance do equipamento aumenta para 45 km. Cabe informar que o equipamento possui regulação automática de potência, evitando a propagação do sinal em distâncias desnecessárias e preservando a vida útil do equipamento.

Possui a Unidade de Teclado e Display Remoto (KDU), que permite operá-lo a certa distância, e GPS interno, que possibilita recebimento e envio de coordenadas. Esse equipamento rádio ainda estabelece comunicação através do recurso Tac Chat, um software que pode ser instalado em qualquer computador e permite estabelecer um chat entre dois ou mais computadores, utilizando o rádio como um roteador.

Com base no Manual de Operações do RF-7800V-HH (2012b), levantou-se as principais e mais significativas tecnologias de Medidas de Proteção Eletrônica do equipamento, que são as seguintes:

a) Antibloqueio (Salto de Frequência)

- O equipamento rádio possui a tecnologia ECCM (Contra-Contra medidas Eletrônicas) Quicklook, que permite a recepção e transmissão no mesmo conjunto ou em conjunto de freqüências diversas, dificultando a monitoração do inimigo.
- As funções disponíveis são a HOPSET e a LOCKSET, sendo HOPSET um conjunto de freqüências pré-determinadas para a transmissão, dentro do qual o rádio faz uma sucessão rápida das frequências, enquanto LOCKSET é uma banda de exclusão, ou seja, configura-se o rádio para que determinada faixa de freqüências não seja utilizada.

b) Codificação de Voz

- O Falcon III (RF-7800V-HH) possui sistemas de codificação de voz para aumentar a segurança das comunicações, evitando que as informações sejam emitidas em claro. São eles: CVSD (Continuously

Variable Slope Delta), que é um processo de digitalização de voz baseado na criptografia; MELP (Mixed-Excitation Linear Predictive), que oferece um áudio de voz digital melhor comparado ao CVSD e um alcance maior comparado ao FM com voz analógica.

c) Criptografia

- Baseada nas tecnologias da Harris Corporation, garante ao usuário uma grande segurança na transmissão de dados, pois uma chave de 128 bits (também é possível criar chaves de 256 bits) demora em torno de 100 anos para ser decifrada e, caso não a possua, o inimigo somente escutará ruídos.

d) Transmissão de dados

> Alta Taxa de Transferência de Dados – O RF-7800V-HH atinge uma taxa de transferência de dados IP de 64kbps em canais com largura de banda de 25 kHz, ou atinge uma taxa de transferência de dados IP de 192 kbps em canais com largura de banda de 75 kHz (Harris Corporations RF Communications Division, 2012b, p.15)

- Esse recurso possibilita que a tropa envie fotos e imagens que sofreram a técnica da estenografia (envio de informações escondidas dentro dos arquivos), por exemplo, ou documentos criptografados por softwares ou hardwares mais eficientes do que os existentes no próprio rádio. É possível enviar uma carta da área de operações para melhor localizar e coordenar o tiro e os elementos da manobra.

- Portanto, a transmissão com o RF-7800V-HH nas Organizações Militares de Artilharia deve ser amplamente difundida para a melhoria do sistema de comando e controle, melhorando assim a qualidade e a segurança das comunicações. Afinal, as mensagens de coordenação do tiro necessitam ser cotejadas e os elementos são enviados um a um, se tornando estereótipos fáceis de serem identificados pelo inimigo.

2.3.4 O ensino da matéria Comunicações no C Art AMAN

Dentro dos diversos documentos que norteiam o planejamento do ensino, a pesquisa irá focar no Plano de Disciplina (PLADIS), documento que o instrutor usa para planejar suas instruções. Os cadetes também têm acesso a este documento, utilizando-o para acompanhar o andamento da matéria e para organizar suas estratégias de estudo.

A matéria Comunicações dentro do Curso de Artilharia da AMAN tem o objetivo de habilitar o futuro oficial à função de Adj O Com, bem como atender algumas competências genéricas como: gerenciar o emprego e a manutenção dos equipamentos e materiais orgânicos das OM; aplicar os fundamentos do sistema operacional comando e controle e; planejar, orientar e avaliar o preparo profissional da tropa no que tange as comunicações.

Por estar diretamente ligada aos meios tecnológicos recentemente adquiridos pelo Exército Brasileiro e fazer parte dos projetos estratégicos de monitoramento de fronteira e transmissão contínua de informações, esta matéria se caracteriza por estar em constante aprimoramento. O PLADIS das Comunicações na Artilharia traz o resquício da doutrina utilizada nas grandes guerras e abre um grande espaço para as novas tendências de exploração do espectro-eletromagnético e da guerra eletrônica.

O meio rádio deve ser muito bem explorado pelo instrutor da matéria, mencionando todas as versatilidades supracitadas visando ensinar ao cadete como estabelecer as comunicações de forma segura e eficiente. Já a parte de rede telefônica com o sistema fio, apesar de conferir uma boa segurança, terá menor destaque, diante do cenário de batalha atual, cada vez mais dinâmico.

Verificou-se que esta matéria compõe uma parte pequena da nota geral de curso, em comparação às demais. Divididas em Avaliações de Acompanhamento (AA) e Avaliações de Controle (AC), sendo que, independente do número de avaliações, as AC têm peso dois na média final da matéria, as matérias Comando de Linha de Fogo e Topografia acabam despertando maior interesse dos discentes devido à complexidade e o maior valor na nota. Portanto, caberá ao instrutor prender a atenção dos cadetes, pois acabam preterindo as Comunicações.

2.3.5 Análise dos resultados do Instrumento de Pesquisa

Quarenta e quatro oficiais de artilharia responderam o instrumento de pesquisa, compondo uma amostra de 36,66% do público alvo, cujas respostas originaram os seguintes resultados:

a) dezessete pessoas afirmaram que, além da palestra, outro tipo de técnica de ensino-aprendizagem foi utilizado, sendo a demonstração do material o exemplo mais recorrente, além de exercícios individuais;

b) a totalidade afirmou que não foram realizados pedidos de cooperação de instrução (PCI) junto ao Curso de Comunicações da AMAN para buscar o conhecimento mais aprofundado no assunto;

c) a grande maioria afirmou que os equipamentos rádios ensinados na AMAN, Motorola e Harris, são os mesmos que mobíliam as Organizações Militares em que servem atualmente;

d) trinta e nove oficiais acreditam que, com a formação da AMAN, não estão efetivamente preparados para exercer a função de Adj O Com. Além disso, pode-se concluir, através dos resultados obtidos, que não foram realizadas no corpo de tropa as capacitações do efetivo profissional no assunto;

e) os oficiais participantes da pesquisa, apesar de não se sentirem aptos para exercer a função, conhecem as principais atribuições do Adj O Com, sabendo descrevê-las sumariamente;

f) a totalidade da amostra afirmou não estar em condições de abordar as influências e possibilidades das novas tendências de Comunicações na Artilharia de Campanha como, por exemplo, configurações de endereço de IP em rádios, saltos de freqüência, modulação digital, rede de computadores e roteamento de dados. Pode-se afirmar também que poucos (somente sete respostas positivas) conhecem as funcionalidades existentes no RF-7800 HH-V (Falcon 3), não sabendo, porém, citar quais seriam úteis para as operações de um GAC.

3 CONCLUSÃO

O constante avante tecnológico é uma das realidades do atual panorama mundial. Poderosos meios de ataque eletrônico, de monitoramento e de captação de informações cruciais estão sendo desenvolvidos e aprimorados. Desta forma, aliar esses materiais de última geração às estruturas bélicas garante a supremacia em relação às demais nações.

Visando proporcionar ao combatente do futuro a capacidade de se adaptar às novas situações e a cenários diversificados, o conceito do Currículo por Competências foi adotado pela Força Terrestre.

Por vezes mal interpretadas, as competências não visam abandonar as disciplinas rumo a uma unificação utópica, mas em realizar situações integradoras mais próximas da realidade, dinamizando o projeto escolar. Além disso, ao serem implementadas no EB, uma instituição estruturada hierarquicamente e cheia de paradigmas, se tornam ainda mais peculiares.

Os resultados encontrados mostram que a função de Adj O Com é simples, porém muito importante para garantir a operacionalidade do GAC. O oficial subalterno que escolhido para o encargo deve ter meticulosidade, zelo com o material e conhecimento técnico para solucionar as eventuais falhas nas trocas de informações.

Embora estejam relacionadas aos equipamentos rádios que realmente mobiliam a maioria dos GAC, as instruções ministradas na AMAN precisam explorar as funcionalidades existentes no material para garantir uma exploração segura. É necessária uma atualização doutrinária que aborde a transmissão de dados em VHF durante as operações, melhorando, assim, a coordenação e o apoio prestado.

Constatou-se que é preciso diversificar o contato do discente com o conteúdo. A palestra, meio usual de transmissão do conhecimento, deve ser aprimorada com meios áudio-visuais e com situações que permitam a participação ativa do discente. Convém também pedir o apoio do Curso de comunicações, tanto de monitores quanto de material.

Diante destes resultados é possível afirmar que o PLADIS analisado contempla os assuntos necessários para uma boa formação, além de aliar a concisão com a flexibilidade. Cabe à equipe de instrução, à luz dos princípios do ensino por competências, estruturar a melhor estratégia de transmissão do conhecimento. A interdisciplinaridade dará mais realidade às situações-problema e o cadete deve ser submetido à função de Adj O Com nos exercícios no terreno.

Portanto, a hipótese da pesquisa foi corroborada, pois existem lacunas na formação dos oficiais de Artilharia da AMAN em relação às comunicações. As instruções ministradas para os cadetes carecem de uma revisão para garantir que o futuro oficial assimile o conteúdo da forma mais eficaz possível. As práticas pedagógicas levantadas realmente fornecerão subsídios para suspender o subemprego do equipamento disponível e buscar a evolução nos procedimentos de exploração das comunicações.

THE CURRICULUM REGARDING COMMUNICATIONS IN AMAN'S ARTILLERY COURSE AND ITS APPLICABILITY ON HEADQUARTERS

ABSTRACT: This research deals with the curriculum regarding communications in the Military Academy of Agulhas Negras (AMAN)'s artillery course and its applicability in the Field. The communications subsystem in artillery is essential to interconnect all the posts involved in the preparation and conduct of shots and in coordination with the elements supported. With the objective of obtaining a more concrete prior knowledge, the analysis of the education by competences and the possibility of using the equipment RF-7800V-HH (Harris Falcon III), used as a parameter to have been recently acquired by the Brazilian Army And for furnishing the vast majority of GACs. Subsequently, the research related the theory to the results obtained through the opinion of the newly formed officers of the AMAN, dealing with their training, preparation in the communications section and knowledge of the material analyzed. It was verified, therefore, that the methods used need to be reformulated and, for this, subsidies were raised that, besides improving the learning of the future leaders of the Brazilian Army, will increase the operability and security in the use of radios equipment during the missions of the Artillery.

Key words: Comunications on Artillery, Radio Falcon 3, Teaching by Skills, AMAN.

REFERÊNCIAS

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Plano de disciplina/Plano integrado de disciplina**: 2º e 3º ano do Curso de Artilharia. Resende, 2015.

BRASIL. Estado-Maior do Exército. C 6-1 EMPREGO DE ARTILHARIA DE CAMPANHA. Manual de campanha. 3. Ed. Brasília: EGGCF, 1997.

_____. C 6-20 GRUPO DE ARTILHARIA DE CAMPANHA. Manual de campanha. 4. Ed. Brasília:EGGCF, 1998.

_____. C 11-06 AS COMUNICAÇÕES NA ARTILHA-

RIA DE CAMPANHA. Manual de campanha. 2ª ed. EGG-CF - Brasília, 1995.

_____. T 21-250 MANUAL DO INSTRUTOR. Manual Técnico. 3ª edição. Brasília, 1997.

BRASIL. Ministério da Defesa. Exército Brasileiro. Departamento de Educação e Cultura do Exército. Portaria Nº. 80, de 07 de agosto de 2013. Instruções reguladoras do ensino por competências: currículo e avaliação. (IREC-E-B60-IR-05.008).

EXÉRCITO BRASILEIRO. Implantação da Educação Por Competências na Formação de Oficiais da Linha de Ensino Bélica, Rio de Janeiro CEP/FDC, 2011.

FLEURY, A.; FLEURY, M. T. L. **Estratégias empresariais e formação de competências**: um quebra cabeça caleidoscópio da indústria brasileira. Ed. atlas 3ª ed. São Paulo, 2006.

LISBÔA, Cristopher Pinto. **As comunicações na Artilharia de Campanha**. Brasília-DF: EsCom, 2014. 34 p, il.

MACEDO, L. **Competências e habilidades**: Elementos para uma reflexão pedagógica. In: J. S. Moraes. (Org.). Exame Nacional do Ensino Médio (ENEM): Fundamentação teórico-metodológica. Brasília: O Instituto (INEP/MEC), 2005.

MELCHIOR, Maria Celina. **Da avaliação dos saberes à construção de competências.** Porto Alegre: Premier, 2003. 180p

PERRENOUD, Philippe et al. **As Competências para Ensinar no Século XXI**: A formação dos professores e o desafio da avaliação. Porto Alegre: Artmed, 2002.176p.

_____. **Dez novas competências para ensinar**. Porto Alegre: Artes Médicas, 2000.

RÁDIO VHF PORTÁTIL RF-7800V-HH, Manual de Operação. Harris Corporation RF Communication Division. Rochester, New York, 2012.

RF COMMUNICATIONS, Harris. Especificações para o RF-7800V-HH. Disponível em: < http://rf.harris.com/media/RF-7800V-HH_Portuguese_web_tcm26- 13772.pdf>. Acesso em 02/05/2017.

RUAS, R. A. **Módulo**: Consolidação, Aplicação e Apropriação do Treinamento. SEBRAE/RS, CEPA/UFRGS, NADE, dezembro de 1998.

SWIERINGA, J.; WIERDSMA, A. **La Organización que Aprende**. Buenos Aires: 1992.

ATAQUES DE ENGENHARIA SOCIAL: MEDIDAS PREVENTIVAS PARA A SEGURANÇA DA INFORMAÇÃO.

Matheus Murari Azzolin
Pós-graduado, Lato Sensu, de Especialização em Comunicações

RESUMO: A presente pesquisa científica tem como tema os ataques de engenharia social contra as Organizações Militares e seus militares. O trabalho tem o objetivo de levantar as medidas preventivas (para elaboração de uma política de segurança da informação) capazes de evitar ataques de engenharia social contra as Organizações do Exército Brasileiro e os militares que nelas servem. Para que fosse possível levantar tais medidas preventivas, foi realizado um trabalho de pesquisa bibliográfica acerca das ameaças de engenharia social e principais vulnerabilidades das OM. Também foi necessário um estudo sobre política de segurança da informação, com a finalidade de selecionar melhores ações, diretrizes e normas capazes de evitar ataques dessa natureza. Como resultado, o trabalho científico mostra quais as medidas preventivas devem ser consideradas para a correta segurança do ativo de informação em relação à engenharia social. Ao fim, expõe como essas medidas devem ser abordadas para a melhor conscientização do público interno e apresenta outras características indispensáveis a uma política de segurança da informação. O conteúdo apresentado torna a pesquisa relevante, ao contribuir para sintetizar medidas preventivas de ataques de engenharia social, voltadas especificamente, para o meio militar e colaborar assim, para a melhoria das políticas de conscientização dos militares e proteção das informações.

Palavras-Chave: Medidas Preventivas. Engenharia Social. Política de Segurança da Informação.

1 INTRODUÇÃO

A cibernética segundo o dicionário Michaelis (2017) é a "ciência cujo objeto de estudo concentra-se na comparação dos sistemas e mecanismos de controle automático, bem como na regulação e comunicação não só nos seres vivos, porém também nas máquinas".

Dentro do campo extenso da cibernética, o presente estudo se concentra nas ameaças de engenharia social contra as Organizações Militares (OM) do Exército Brasileiro (EB). O tema explora a importância de se considerar medidas para prevenir ataques de engenharia social contra OM e seus militares em uma Política de Segurança da Informação (PSI).

A ocorrência de crimes digitais vem aumentando muito, principalmente na última década. Reflexo da evolução constantes das tecnologias e da maior quantidade de máquinas e redes presentes em instituições que dependem cada vez mais do emprego desses meios para sobreviver.

Portanto, é necessário que as medidas de segurança se tornem, cada vez mais, parte da rotina dos funcionários de uma instituição que busca a salvaguarda dos seus dados:

> Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus e worms, que são cada vez mais sofisticados. Utilizando técnicas que incluem a engenharia social, [...] os ataques visam a contaminação e a disseminação rápida, além do uso das vítimas como origem para novos ataques (NAKAMURA E GEUS, 2007, p. 27).

Ataques de engenharia social são lançados na tentativa de obter informações para a prática de crimes contras as instituições ou seus funcionários.

Por isso, o artigo tem a seguinte hipótese: as medidas preventivas para evitar ataques de engenharia social às OM e seus militares são indispensáveis em uma Política de Segurança

da Informação (PSI).

A pesquisa buscou levantar as medidas preventivas que visam impedir tanto a obtenção de dados e informações das OM (sejam elas do viés operacional, administrativo ou da segurança orgânica), quanto o vazamento de informações que tornem os militares e suas famílias vulneráveis a ataques de engenharia social.

O artigo se justifica por levantar as medidas preventivas de ataques de engenharia social, voltadas especificamente, para o meio militar, colaborando para a melhoria das políticas de segurança da informação das OM.

1.1 OBJETIVOS

O objetivo geral é levantar quais são as medidas a serem consideras para a elaboração de uma política de segurança da informação a fim de evitar ataques de engenharia social contra as OM e seus militares.

Foram formulados os seguintes objetivos específicos:

a) descrever o que é engenharia social e como ocorre um ataque;

b) descrever o que é uma política de segurança da informação;

c) elencar e descrever quais são as principais ameaças de engenharia social às OM;

d) elencar as medidas que devem ser consideradas para a elaboração de uma política de segurança da informação.

1.2 PROCEDIMENTOS METODOLÓGICOS

Ao apresentar medidas preventivas para elaborar uma política de segurança da informação a fim de impedir ataques de engenharia social este artigo busca soluções práticas para problemas concretos. Portanto, em relação à natureza, ele pode ser classificado como uma pesquisa aplicada e de abordagem qualitativa.

Por ter sua execução pautada na obtenção de informações já existentes em outros documentos, publicações, artigos e reportagens, o presente artigo é classificado como uma pesquisa bibliográfica.

Para o subsídio bibliográfico as fontes de consulta selecionadas foram de instituições públicas e privadas que possuem atividades voltadas ao combate à engenharia social e elaboração de políticas de segurança da informação. Foram consideradas fontes de especialistas no assunto, documentários, reportagens e documentos relacionados ao tema.

O desencadeamento lógico do desenvolvimento pretende abordar os tópicos previamente definidos nos capítulos:

a) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - define o que é uma política de segurança da informação;

b) ENGENHARIA SOCIAL – descreve de forma pormenorizada o entendimento sobre a engenharia social e as ameaças às OM;

c) MEDIDAS PREVENTIVAS – esse capítulo apresenta as medidas preventivas contra ataques de engenharia social às OM e seus militares.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

2.1 INFORMAÇÃO

Para esta pesquisa considerou-se a seguinte definição de Raphael Mandarino (2009): “Infraestrutura Crítica da Informação é o subconjunto dos ativos de informação que afetem diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade”.

Ou seja, os ativos de informação podem ser definidos como todas as informações que de posse de alguém mal intencionado possam afetar as missões de uma OM e a segurança dos militares que trabalham nesse local.

2.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para Fontes (2006) segurança da informação "é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada".

Uma PSI é importante, pois, segundo Nakamura e Geus (2007, p.27) "[...] quando o profissional não conhece os riscos, ele tende a achar que tudo está seguro com o ambiente. Com isso, a organização passa, na realidade, a correr riscos ainda maiores, que é o resultado da negligência".

De acordo com Nakamura e Geus (2007, p.73) "[...] os aspectos humanos, sociais e pessoais não podem ser esquecidos na definição da estratégia de segurança". É justamente esse aspecto humano que dá origem aos ataques de engenharia social, que se aproveitam da má gestão da informação e fragilidades dos funcionários para causar diversos danos às organizações e, principalmente, às pessoas que fazem parte delas.

Por isso, é extremamente necessário que uma PSI contemple as medidas preventivas contra engenharia social.

3 ENGENHARIA SOCIAL

3.1 DEFINIÇÕES

Existem diversas técnicas para a obtenção de informações e invasão de sistemas. Umas das mais utilizadas é a engenharia social:

> A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança (NAKAMURA E GEUS, 2007).

De acordo com Assunção (2011, p. 30), entre os fatores que tornam as redes inseguras o fator humano, justo o não técnico, é o pior deles:

> Através de técnicas de Engenharia Social, a manipulação do fator humano causa enormes desastres como: fazer um usuário rodar um cavalo de tróia sem saber, conseguir informações privilegiadas sobre empresas, obter especificações de um novo produto, etc. [...] (ASSUNÇÃO, 2011, p. 31).

De acordo com a definição de Nakamura e Geus, a engenharia social visa também, por meio da manipulação "quebrar procedimentos de segurança". É possível inferir que se trata de sua utilização para abrir brechas nos sistemas e obter a informação por meio de outras ferramentas, como a instalação de vírus:

> O fato mais recente envolvendo a engenharia social é sua ampla utilização em busca de um maior poder de disseminação de vírus. Procurando ludibriar os usuários para que abrissem arquivos anexados, vírus como o I Love You, Anna Kournikova e Sircam espalharam-se rapidamente pelo mundo (NAKAMURA E GEUS, 2007, p. 86).

A engenharia social também é utilizada quando a obtenção da informação só pode ser feita por meio do contato pessoal (como por exemplo, a rotina da OM ou horário de saída de uma viatura) ou de forma física (informações que não se encontram em bancos de dados virtuais, somente em pastas e arquivos físicos).

3.2 ATAQUES DE ENGENHARIA SOCIAL

3.2.1 Engenheiros sociais

O engenheiro social utiliza os sentimentos para manipular as pessoas e obter a informação que deseja. Porém, isso não significa que ele não tem conhecimento na área de cibernética, mas sim que ele apenas utiliza a engenharia social como uma de suas várias ferramentas para conquistar seus objetivos (NAKAMURA E GEUS, 2007, p. 85).

Os engenheiros sociais podem ter diversos motivos para realizarem um ataque. Normalmente tem a intenção de realizar ações para obter vantagens financeiras por meio de crimes, como o estelionato e furto. Porém, podem existir outras motivações, tais como, o sentimento de vingança contra algum militar ou contra a instituição, autoafirmação ou até mesmo vandalismo cibernético.

Entre todos os tipos de engenheiros sociais, os que mais preocupam são os pertencentes ao público interno, pois "[...] os ataques que vêm causando os maiores problemas para as organizações são aqueles que acontecem a partir da sua própria rede, ou seja, os ataques internos" (NAKAMURA E GEUS, 2007, p.28).

O público interno consiste em todas as pessoas que trabalham na OM, como os militares, funcionários civis e cessionários que prestam serviços no interior da OM. Essas pessoas têm uma vantagem muito importante que é a confiança daqueles que fazem parte da instituição. Além disso, conhecem a OM, seu organograma, a rotina, as instalações e detalhes específicos do serviço e das operações realizadas.

3.2.2 Meios e técnicas utilizadas

Os ataques de engenharia podem ser feitos por vários meios, entre eles o e-mail, o telefone, os CD/pendrives infectados com vírus e as redes sociais.

Entre as técnicas utilizadas estão: a observação, vasculhar o ambiente de trabalho, se passar por outras pessoas, usando a persuasão e realizar conversas aparentemente "inocentes" com militares das OM.

Muitas vezes uma ação de engenharia social é associada a outras técnicas para a obtenção de informação como, por exemplo, o trashing (revirar o lixo) e Captura de Informações Livre. Quando combinadas, essas técnicas podem causar problemas sérios às instituições atacadas, pois as informações obtidas por diferentes meios são cruzadas e dão origem a dados mais relevantes.

Independente do meio ou técnica utilizada, as principais características exploradas por um engenheiro social em relação ao fator humano são: reciprocidade, consistência, busca por aprovação social, simpatia, autoridade e medo (NAKAMURA E GEUS, 2007, p. 85). Ainda, segundo Assunção (2011, p.150) "os engenheiros sociais utilizam os sentimentos para manipulação e os casos mais comuns são: curiosidade, confiança, simpatia, culpa e medo".

3.2.2.1 E-mail

O e-mail é uma das ferramentas mais utilizadas por um engenheiro social devido à grande capilaridade que possui. As técnicas utilizadas para ataques por e-mail também podem ser aplicadas em outros meios como mensagens de telefone celular, aplicativos de relacionamento social e até mesmo correspondência física.

Uma técnica muito comum é a do e-mail com remetente falso, na qual o engenheiro social utiliza programas que podem gerar e-mails com endereço de remetentes que realmente existem, assim faz com que a vítima acredite que está recebendo uma mensagem de alguém confiável.

Outra técnica é a do e-mail manipulativo, em que a mensagem possui um conteúdo que pretende explorar a curiosidade ou ganância do militar. Normalmente, a mensagem trata de assuntos como "você ganhou 10 mil reais" ou "fotos comprometedoras que vazaram". O destinatário é levado a acessar os anexos, um link ou mandar informações para receber o tal prêmio e assim se torna mais uma vítima.

3.2.2.2 Hardware infectado

Ao aproveitar-se da confiança dos demais militares no ambiente de trabalho, um engenheiro social pode ter acesso a uma máquina e, por meio dos dispositivos ou de algum tipo de malware, conseguir extrair informações dos computadores e dos sistemas.

Também pode ser utilizado por engenheiros sociais externos às OM. Basta o atacante largar um hardware infectado em um local de

circulação dos militares da OM. Provavelmente este material será levado para a OM e infectará uma máquina.

3.2.2.3 Redes sociais

É por meio das redes sociais que um engenheiro social pode obter facilmente inúmeras informações sobre os militares, suas família e a OM.

A rede social pode ser utilizada para realizar ataques parecidos com os realizados por e-mails, com troca de mensagens em diálogos manipulativos que fazem com que a vítima forneça as informações desejadas; ou para a coleta de informações livres, onde o engenheiro social explora os perfis dos usuários em busca de informações como endereço, nomes, parentescos, profissão, local de trabalho, e-mail e telefone da vítima.

Além disso, criar um perfil falso em uma rede social como, por exemplo, o Facebook e o Whatsapp é muito fácil. Com algumas fotos já é possível criar um perfil e adicionar pessoas à sua conta. Assim, um engenheiro social pode se passar por um conhecido ou parente e solicitar informações que só seriam fornecidas a pessoas de confiança.

3.2.2.4 Telefone

O telefone é uma ferramenta muito utilizada. Com poucas informações o engenheiro consegue manter um diálogo que, por meio da manipulação dos sentimentos da vítima, o levará ao informe desejado. Não é uma técnica tão fácil, pois exige frieza e astúcia do engenheiro. Porém, quando bem utilizada, pode gerar vários problemas para uma instituição, sem oferecer grandes riscos ou gastos a quem realiza o ataque.

3.2.2.5 Ataques presenciais (personificação)

Um ataque clássico de engenharia social consiste em se fazer passar por um alto funcionário que tem problemas urgentes de acesso ao sistema. O hacker, assim, é como um ator, que, no papel que está representando, ataca o elo mais fraco da segurança de uma organização, que é o ser humano. (NAKAMURA E GEUS, 2007, p.85).

Acima temos um exemplo clássico de engenharia social, na qual um atacante se passa por um militar, conhecido/parente de algum militar, fornecedor, ou qualquer outro papel que lhe sirva. Deste modo, ele acaba obtendo acesso ao local ou consegue informações sobre a OM. A partir daí pode explorar o ambiente e outras vulnerabilidades.

3.2.2.6 Explorando o ambiente

Explorar o ambiente interno de uma OM é a única forma de obter informações que não se encontram disponíveis nos meios virtuais, como, por exemplo, plano de chamada. Outras informações podem ser obtidas ao se explorar o ambiente, como senha, logins e documentos deixados sobre as mesas de trabalho ou salvas nos computadores.

3.3 RISCOS ÀS OM E SEUS MILITARES

Uma vulnerabilidade presente nas OM é o fato de que grande parte dos militares oriundos do serviço militar obrigatório não tem nenhuma qualificação e possuem um baixo nível de escolaridade. Mesmo assim, muitos desses acabam trabalhando na operação de diversos sistemas dentro do quartel e têm acessos a diversas informações. Desconhecendo a importância que essas informações têm, eles podem se tornar vítimas ou deixar a instituição vulnerável.

Além disso, o compartilhamento dos computadores existentes, e o uso de equipamentos particulares, como pendrive e notebooks são práticas comuns, porque muitas OM sofrem com a falta desse tipo de material. Isso faz com que qualquer OM seja um alvo fácil para a instalação de vírus que pode comprometer os sistemas, extrair armazenar senhas e acessar bancos de dados.

Soma-se a tudo isso o fato de que o militar tende a confiar em todos aqueles que o cer-

cam no ambiente de trabalho. Porém, isso não é o ideal para uma instituição que pretende manter o ambiente de trabalho com boas práticas de segurança da informação, pois a confiança é um dos principais sentimentos explorados pelos engenheiros sociais.

4 MEDIDAS PREVENTIVAS

As medidas preventivas consideradas neste capítulo, compreendidas nos quadros de 1 a 5, têm como objetivo evitar os ataques de engenharia social contra as OM e seus militares.

QUADRO 1 - Ataques por e-mail (e similares)

TÉCNICA	MEDIDA PREVENTIVA
E-mail falso ou manipulativo	Desconfie sempre de mensagens de instituições financeiras, de ofertas imperdíveis, prêmios de promoções e mensagens com conteúdo do tipo "fotos comprometedoras".
	Evite fornecer informações sigilosas, mesmo para usuários de confiança.
	Mensagens de conhecidos nem sempre são confiáveis (o campo de remetente do e-mail pode ter sido falsificado, ou podem ter sido enviadas de contas falsas ou invadidas. (CERT.BR, 2017).
	Utilizar exclusivamente o correio eletrônico corporativo para troca de mensagens relativas ao serviço. (DCT, 2011).
	Não clicar em links ou abrir arquivos recebidos por e-mail, a menos que se tenha absoluta certeza da origem e integridade do mesmo. Ter em mente que um arquivo enviado por uma pessoa de confiança pode não ter sido realmente enviado por ela. (DCT, 2011).
	Não utilizar a conta de correio corporativo funcional em cadastros de sítios na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo, Hotmail, etc) para esta finalidade.

Fonte: AZZOLIN, 2017.

QUADRO 2 - Ataques por telefone (ou qualquer meio VoIP)

TÉCNICA	MEDIDAS PREVENTIVAS
Coleta de informações livres	Os atendes devem evitar se identificar de imediato ao atender a ligação.
Persuasão	Sempre confirmar a veracidade de informações recebidas
	Não fornecer/confirmar informações que não dizem respeito ao seu trabalho dentro da OM ou quando não se tem certeza de quem está do outro lado da linha.

Fonte: AZZOLIN, 2017.

QUADRO 3 - Redes Sociais

TÉCNICA	MEDIDAS PREVENTIVAS
Coleta de informações livres	Manter suas contas com configurações de privacidade mais restritas possíveis (evitar a configuração pública).
	Evitar expor informações pessoais como telefone, e-mail, endereço e até mesmo as relações familiares existentes com outros usuários.
	Desconfiar de perfis desconhecidos que solicitam permissão para se tornar "amigo" nas redes sociais.

TÉCNICA	MEDIDAS PREVENTIVAS
Persuasão	Evitar diálogos com perfis desconhecidos que exponham informações pessoais ou relacionadas com o trabalho em “chats” das diversas redes sociais existentes.
	Desconfie também de perfis de conhecidos solicitando informações (contas podem ser falsificadas facilmente).

Fonte: AZZOLIN, 2017.

QUADRO 4 - Ataques físicos

TÉCNICA	MEDIDAS PREVENTIVAS
Vasculhamento das instalações	Nunca deixar documentos sigilosos sobre as mesas ou de fácil acesso, assim como senha e login expostos.
	O controle de entrada e saída de pessoas pela guarda deve ser criterioso.
instalações	Pessoal externo à OM deve andar sempre acompanhado por um militar.
	Evite digitar senhas na presença de outras pessoas.
Persuasão	Exigir a apresentação do documento de identidade militar.
	Não forneça informações a recém conhecidos.
Acesso a máquinas/sistemas	Senhas e login de usuários não devem estar expostas.
	Evitar deixar senhas e login salvos nos navegadores, pois as senhas podem ser facilmente obtidas com recursos básicos de informática.
	Executar rigoroso controle das máquinas e dos usuários que podem ter acesso à rede de computadores da OM. Não permitir que máquinas de visitantes sejam conectadas à rede local. (DCT, 2011).
	Não possua senhas “universais” (iguais para todos os sistemas).
	Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. (DCT, 2011).
	Os cadastros de usuários que acessam os sistemas devem ser mantidos atualizados e supervisionados pela contrainteligência da OM. (DCT, 2011).
	Estabelecer uma política clara e supervisionada relativa ao descredenciamento de usuários que tenham sido transferidos de OM ou de função. (DCT, 2011).
Vasculhamento do lixo	Não jogue fora documentos com informações sigilosas. Separe e elimine de forma eficiente.

Fonte: AZZOLIN, 2017.

QUADRO 5 - Controle de Hardwares

TÉCNICA	MEDIDAS PREVENTIVAS
Instalação de vírus por meio de hardwares infectados	Proibir a utilização de dispositivos móveis de armazenamento (pendrives, HD externos ou cartões de memória), particularmente em ambientes onde operam máquinas com dados sensíveis. Quando absolutamente necessário, liberar o acesso de tais dispositivos, sob supervisão. (DCT, 2011).
	Configurar o antivírus para verificar automaticamente todos os dispositivos de armazenamento removíveis (CD, DVD, pendrive, cartão de memória, HD externo etc.) conectados ao computador. (DCT, 2011).

Fonte: AZZOLIN, 2017.

É importante que haja em cada OM uma política para a restrição de circulação dos próprios militares dentro das repartições administrativas. Acreditar que o ambiente militar é sempre seguro e confiável é um dos erros mais cometidos por possíveis vítimas.

Todos os ataques e situações suspeitas

devem ser reportados à Seção de Inteligência da OM, para que seja repassado aos militares interessados e ao pessoal de serviço, a fim de evitar outros ataques.

5 CONCLUSÃO

As medidas preventivas apresentadas nessa pesquisa científica têm como objetivo evitar que militares e instituições do EB sofram danos causados por ações de engenharia social. Dessa forma, essa pesquisa visa ajudar na confecção de uma PSI quando o assunto considerado for a engenharia social.

Porém, essas medidas são apenas uma parte do que deve haver em uma PSI, pois ela abrange muitos outros aspectos de segurança da informação relacionados à cibernética, instalações físicas e gestão de recursos humanos.

Essa correta gestão da segurança da informação pode mitigar a prática de crimes cibernéticos preservando a segurança orgânica da OM e a integridade dos militares, melhorando a imagem e credibilidade das instituições.

Isso cresce de importância, à medida que os crimes cibernéticos estão se tornando cada vez mais comuns. Tanto contra instituições, quanto contra pessoas. Por isso, as:

> [...] políticas de segurança das informações não podem ser inflexíveis. Uma empresa precisa mudar à medida que surgem novas tecnologias de segurança, e à medida que as vulnerabilidades de segurança evoluem, as políticas precisam ser modificadas ou suplementadas (FONSECA, 2009, p. 06).

Portanto, o assunto não se esgota aqui. É necessário sempre atualizar a PSI e as medidas preventivas quanto aos novos tipos e ataques e ameaças que surgirem.

Em relação à segurança do aquartelamento é possível considerar que “seria um grande erro focar só no lado físico da coisa, o treinamento dos empregados é essencial” (ASSUNÇÃO, 2011, p. 164). Portanto, instruções com a finalidade de apresentar os novos tipos de ataques aos militares da OM devem ocorrer com frequência.

Todas as pessoas de uma empresa que lidam com informações importantes devem passar por um treinamento no qual irão aprender a identificar os tipos de ataque e como reagir a cada um deles (ASSUNÇÃO, 2011, p. 164). Isso deve ocorrer sempre que alguém assumir uma função que demanda maior cuidado com as informações.

Porém, a simples realização de um programa de conscientização não é o suficiente. É necessário que haja fiscalização em todos os níveis e de todos os procedimentos. Os militares devem ser alertados dos perigos constantemente e corrigidos (inclusive dentro do aspecto disciplinar) ao executarem algum procedimento incorreto. Para a fiscalização, podemos considerar o seguinte:

> [...] testes periódicos de penetração e avaliações de vulnerabilidade que usamos métodos e as táticas da engenharia social devem ser conduzidos para expor os pontos fracos do treinamento ou a falta de cumprimento das políticas e dos procedimentos da empresa (FONSECA, 2009, p. 06).

Diante de tudo que foi apresentado, é inegável que a defesa cibernética, seja ela no nível tático ou estratégico, merece cada vez mais atenção dos órgãos e competentes, assim como do comando de cada OM.

É imperativo que, em todos os níveis, exista conscientização e preparo para agir perante os mais diversos tipos de ataque, negando sempre que possível, a obtenção de informações por organizações criminosas ou pessoas isoladas. Tudo isso para que o EB possa dar continuidade ao seu trabalho como Instituição permanente das Forças Armadas.

SOCIAL ENGINEERING ATTACKS: PREVENTIVE MEASURES FOR INFORMATION SECURITY

ABSTRACT. The present scientific research has as its theme the social engineering attacks

on the OM and its military. The aim of the work is to raise the preventive measures (to elaborate an information security policy) capable of avoiding social engineering attacks against the Brazilian Army Organizations and the military that serve them. In order to be able to raise such preventive measures, a bibliographical research was carried out about the social engineering threats and main vulnerabilities of OM. A study on information security policy was also necessary, in order to select better actions, guidelines and standards capable of avoiding attacks of this nature. As a result, the scientific work shows what preventive measures should be considered for the correct safety of the information asset in relation to social engineering. Finally, the research explains how these measures should be approached for the better awareness of the internal public and presents other characteristics indispensable to an information security policy, so that it fulfills its purpose. The content presented makes the research relevant by helping to synthesize preventive measures of social engineering attacks directed specifically to the military environment and to collaborate in this way to improve the policies of military awareness and protection of information.

Keywords: Precautionary Measures. Social Engineering. Information Security Policy.

REFERÊNCIAS

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. 4. ed. Florianópolis: Visual Books, 2011.

BRASIL. Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações. 1. Ed. 09f. [S.l.]: Departamento de Ciência e Tecnologia, 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de segurança para internet. [S.l.]: 2017. Disponível em: <https://cartilha.cert.br/golpes/>. Acesso em: 15 maio 2017.

CRESPO, Marcelo Xavier De Freitas. **Crimes Digitais**. 1. ed. São Paulo: Saraiva, 2011.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação**: O Fator Humano. 16f. Artigo Científico. Curitiba: Pontifícia Universidade Católica do Paraná, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acesso em: 15 maio 2017.

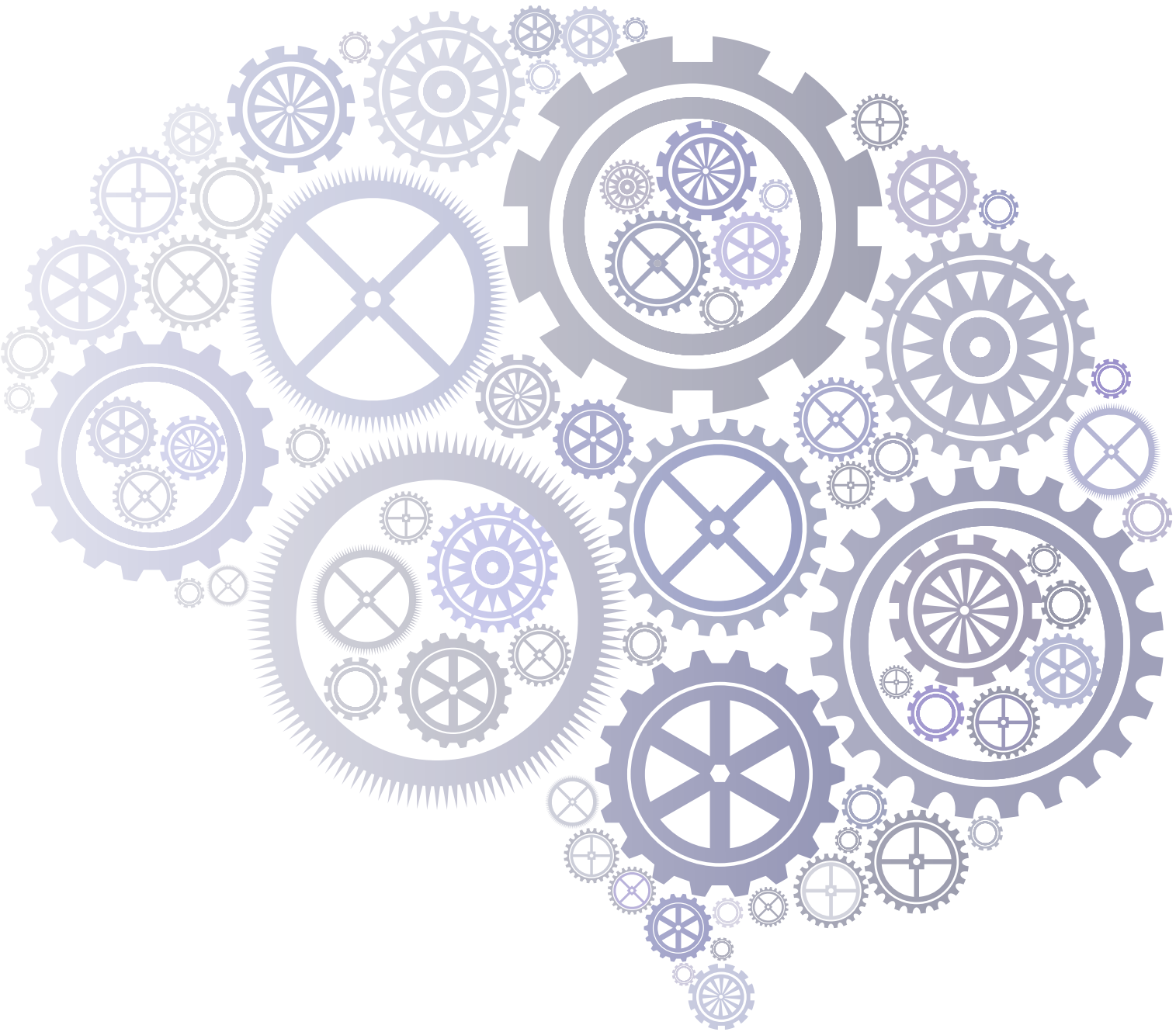
FONTES, Edison. **Segurança da Informação: o usuário faz a diferença**. 1. ed. São Paulo: Saraiva, 2006.

MANDARINO, Raphael. **Um estudo sobre a segurança do espaço cibernético brasileiro**. Brasília: Cubzac, 2009.

MICHAELIS. **Significado da palavra cibernética**. [S.l.]: 2017. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=cibernetica>. Acesso em: 18 maio 2017.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Licio. **Segurança de redes em ambientes cooperativos**. 1. ed. São Paulo: Novatec, 2007.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras - AMAN, pós-graduado, Lato Sensu, em em Oficial de Comunicações pela EsCom e pode ser contactado pelo e-mail matheusmurari@hotmail.com.



Endereço

Estrada Parque do Contorno, Rodovia DF - 001, KM 5
Setor Habitacional Taquari - Lago Norte - Brasília - DF
CEP: 71559-902
Telefone: (0xx61) 3415-3742
(PABX) 3415-3131 (Voz/Fax)
Sitio: www.escom.ensino.eb.br