



BOLETIM

ADITAMENTO

DO CORPO DE BOMBEIROS MILITAR DO PARÁ
E COORDENADORIA ESTADUAL DE DEFESA CIVIL

Nº 88/2021
Belém, 10 DE MAIO DE 2021

(Total de 11 Páginas)

(Instituído pela Portaria nº; 129, de 17 de março de 2021, DOE nº 34.525)

Funções:

HAYMAN APOLO GOMES DE SOUZA - CEL QOBM
COMANDANTE-GERAL DO CBMPA
(91) 4006-8313/4006-8352

ALEXANDRE COSTA DO NASCIMENTO - CEL QOBM
SUBCOMANDANTE-GERAL DO CBMPA
(91) 98899-6589

REGINALDO PINHEIRO DOS SANTOS - CEL QOBM
COORD ADJ CEDEC
(91) 98899-6582

MARCOS ROBERTO COSTA MACEDO - CEL QOBM
CMT DO COP
(91) 98899-6409

VIVIAN ROSA LEITE - TEN CEL QOBM
CHEFE DE GABINETE
(91) 98899-6491

CARLOS AUGUSTO DE OLIVEIRA RIBEIRO - CEL QOBM
AJUDANTE GERAL
(91) 98899-6328

MARÍLIA GABRIELA CONTENTE GOMES - TEN CEL QOBM
DIRETOR DE APOIO LOGÍSTICO
(91) 98899-6377

EDUARDO CELSO DA SILVA FARIAS - TEN CEL QOBM
DIRETOR DE ENSINO E INSTRUÇÃO
(91) 98899-5642

JAYME DE AVIZ BENJO - CEL QOBM
DIRETOR DE FINANÇAS
(91) 98899-6344

JAIME ROSA DE OLIVEIRA - CEL QOBM
DIRETOR DE PESSOAL
(91) 98899-6442

ROGER NEY LOBO TEIXEIRA - CEL QOBM
DIRETOR DE SAÚDE
(91) 98899-6415

RAIMUNDO REIS BRITO JUNIOR - CEL QOBM
DIRETOR DE SERVIÇOS TÉCNICOS
(91) 98899-6350

ANDRE LUIZ NOBRE CAMPOS - CEL QOBM
DIRETOR DE TELEMÁTICA E ESTATÍSTICA
(91) 98899-6584

VALTENCIR DA SILVA PINHEIRO - TEN CEL QOBM
CHEFE DA BM/1 DO EMG
(91) 98899-6496

JOHANN MAK DOUGLAS SALES DA SILVA - TEN CEL QOBM
CHEFE DA BM/2 DO EMG
(91) 98899-6426

ADRIANA MELENDEZ ALVES - TEN CEL QOBM
CHEFE DA BM/3 DO EMG
(91) 98899-6497

MONICA FIGUEIREDO VELOSO - TEN CEL QOBM
CHEFE DA BM/4 DO EMG
(91) 98899-6315

ÁTILA DAS NEVES PORTILHO - TEN CEL QOBM
CHEFE DA BM/5 DO EMG
(91) 98899-6416

LUIS ARTHUR TEIXEIRA VIEIRA - TEN CEL QOBM
CHEFE DA BM/6 DO EMG
(91) 98899-6542

THAIS MINA KUSAKARI - TEN CEL QOCBM
PRESIDENTE DA COJ
(91) 98899-5849

GENILSON MARQUES DA COSTA - TEN CEL QOBM
PRESIDENTE DA CPCI
(91) 98899-6447

MOISES TAVARES MORAES - TEN CEL QOBM
PRESIDENTE DA CPL
(91) 98899-6515

ELILDO ANDRADE FERREIRA - MAJ QOBM
CHEFE DO ALMOXARIFADO CENTRAL
(91) 98899-6321

MICHEL NUNES REIS - TEN CEL QOBM
CHEFE DO CSMV/MOP
(91) 98899-6272

JORGE EDISIO DE CASTRO TEIXEIRA - TEN CEL QOBM
CMT DO 1º GBM
(91) 98899-6342

THIAGO AUGUSTO VIEIRA COSTA - MAJ QOBM
CMT DO 2º GBM
(91) 98899-6366

ROBERTO CARLOS PAMPLONA DA SILVA - TEN CEL QOBM
CMT DO 3º GBM
(91) 98899-6557

FRANCISCO DA SILVA JUNIOR - TEN CEL QOBM
CMT DO 4º GBM
(93) 98806-3816

JOSE RAIMUNDO LELIS POJO - TEN CEL QOBM
CMT DO 5º GBM
(94) 98803-1416

ALLE HEDEN TRINDADE DE SOUZA - TEN CEL QOBM
CMT DO 6º GBM
(91) 98899-6552

CELSO DOS SANTOS PIQUET JUNIOR - MAJ QOBM
CMT DO 7º GBM
(93) 98806-3815

MARCELO HORACIO ALFARO - TEN CEL QOBM
CMT DO 8º GBM
(94) 98803-1415

SAIMO COSTA DA SILVA - MAJ QOBM
RESP. PELO CMD DO 9º GBM
(93) 98806-3817

CHARLES DE PAIVA CATUABA - MAJ QOBM
CMT DO 10º GBM
(94) 98803-1413

JORGE CIRILO OLIVEIRA SOUZA - MAJ QOBM
CMT DO 11º GBM
(91) 98899-6422

EDGAR AUGUSTO DA GAMA GOES - TEN CEL QOBM
CMT DO 12º GBM
(91) 98899-5621

ADOLFO LUIS MONTEIRO LOPES - MAJ QOBM
CMT DO 13º GBM
(91) 98899-6576

DAVID RICARDO BAETA DE OLIVEIRA - TEN CEL QOBM
CMT DO 14º GBM
(91) 98899-6293

LUIS CLAUDIO DA SILVA FARIAS - TEN CEL QOBM
CMT DO 15º GBM
(91) 98899-6412

SHERDLEY ROSSAS CANSANCAO NOVAES - MAJ QOBM
CMT DO 16º GBM
(91) 98899-6498

CARLOS AUGUSTO SILVA SOUTO - MAJ QOBM
CMT DO 17º GBM
(91) 98899-6569

DIEGO DE ANDRADE CUNHA - MAJ QOBM
CMT DO 18º GBM
(91) 98899-6300

EDSON AFONSO DE SOUSA DUARTE - MAJ QOBM
CMT DO 19º GBM
(91) 98899-6575

LUIZ ROAN RODRIGUES MONTEIRO - MAJ QOBM
CMT DO 20º GBM
(91) 98899-6279

EDINALDO RABELO LIMA - TEN CEL QOBM
CMT DO 21º GBM
(91) 98899-6567

JACOB CHRISTOVAO MACIEIRA - TEN CEL QOBM
CMT DO 22º GBM
(91) 98899-6580

HUGO CARDOSO FERREIRA - MAJ QOBM
CMT DO 23º GBM
(94) 98803-1412

DINALDO SANTOS PALHETA - MAJ QOBM
CMT DO 24º GBM
(91) 98899-2647

LEANDRO HENRIQUE DINIZ COIMBRA - MAJ QOBM
CMT DO 25º GBM
(91) 98899-6402

FLÁVIA SIQUEIRA CORRÊA ZELL - TEN CEL QOBM
CMT DO 26º GBM
(91) 98899-6322

OLIMPIO AUGUSTO COELHO DE OLIVEIRA - TEN CEL QOBM
CMT DO 28º GBM
(91) 98899-6346

MARIO MATOS COUTINHO - TEN CEL QOBM
CMT DO 29º GBM
(91) 98899-6428

SAMARA CRISTINA ROMARIZ DE CARVALHO - TEN CEL QOBM
CMT DO 1º GB5
(91) 98899-6458

RICARDO LENO ANAISSI PEREIRA - MAJ QOBM
CMT DO 1º GMAF
(91) 98899-5636

CEZAR ALBERTO TAVARES DA SILVA - MAJ QOBM
CMT DO 1º GPA
(91) 98899-6405

ALYNE GISELLE CAMELO LOUZEIRO - TEN CEL QOBM
CMT DO CFAE
(91) 98899-2695

ÍNDICE**1ª PARTE****ATOS DO PODER EXECUTIVO**

Sem Alteração

2ª PARTE**ATOS DO GABINETE DO CMT GERAL / EMG /
CEDEC****Atos do Gabinete do Comandante-Geral**MANUAL DE SEGURANÇA ORGÂNICA DO CORPO DE
BOMBEIROS MILITAR DO PARÁ E COORDENADORIA
ESTADUAL DE DEFESA CIVIL pág.11**Atos do Gabinete do Chefe do EMG**

Sem Alteração

Atos do Gabinete do Coord. Adjunto da CEDEC

Sem Alteração

3ª PARTE**ASSUNTOS GERAIS E DE JUSTIÇA****4ª PARTE****ÉTICA E DISCIPLINA**

Sem Alteração

**139º** ANO

1ª PARTE ATOS DO PODER EXECUTIVO

Sem Alteração

2ª PARTE ATOS DO GABINETE DO CMT GERAL / EMG / CEDEC

ATOS DO GABINETE DO COMANDANTE-GERAL

MANUAL DE SEGURANÇA ORGÂNICA DO CORPO DE BOMBEIROS MILITAR DO PARÁ E COORDENADORIA ESTADUAL DE DEFESA CIVIL

MANUAL DE SEGURANÇA ORGÂNICA DO CORPO DE BOMBEIROS MILITAR DO PARÁ E COORDENADORIA ESTADUAL DE DEFESA CIVIL



MANUAL DE SEGURANÇA ORGÂNICA DO CORPO DE BOMBEIROS MILITAR DO ESTADO DO PARÁ E COORDENADORIA ESTADUAL DE DEFESA CIVIL

FUNDAMENTOS DOUTRINÁRIOS

2021

Governador do Estado do Pará

Helder Zaluth Barbalho

Comandante-Geral do Corpo de Bombeiros Militar do Pará e Coordenador Estadual de Defesa Civil

Coronel QOBM Hayman Apolo Gomes De Souza

Chefe do EMG e SubComandante Geral do Corpo de Bombeiros Militar do Pará

Coronel QOBM Alexandre Costa do Nascimento

Chefe da BM/2 do EMG

Johann Mak Douglas Sales da Silva

Realização: 2ª SEÇÃO DO EMG

Coordenação e Responsabilidade técnica

Johann Mak Douglas Sales da Silva - Tenente Coronel QOBM

João Francisco Garcia Reis - Doutor em Ciências

Wando Dias Miranda - Doutor em Ciências

Equipe Técnica

Roberto Magno Reis Netto - Mestre em Segurança Pública

Paulo Cesar da Silva - Especialista em Atividade de Inteligência

Jefferson Lima Alves - Engenheiro Elétrico

Colaboradores

1º Sgt BM Eros Nazareno Dias.

2º Sgt BM Natanael Cardoso da Silva.

2º Sgt BM Sergio Ramos Lopes.

3º Sgt BM Edemir Junior Gomes Salgado;

3º Sgt BM Wellington Souza da Silva Castro.

CB BM Amauri Ferreira Fonseca.

CB BM Edilayne Costa Gama Pereira.

CB BM Renan Luiz Lacerda Façanha.

CB BM Bruno Dias de Oliveira;

SD BM Yngrid Cristina da Silva Santos

1- Sobre o Corpo de Bombeiros

Ao ser criado através de uma Portaria Provincial, datada do dia 24 de novembro de 1882, o Corpo de Bombeiros Militar surge no Estado do Pará como uma companhia da Polícia Militar e, teve como primeiro comandante o então Capitão BM Antônio Veríssimo Ivo de Abreu. O atual Comandante-Geral da Corporação, o Coronel QOBM Hayman Apolo Gomes de Souza, é o 51º Comandante do Corpo de Bombeiros. A Corporação tem como patrono nacional Dom Pedro II (assim como todos os Corpos de Bombeiros do Brasil) e, como patrono estadual – o Intendente Antônio Lemos.

Com a promulgação da Constituição Estadual de 1989 o, então, Corpo de Bombeiros da Polícia Militar do Estado do Pará se emancipa. Além de obter autonomia ganha também um novo regime jurídico, passando a ser subordinado diretamente ao Governo do Estado e, passando, enfim, a se chamar Corpo de Bombeiros Militar do Pará. A nova Constituição do Estado também unificou o Comando do CBMPA com a Coordenadoria Estadual de Defesa Civil – CEDEC, passando o Comandante-Geral do CBMPA a coordenar também a Defesa Civil do Estado.

O Quartel do Comando Geral do Corpo de Bombeiros do Pará está sediado na própria capital paraense, no município de Belém e, localiza-se à Avenida Júlio César nº 3.000, com a Avenida Pedro Álvares Cabral, Bairro de Val-de-Cans. Além do Quartel do Comando Geral, a Corporação conta com 30 unidades operacionais 07 unidades e setores distribuídas na região metropolitana de Belém – RMB e interior do estado. Hoje, além da capital, mais 25 municípios contam com a presença do serviço do Corpo de Bombeiros no Estado do Pará.

Atualmente, o CBMPA possui um efetivo de 2.600 militares entre homens e mulheres, praças e oficiais. Existem apenas duas formas de ingresso na Corporação, por meio de concurso público para soldados ou para oficiais.

2- Missão

Contribuir para proteger a vida, o patrimônio e o meio ambiente a fim de garantir a prestação de serviços Bombeiro Militar e de Defesa Civil à sociedade.

3- Visão

Ser conhecida como uma corporação Bombeiro Militar de excelência e referência nacional na gestão de riscos e desastres, com o emprego de tecnologias avançadas e profissionais capacitados e motivados.

4- Valores

Respeito à hierarquia e disciplina, proatividade, probidade, coragem, lealdade e aprimoramento.

5- Apresentação

A Atividade de Inteligência¹ e a Contra Inteligência² são duas faces de uma mesma moeda, que ao longo dos anos, mas em especial pós 11 de setembro de 2001, vem ganhando cada vez mais espaço, seja nos círculos de Estado e Poder mais reservados, seja nos meios de comunicação e na opinião pública, mas poucos são realmente aqueles que compreendem a importância dessa ferramenta de Estado e suas implicações para o futuro das instituições.

Como podemos observar na frase Scientia potentia est, conhecimento é poder, atribuída a Thomas Hobbes (1588-1679) na obra Leviatã de 1668, o conhecimento é representado como um dos principais pilares do Estado. Mas essa associação entre conhecimento e poder é muito mais antiga, pois pode ser observada nos textos clássicos de Sun Tzu, na obra A arte da guerra, Kautliya em Arthashastra e em Júlio Cesar em De Bello Gallico, como posterior a obra de Hobbes no clássico de Clausewitz, Da Guerra.

Podendo fazer uma atualização para nossos tempos com a adição de um novo termo à frase que dá muito mais sentido a palavra prático, assim temos: Conhecimento prático é Poder, o que defini por si a natureza do conhecimento moderno, a capacidade de tornar prático e útil o conhecimento idealizado, testando e atualizando, sempre que aparecer novos desafios para a produção e a segurança de conhecimento.

Para Cepik (2003 e 2011) em uma sociedade cada vez mais conectada e com diversas possibilidades de acesso aos mais diferentes bancos de dados e sistema de Estado, a atividade de proteção da informação, conhecida pelos nomes de Segurança Orgânica ou Segurança Institucional, um sub-ramo da Atividade de Contra-Inteligência vem ganhando cada vez mais espaço como ferramenta que busca aumentar o grau de segurança e reduzir os riscos e vulnerabilidades dos sistemas, assim, onde existe a produção de conhecimento estratégico, obrigatoriamente deve existir a segurança dos meios (segurança de pessoas, áreas, instalações, documentos e materiais e tecnologias).

Instituições de Segurança Pública e Defesa Social, que por natureza, são produtoras de conhecimento estratégico de alto valor de Estado devem criar suas normas, procedimentos, protocolos e documentos institucionais destinados a fazer a regulamentação da atividade de salvaguarda, assim como garantir a atualização periódica desses documentos e favorecer para uma cultura institucional de segurança interna.

Nesse sentido, o Corpo de Bombeiros Militar do Pará e a Coordenadoria Estadual de Defesa Civil, por meio de seu comandante em chefe e da 2ª Seção do EMG, reuniram um grupo de profissionais técnicos e especialistas civis e militares para o desenvolvimento do Manual de Segurança Orgânica do Corpo de Bombeiros Militar do Pará e a Coordenadoria Estadual de Defesa Civil, com o objetivo de criar uma cultura permanente de Segurança Institucional com abrangência de todos os setores, Seções e Diretorias da Instituição, visando assim aumentar a segurança de pessoas e instalações do CBMPA e CEDEC.



6- Introdução

A Atividade de Contra-Inteligência objetiva prevenir, detectar, reduzir os riscos e neutralizar atividades e situações adversas, de qualquer natureza, que constituam ameaça às instituições de Estado, buscando criar instrumentos diversos de proteção organizacional (procedimentos, protocolos, manuais...) visando dar segurança às áreas, instalações, informações, meios e processos e pessoas, envolvidas com a produção e manuseio de conhecimento estratégico e sensível a instituição.

Segundo Miranda (2018) da mesma forma que a Atividade de Inteligência visa a produção de conhecimento específico cuja finalidade é auxiliar o tomador de decisão durante o processo decisório, buscando limitar os riscos ao máximo possível após análise e validação das informações disponíveis, cabe a Contra-Inteligência, através da Segurança Orgânica dar os procedimentos e os protocolos de segurança interna a serem adotados pela instituição, assim como atuar de forma ativa na busca de vulnerabilidades nas estratégias de segurança, atualizando-se das novas ameaças e suas metodologias de segurança interna.

A Atividade de Contra-Inteligência é definida no Decreto nº 4.376 de 13 de setembro de 2020, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (SISBIN), instituído pela Lei nº 9.883 de 07 de dezembro de 1999, nela temos:

Art. 3º Entende-se como contra-inteligência a atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem. (BRASIL. Decreto nº 4.376 de 13 de setembro de 2020)

Para Miranda (2018) e Ferro (2008) dois pontos merecem atenção reforçada na hora de selecionar, pelo comandante, diretor ou chefe, o perfil dos profissionais que desenvolveram atividades, seja na Inteligência ou na Contra-Inteligência: a) a necessidade de uma formação específica para o exercício da atividade, pois essa atividade exige, por natureza, conhecimentos teóricos, práticos e tecnológicos para o seu desenvolvimento, não sendo assim, espaço para pessoas sem a devida formação e capacidades cognitivas para lidar com o sigilo e a responsabilidade inerentes ao posto, ou seja, ter perfil para o cargo; e b) a capacidade de avaliação dos diferentes cenários e avaliação de risco, visando oferecer ao tomador de decisão, informações mais objetivas possíveis dos cenários em análise, garantindo a imparcialidade dos fatos e a clareza do conhecimento produzido.

Da mesma forma, esse profissional deve estabelecer processos e métodos de seleção de sua equipe de trabalho, sempre levando em consideração o perfil do profissional desejado para o desenvolvimento das atividades, além de atentar para a natureza de cada procedimento ou ação que busque a segurança da instituição Corpo de Bombeiros Militar do Pará e da Coordenadoria Estadual de Defesa Civil.

7- Segurança Orgânica

A Doutrina de Inteligência define a Segurança Orgânica como um conjunto de medidas que visam a prevenir e obstruir ações adversas de qualquer natureza que incidam ou possam incidir sobre: recursos humanos, documentação e material, comunicações, informação, áreas e instalações.

As quatro primeiras atividades estão relacionadas à proteção direta do conhecimento, pois atuam objetivamente sobre seus elementos: o homem, o documento, o material e os meios de transmissão da comunicação e processamento das informações.

A Segurança das Áreas e Instalações possui objetivo de garantir a eficácia dos demais grupos. É materializada com a definição de medidas protetoras às instalações e de colocação de barreiras para inibir ou impedir ações adversas, posicionadas em locais onde o acesso deva ser controlado para minimizar riscos de ação criminosa e atos de sabotagem, bem como para proteção de locais de produção de conhecimentos e informações, onde são tratados, manuseados ou guardados.

7.1 Objetivos

Documento a ser destinado a analisar e construção, à luz dos elementos doutrinários da Atividade de Inteligência, as bases conceituais para a elaboração da Doutrina de Segurança Orgânica do Corpo de Bombeiros Militar do Estado do Pará - CBMPA e da Defesa Civil Estadual, voltado a identificação das vulnerabilidades institucionais e às oportunidades.

7.2 Vantagens Estratégicas

Dar base para a elaboração dos Planos de Segurança Institucional do CBMPA e da Defesa Civil Estadual possibilitando a identificação de possíveis vulnerabilidades existentes na estrutura do Corpo de Bombeiros Militar do Pará e da Defesa Civil Estadual, contribuir na redução ou eliminação dos possíveis problemas identificados, assim, maximizando ações do planejamento da Instituição e garantindo a segurança das equipes de trabalhos, documentos produzidos e instalações de produção de conhecimento sensível.

8- O MANUAL DE SEGURANÇA ORGÂNICA DO CORPO DE BOMBEIROS MILITAR DO ESTADO DO PARÁ E COORDENADORIA ESTADUAL DE DEFESA CIVIL

O MANUAL DE SEGURANÇA ORGÂNICA DO CBMPA e CEDEC tem por finalidade apresentar os elementos doutrinários para elaboração de Planos de Segurança Orgânica - PSO para a Corporação Corpo de Bombeiros e para Defesa Civil Estadual, voltado para a salvaguarda dos interesses da instituição, contra ações de qualquer natureza, buscando atuar de forma ostensiva na identificação de ameaças internas e externas e contribuir para a construção de uma cultura de Segurança Orgânica dentro da Instituição.

O Manual é composto de 07 (sete) partes sendo:

Quanto a Segurança de Pessoas

Quanto a Segurança da Documentação e do Material

Quanto a Segurança das Comunicações

Quanto a Segurança das Áreas e Instalações

Quanto a Segurança da Informática

Quanto ao Planejamento de Segurança Orgânica e

Grupo de Detentores de Conhecimento Estratégico - GDCE

8.1- Quanto a Segurança de Pessoas

Destina-se a análise da Segurança dos Recursos Humanos ou Segurança de Pessoal. Compreende

o conjunto de medidas destinadas a assegurar comportamentos adequados à proteção do conhecimento sensível produzido na instituição e das pessoas envolvidas sejam elementos orgânicos e não orgânicos a instituição.

8.1.1- Considerações Gerais

a- As normas específicas de Segurança do Pessoal objetivam reduzir a possibilidade de admissão de pessoal, militar ou civil (voluntários ou terceirizados), comprometido com interesses adversos ao Corpo de Bombeiros Militar, bem como estabelecer padrões educativos.

b- Implementa-se mediante a observância de regras de sigilo e de conduta por parte de todos os recursos humanos da Instituição. Obriga a uma rigorosa seleção, recrutamento, classificação, instrução, atribuição de responsabilidades, adequado credenciamento, controle e dispensa de pessoal de qualquer nível.

c- A Segurança do Pessoal Militar, implementada em normas específicas, é baseada em três princípios:

c.1 a necessidade de conhecer está ligada à função desempenhada;

c.2 o acesso a documentos sensíveis só é permitido a pessoas credenciadas e;

c.3 o conhecimento de assunto sensível depende da função e não do grau hierárquico.

OBSERVAÇÃO - O atendimento a esses princípios evita a ocorrência de vazamentos envolvendo o público interno e o externo

d. A admissão do pessoal militar, para atuação em setores específicos da Instituição deverá ser realizada cumprindo as normas de Segurança Orgânica, com destaque para:

(1) formação acadêmica e profissional específica para atuação em setores específicos da instituição, como jurídico, administrativo, tecnológico, etc. e

(2) a seleção para o Serviço Voluntário deverá incluir consultas aos órgãos de segurança pública e a B2, visando à dispensa de conscritos com indícios de envolvimento criminal ou com a contravenção.

(3) o sistema de senhas do sistema de informática das pessoas envolvidas na fase de produção do conhecimento e em seu manuseio deverá ser de uso pessoal e intransferível, sendo que o mesmo deverá ser suspenso após o desligamento da pessoa do setor.

e. O Planejamento da Segurança Pessoal dos envolvidos na produção, guarda e transferência do conhecimento produzido é de responsabilidade da B2 é implementada através das Normas de Segurança do Pessoal do Sistema da B2.

f. A Segurança do Pessoal Prestador de Serviço, deverá ser implementada por medidas de credenciamento na portaria, fornecimento de identificação específica e acompanhamento ao local de execução do serviço. Ao final do trabalho um militar ou responsável, será destinado a inspecionar o serviço executado e ao recolhimento das credenciais temporárias de trabalho fornecidas na portaria e a inspeção do veículo utilizado.

g. A Seleção do Pessoal Voluntário Civil - SPVC deverá ser realizada objetivando a detecção, a identificação e a inabilitação de elementos que possam causar futuras vulnerabilidades ao Corpo de Bombeiros Militar. Para tanto, caberá ao encarregado do processo de admissão, a análise das informações dos candidatos, a consulta de informações pessoais nos órgãos de Segurança Pública, a realização de entrevistas, e em fontes abertas (redes sociais) e etc. Cópias das informações levantadas deverão ser destinadas ao B2 para acompanhamento e armazenamento dos dados.

h. A Segurança Pessoal Civil (prestador de serviço ou voluntário civil) que presta serviços ao Corpo de Bombeiros Militar do Pará será implementada através das seguintes normas de Segurança Orgânica:

(1) incentivo ao desenvolvimento de uma mentalidade de Segurança Orgânica, por intermédio de programas educacionais (instruções e palestras) voltados para a observância de regras de sigilo e de conduta similar dos integrantes do Corpo de Bombeiros;

(2) comunicação ao setor responsável de contratação e a B2 das alterações ocorridas com o pessoal civil, que caracterizem vulnerabilidade para Segurança Orgânica; e

(3) incentivo a condutas de relações interpessoais positivas baseadas em princípios éticos e de educação.

8.1.2 Medidas de segurança do pessoal

Para efeito de sua aplicação, as medidas de segurança do pessoal estão agrupadas em três tipos particulares de segurança:

SEGURANÇA NO PROCESSO SELETIVO

As medidas de segurança no processo seletivo visam a dificultar as ações adversas de infiltração e a admissão de indivíduos com características e antecedentes pessoais que possam levá-los a causar o comprometimento de ações desenvolvidas pelo Corpo de Bombeiros Militar do Pará e de depreciação da imagem da Instituição.

Medidas a serem executadas

1- Avaliação de sensibilidades das funções

a- As diversas funções desenvolvidas no CBMPA, particularmente na B2- Seção, pela sua natureza, possuem necessariamente um grau de sensibilidade. Isto decorre da maior ou menor possibilidade de as pessoas que as desempenham virem a causar, direta ou indiretamente, o comprometimento.

b- Como decorrência da avaliação da sensibilidade das funções, serão determinadas as características pessoais julgadas necessárias para que, sob o ponto de vista da Contra-Inteligência - CI, uma pessoa desempenhe uma função com o mínimo de risco para a salvaguarda do conhecimento e/ou dado.

2- Investigação de segurança

Paralelamente à execução das ações administrativas com o objetivo de suprir as necessidades de recursos humanos para uma função sensível, será desencadeado um processo de levantamento de dados biográficos de cada um dos candidatos (processo de qualificação). Este processo será concluído com o parecer sobre a conveniência ou não da admissão dos mesmos.

Ressalta-se que para o desempenho das funções de Inteligência, são consideradas indispensáveis a lealdade e a discrição.



Para as demais funções onde o grau de sigilo foi considerado de menor potencial, deverá prevalecer o critério de mérito por cursos e formação específica para o desempenho da função, onde os ocupantes receberam informações sobre como trabalhar sobre a segurança das informações, de acordo com a Lei nº 12.527/2011 – Lei de Acesso à Informação e o Decreto nº 7.845/2012.

As condutas de Segurança Orgânica devem prevalecer no agir do profissional Bombeiro Militar tanto no ambiente interno da Instituição, quanto no ambiente externo privado.

Controle de segurança na consulta ao candidato

Esta medida objetiva estabelecer procedimentos cautelares quando da consulta ao assinalado sobre a possibilidade de desempenhar uma função sensível.

Esses procedimentos cautelares procurarão evitar o comprometimento dos trabalhos que envolvem o processo seletivo, caso surjam situações de insucesso no convite formulado.

Todo o processo de controle será controlado por uma comissão interna que ao final emitirá parecer de caráter reservado aos tomadores de decisão e o Comandante-Geral do CBMPA.

SEGURANÇA NO DESEMPENHO DA FUNÇÃO:

As medidas de segurança no desempenho da função visam a validar o credenciamento, a proceder à educação de segurança e a confirmar as características pessoais exigidas.

Medidas a serem executadas

Credenciamento para a função

Confirmadas as exigências de segurança inerentes à função, será expedida a credencial de segurança apropriada, por meio de ato administrativo exarado por autoridade competente, estabelecendo o grau de sigilo a que poderá ter acesso o credenciado.

A credencial de segurança poderá ser alterada em função de novas necessidades relativas à mesma função ou à outra para a qual o servidor for designado.

O credenciamento é de caráter pessoal e não pode ser repassada a terceiro em nenhuma situação.

Caso haja suspeita de acesso não autorizado, o detentor da credencial deverá informar imediatamente sua chefia direta e o diretor da B2 para que medidas de contenção possam ser tomadas visando a segurança das informações.

Educação de segurança

A necessidade da existência de padrões de comportamento que atendam aos princípios de CI, evitando que o Sistema torne-se potencialmente vulnerável ao vazamento, exige um processo educacional. Para isso deverão ser observadas as seguintes medidas:

a.1 previsão de objetivos educacionais adequados de CI nos currículos dos cursos de formação de oficiais e praças e na instrução de quadros; da mesma forma instruções sobre os procedimentos de segurança orgânica para os colaboradores (terceirizados e voluntários civis)

a.2 enfatizar a observância das medidas de Segurança Orgânica nos ambientes das escolas de formação e aperfeiçoamento, visando ao desenvolvimento da mentalidade desejada;

a.3 incentivar a utilização dos preceitos previstos para a implementação da Segurança Orgânica no CBMPA e;

a.4 implantar, em todos os escalões, o credenciamento de segurança.

Os novos integrantes do CBMPA devem ser submetidos a um processo de educação de segurança, com o objetivo de criar, desenvolver e manter uma efetiva mentalidade de segurança, bem como transmitir os procedimentos cautelares necessários ao trato com o conhecimento ou dado ou material sensíveis. O processo de educação de segurança terá início na admissão e só será finalizado por ocasião do desligamento.

A educação de segurança deve conter quatro elementos básicos:

c.1 uma orientação inicial visando explicar a razão das medidas de segurança e os motivos para o seu cumprimento;

c.2 uma orientação específica, visando informar quais são as medidas de segurança e como proceder para cumpri-las;

c.3 uma orientação periódica, reavivando a necessidade da adequada observância às normas previstas; e

c.4 uma sinalização de advertência, na qual, por meio de cartazes, adesivos e outros meios, procurar-se-á manter a mentalidade de segurança, lembrando permanentemente aos envolvidos, as medidas de segurança preconizadas nas orientações referidas.

c.5 as medidas de segurança visam a criar uma cultura de Segurança Orgânica para todos os integrantes, sejam permanentes ou temporários, do CBMPA.

Controle de segurança no desempenho da função

A partir da admissão até o desligamento, deve ser feito um acompanhamento com o objetivo de detectar indícios de infiltração e recrutamento adversos e de comportamentos incompatíveis com o exercício da função, por representarem riscos à salvaguarda do conhecimento e/ou dado.

Todo indicio de procedimento inadequado deve ser objetivo de investigação para esclarecimento da suspeita.

SEGURANÇA NO DESLIGAMENTO:

A segurança no desligamento visa, previamente, a levantar indícios de vulnerabilidade de segurança e, posteriormente, a verificar a existência de um comportamento adequado.

a.1 a fase de desligamento será acompanhada por um processo de transferência de funções e rotinas, para dar continuidade às atividades sem risco de rupturas.

a.2 na medida que os sistemas de senhas e credenciais for passado para o novo gestor, o antigo gestor perde automaticamente o acesso às informações.

a.3 será estabelecido um período de quarentena, onde não será permitido o compartilhamento de informações e rotinas da antiga função, tempo necessário para que todos os sistemas de segurança (senhas e rotinas) sejam alterados para garantia da segurança das informações e das pessoas envolvidas no processo.

8.2- QUANTO A SEGURANÇA DA DOCUMENTAÇÃO E DO MATERIAL

Compreende o conjunto de medidas voltadas para os documentos e materiais, no sentido de evitar o comprometimento.

8.2.1- Considerações Gerais

Os documentos e os materiais, por constituírem os suportes mais comuns dos conhecimentos e/ou dados sensíveis, tornam-se alvos permanentes às ações adversas, em particular da espionagem e da sabotagem.

O comprometimento poderá efetuar-se, ainda, em decorrência de ações desenvolvidas sem objetivo deliberado de afetar conhecimento e/ou dado, mas também de fenômenos naturais.

As medidas de Segurança da Documentação e do Material visam, portanto, a fazer frente a essas ameaças e estão previstas na Lei nº 12.527/2011 – Lei de Acesso à Informação e o Decreto nº 7.845/2012 – que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, estão previstos os procedimentos fundamentais para esta finalidade; no entanto, tais procedimentos devem ser adaptados ou complementados para atender às peculiaridades de cada setor do CBMPA.

A Segurança da Documentação e do Material é garantida através do exato cumprimento dos regulamentos, instruções ou normas que regem a produção, a classificação, a expedição, o recebimento, o registro, o manuseio, a guarda, o arquivamento e a destruição de documentos e materiais sensíveis.

8.2.2 MEDIDAS DE SEGURANÇA DA DOCUMENTAÇÃO E DO MATERIAL

a. Os documentos e materiais possuem um ciclo de vida que pode ser desdobrado nas seguintes etapas: produção, difusão, recepção, manuseio, arquivamento/guarda e destruição.

b. As medidas de segurança da documentação e do material estão agrupadas em cinco tipos particulares de segurança:

b.1 segurança na produção;

b.2 segurança na difusão e recepção;

b.3 segurança no manuseio;

b.4 segurança no arquivamento; e

b.5 segurança na destruição.

c. As medidas a seguir descritas estão relacionadas objetivamente aos documentos sigilosos, devendo sofrer as necessárias adaptações de acordo com a legislação vigente (Lei nº 12.527/2011 e o Decreto nº 7.845/2012) quando da sua aplicação aos materiais e aos documentos não sigilosos.

8.2.3 SEGURANÇA NA PRODUÇÃO

a. As medidas de segurança na produção visam à atribuição de um grau de sigilo, ao controle dos recursos utilizados na produção de documentos sigilosos e à marcação destes documentos com sinais de segurança.

b. Medidas a serem executadas

b.1 Atribuição preliminar de um grau de sigilo - Atribuir preliminarmente um grau de sigilo ao documento ou material em fase de produção, levando em consideração fatores, tais como: a natureza do assunto, a finalidade, o usuário, os aspectos essenciais, etc.

b.2 Controle dos recursos utilizados - Alguns dos recursos utilizados na elaboração de documento ou material sigilosos, tais como rascunhos, notas, desenhos, gravações, imagens, cópias e etc., devem ser objeto de controle de segurança por parte de seus responsáveis. Entre estes recursos, alguns devem ser destruídos após a sua utilização e outros devem ser objeto de cuidados especiais relativos à sua segurança

b.3 Numeração das páginas. Esta medida tem por objetivo estabelecer procedimentos uniformes quanto à numeração das páginas que compõem o documento já formalizado, representando um sinal de segurança contra o extravio e a subtração de páginas.

c. Classificação e marcação do grau de sigilo

c.1 Considerando-se, pois, o documento já formalizado, será definido seu grau de sigilo com base nos critérios contidos na Legislação. O ato de atribuir um grau de sigilo ao documento formalizado denomina-se classificação. Nos casos dos documentos acabados, esta classificação irá ratificar ou retificar o grau de sigilo atribuído preliminarmente ao mesmo.

c.2 O grau de sigilo atribuído a um documento irá condicionar os procedimentos de segurança a serem adotados na difusão, na recepção, no manuseio, no arquivamento e na sua destruição. A atribuição de um grau de sigilo inadequado poderá causar o comprometimento ou gerar entraves



burocráticos desnecessários além de prejuízo ao planejamento de ações.

c.3 Ressalte-se, ainda, que todas as pessoas que tenham classificado um documento como sigiloso devem, periodicamente, proceder a uma revisão, reclassificando-o ou cancelando a classificação sigilosa que lhe foi atribuída, sempre que as circunstâncias o exigirem. Esta providência é importante para a segurança orgânica, pois poderá evitar a depreciação das suas medidas e respeitando os princípios da administração pública da transparência de seus atos.

c.4 A classificação sigilosa dos documentos é formalizada com a marcação do grau de sigilo, indicando àqueles que venham a difundi-los, a manuseá-los, a arquivá-los e a destruí-los, os procedimentos de segurança a serem adotados.

c.5 Autenticação do documento - A autenticação do documento tem por objetivo garantir ao usuário a fidelidade da origem, ou seja, confirmar a verdadeira procedência da documentação. O correto uso do sinal convencionado é mais uma prova de segurança para reconhecer a autenticidade do documento.

8.2.4 SEGURANÇA NA DIFUSÃO E RECEPÇÃO

As medidas de segurança na difusão e recepção visam a estabelecer controles de segurança na rotina de tramitação dos documentos entre o produtor e o usuário.

Medidas a serem executadas

a.1 Acondicionamento do documento - Esta medida tem por objetivo estabelecer procedimentos relativos ao acondicionamento do documento a ser expedido, por intermédio de providências cautelares que dificultam as ações adversas, permitindo a identificação de indícios de comprometimento pela violação de seu acondicionamento.

a.2 Controle de saída - É efetivado pela adoção de procedimentos relacionados com o registro de saída, com a atribuição de responsabilidades pela expedição e pelo tráfego do documento sigiloso, no sentido de possibilitar um eficaz controle na sua difusão. Especial atenção merece o endereçamento dos documentos, o qual deve ser antecipadamente confirmado, se necessário.

a.3 Controle de entrada - Tem por objetivo estabelecer efetivo controle de recepção e da tramitação interna dos documentos sigilosos recebidos, adotando-se procedimentos relativos à inspeção do acondicionamento e à autorização para abertura de invólucros, assinatura de recibos, distribuição interna, enfim, todos os tipos de registros que possibilitem a definição de responsabilidades quando da constatação de comprometimento.

8.2.5 SEGURANÇA NO MANUSEIO

As medidas de segurança no manuseio visam a estabelecer procedimentos para reprodução, custódia e revisão de classificação sigilosa dos documentos no sentido de implementar controles de segurança durante sua utilização.

Medidas a serem executadas

a.1 Controle de reproduções - É preciso estabelecer procedimentos relativos à autorização para reproduzir documentos, seja tirar cópias, seja elaborar extratos. Objetiva limitar riscos de comprometimento pelo controle do processo de reprodução dos documentos sigilosos. Cuidados especiais merecem as cópias e os extratos quando da sua destruição, e principalmente, na difusão da reprodução, inserindo no documento uma codificação ou um código alfanumérico específico para cada destinatário que vier a receber a respectiva cópia ou extrato, a fim de que se possa identificar a origem de um possível vazamento.

a.2 Controle de custódia - Enquanto permanecer nas mãos do usuário, deve existir um efetivo e permanente controle do documento sigiloso. Para tanto, devem ser estabelecidos procedimentos cautelares em termos de custódia e da guarda dos documentos durante o período de utilização.

a.3 Reclassificação ou desclassificação - Enquanto o documento sigiloso for considerado útil, deve o usuário preocupar-se com o grau de sigilo estabelecido na origem, no sentido de alterar a classificação sigilosa do documento ou mesmo de desclassificá-lo, visto não julgar-se mais necessário restringir-lhe o acesso.

a.4 Seleção dos documentos a serem arquivados ou destruídos - Esta medida tem por objetivo estabelecer critérios para selecionar a documentação que deve ser arquivada e a que deve ser destruída. Estes critérios devem ter por base o conteúdo, verificando a oportunidade de seu possível reaproveitamento.

8.2.6 SEGURANÇA NO ARQUIVAMENTO

As medidas de segurança no arquivamento visam a definir locais e processos adequados de arquivamento e recuperação dos documentos sigilosos e a estabelecer rotinas para situações de emergência.

a. Medidas a serem executadas

a.1 Escolha do local - Esta medida objetiva selecionar o local adequado, sob o enfoque de segurança, para a instalação dos arquivos que abrigam documentos sigilosos. Entre outras, impõem-se as preocupações quanto à circulação de pessoas e ao deslocamento da documentação em casos de emergência.

a.2 Escolha do tipo de arquivo ou cofre - O tipo de arquivo ou cofre, por sua vez, decorre da avaliação do modelo adequado para abrigar os documentos de diferentes graus de sigilo.

a.3 Controle no arquivamento e na recuperação - É efetivado pelo estabelecimento de rotinas para o arquivamento e a recuperação dos documentos nos arquivos. Exige-se a definição de responsabilidades para o manuseio e controle dos documentos sigilosos arquivados

a.4 Estabelecimento de rotinas para evacuação em situações de emergência - É importante, também, que se estabeleçam procedimentos relativos à evacuação da documentação sigilosa em situações de emergência. Esta medida requer a necessidade de se estabelecer prioridades e responsabilidades para estas situações e de se determinar, antecipadamente, locais alternativos para abrigar os documentos a serem salvos.

8.2.7 SEGURANÇA NA DESTRUIÇÃO

As medidas de segurança na destruição visam a definir meios e locais de destruição, a determinar formas de controle, bem como estabelecer rotinas para situações de emergências.

Medidas a serem executadas

a.1 Escolha dos meios e dos locais de destruição - Selecionados os documentos, é preciso escolher os meios a serem utilizados (incineradores ou trituradores), bem como os locais onde eles serão destruídos.

a.2 Controle da destruição - Objetiva estabelecer rotinas criteriosas para a efetiva destruição dos documentos sigilosos julgados inservíveis. Todos os procedimentos devem ser controlados e executados de forma centralizada, a fim de evitar desvios de documentos e falhas no processo que não levem a sua plena destruição. Exigem-se providências referentes a relações e/ou termos de destruição, obedecendo às prescrições contidas na Lei nº 12.527/2011 e no Decreto nº 7.845/2012.

a.3 Estabelecimento de rotinas para destruição em situações de emergência - Da mesma forma que a segurança no arquivamento preconiza uma medida relativa à situações de emergência, é necessário o estabelecimento de procedimentos referentes à destruição da documentação sigilosa nas mesmas situações. Esta medida será implementada quando existir o risco de comprometimento por acesso não autorizado ou em casos nos quais se devam estabelecer prioridades para preservação dos documentos sigilosos

8.3- QUANTO A SEGURANÇA DAS COMUNICAÇÕES

A segurança das comunicações compreende um conjunto de medidas voltadas para as comunicações, no sentido de salvaguardar conhecimento e/ou dado, de modo a impedir ou dificultar a interceptação, análise da transmissão e do tráfego

8.3.1 CONSIDERAÇÕES GERAIS

a. É frequente a busca adversa de conhecimento e/ou dado através de um trabalho inicial de interceptação, decorrendo, ainda, análises, simultâneas ou sucessivas, relacionadas com os meios de comunicações, com o fluxo de mensagens entre os correspondentes e com o conteúdo das mesmas. Em suma, a busca adversa de conhecimento e/ou dado por meio das comunicações exige, além da capacidade de interceptar, a competência para desenvolver a análise de transmissão, a análise do tráfego e a criptoanálise.

b. Quando de posse do conhecimento e/ou dado, resultante desta citada ação, o adversário irá utilizá-los com a preocupação de não revelar, ao interceptado, qualquer indício sobre a fragilidade de seus meios de comunicações.

c. É por isso que, para fazer frente a essa ação adversa, são efetivadas as medidas de Segurança das Comunicações, no que se refere particularmente aos meios de comunicações, ao fluxo de mensagens e ao seu conteúdo. Isto é garantido pela observância de normas especiais de exploração e regras operacionais, com a finalidade de impedir que assuntos sensíveis cheguem ao conhecimento de pessoas e/ou organizações não autorizadas. Em consequência, a segurança das comunicações se particulariza através da:

- 1. segurança da transmissão; e
- 2. segurança do conteúdo.

8.3.2 SEGURANÇA DA TRANSMISSÃO

As medidas de segurança da transmissão visam a proteger fisicamente os meios de comunicações e a dificultar a interceptação de mensagens e a consequente análise do fluxo das mesmas.

Medidas a serem executadas

a.1 Escolha dos locais para instalação dos equipamentos devidamente preparados com suporte de energia e backup

a.2 Como primeira providência básica, impõe-se a necessidade de se escolher, adequadamente, os locais para instalação dos equipamentos de comunicação. Objetiva, esta medida, criar obstáculos às ações adversas de interceptação, em particular, àquelas voltadas para as linhas que configuram

a.3 o esquema dos meios de telecomunicações (telefone, internet, Wi-Fi etc).

a.3 Os locais escolhidos devem ser avaliados em razão da possibilidade de controle da circulação de pessoas e, em consequência, da dificuldade de implementação de ações adversas de espionagem e, também, de sabotagem.

Escolha do meio de comunicações

b.1 Com base nos meios disponíveis, deve ser selecionado o meio de comunicações de acordo com a sensibilidade do conhecimento e/ou dado a ser transmitido, e de tal forma que chegue às mãos do usuário em tempo hábil.

Esta perfeita adequação deverá ser determinada pelo justo equilíbrio entre os princípios da Oportunidade e da Segurança com tecnologia segura e confiável

b.2 Na escolha do meio a ser empregado, deve ser considerado também, o aspecto da alternância, buscando-se atualizações constantes. Estas variações dizem respeito à:

Alternância dos meios, fruto da relação conteúdo/recurso adequado; e

Alternância dos operadores dos equipamentos ou dos messageiros.

c. Exploração adequada dos meios de comunicações - Esta medida, intimamente ligada à anterior, tem por objetivo estabelecer não só os procedimentos que permitam o uso correto dos meios, mas também um disciplinamento na sua exploração, determinando assim, quem pode transmitir o que, através de que meios e em que momento.

d. Utilização do código de chamada - Objetiva estabelecer os procedimentos relativos à exploração de um sistema de sinais convencionados que confirme ao receptor a real origem da chamada. Visa, em última análise, a dificultar ações adversas de intromissão na rede de comunicações.

8.4- QUANTO A SEGURANÇA DAS ÁREAS E INSTALAÇÕES

Compreende um conjunto de medidas voltadas para os locais onde são elaborados, tratados, manuseados ou guardados conhecimentos e dados sensíveis, com a finalidade de salvaguardá-los.

8.4.1 CONSIDERAÇÕES GERAIS

a. Assim, como para os demais tipos de segurança, também para a Segurança das Áreas e Instalações, assumem importância destacada as ações adversas desenvolvidas com o objetivo deliberado de causar o comprometimento ou indireto de pessoas não autorizadas em locais de produção de conhecimento sensível. As instalações e setores de importância ao CBMPA e a intersetão (intencional ou não) nas rotinas internas de trabalho



- b. No interior das instalações do CBMPA poderão, ainda, ocorrer acidentes de qualquer natureza que também causem o comprometimento da normalidade das ações, (tais como o tráfego de veículos em alta velocidade decorrente a chamadas de emergência ou o deslocamento de equipamentos pesados ou sensíveis ao uso sem a devida competência), esses atos intencionais ou não devem ser motivo de preocupação para Segurança das Áreas e Instalações.
- c. A implementação da Segurança das Áreas e Instalações exige como providência prévia o cumprimento das prescrições referentes à proteção de áreas, edificações, instalações e serviços essenciais.
- d. É obtida pela adoção de medidas de proteção geral, fiscalização e controle do acesso a locais sensíveis, de pessoal orgânico ou não, bem como pela demarcação de áreas de serviços específicos (como o controle de estacionamento), bloqueio e permanente controle das áreas sigilosas e restritas ou de tomada de decisões.
- e. Para tanto, impõe-se a avaliação das necessidades de segurança das áreas e instalações que pertençam as unidades do CBMPA. Estas providências objetivam definir os locais a serem preservados por abrigarem conhecimento e/ou dado sigilosos (áreas sigilosas) ou por serem consideradas vitais para o pleno funcionamento do CBMPA (áreas restritas), da mesma forma como o controle da circulação de agentes não orgânicos nas unidades com uma rápida e segura identificação.
- f. As necessidades de segurança das áreas sigilosas dependem dos diferentes graus de sigilo e as necessidades das áreas restritas derivarão dos níveis de importância de cada uma delas

8.4.2 MEDIDAS DE SEGURANÇA DAS ÁREAS E INSTALAÇÕES

Abrange as barreiras de acesso físico ou virtual; o estabelecimento de protocolos de ação e a aplicação de sistemas de códigos. E o estudo destinado a planejar a distribuição das áreas por atividades de interesse à Instituição, seus acessos e meios de evacuação, segurança das instalações e a circulação e acesso de pessoas as diversas dependências. Podemos destacar assim:

Demarcação das áreas

Tem por objetivo a sinalização de todas as áreas das unidades do CBMPA, de acordo com suas funções, em um sistema de códigos (cor, letras, números). Esse sistema permite uma rápida identificação das áreas sensíveis da instituição e proporciona o encaminhamento preciso de pessoas que não sejam da instituição.

Esse sistema deve ser aplicado para o controle e direcionamento das vagas de estacionamento interno da Corporação, uma vez que o CBMPA deve destinar vagas estrategicamente posicionadas as viaturas oficiais, aos tomadores de decisões e ao público interno, ao público externo deve ser destinado uma área específica de estacionamento com a identificação dos veículos (cartões fixados no para-brisa dos carros com uma codificação, por letra e cor) para melhor visualização das equipes responsáveis pela segurança interna da instituição.

Os procedimentos de vistoria dos veículos do público externo devem ser estabelecidos como normas de segurança orgânica voltadas para salvaguarda do patrimônio da instituição, da mesma forma que o procedimento deve ser aplicado respeitando os parâmetros da cortesia e objetividade para não ocupar tempo dos condutores ao deixar a instituição.

Da mesma forma que a equipe de portaria deve fazer a identificação (nome do condutor, CNH, Placa, cor e modelo do carro, horário de entrada e local a que se destina) a equipe deve se dirigir ao condutor na hora da saída dele da instituição, checando as informações visualmente e fazendo a vistoria.

Implantação de barreiras

- b.1 É implementada através da criação de obstáculos de qualquer natureza, para impedir o ingresso de pessoas não autorizadas nas diferentes instalações do CBMPA e nas áreas sigilosas ou restritas e permitir um efetivo controle da circulação das pessoas que possuam autorização para tal.
- b.2 Diferentes tipos de barreiras podem ser utilizadas, sendo as mais usuais cercas, muros, guardas, sistemas de identificação e controle de pessoas e veículos, alarmes, iluminação de segurança, câmeras conectadas a uma central de controle interna com sistema de gravação e, até mesmo, animais.
- b.3 Utilização de sistema de controle de identificação de pessoas e veículos nas barreiras físicas, com o controle na portaria e o isolamento de áreas (andares, setores) com portas (vidro ou madeiras) para pessoas não autorizadas
- c. Controle de Acesso
- c.1 O controle de acesso é um processo, por meio do qual se permite ou proíbe-se que um indivíduo tenha acesso a qualquer área ou objeto específicos.
- c.2 Predominando a finalidade de segurança, pode-se proceder ao controle de acesso a partir da proteção de uma área, instalação, uma sala ou uma dependência qualquer.
- c.3 O controle de acesso baseia-se na identificação e na avaliação dos graus de autorização de acesso, podendo ser desde a liberação direto ao setor ao encaminhamento de sala de espera.
- c.3 Entre os métodos de acesso, incluem-se normalmente um ou mais dos seguintes exemplos abaixo:
- Algo que esteja em poder de uma pessoa: uma chave, um crachá, um cartão, identificação biométrica; e
 - Algo que seja de conhecimento de alguém: uma senha, um código ou uma contribuição de palavra, frase e número.

d. Níveis de Segurança

- d.1 A fechadura e chave constituem as mais conhecidas formas de controle de acesso. Tais dispositivos proporcionam, por sua vez, os mais baixos níveis de segurança e controle de acesso, já que dependem inteiramente de algo que esteja em poder de uma pessoa, tal como uma chave que pode ser perdida, roubada, ou esquecida em um lugar qualquer e encontrada por alguém que possa utilizá-la. No caso do controle de acesso por senha, seu uso sem os devidos cuidados constitui situação análoga.
- d.2 Um alto nível de segurança exige que seja comprovada qualquer identificação, como no emprego de um cartão ou passe único com a fotografia do portador, o qual poderia ser examinado e conferido por uma guarda de segurança.

e. Sistemas de Controle de Acesso

- e.1 Os sistemas de equipamento e de controle de acesso variam desde as fechaduras até os dispositivos que realizam análises biométricas. Entre estes dois extremos existe uma infinidade de sistemas baseados em cartões e teclado digital.
- e.2 Os sistemas de controle de acesso podem ser classificados em:
- Não automático - porteiros, recepcionistas;
 - Semi-automático - interfones, porteiros eletrônicos e porteiros eletrônico supervisionados; e
 - Automático - teclados (a partir do correto acionamento de senha numérica digitada) e cartões de diferentes tipos, tais como: tarja magnética, magnéticos de proximidade, óticos, perfurados, leitura de barras, etc.

f. Detecção de Intrusão e Monitoração de Alarme

- f.1 Os sistemas destinados a detectar intrusão ou violação possuem três elementos básicos:
- f.1.1 dispositivos de detecção - sensores que detectam a presença de um intruso;
- f.1.2 sistemas de transmissão - métodos utilizados para transmitir um sinal de alarme; e
- f.1.3 sistema de monitoração - equipamento e método usados para controlar e monitorar o sistema e gravação de áudio e vídeo
- f.2 Será de responsabilidade da B2 o acompanhamento preventivo de ameaças de interceptação de comunicação telefônica, de internet e ambiental nas áreas onde ocorrer o processo decisório (gabinete do Comandante-Geral, Salas de Reunião, Salas de controle, e outras que forem consideradas de importância para a segurança de ações a serem desenvolvidas pelo CBMPA e a Defesa Civil)
- f.3 Tais equipamentos funcionam com sensores infravermelhos, micro-ondas, de deslocamentos de imagens, fotoelétrico, de proximidade, sísmico, choque e/ou combinação dos mesmos, cabe ao CBMPA a definição, junto a B2 do melhor sistema de monitoramento de acordo com a esfericidade do local a ser guardado

g. Elaboração de planos de Prevenção e Combate a Incêndios e de Defesa do Aquartelamento

- g.1 Essas medidas objetivam a estabelecer procedimentos preventivos e corretivos quando da ocorrência de sinistros de qualquer espécie, no sentido de evitar o comprometimento dos conhecimentos e/ou dados sensíveis contidos nas diferentes áreas do CBMPA.
- g.2 Na elaboração dos planos, ainda, devem ser consideradas todas as necessidades preconizadas pela Segurança da Documentação e do Material, interagindo com a medida de Segurança do Pessoal denominada Educação de Segurança, dada a necessidade de se realizarem treinamentos do pessoal para adoção de comportamentos adequados, quando da ocorrência de situações de emergência

- g.3 O estabelecimento de protocolos de evacuação de áreas e instalações, equipes responsáveis por ações específicas e pontos de acomodação das pessoas evacuadas pela livre circulação de rotas e vias para as equipes de combate ao sinistro e socorro
- g.4 Por último, há que se efetivar investigações quando da ocorrência de tais situações, no sentido de identificar as suas causas, procurando levantar as possíveis ações deliberadas que tenham por objetivo causar o comprometimento e de identificar os conhecimentos e/ou dados que tenham sido comprometidos.

8.5- QUANTO A SEGURANÇA DA INFORMÁTICA

É o conjunto de medidas destinadas a preservar o sigilo das atividades de processamento, de transmissão de dados e a integridade dos sistemas, materiais e programas de Informática do CBMPA e da Defesa Civil do Estado do Pará.

8.5.1 OBJETIVOS DA SEGURANÇA DA INFORMÁTICA

- a. Garantir a continuidade da atividade de Informática.

A área de Informática torna-se cada vez mais importante à medida que praticamente todas as atividades do Sistema de Segurança Pública do Pará, do CBMPA e da Defesa Civil Estadual dependem de sua atuação e atualização. Qualquer paralisação ou falha de processamento de dados pode comprometer o funcionamento eficaz da instituição.

- b. Garantir a integridade dos conhecimentos que estão sob controle dos sistemas informatizados

Considerável parcela dos principais conhecimentos do CBMPA e da CEDEC são controlados por sistemas informatizados. Deste modo, torna-se crítica a segurança dos arquivos de dados e sistemas de aplicação, cujas falhas podem causar o comprometimento dos mesmos, provocadas por erros humanos, técnicos ou ações criminosas.

Manter a integridade e confiabilidade dos conhecimentos

A área de Informática é detentora de grande volume de conhecimentos de alto valor para estratégia para o CBMPA e a Defesa Civil. Estes conhecimentos devem ser protegidos contra o uso indevido, prevendo-se a exclusividade de utilização do conhecimento pelo usuário.

8.5.2 MEDIDAS DE SEGURANÇA DA INFORMÁTICA

- a. Em virtude da crescente importância dos sistemas de processamento de dados para a Segurança Pública e a Defesa Social do Estado do Pará, impõe-se ao CBMPA e a Defesa Civil Estadual a adoção de medidas de segurança, que podem ser dos seguintes tipos:
- Física;
 - De “Software”;
 - De “Hardware”;
 - De Pessoal.

- b. Essas medidas devem ser aplicadas sempre em conjunto, para que os conhecimentos e/ou dados estejam sempre íntegros, confiáveis e disponíveis na oportunidade desejada.

8.5.3 SEGURANÇA FÍSICA

- a. Medidas de segurança física

As medidas de segurança física visam a proteger o Ambiente de Processamento de Dados (APD), os locais onde se encontram os computadores, terminais de computação, HD Externos, Pen Drives institucionais, Sistema de Wi-Fi, Ilhas de Impressão e documentos em geral, relativos aos



sistemas, programas e esquemas de banco de dados contra o acesso de pessoas não autorizadas e a proteger dos riscos naturais e/ou intencionais.

b. Além das Medidas de Segurança das Áreas e Instalações devem ser observados os seguintes procedimentos:

b.1 armazenagem externa de dados (“back-up”)

b.1.1 A armazenagem externa dos dados visa evitar a interrupção do processamento de dados nos casos de sinistro ou sabotagem dos dados originais;

b.1.2 Para esse efeito, o local de armazenagem deverá ser afastado do local do arquivo original, de forma a impossibilitar a destruição simultânea;

Transporte de meios de dados digitais

Para se preservar a integridade dos meios digitais durante o transporte deverão ser adotadas algumas providências, entre elas:

c.1 Prevenir choques térmicos, choques físicos e desmagnetização;

c.2 Utilizar meios adequados de transporte; e

c.3 Usar equipamentos de armazenamento adequados.

8.5.4 SEGURANÇA DE “SOFTWARE”

a. Os programas que processam e analisam no interior de um Equipamento de Informática, micro computadores, computadores de grande ou médio portes, periféricos, etc. são denominados “software”. Eles podem ser de diferentes tipos como: de sistema operacional, de processador de texto, de mineração de banco de dados, de editoração eletrônica, de processador gráfico, de planilhas, etc.

b. Ao serem instalados os equipamentos, os “software” possibilitam o contato do usuário com a máquina, por intermédio do sistema implantado, possuindo na maioria das vezes, em sua organização, pontos críticos de entrada e, até mesmo, de colocação de senhas adequadas.

c. As medidas de segurança de “software” constituem-se nos procedimentos que devem ser adotados ou explorados nos diferentes “software”, objetivando que eles não sejam violados em sua estrutura ou não sejam instalados ou operados por elementos não credenciados.

d. Podem ser citados:

d.1 testar exaustivamente os “software” a serem adquiridos, observando com atenção as especificações dos manuais do usuário e de instalação, principalmente nos pontos que possam deixar vulnerabilidades de acesso;

d.2 verificar a idoneidade do fabricante e o respaldo de aprovação do “software” em nível nacional e internacional;

d.3 solicitar à firma proprietária do “software” os testes desejados, bem como uma demonstração específica no equipamento existente no CBMPA e da Defesa Civil;

d.4 usar senhas de acesso de roteadores e Wi-Fi, normais e codificadas, em nível individual, que controlem o acesso aos diferentes programas e a sistemas predeterminados;

d.5 utilizar “software” que permita acesso a programas e bancos de dados em horas e intervalos predeterminados, em terminais específicos e em seções ou divisões anteriormente definidas e protegidas;

d.6 realizar um controle geral, via “software”, de todas as operações executadas por um determinado elemento, de modo que, a qualquer momento, se possam ter estatísticas e controle dos envolvidos no processo;

d.7 colocar “password” ou atributos de leitura a gravação nos diferentes relatórios e arquivos, de modo a manter a individualidade de acesso e gravação, aprimorando a segurança;

d.8 usar, de modo planejado e em todas as ocasiões possíveis, “software” específico para verificar se os dispositivos móveis possuem a capacidade de armazenamento, bem como, os discos rígidos (“WINCHESTER”) estejam “limpos de vírus”, que comprometam a integridade dos programas e dos sistemas operacionais instalados;

d.9 realizar credenciamento de terminais e computadores às redes instaladas nos diferentes equipamentos, de modo que não permitam a interceptação e/ou interferência por outros não autorizados; e

d.10 realizar cópias (“back-up”) dos dados e programas em uso; e

d.11 credenciamento das firmas fornecedoras de “software” e o processo de atualização dos sistemas.

e. As Seções e áreas do CBMPA e da CEDEC que produzem conhecimentos de sensível nível estratégico devem preservar a identificação e as especificações técnicas dos softwares empregados.

f. O compartilhamento de dados em “Sistema de Nuvens” deve ser feito de forma protocolar por meio de identificação das pessoas com acesso ao sistema, com a identificação dos meios usados, usuários, horários e o conteúdo acessado.

8.5.5 SEGURANÇA DE “HARDWARE”

a. O equipamento de Informática, de grande, médio e pequeno porte ou mesmo microcomputadores, seus componentes e suas placas internas de diferentes naturezas são considerados “hardware”.

b. Medidas de segurança podem ser adotadas para verificar ou mesmo impedir a sua vulnerabilidade e manter o perfeito funcionamento dos equipamentos. Algumas medidas são:

b.1 verificar, durante a aquisição dos Equipamentos, os tipos de segurança existentes, os testes a que foram submetidos e se estão dentro dos padrões e normas técnicas de fabricação nacional ou internacional;

b.2 certificar-se, durante a aquisição, do recebimento dos termos de garantia e da disponibilidade de rede autorizada de manutenção dos equipamentos;

b.3 introduzir senhas de acesso no sistema básico de entrada e saída (BIOS) no interior das placas internas do computador, que impossibilitem o acesso inicial por operador não credenciado.

b.4 credenciamento das firmas fornecedoras de “hardware”.

c. As Seções e áreas do CBMPA e da CEDEC que produzem conhecimento sensível de nível estratégico devem preservar a identificação e as especificações técnicas dos equipamentos empregados.

8.5.6 SEGURANÇA DE PESSOAL

As medidas de segurança de pessoal específicas para a Informática, além das previstas na Segurança de Pessoal, são as seguintes:

a. as funções do pessoal de Informática devem ser adequadamente compartimentadas, de forma a evitar ao operador o acesso a mais informações do que o exigido pela necessidade de conhecer, indispensável ao cumprimento de suas tarefas;

b. atribuição de uma senha pessoal - “password” - a cada usuário do sistema de Informática. Recomendar o uso individual da referida senha e proibir a sua divulgação para outras pessoas;

c. troca periódica de “password” do usuário de cada sistema;

d. instrução de Segurança da Informática, sempre que ocorrer troca de senha ou quando julgada necessária;

e. credenciamento do pessoal técnico das firmas de manutenção que prestam serviços de assistência técnica ao sistema; e

f. Estabelecer sistemas e protocolos de desc credenciamento das pessoas desligadas dos setores produtores de conhecimento.

8.6- QUANTO AO PLANEJAMENTO DE SEGURANÇA ORGÂNICA

O Planejamento de Segurança Orgânica é um instrumento que possibilita a adoção de medidas de segurança adequadas às necessidades particulares de cada Seção e/ou áreas do CBMPA e da Defesa Civil Estadual, com a adoção de procedimentos, protocolos e medidas de segurança sem a necessária análise dos aspectos envolvidos poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação.

8.6.1- FASES DO PLANEJAMENTO DE SEGURANÇA ORGÂNICA

a. Um eficaz planejamento de Segurança Orgânica, para o CBMPA e a CEDEC, de qualquer tipo e nível, é alcançado pela execução das seguintes fases:

a.1 Estudo de Situação;

a.2 Decisão;

a.3 Elaboração do Plano de Segurança Orgânica - PSO;

a.4 Implantação do PSO;

a.5 Supervisão das ações planejadas.

b. Estudo de Situação

Esta fase consiste no estudo de todos os fatores que envolvem a segurança do CBMPA e da Defesa Civil Estadual, bem como na elaboração de alternativas de, procedimentos que possam fornecer à organização a segurança necessária.

b.1 Estudo dos fatores

Entre os fatores que condicionam a segurança do CBMPA e da CEDEC, destacam-se os seguintes:

b.1.1 legislação;

b.1.2 diretrizes;

b.1.3 riscos à segurança; e

b.1.4 recursos.

c. Elaboração de alternativas

c.1 Nesta etapa, após o estudo dos fatores, serão definidos os objetivos a alcançar e elaboradas as alternativas para o seu atingimento.

c.2 Basicamente, cada alternativa deverá conter respostas às seguintes perguntas:

c.2.1 o que fazer?

c.2.2 quando fazer?

c.2.3 onde fazer?

c.2.4 como fazer?

c.2.5 com quem fazer?

d. Decisão

A responsabilidade pela segurança do CBMPA e da Defesa Civil Estadual é do seu comandante. Desta forma, cabe a ele a decisão adotada.

e. Elaboração do Plano de Segurança Orgânica - PSO

e.1 O Plano a ser elaborado é, na verdade, a materialização da decisão do Comandante do CBMPA e Coordenador Estadual de Defesa Civil.

Cabe aos planejadores detalhar os padrões de desempenho que serão exigidos para cada tarefa a ser cumprida e dar a redação final ao documento.

e.2 Algumas considerações a serem efetuadas:

e.2.1 assegurar um equilíbrio entre a segurança e o funcionamento eficaz do CBMPA e da CEDEC;

e.2.2 ser flexível;

e.2.3 evitar medidas de segurança excessivas ou que possam provocar situações degradantes ou vexatórias;

e.2.4 estabelecer coordenação com outras órgãos do Sistema de Segurança Pública do Pará ou da União ou dos municípios, nos aspectos que lhes forem comuns; e

e.2.5 atender às peculiaridades do CBMPA e da Defesa Civil Estadual.

f. Implantação do PSO



A implantação do Plano de Segurança Orgânica decorre de ordens contidas no próprio documento.

g. Supervisão das ações planejadas

g.1 Durante a implantação e a execução das ações previstas no Plano de Segurança Orgânica serão adotados procedimentos que permitam um acompanhamento de tais ações.

g.2 O acompanhamento das ações planejadas, será efetuado através de inspeções programadas, inopinadas ou situacionais. Através destas inspeções, serão levantados os dados que permitirão o controle e a avaliação das ações executadas. Decorrentes das avaliações, poderão ser necessárias ações de replanejamento, corrigindo distorções porventura encontradas.

8.6.2 PLANO DE SEGURANÇA ORGÂNICA - PSO

É o documento elaborado pelo chefe da 2ª Seção auxiliado pelos oficiais do EMG e Oficiais Comandantes do CBMPA e da Defesa Civil, que consubstancia as medidas necessárias à implementação da Segurança Orgânica a serem adotadas por todos os setores do CBMPA e da CEDEC.

a. Situação

Relatar, de forma sucinta, clara e objetiva, os aspectos abordados no Estudo de Situação realizado, assim como as razões que levaram o Comandante do CBMPA e o Coordenador Estadual da Defesa Civil a decidir pela adoção das medidas de segurança consubstanciadas no PSO.

b. Missão

Transcrever a decisão do Comandante do CBMPA, estabelecer normas peculiares de segurança e as tarefas necessárias relacionadas aos aspectos ligados à Pessoal, Documentação e Material, Comunicações, Áreas e Instalações, Informática, e outras julgadas necessárias, de acordo com as características do CBMPA e da Defesa Civil Estadual.

e. Execução

e.1 Relatar de forma objetiva como a Segurança Orgânica será implementada no CBMPA e na Defesa Civil Estadual; as atribuições, as responsabilidades, as normas e os procedimentos a serem cumpridos pelo CBMPA.

e.2 Poderá, a critério do Comandante, estar contida em anexos referentes a cada aspecto de segurança abordado.

e.3 Cada um dos anexos, deverá ter, como apêndice, a Lista de Verificação Aplicada que foi utilizada na aferição do nível de segurança do CBMPA e da Defesa Civil.

f. Medidas Administrativas

Explicitará as providências administrativas que viabilizarão o desencadeamento do PSO.

g. Prescrições Gerais

Estabelecimento de orientações particulares, prazos, ligações, alarmes, data de entrada em vigor, etc., e demais aspectos ligados à execução do PSO e não relatados anteriormente.

O PSO completo receberá a classificação sigilosa CONFIDENCIAL, e terá a sua distribuição controlada pela B2 do CBMPA.

Algumas partes do PSO poderão, a critério do Comandante do CBMPA, assessorado pelo Chefe da BM/2 do EMG, ser distribuídas, exclusivamente, aos responsáveis diretos pela execução das medidas previstas no PSO.

8.7- GRUPO DE DETENTORES DE CONHECIMENTO ESTRATÉGICO – GDCE

Grupo de pessoas com formação acadêmica e tecnológica específica, detentora de conhecimento notório, em áreas de interesse do CBMPA, que possam ser consultadas sobre eventos críticos envolvendo a atuação do CBMPA e da Defesa Civil Estadual, fornecendo informações estratégicas para o planejamento de ações do CBMPA e da CEDEC.

8.7.1- COMPOSIÇÃO DO GDCE

O GDCE é formado por profissionais não orgânicos ao CBMPA e a Defesa Civil Estadual, através da seleção de currículos em plataformas acadêmicas, acompanhamento de trabalhos de pesquisa desenvolvidos em instituições de Ensino Superior – IES, experiência profissional reconhecida em áreas específicas, entre outros, que possam ser contatadas pela B2 e convidadas a formarem um banco de dados de profissionais destinados a consultas ocasionais.

O banco de dados deverá ser composto pela identificação pessoal do profissional, sua área de atuação, contatos telefônicos, e-mail e aceite para consultoria em situações de crises e emergência.

Os profissionais consultados não farão parte de folha de pagamento do CBMPA, da Defesa Civil Estadual ou da SEGUP, mas poderão vir a receber proventos de acordo com a complexidade, expertise e tempo do trabalho realizado

O tempo máximo para a consulta não remunerada será de 3 (três) dias corridos, sendo que o mesmo só será contatado em situações excepcionais que fujam a competência dos profissionais do CBMPA e da CEDEC.

Durante as comemorações do Aniversário do CBMPA, esses profissionais que prestaram serviços de relevância a Corporação serão agraciados com diplomação e/ou medalha por trabalhos prestados ao CBMPA e a Defesa Civil Estadual, sendo reconhecidos como colaboradores de valor estratégico para instituição.

9. Considerações Finais

Este Manual representa o esforço de homens e mulheres que são o corpo e a alma do Corpo de Bombeiros Militar do Pará e da Defesa Civil Estadual, sendo o primeiro passo para a criação de uma cultura de Segurança Institucional permanente e de acordo com os princípios legais de um Estado Democrático de Direitos, respeitando a natureza de cada conhecimento produzido e protegido voltado para proteção e a segurança da sociedade paraense.

Referências

ANTUNES, Priscila Carlos Brandão. Serviço secreto e democracia no Cone Sul: Premissas para uma convivência legítima, eficiente e profissional. Niterói, RJ: Impetus, 2010.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília/DF: Senado Federal, 2018.

_____. LEI Nº 9.883, de 7 de dezembro de 1999 que Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Diário Oficial da União, Brasília, 1999.

_____. LEI Nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em: 12 mar. 2021.

_____. 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 mar. 2021.

_____. LEI Nº 12.528, de 18 de novembro de 2011. Dispõe sobre a Criação da Comissão Nacional da Verdade no âmbito da Casa Civil da Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12528.htm. Acesso em: 10 mar. 2021.

_____. Doutrina Nacional de Inteligência de Segurança Pública. Brasília: SENASP, 2016.

_____. Manual de Campanha. Atividade de Inteligência Militar. Brasília: Ministério da Defesa, 1995.

_____. Manual de Campanha. Atividade de Inteligência Militar – 2ª Parte. A atividade de inteligência nas Operações Militares. Brasília: Ministério da Defesa, 1999.

_____. Manual de Campanha. Contra-Inteligência Inteligência. Brasília: Ministério da Defesa, 2009

_____. DECRETO Nº 60.417, de 11 de março de 1967. Aprova o Regulamento para a Salvaguarda de Assuntos Sigilosos. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D60417.htm. Acesso em 20/mar/2021.

_____. DECRETO Nº 2.134, de 24 de janeiro de 1997. Dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2134.htm. Acesso em: 20 mar. 2021.

_____. DECRETO Nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em 18 mar 2021.

_____. DECRETO Nº 2.910, de 29 de dezembro de 1998. Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2910.htm. Acesso em 20/mar/2021.

_____. DECRETO Nº 2.182, de 20 de março de 1997. Estabelece normas para a transferência e o recolhimento de acervos arquivísticos públicos federais para o Arquivo Nacional Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2182.htm. Acesso em 17mar 2021.

_____. DECRETO Nº. 4.376, de 13 de setembro de 2002, dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, e dá outras providências. Diário Oficial da União, Brasília, 2021.

CÉSAR, Júlio. Comentários sobre a guerra Gálica – De Bello Gallico. Tradução Francisco Sotero dos Reis e Otto Maria Carpeaux. São Paulo: Edilouro. 2001

CEPIK, Marco. Sistemas Nacionais de Inteligência: Origens, Lógica de Expansão e Configuração atual. Rio de Janeiro: DADOS – Revista de Ciências Sociais, Vol. 46, nº 1, 2003, p 75-127

_____. (Org.) Inteligência Governamental: Contextos nacionais e desafios contemporâneos. Niterói. RJ: Impetus, 2011.

CLAUSEWITZ, Carl Von. Da Guerra: tradução Maria Tereza Ramos; preparação do original Mauricio Baltazar Leal. São Paulo. Ed Martins Fontes. 1996.

FARIAS, Antônio Cláudio Fernandes. A atividade de inteligência: o ciclo da produção do conhecimento. Belém/PA: Sagrada Família. 2017.

FERRO JUNIOR, Celso Moreira. A Atividade de Inteligência e a Gestão da Informação Policial: Conceitos, Técnicas e Tecnologias definidos pela experiência profissional e acadêmica. Brasília/DF: Fortium. 2008.



GONÇALVES, Joanisval Brito. Sed Quis Custodiet Ipso Custodes? O controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá. Tese de Doutorado em Relações Internacionais. Brasília: Instituto de Relações Internacionais, Universidade de Brasília, 2008.

_____. Políticos e Espiões: O controle da atividade de Inteligência. Niterói. RJ: Impetus, 2010.

HOBBS, Thomas. Leviatã. (Tradução de João Paulo Monteiro, Maria Beatriz Nizza da Silva e Cláudia Berliner.) 1. ed. São Paulo: Martins Fontes, 2003.

KAUTILYA. Arthashastra, O Maquiavel da Índia. Brasília/DF. Editora Universidade de Brasília. 1994.

LOWENTHAL, Mark. Intelligence: From Secrets to Policy. Washington D.C. CQ Press. 2000.

_____. U.S. Intelligence: Evolution and Anatomy. New York: Praeger Publishers. 1992.

_____. U.S. Intelligence Community: An Annotated Bibliography. New York: Garland. 1994.

MIRANDA, Wando Dias. O CONTROLE PARLAMENTAR DA ATIVIDADE DE INTELIGÊNCIA NO BRASIL: Um estudo sobre a produção legislativa da CCAI e da CREDN entre os anos de 2003 à 2010. Tese de Doutorado. Programa de Doutorado em Desenvolvimento Sustentável do Trópico Úmido, do Núcleo de Altos Estudos Amazônicos - NAEA, da Universidade Federal do Pará - UFPA. Belém/Pará. 2018.

PLATT, Washington. A Produção de Informações Estratégicas. Rio de Janeiro: Biblioteca do Exército, 1974

TZU, Sun e PIN, Sun. A Arte da Guerra - Edição completa. São Paulo: Martins Fontes, 2004.

[1](#) Brasil (1999) de acordo com a lei 9,883 art. 2º, Inteligência pode ser definida como a atividade que objetiva a obtenção, análise e disseminação de conhecimentos, dentro e fora do território nacional, sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado (Grifo nosso) esse conceito é corroborado por Cepik (2003); Antunes (2010) Gonçalves (2010), Farias (2017) e Miranda (2018), pois existe um consenso entre diferentes autores sobre a definição a atividade de inteligência.

[2](#) Entende-se como contra-inteligência a atividade que objetiva neutralizar a inteligência adversa através da criação e normatização de procedimentos, protocolos e estratégia de segurança orgânica.

Fonte: Nota nº 32.837 - 2021 - AJG

ATOS DO GABINETE DO CHEFE DO EMG

Sem Alteração

ATOS DO GABINETE DO COORD. ADJUNTO DA CEDEC

Sem Alteração

3ª PARTE ASSUNTOS GERAIS E DE JUSTIÇA

4ª PARTE ÉTICA E DISCIPLINA

Sem Alteração

**CARLOS AUGUSTO DE OLIVEIRA RIBEIRO - CEL QOBM
AJUDANTE GERAL**

