A CONTRAINTELIGÊNCIA COMO INDUTORA DA SEGURANÇA ORGÂNICA DAS UNIDADES DO EXÉRCITO BRASILEIRO

RODRIGO ALMEIDA **BRITES**[1]

1. INTRODUÇÃO

A rápida evolução experimentada por novas tecnologias, observada a partir da metade do século passado, trouxe a internet e novas formas de interação entre os diversos países. Graças a "facilidade" atual de acesso a essas novas tecnologias, fator que aumenta exponencialmente a "intercomunicabilidade" entre as pessoas do mundo todo, verificamos o surgimento da Era do Conhecimento.

Tal cenário, sem questionar os inúmeros benefícios oriundos da agilidade do processo decisório e pela circulação da informação em tempo real, contraditoriamente, torna o ser humano e as instituições vulneráveis à novas ameaças, podendo atingir as Forças Armadas e em especial o Exército Brasileiro (EB).

A palavra Proteção sempre esteve no rol das mais importantes em um planejamento de Segurança Orgânica, sendo a Contrainteligência (C Intlg) responsável por isso. Em todas as Organizações Militares (OM) do EB existe militares trabalhando com afinco, a fim de evitar ações perpetradas pelas ameaças, no intuito de manter sempre as OM em níveis de segurança adequados.

Algumas normas e diretrizes têm sido produzidas no intuito de mitigar ou até neutralizar danos e riscos à Instituição. Como exemplo, podemos citar a Caderneta de Prevenção de Acidentes na Instrução, a normatização de funções do Oficial de Prevenção de Acidentes, as diretrizes de Gestão e Gerenciamento de Riscos e a Cartilha de Prevenção ao Suicídio, tudo isso com a finalidade de salvaguardar os ativos do Exército (recursos humanos, informação, material e áreas e instalações).

O Sistema de Inteligência do Exército (SIEx), em consonância com os esforços de atualização doutrinária da Força Terrestre, em 2018, realizou o aperfeiçoamento do Manual de Contrainteligência (em aprovação) apresentando os processos, as medidas e as ações de Segurança Orgânica ou Ativa, bem como o passo a passo para o Planejamento de Contrainteligência.

Segundo esse novo manual, as conjunturas nacional e internacional são afetadas pelas mais diversas ameaças, ou seja, existem os mais variados atores, motivados e com capacidade de realizar ação hostil, que exploram as deficiências existentes e, com isso, podem comprometer a Força.

O EB é uma instituição que pode ser alvo desses atores hostis. Em decorrência disso, é necessário estar alerta para facilitar a percepção dos estímulos externos, fundamentais para a tomada de decisão e para a manutenção de níveis satisfatórios de segurança.

Baseado nesses conceitos e com a intenção de categorizar a Contrainteligência como um reforço para a segurança dos ativos de todas as organizações militares do EB, esse trabalho busca definir os principais conceitos da Segurança Orgânica e descreve, de forma prática, o papel do Planejamento de Contrainteligência como forma de melhorar a segurança das nossas unidades.

2. DESENVOLVIMENTO

2.1 CONTRAINTELIGÊNCIA NO EXÉRCITO BRASILEIRO

A ABNT NBR ISO/IEC 27002:2013 na sua introdução, afirma que o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas obrigações funcionais, são informações que, como outros ativos importantes, têm

1. Oficial de Infantaria do Exército Brasileiro; Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras; Pós-graduado em Operações Militares pela Escola de Aperfeiçoamento de Oficiais; Especialista em Operações de Inteligência e Pós-graduado em Gestão de Organizações de Inteligência pela Escola de Inteligência Militar do Exército.

valor para a organização e, consequentemente, requerem proteção contra vários riscos.

As OM coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, o físico e o verbal. Em virtude disso, são alvos em potencial de ações criminosas ou atores hostís, geralmente objetivando subtrair armamento e munições. Destaca-se que, tais ações, em sua maioria, são realizadas com a participação de militares ou ex-militares associados à grupos criminosos que conhecem bem a rotina do serviço e as particularidades do aquartelamento. Quando bem-sucedidas, provocam prejuízos materiais e até de vidas humanas, que afetam negativamente a imagem da Instituição.

Para fazer frente às ações das mais diversas ameaças contra os ativos e evitar a cooptação de jovens militares, a Inteligência Militar no seu ramo Contrainteligência é responsável por prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar a atuação da Inteligência adversa e as ações de qualquer natureza que possam se constituir em ameaças à salvaguarda de dados, conhecimentos, áreas, instalações, pessoas e meios que o Exército Brasileiro tenha interesse de preservar.

Figura 1: Contrainteligência no EB

Fonte: Autor

Conforme preconiza o novo Manual de Contrainteligência (em aprovação), entende-se que a Contrainteligência é um instrumento eficaz do Comando em todos os escalões. Suas ações não se restringem ao SIEx. Por conseguinte, cada um dos integrantes do Exército tem responsabilidades para com as atividades e tarefas de proteção da Força. Envolve comportamentos, atitudes preventivas, proatividade e adoção consciente de medidas efetivas.

As atividades e tarefas concernentes a esse ramo são desenvolvidas de maneira constante e ininterrupta, buscando-se a antecipação às potenciais ações hostis. É desenvolvida de forma dinâmica, necessitando ser constantemente aplicada e retroalimentada, em face da incerteza inerente às ameaças, que estão em constante evolução.

A Contrainteligência orienta-se pelo mapeamento dos ativos do Exército, pelo levantamento das deficiências na segurança desses ativos e pelas ameaças reais ou potenciais.

Para atingir os objetivos propostos de proteção, segue as seguintes premissas:

a. impedir que ações hostis de qualquer natureza:

1. provoquem danos à integridade física de pessoal militar ou civil;

2. Comprometam dados, informações, conhecimentos e sistemas a eles relacionados;

3. levem à perda de armamento e outros materiais de emprego militar;

4. inviabilizem a utilização de áreas, instalações e meios de transporte; e

5. atentem contra os valores, os deveres e a ética militar no Exército;

b. impedir a realização de atividades de espionagem, sabotagem, propaganda hostil, terrorismo ou desinformação;

O manual preconiza que para racionalizar os trabalhos, as ações a serem executadas agrupam-se, segundo o caráter preventivo e preditivo que as caracterizam em dois segmentos distintos:

a. Segurança Orgânica; e

b. Segurança Ativa.

Enquanto a Segurança Orgânica, em linhas gerais, objetiva proteger os ativos do Exército Brasileiro, a Segurança Ativa visa a atuar contra as ameaças. Na atual reflexão, iremos nos ater à Segurança Orgânica.

2.2 SEGURANÇA ORGÂNICA

O novo Manual de Contrainteligência, em aprovação, ensina que a Segurança Orgânica preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza dirigidas contra pessoas, dados, informações, materiais, áreas

e instalações.

Visa também a proteger os ativos do nosso Sistema frente as ameaças existentes e as futuras, atuando de forma a mitigar, neutralizar, compartilhar ou até aceitar os riscos que ameaçam ou possam vir a ameaçar a Instituição, implicando uma postura preventiva de todos os integrantes da Força. Para tal, é necessária a criação, o desenvolvimento e a manutenção de uma mentalidade de segurança em toda a estrutura hierárquica, com a finalidade de obter um grau de proteção ideal.

No Brasil, segundo dados do Observatório Digital de Saúde e Segurança do Trabalho – OIT, mais de R$ 1 bilhão de reais foram os gastos estimados com benefícios acidentários, somente no 1º semestre de 2018, somando auxílio-doença, aposentadoria por invalidez, pensões por morte e auxílio-acidente. Para a presidente da Associação Nacional de Medicina do Trabalho (ANAMT), Marcia Bandini, é necessário atuar mais firmemente em prevenção, investir em proteção e realizar mais treinamentos para os trabalhadores, de forma a buscar reverter esse quadro. Tais recomendações cabem, de forma semelhante ao Exército Brasileiro, uma vez que os custos na prevenção são bem inferiores aos custos para recuperar ativos perdidos ou destruídos.

Compreender a complexidade da atividade de segurança no cenário contemporâneo, entender os desafios presentes e encontrar respostas para estes desafios, sugerindo medidas e/ou ações a realizar, com enfoque sistêmico são alguns dos objetivos da Segurança Orgânica (Seg Org).

De acordo com a doutrina prevista no Manual de Contrainteligência, a Seg Org é dividida nos seguintes grupos de medidas: Segurança dos Recursos Humanos (Seg RH), Segurança do Material (Seg Mat), Segurança das Áreas e Instalações (Seg A Inst) e Segurança da Informação (Seg Info) (BRASIL, 2019 - Em aprovação).

Figura 2: Grupos de Medidas de Seg Org

Fonte: Autor

O militar, considerado o bem mais precioso do Exército, deve ser protegido e preservado a qualquer custo. Por esse motivo, a Seg RH reúne as medidas destinadas a preservar a integridade física desses ativos, buscando reduzir ao máximo a ocorrência de danos ocasionados por falhas humanas, evitando que os integrantes da instituição sejam utilizados como meio para a consecução de fins favoráveis as ações adversas e a preservar neles os princípios éticos e morais individuais e os valores institucionais do EB.

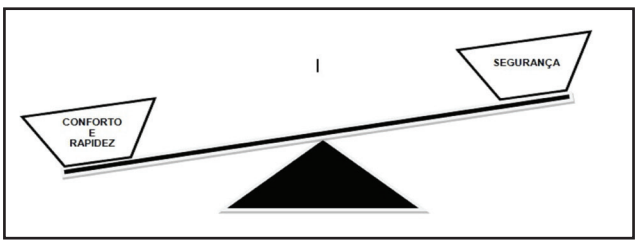
Sobre a proteção dos materiais da instituição, deve-se avaliar sua importância, considerando o impacto da ocorrência de um dano ou extravio para o cumprimento da missão da OM, bem como sua dificuldade de reposição, entre outros fatores, o que indicará a real necessidade de sua proteção e preservação.

Voltada para os locais onde ocorrem atividades humanas, ou nos quais são elaboradas, tratadas, manuseadas ou guardadas informações e materiais, com a finalidade de salvaguardá-los, a Seg A Inst tem importância destacada contra as ações adversas desenvolvidas com o objetivo deliberado de causar danos ao pessoal, material, patrimônio ou comprometer a informação.

A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou difundida verbalmente. Seja qual for a forma apresentada ou o meio pelo qual a informação sensível é compartilhada ou armazenada, é necessário que haja uma proteção adequada.

No que concerne à Segurança Orgânica, normalmente, a segurança é inversamente proporcional ao conforto e a rapidez. Assim, o planejamento poderá indicar maior relevância daquela, em detrimento desses, o que ressalta a importância do desenvolvimento da mentalidade de Contrainteligência.

Figura 3: Relação segurança x conforto e rapidez



Fonte: BRASIL, 2019 (em aprovação)

Figura 4: Segurança x Funcionalidade

Fonte: Autor

Os grupos de medidas visam facilitar a didática e a compreensão do assunto, assim como possibilita, de forma mais simples, a identificação das deficiências existentes nos diversos setores das Unidades do EB. Contudo, para se fazer um bom uso dessa doutrina, é importante saber como empregá-la no Planejamento de Contrainteligência, de forma a realizar uma adequada identificação das deficiências e dos riscos a elas inerentes.

Assim, a Segurança Orgânica deve existir para possibilitar que as Organizações Militares utilizem de maneira confiável os seus recursos humanos, o seu material, as suas áreas e instalações e saibam manusear de forma segura a informação em todos os níveis, do estratégico ao tático.

2.3 PLANEJAMENTO DE CONTRAINTELIGÊNCIA

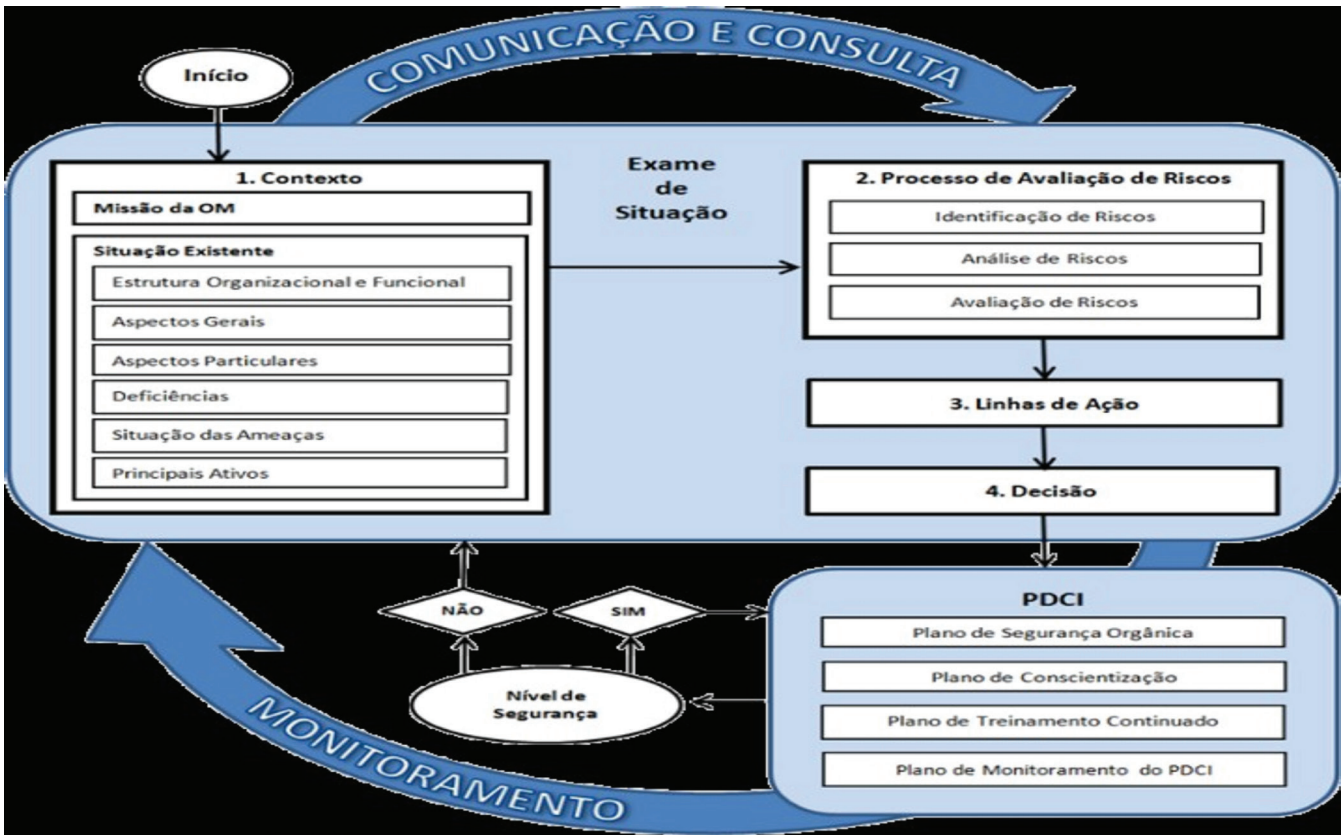
O Planejamento de Contrainteligência (Plj C Intlg) se destina a assegurar o equilíbrio entre a segurança e o funcionamento eficaz, eficiente e efetivo das Unidades do EB. Sua concepção considera que cada integrante da instituição tem responsabilidades para com as atividades e tarefas de proteção, adotando medidas adequadas às peculiaridades da OM, buscando desta forma, manter um adequado grau de segurança sem, no entanto, comprometer a funcionalidade por meio de medidas de segurança excessivas ou desnecessárias.

Na busca por atingir os objetivos propostos, o Plj C Intlg se divide em duas fases, o Exame de Situação (Exm Sit) e o Processo de Desenvolvimento da Contrainteligência (PDCI), como pode ser observado na Figura 5.

2.3.1 Exame de Situação

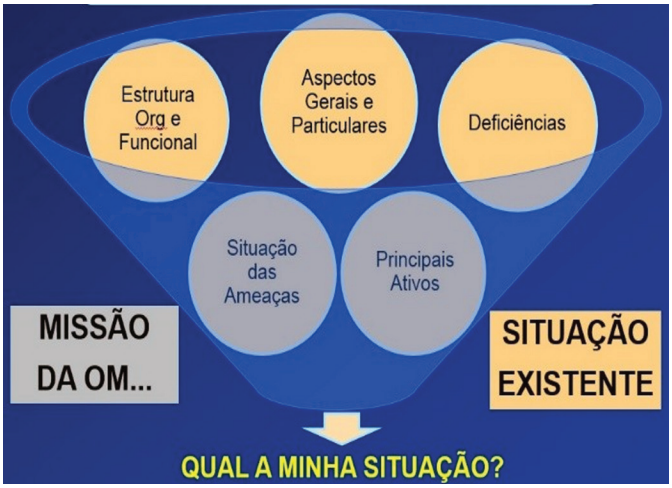
O Exame de Situação é uma fase de suma importância para o processo. É neste momento que se faz um

Figura 5: Fluxograma do Planejamento da Contrainteligência



Fonte: BRASIL, 2019 (em aprovação)

Figura 6: Exame de Situação



Fonte: Autor

estudo profundo da real situação da OM, por meio de um planejamento detalhado, que visa a dar uma sequência lógica e ordenada aos diversos fatores que envolvem o processo decisório relacionado à C Intlg.

É necessário que, durante o Exm Sit, seja realizado um levantamento das deficiências potenciais e existentes na OM, assim como, que seja claramente definido o que efetivamente precisa ser protegido, ou seja, quais são os principais ativos da Unidade e quais os atores com capacidade de realizar ações hostis e que se caracterizam como ameaças contra esses ativos.

Durante o Exame é importante a adoção de uma postura crítica acerca das deficiências encontradas, de forma que elas possibilitem que sejam identificadas as vulnerabilidades da OM diante de ameaças existentes. O estudo da situação das ameaças e o levantamento dos principais ativos são subsídios fundamentais para a identificação dos riscos.

Após a identificação dos riscos, parte-se para sua análise e avaliação. Elas visam auxiliar na definição de prioridades e opções de tratamento aos riscos identificados. A metodologia a ser utilizada possui dois parâmetros claros a serem considerados, a probabilidade e o impacto. Desta forma, busca-se estabelecer a probabilidade de determinado risco ocorrer, bem como os seus impactos nos ativos da OM. As Tabelas 1 e 2, a seguir, extraídas do Manual de Contrainteligência, exemplificam as escalas qualitativas que auxiliam na análise de probabilidades e impactos de ocorrência dos riscos.

A definição da probabilidade e do impacto, descritos no manual, apresentam exemplos de descrições e de critérios a serem considerados para o estabelecimento da gradação de cada um desses itens.

Com o objetivo de melhor visualizar e, ao mesmo tempo, auxiliar na tomada de decisão para o tratamento dos riscos, o resultado da avaliação dos riscos (valor do risco) será apresentado na Matriz de Exposição a Riscos, como pode ser visto na Tabela 3.

Tabela 1: Avaliação de Probabilidade

PROBABILIDADE	
NÍVEL	VALOR
1	MUITO BAIXA
2	BAIXA
3	MÉDIA
4	ALTA
5	MUITO ALTA

Fonte: BRASIL, 2019 (em aprovação)

Tabela 2: Avaliação de Impacto

IMPACTO	
NÍVEL	VALOR
1	MUITO BAIXO
2	BAIXO
3	MÉDIO
4	ALTO
5	MUITO ALTO

Fonte: BRASIL, 2019 (em aprovação)

Tabela 3: Matriz de Exposição a Riscos

Fonte: BRASIL, 2019 (em aprovação)

A Matriz de Exposição a Riscos (Tabela 3) demonstra os pontos de cruzamento da probabilidade de ocorrência e do impacto dos riscos. Desta forma, pela di-

visão do diagrama em quadrantes, pode-se avaliar a criticidade dos riscos. Quanto maior for a probabilidade e o impacto de um risco, maior será seu nível de criticidade.

O grande desafio para os Comandantes de OM é reduzir a criticidade do risco em termos de probabilidade e impacto, colocando-o num nível aceitável. Desta forma, as OM deverão identificar qual estratégia seguir (aceitar, compartilhar, evitar ou mitigar) em relação ao tratamento dos riscos identificados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos na avaliação realizada e a priorização deve estar embasada no valor atribuído ao risco, de acordo com a Matriz de Exposição a Riscos, ou seja, o risco no quadrante vermelho deverá receber prioridade no tratamento.

2.3.2 Processo de Desenvolvimento da Contrainteligência

O Processo de Desenvolvimento da Contrainteligência (PDCI) pode ser entendido como um conjunto de atividades contínuas de C Intlg, destinadas a planejar, controlar e otimizar as medidas de segurança para a proteção de uma OM. Na busca do atendimento desses objetivos, o PDCI deve ser estruturado em Plano de Segurança Orgânica (PSO), Plano de Conscientização, Plano de Treinamento Continuado e Plano de Monitoramento.

Por se tratar de um processo, o PDCI tem um caráter permanente e cíclico. As inovações e melhorias são constantes no processo e deverão respeitar as práticas já consolidadas e testadas nas OM, buscando a efetividade ao longo do tempo.

Figura 7: PDCI

Fonte: Autor

Na confecção do Planos do PDCI, as OM devem buscar utilizar o princípio da simplicidade, com objetivos e conteúdo claros, a fim de que os mesmos possam ser compreendidos por todos e, ao mesmo tempo, reduzindo a possibilidade de serem criadas eventuais resistências.

O PDCI deve ser conduzido pelas lideranças da OM. Este é um fator crítico para o sucesso do processo, de forma que, quando as lideranças acreditam e seguem as diretrizes estabelecidas, todo o efetivo da OM tenderá para o mesmo rumo. Fato que pode ser sintetizado por um ditado há muito utilizado na caserna: "As palavras convencem, o exemplo arrasta!"

Figura 8: PDCI (Fatores Críticos de Sucesso)

Fonte: Autor

3. CONCLUSÃO

Muitas vezes, por desconhecimento, a Contrainteligência poderá ser tratada de forma secundária ou até mesmo desconsiderada. Isto acontece porque temos a falsa ilusão de estarmos sempre seguros ou que nada acontecerá na Organização Militar a qual o militar trabalha. Não percebemos que, com o advento e avanço de novas tecnologias e o surgimento de novas ameaças, o sentimento de segurança anteriormente presente mudou. Agora estamos completamente vulneráveis a novas ameaças físicas e virtuais.

Medidas de Contrainteligência (Exm Sit e PDCI) mexem com a rotina da Organização e parecerão, num primeiro momento, medidas desconfortáveis, causando constrangimentos. Por isso, é de fundamental importância um prévio processo de conscientização e treinamento, para conquistar "corações e mentes" dos militares e realizar o monitoramento constantemente, a fim de identificar e tratar os riscos a que a Organização está ou possa vir a ser submetida.

As causas de um incidente de segurança estão normalmente associadas às falhas nos procedimentos (obscuros, pouco práticos ou inexistentes), no treinamento

(procedimentos existentes, mas não conhecidos, aceitos ou entendidos), na liderança (deficiência na ação de comando) ou no indivíduo, componente mais frágil de qualquer sistema de segurança.

Ratificamos que a responsabilidade pela SEGURANÇA é de TODOS e os militares de maior posto e graduação necessitam estar atentos e motivados, pois serão os supervisores, coordenadores e controladores do processo de proteção dos ativos do Exército Brasileiro.

É necessária e imprescindível a adoção de postura preventiva por todos os integrantes, sendo primordial a criação, o desenvolvimento e a manutenção de uma MENTALIDADE DE CONTRAINTELIGÊNCIA em toda a estrutura hierárquica, visando a obtenção de um grau de proteção ideal.

Por fim, é necessário refletir que sempre seremos vulneráveis à ação de atores hostis mal-intencionados e que agirão sobre o elo mais fraco de um sistema de segurança: o fator humano. Portanto, o objetivo permanente deverá ser o de salvaguardar o Sistema Exército contribuindo para reduzir as deficiências, dificultar a atuação das ameaças e transformar o elo mais fraco, na barreira mais forte.

REFERÊNCIAS

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3o do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, 18 nov. 2011.

_____. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências.

_____. Decreto nº 4.073, de 3 de janeiro de 2002. Regulamenta a Lei nº 8.159/2000.

_____. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Diário Oficial da União, Brasília, 16 maio 2012.

_____. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento. Diário Oficial da União, Brasília, 14 nov. 2012.

_____. Exército Brasileiro. **Estado-Maior do Exército. Manual de Campanha Contrainteligência. EB70-MC-10.3**___. 2019 (EM APROVAÇÃO)

_____. CIE. **Treinamento para gestão de riscos no CIE/ESIMEX** .2017.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações.** São Paulo: Atlas, 2005.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem social.** 2006. 211 f. Tese (Doutorado) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília (UnB), Brasília, 2006. Disponível em: <http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf>. Acesso em: 07 ago. 2008.

MARINHO, Fernando, **Como proteger e manter seus negócios: Um plano básico para contingências e continuidade nas empresas**. Rio de Janeiro: Ciência Moderna Editora LTDA, 2008.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de, **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2010.

NASCIMENTO, Marta Sianes Oliveira do. O. **Proteção ao conhecimento: uma proposta de fundamentação teórica**. 2008. 181 f. Dissertação (mestrado) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília (UnB), Brasília, 2008. Disponível em: <http://www.repositorio.bce.unb.br/handle/10482/5286>. Acesso em: 30 jun. 2012.

PEIXOTO, Mário César Pintaudi. **Engenharia social & segurança da informação na gestão corporativa**. Rio de janeiro: Brasport, 2006.

RAMOS, Anderson et al. **Security Officer 1: guia oficial para a formação de gestores em segurança da informação.** Porto Alegre: Zouk, 2006.

RAMOS, Anderson et al. **Security Officer 2: guia oficial para a formação de gestores em segurança da informação**. Porto Alegre: Zouk, 2008.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: **Sistema de gestão de segurança da informação – requisitos**. Rio de Janeiro, 2013.

_____. NBR ISO/IEC 27002: **Código de Prática para a gestão da segurança da informação.** Rio de Janeiro, 2013.

_____. NBR ISO/IEC 27005: **Gestão de risco de segurança da informação**. Rio de Janeiro, 2011.

_____. NBR ISO/IEC 31000: **Gestão de riscos.** Rio de Janeiro, 2009.

LOGOS. **Manual do curso gerenciamento de incidentes e planejamento de contingencia** 4 ed. 2017

NORMAS DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – DSIC/GSIPR. Disponíveis em <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: 13 maio 2018.