Secretária Nacional de Segurança Pública

Ministério da Justiça

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

DOUTRINA NACIONAL DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Brasilia, julho de 2009

RESERVADO

DOUTRINA NACIONAL DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

Brasília, julho de 2009

RESERVADO

DEDICATÓRIA

Dedicamos este trabalho a todos profissionais de inteligência em Segurança Pública, que colaboraram direta ou indiretamente para que este resultado grandioso fosse alcançado.

CAPÍTULO 1 – FUNDAMENTOS DOUTRINÁRIOS

RESERVADO

PRÓLOGO

Nas últimas décadas afloraram discussões sobre as diretrizes de uma Política Nacional que conduzisse ao estabelecimento de um Sistema Brasileiro de Inteligência, o qual se deu com o advento da Lei nº 9883/99. Em seguida, o Decreto 3695/2000 especifica o Subsistema de Inteligência de Segurança Pública, cujos fundamentos centram-se na preservação e defesa do Estado e das Instituições, na responsabilidade social, em respeito e obediência ao Estado Democrático de Direito, na medida em que oferece assessoria qualificada para a redução de incertezas no complexo cenário dos fenômenos criminais.

Todavia, sua doutrina ficou a mercê de uma instrução mais substantiva, mais específica e duradoura. Nesse sentido, coube à Secretaria Nacional de Segurança Pública, por meio da CGI/SENASP, a construção de tal instrumento normativo, levado a efeito a partir de muito estudo, pesquisa e contribuições de diversos atores importantes que ser encontravam dentro e fora dos muros desta Secretaria.

Refletimos e compreendemos a evolução fenomenológica da questão, concluindo que esta não deve ser tratada de forma nem monolítica, nem empírica. Precisa, cada vez mais, de método adequado, preservando-se os direitos e garantias fundamentais - escopo da doutrina ora apresentada.

Assim, sob a orientação e apoio do Secretário Nacional de Segurança Pública, Dr. Ricardo Brisolla Balestreri, a Coordenação-Geral de Inteligência apresenta a Doutrina Nacional de Inteligência de Segurança Pública. Entendemos que ela é fruto de uma realidade inaugural, alicerçada nos novos conceitos de justiça, sociedade, democracia, e paz social. Dessarte, ressaltamos com bastante convicção, que a DNISP hoje apresentada como uma significativa contribuição, deve ser celebrada e tida por toda comunidade como uma conquista - ainda que seja a primeira no gênero - pois precisamos ter sempre o horizonte da evolução de conceitos, processos e métodos.

Régis Limana
Coordenador-Geral de Inteligência
CGI/SENASP/MJ

CAPÍTULO 1 – FUNDAMENTOS DOUTRINÁRIOS

ATIVIDADE DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

1.1 – CONCEITO

A atividade de ISP é o exercício permanente e sistemático de ações especializadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera de Segurança Pública, basicamente orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os governos federal e estaduais a tomada de decisões, para o planejamento e à execução de uma política de Segurança Pública e das ações para prever, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza ou atentatórios à ordem pública.

1.2 - FINALIDADES

São finalidades da ISP:

- Proporcionar diagnósticos e prognósticos sobre a evolução de situações do interesse da segurança Pública, subsidiando seus usuários no processo decisório.

- Contribuir para que o processo interativo entre usuários e profissionais de Inteligência produza efeitos cumulativos, aumentando o nível de efetividade desses usuários e de suas respectivas organizações.

- Subsidiar o planejamento estratégico integrado do sistema e a elaboração de planos específicos para as diversas organizações do Sistema de Segurança Pública.

- Apoiar diretamente com informações relevantes as operações policiais de prevenção, repressão, patrulhamento ostensivo e de investigação criminal.

- Prover alerta avançado para os responsáveis civis e militares contra crises, grave perturbação da ordem pública, ataques surpresa e outras intercorrências.

- Auxiliar na investigação de delitos.

- Preservar o segredo governamental sobre as necessidades informacionais, as fontes, fluxos, métodos, técnicas e capacidades de Inteligência das agências encarregadas da gestão da segurança pública.

1.3 – CARACTERÍSTICAS

Características da ISP são os principais aspectos distintivos e as particularidades que a identificam e a qualificam como tal.

Suas principais características são:

- Produção de Conhecimento
- Assessoria
- Verdade com Significado
- Busca de Dados Protegidos
- Ações Especializadas
- Economia de Meios
- Iniciativa
- Abrangência
- Dinâmica
- Segurança

Produção de Conhecimento: é a característica da ISP que a qualifica como uma atividade de Inteligência, na medida em que coleta e busca dados e, por meio de metodologia específica, transforma-os em conhecimento preciso, com a finalidade de assessorar os usuários no processo decisório.

Assessoria: é a característica da ISP que a qualifica como órgão de assessoramento, produzindo conhecimentos para o processo decisório e para auxiliar as polícias em suas atividades.

Verdade com Significado: é a característica da ISP que a torna uma produtora de conhecimentos precisos, claros e imparciais, de tal modo que consiga expressar as intenções, óbvias ou subentendidas, das pessoas envolvidas ou mesmo as possíveis ou prováveis conseqüências dos fatos relatados.

Busca de Dados Protegidos: é a característica da ISP de obter dados não disponíveis e protegidos, em um universo antagônico, uma vez que os dados relevantes do ambiente criminal encontram-se, invariavelmente, protegidos.

Ações Especializadas: é a característica da ISP que, em face da metodologia, técnica e linguagem próprias e padronizadas, exige dos seus integrantes formação acadêmica, permanente, complementada por treinamento e experiência.

Economia de Meios: é a característica da ISP que permite otimizar os recursos disponíveis, proporcionada pela produção de conhecimentos objetivos, precisos e oportunos.

Iniciativa: é a característica da ISP que induz a produção constante de conhecimentos antecipados em atitude pró-ativa.

Dinâmica: É a característica da ISP que lhe possibilita evoluir adaptando-se às novas tecnologias, métodos, técnicas, conceitos e processos.

Abrangência: É a característica da ISP que, em razão dos métodos e sistematização peculiares, lhe permite ser empregada em qualquer campo do conhecimento de interesse da Segurança Pública.

Segurança: é a característica da ISP que visa garantir sua existência, protegida de ameaças.

1.4 – PRINCÍPIOS DA ISP

A ISP é exercida em perfeita sintonia com as suas finalidades e sob a égide de determinados princípios, de forma que a aplicação de um deles não acarrete prejuízo no emprego dos demais. Os princípios são as proposições diretoras - as bases, os fundamentos, os alicerces, os pilares - que orientam e definem os caminhos da atividade.

Os mais importantes princípios da ISP são:

- Amplitude
- Interação
- Objetividade
- Oportunidade
- Permanência
- Precisão
- Simplicidade
- Imparcialidade
- Compartimentação
- Controle
- Sigilo

Amplitude: é o princípio da ISP, que consiste em alcançar os mais

completos resultados possíveis nos trabalhos desenvolvidos.

Interação: é o princípio da ISP, que implica estabelecer ou adensar relações sistêmicas de cooperação, visando otimizar esforços para a consecução dos seus objetivos.

Objetividade: É o princípio que norteia a ISP, para que cumpra suas funções de forma organizada, direta e completa, planejando e executando ações de acordo com objetivos previamente definidos.

Oportunidade: É o princípio da ISP, que orienta a produção de conhecimentos, a qual deve realizar-se em prazo que permita seu aproveitamento.

Permanência: é o princípio da ISP, que visa proporcionar um fluxo constante de dados e de conhecimentos.

Precisão: é o princípio da ISP, que objetiva orientar a produção do conhecimento verdadeiro - com a veracidade avaliada -, significativo, completo e útil.

Simplicidade: é o princípio da ISP, que orienta a sua atividade de forma clara e concisa, planejando e executando ações com o mínimo de custos e riscos.

Imparcialidade: é o princípio da ISP, que norteia a atividade de modo a ser isenta de idéias preconcebidas e\ou tendenciosas, subjetivismos e distorções.

Compartimentação: é o princípio da ISP, que objetiva, a fim de evitar riscos e comprometimentos, restringir o acesso ao conhecimento sigiloso somente para aqueles que tenham a real necessidade de conhecê-lo.

Controle: é o princípio da ISP, que recomenda a supervisão e o acompanhamento sistemático de todas as suas ações, de forma a assegurar a não interferência de variáveis adversas no trabalho desenvolvido.

Sigilo: é o princípio da ISP, que visa preservar o órgão, seus integrantes e ações.

1.5 – VALORES

A atividade de ISP é constituída como um serviço à causa pública, submetida aos princípios constitucionais da moralidade, impessoalidade, eficiência e legalidade, e, em especial, à observância ao direito básico à vida, à ética, aos direitos e garantias individuais e sociais e ao Estado democrático de direito.

1.6 – RAMOS DA ATIVIDADE DE ISP

A atividade de ISP possui dois ramos: a Inteligência e a Contra-Inteligência.

Inteligência é o ramo da ISP que se destina à produção de conhecimentos de interesse da Segurança Pública.

Contra-Inteligência é o ramo da ISP que se destina a produzir conhecimentos para neutralizar a inteligência adversa, a proteção da atividade e da instituição a que pertence.

Os dois ramos, intrinsecamente ligados, não possuem limites precisos, uma vez que se interpenetram, se inter-relacionam e interdependem.

1.7 – FONTES DE ISP

A atividade de ISP dispõe de duas naturezas de fontes: abertas e protegidas.

Fontes abertas são aquelas de livre acesso.
Fontes protegidas: são aquelas cujos dados são negados.

1.8 – MEIOS DE OBTENÇÃO DE DADOS E/OU CONHECIMENTOS

Existem basicamente dois meios de obtenção: humanos e eletrônicos.

Na Inteligência Humana (Int Hum) o foco da obtenção de dados e/ou conhecimentos é o homem.

Na Inteligência Eletrônica (Intel) o foco central é o equipamento.

Desse modo, de acordo com o tipo de equipamento, temos a Intel de Sinais, a Intel de Imagens e a Intel de Dados.

Intel de Sinais é responsável pela interceptação e pré-análise de comunicações, radares, telemetria etc, e pela transcrição de informações obtidas em línguas estrangeiras, pela decodificação de mensagens criptografadas, pelo processamento de imagens digitais, além de outras funções.

Intel de Imagens envolve a coleta e o processamento de imagens obtidas através de fotografias, satélites, radares e sensores infra-vermelho.

Intel de Dados envolve a captura de dados pela interceptação de sistemas de informática, telecomunicações e telemática.

CAPÍTULO 2 – PRODUÇÃO DE CONHECIMENTO.

A atividade de ISP centra-se na produção e na salvaguarda de conhecimentos utilizados em uma tomada de decisão, ou em apoio às instituições de Segurança Pública.

Para o correto exercício da ISP é imperativo o uso de metodologia própria, de procedimentos específicos e de técnicas acessórias voltadas para a produção do conhecimento, excluídas a prática de ações meramente intuitivas e a adoção de procedimentos sem orientação racional.

A *Produção de Conhecimento* compreende o tratamento, pelo profissional de ISP, de dados e conhecimentos.

Dado é toda e qualquer representação de fato, situação, comunicação, notícia, documento, extrato de documento, fotografia, gravação, relato, denúncia, etc, ainda não submetida, pelo profissional de ISP, à metodologia de Produção de Conhecimento.

Conhecimento é o resultado final - expresso por escrito ou oralmente pelo profissional de ISP - da utilização da metodologia de *Produção de Conhecimento* sobre dados e/ou conhecimentos anteriores.

Produzir conhecimento é, para a ISP, transformar dados e/ou conhecimentos em conhecimentos avaliados, significativos, úteis, oportunos e seguros, de acordo com metodologia própria e específica.

O *Conhecimento* é produzido pela Agência de Inteligência (AI) nas seguintes situações:

a) de acordo com um Plano de Inteligência.
b) em atendimento à solicitação de uma agência congênere.
c) em atendimento à determinação da autoridade competente.
d) por iniciativa própria do analista.

2.1 – ESTADOS DA MENTE

A verdade, como contrária do erro, consiste na perfeita concordância do conteúdo do pensamento (sujeito) com o fato (objeto). Em relação à verdade, a mente humana pode encontrar-se em quatro diferentes estados: certeza, opinião, dúvida, ignorância.

a) Certeza: consiste no acatamento integral, pela mente, da imagem por ela mesma formada, como correspondente a determinado fato e/ou situação.
b) Opinião: é um estado no qual a mente se define por um objeto, considerando a possibilidade de um equívoco. Por isso, o valor do estado de opinião expressa-se por meio de indicadores de probabilidades.

c) Dúvida: é o estado em que a mente encontra, metodicamente, em situação de equilíbrio, razões para aceitar e negar que a imagem, por ela mesma formada, esteja em conformidade com determinado objeto.
d) Ignorância: é o estado em que a mente encontra-se privada de qualquer imagem sobre uma realidade específica.

2.2 TRABALHOS INTELECTUAIS

O ser humano, para conhecer determinados fatos ou situações, pode realizar três trabalhos intelectuais: conceber idéias, formular juízos e elaborar raciocínios.

a) *Idéia* é a simples concepção, na mente, da imagem de determinado objeto sem, contudo, qualificá-lo.
b) *Juízo* é a operação pela qual a mente estabelece uma relação entre idéias.
c) *Raciocínio*: é a operação pela qual a mente, a partir de dois ou mais juízos conhecidos, alcança outro que deles decorre logicamente.

2.3 – TIPOS DE CONHECIMENTO

A Doutrina de ISP preconiza uma diferenciação dos tipos de conhecimentos produzidos, resultantes dos seguintes fatores:

a) os diferentes estados em que a mente humana pode situar-se em relação à verdade (certeza, opinião, dúvida e ignorância);
b) os diferentes graus de complexidade do trabalho intelectual necessário à produção do conhecimento (idéia, juízo e raciocínio), e;
c) a necessidade de elaborar, além de trabalhos relacionados com fatos e/ou situações passados e presentes, outros, voltados para o futuro.

Informe: É o *Conhecimento* resultante de juízo(s) formulado(s) pelo profissional de ISP, que expressa seu estado de certeza, opinião ou de dúvida frente à verdade sobre fato ou situação passado e/ou presente. A sua produção exige o domínio de metodologia própria e tem como objeto apenas fatos e situações pretéritos ou presentes.

Informação: É o *Conhecimento* resultante de raciocínio(s) elaborado(s) pelo profissional de ISP, que expressa o seu estado de certeza frente à verdade sobre fato ou situação passados e/ou presentes; A Informação decorre da operação mais apurada da mente, o raciocínio. Portanto, extrapola os limites da simples narração dos fatos ou das situações, contemplando interpretação dos mesmos. A sua produção requer, ainda, o pleno domínio da metodologia de produção do conhecimento.

Apreciação: É o *Conhecimento* resultante de raciocínio(s) elaborado(s) pelo profissional de ISP, que expressa o seu estado de opinião frente à verdade, sobre fato ou situação passados e/ou presentes.

Apesar de ter essencialmente como objeto fatos ou situações presentes ou passados, a *Apreciação* admite a realização de projeções. Porém, diferentemente do *Conhecimento Estimativa*, que será abordado a seguir, as projeções da *Apreciação* resultam tão-somente da percepção, pelo profissional de ISP, de desdobramentos dos fatos ou situações objeto da análise e não da realização de estudos especiais, necessariamente auxiliados por métodos e técnicas prospectivas.

Estimativa: É o *Conhecimento* resultante de raciocínio(s) elaborado(s), que expressa o seu estado de opinião sobre a evolução futura de um fato ou de uma situação. A sua produção requer não só o pleno domínio da metodologia própria da atividade de Inteligência, mas também o domínio de técnicas prospectivas complementares a essa metodologia.

2.4 – CICLO DA PRODUÇÃO DO CONHECIMENTO (CPC)

O CPC é definido sinteticamente, como um processo formal e regular, separado em duas etapas principais (uma vinculada à reunião de dados e outra ao processo de análise), no qual o conhecimento produzido é disponibilizado aos usuários, agregando-se medidas de proteção e negação do conhecimento.

O resultado deste conjunto de ações sistemáticas é um conhecimento de Inteligência, materializado em documentos de inteligência, atendidas as peculiaridades de sua finalidade.

Dentro de uma perspectiva menos sintética, trata-se, o CPC, de um processo contínuo e sequencial, composto por quatro fases - Planejamento, Reunião de Dados, Processamento e Difusão - que não são desenvolvidas em uma ordem necessariamente cronológica. Enquanto as necessidades de conhecimento já definidas estão sendo processadas, podem surgir novas demandas que exijam a reorientação dos trabalhos.

Metodologicamente, o CPC atende às seguintes etapas:

2.4.1 – Planejamento

a) Conceito:

Planejamento é a fase do CPC na qual são ordenadas de forma sistematizada e lógica, as etapas do trabalho a ser desenvolvido, estabelecendo o objetivo ou necessidades, prazos, prioridades e cronologia, definindo os parâmetros e as técnicas a serem utilizadas, partindo-se dos procedimentos mais simples para os mais complexos. Planejar deve constituir-se em uma ação rotineira do profissional de Inteligência.

b) Esquematização

O *Planejamento* pode ser, esquematicamente, assim apresentado:

- determinação do assunto a ser estudado;
- determinação da faixa de tempo a ser considerada;
- determinação da faixa de tempo a ser considerada
- determinação do usuário do conhecimento;
- determinação da finalidade do conhecimento;
- determinação do prazo disponível para a produção;
- determinação dos aspectos essenciais do assunto;
- verificação dos aspectos essenciais conhecidos; e
- verificação dos aspectos essenciais a conhecer.

Determinação do assunto: consiste em especificar o fato ou a situação, objeto do conhecimento a ser produzido, através de uma expressão oral ou escrita. O assunto deve ser preciso, determinado e específico.

Determinação da Faixa de Tempo a ser considerada: Este procedimento consiste em estabelecer marcos temporais para o desenvolvimento do estudo considerado.

Determinação do usuário: *a* execução deste procedimento objetiva identificar a autoridade governamental ou o órgão congênere que, pelo menos potencialmente, utilizará o *Conhecimento* que está sendo produzido. Visa, ainda, estabelecer o nível de profundidade do *Conhecimento* a ser produzido.

Determinação da Finalidade: diz respeito à virtual utilização, pelo usuário, do *Conhecimento* em produção. Devido à *compartimentação* inerente ao exercício da atividade de ISP, nem sempre é possível a determinação da finalidade. Neste caso, o planejamento é orientado para esgotar o assunto tratado, de tal modo, que o usuário venha a encontrar em algum ponto do *Conhecimento* que está sendo produzido subsídios úteis a sua atuação.

Determinação de Prazos: Nos casos de produção do *Conhecimento*, em obediência a planos de Inteligência ou estímulos específicos, é normal que os prazos estejam previamente estabelecidos. Quando isso não ocorrer ou quando a iniciativa de produção do *Conhecimento* é da própria AI, os prazos são estabelecidos observando-se o princípio da oportunidade.

Determinação dos Aspectos Essenciais do Assunto: Trata-se de listar o que o analista, nesta etapa do estudo, acredita necessitar saber para extrair conclusões sobre o assunto estudado. Tal lista poderá ser ampliada ou sofrer supressões em decorrência da evolução do estudo.

Verificação dos Aspectos Essenciais Conhecidos: Este procedimento consiste em verificar, dentre os aspectos essenciais já determinados, aqueles para os quais já se tenha algum tipo de resposta, antes do desencadeamento de qualquer medida de reunião. É importante separar as respostas completas das incompletas e as que expressam certeza das que expressam opinião.

Aspectos Essenciais a Conhecer: Neste procedimento se verificam os aspectos essenciais, com os quais o profissional de ISP deve obter novas respostas, novos elementos de convicção para as respostas já disponíveis e os seus complementos, se necessários.

2.4.2 - Reunião de Dados e/ou Conhecimentos

Compreende a etapa do CPC em que se procura obter dados e/ou *Conhecimentos,* que respondam e/ou complementem os aspectos essenciais a conhecer, por meio de ações de *Coleta* e *Busca*.

Esquematização

A *Reunião de Dados* pode ser assim esquematizada:

- pesquisa
- consulta aos arquivos e bancos de dados
- ligações com órgãos congêneres.
- acionamento do Elemento de Operações [ELO];
- autorização judicial em hipótese de sigilo legal e investigação criminal.

2.4.3 – Processamento

Fase do ciclo na qual o conhecimento é produzido. É a fase intelectual em que o analista percorre quatro etapas, não necessariamente de forma cronológica, a saber:

- Avaliação
- Análise
- Integração;
- Interpretação.

a) Avaliação

Conceito

É a etapa na qual se determina a pertinência e o grau de credibilidade dos dados e/ou conhecimentos, a fim de classificar e ordenar àqueles que, prioritariamente, serão utilizados e influenciarão decisivamente no *Conhecimento* a ser produzido, e que expressará, quando de sua formalização, o estado de certeza, de opinião ou de dúvida do analista.

A avaliação de um dado e/ou conhecimento é realizada na AI que primeiro o recebe, por um especialista de Inteligência. A habilitação para avaliar um

dado decorre do especialista de Inteligência possuir os seguintes requisitos: o domínio da Técnica de Avaliação de Dados (TAD) e a competência funcional.

A TAD é adquirida pelo completo conhecimento e sistemático emprego das etapas por ela preconizadas.

A competência funcional é a faculdade concedida a um especialista de Inteligência para avaliar um dado, decorrente de função ou cargo por ele exercido, ou seja, é uma atribuição regulamentar.

A avaliação de um dado depende, dentro da técnica respectiva, do perfeito entendimento de como ocorre a comunicação do dado entre o emissor ou fonte, até o receptor.

Pertinência

É a etapa na qual o analista verifica se o dado ou conhecimento reunido é coerente e compatível com o objeto do conhecimento a ser produzido. Inicia-se por um exame preliminar do relacionamento entre o obtido e o desejado se esgota pela determinação das frações significativas, isto é, das parcelas de dados e/ou *Conhecimentos* que interessam aos aspectos essenciais determinados na fase do Planejamento.

No julgamento das frações significativas, são comparadas as frações entre si e o que o analista planejou e sabe sobre o assunto. Ao final do procedimento, o analista disporá de frações significativas preliminarmente graduadas em credibilidade.

Os dados e/ou conhecimentos avaliados como não-pertinentes serão descartados para o assunto específico.

Credibilidade

É a etapa na qual o analista verifica e estabelece julgamentos sobre:

1 - a fonte.
2 - o conteúdo.

No julgamento da fonte (pessoas, organização ou documento), busca-se seu grau de idoneidade, verificando-se três aspectos:

a) *Autenticidade*: verificação se o dado ou conhecimento provém realmente da fonte presumida (originou o dado), ou de intermediários. Esta verificação pode ser realizada mediante o estudo das peculiaridades e dos possíveis indícios que permitam caracterizar a fonte.

b) *Confiança* (atributo subjetivo): observa-se da fonte, os seus antecedentes e comportamento social, colaboração anterior procedente e motivação de ordem ética ou profissional. Pode-se considerar, ainda, o grau de instrução, valores, convicções e sua maturidade.

c) *Competência*: verifica-se se a fonte é habilitada (técnica, intelectual e fisicamente) e se detinha localização adequada para obter aquele dado específico.

No julgamento do conteúdo, devem ser verificados três aspectos:

a) *Coerência*: verifica-se se o dado apresenta contradições em seu conteúdo, no encadeamento lógico (cronologia) e na harmonia interna (seqüência lógica); (também pode ser empregado para definir a autenticidade da fonte).

b) *Compatibilidade*: verifica-se o grau de harmonia com que o dado se relaciona com outros dados já conhecidos (se é factível).

c) *Semelhança*: verifica-se se há outro dado, oriundo de fonte diversa, que venha reforçar, por semelhança, os elementos do dado sob observação.

Resultado da Avaliação

A credibilidade das frações que compõem o conhecimento será traduzida, quando de sua formalização, por meio de recursos de linguagem que expressem o estado de certeza, de opinião ou dúvida do profissional de inteligência. Tradicionalmente, existem duas tabelas que podem auxiliar o analista das AI/SISP.

Tabela de julgamento da fonte

- A: inteiramente idônea
- B: normalmente idônea
- C: regularmente idônea
- D: normalmente inidônea
- E: inidônea
- F: não pôde ser avaliada

Tabela de julgamento do conteúdo

- 1: confirmado por outras fontes

- 2: provavelmente verdadeiro
- 3: possivelmente verdadeiro
- 4: duvidoso
- 5: improvável
- 6: não pôde ser avaliado

Ponto de Interesse

Antes de submeter um dado ao processo de avaliação, uma das preocupações do analista de ISP deve ser com a definição do ponto de interesse. Significa determinar qual o ponto do conteúdo de um dado recebido, que interessa efetivamente ao analista para o desempenho da sua atividade em determinado caso.

A importância da definição prévia do ponto de interesse relativo a um dado decorre, de como isto auxiliará na identificação da fonte a ser avaliada, bem como, determinará o enfoque a ser adotado pelo analista, por ocasião de sua utilização para a elaboração de um *Conhecimento* de Inteligência. É igualmente importante, para a redação dos documentos de Inteligência, particularmente o *Informe*, a *Apreciação*, a *Informação* e a *Estimativa*, pois permite a perfeita definição do "assunto" que está sendo tratado.

b) Análise

Etapa na qual o analista decompõe os dados e/ou conhecimentos reunidos e pertinentes, em suas partes constitutivas, já devidamente avaliadas, relacionadas aos Aspectos Essenciais levantados e, examina cada uma delas, a fim de estabelecer sua importância em relação ao assunto, que está sendo estudado.

c) Integração

É a etapa na qual o analista monta um conjunto coerente, ordenado, lógico e cronológico, com base nas frações significativas, já devidamente avaliadas. O aproveitamento de uma fração significativa varia de acordo com o tipo de conhecimento que se pretende produzir, porém é desejável que sejam aproveitadas, principalmente, as frações significativas com grau máximo de credibilidade.

O conjunto lógico e cronológico preconizado visa proporcionar o melhor entendimento do *conhecimento* produzido. Entretanto, o centro do *conhecimento* - o assunto objeto do *conhecimento* - deverá constar no início do documento produzido.

d) Interpretação

É a etapa na qual o profissional de ISP esclarece o significado final do assunto tratado. Após o processo de avaliação, análise e integração, deve-se buscar estabelecer as relações de causa e efeito, apontar tendências e padrões e fazer previsões, baseadas no raciocínio.

Os procedimentos tratados nesta fase interpenetram-se de tal forma que, qualquer tentativa de ordenação e delimitação se torna difícil. Neste sentido, apenas para fins de explicação, eles são apresentados na seguinte sequência: delineamento de trajetória, estudo dos fatores de influência e significado final.

Delineamento de trajetória - consiste no encadeamento sistemático, com base na integração, de aspectos relacionados com o assunto, objeto do trabalho em execução. Integra todos os elementos fundamentais, dentro de uma cadeia de causa e efeito, definindo, desta forma, o delineamento da trajetória do assunto. Os limites a serem considerados para o estabelecimento da trajetória são o início da faixa de tempo identificada no planejamento e determinado ponto do passado, do presente ou ainda, no futuro.

Estudo dos fatores de influência – consiste em identificar e ponderar os fatores que influem no fato ou situação, considerando-se a freqüência, a intensidade e os efeitos. Os fatores de influência são, na maioria das vezes, encontrados na própria integração e identificados dinamicamente no delineamento de trajetória da situação. Algumas vezes são inferidos a partir de evidências contidas na integração. Em outras oportunidades, devem ser, ainda, admitidos no estudo como imposições do usuário.

Significado final – nesta fase os resultados dos procedimentos anteriormente executados são revistos e o profissional de ISP já tem em sua mente, pelo menos, um esboço da solução do problema em estudo. Assim, o significado final será muito mais um aperfeiçoamento do esboço, do que a descoberta integral do significado do problema em questão.

2.4.4 - Difusão

Nesta fase do CPC, o conhecimento produzido será *formalizado* em Documentos de Inteligência, e *disponibilizado* para o usuário ou outras agências de

Inteligência - atendidos os princípios do sigilo e da oportunidade e a necessidade de conhecer - e posteriormente arquivado. Em atendimento ao princípio da oportunidade admite-se a difusão informal, previamente à sua formalização.

O *Arquivamento* consiste na embalagem e na estocagem de documentos de forma adequada à sua conservação, obedecendo a uma ordem estabelecida, a fim de facilitar o seu manuseio e a sua recuperação.

2.5 – AVALIAÇÃO DE RESULTADOS

Trata-se de uma avaliação sobre o resultado produzido pelo conhecimento difundido. As AI do SISP, periodicamente, avaliarão esses resultados.

2.6 - DOCUMENTOS DE INTELIGÊNCIA (DI)

Documentos de Inteligência são os documentos padronizados, sigilosos, redigidos em texto simples, ordenado e objetivo, devidamente classificados, que circulam internamente ou entre as AI, a fim de transmitir ou solicitar conhecimentos.

2.6.1 – Documentos externos

São os Documentos de Inteligência difundidos para outras AI. Os principais tipos são:

1 - *Relatório de Inteligência* (RELINT)
2 - *Pedido de Busca* (PB)
3 – *Mensagem* (Msg)
4 - *Sumário*

Outros tipos poderão ser criados, a fim de atender a necessidades específicas.

1) ***Relatório de Inteligência (Relint)***

É o documento externo, padronizado, no qual o analista transmite conhecimentos para usuários ou outras AI, dentro ou fora do sistema de ISP. O tipo de conhecimento transmitido deverá estar explícito na forma da redação - *Informes*, *Informações*, *Apreciações* e *Estimativas* – e o documento deverá conter uma avaliação considerando a fonte produtora e o conteúdo.

2) ***Pedido de Busca (PB)***

É o documento externo, padronizado, utilizado para solicitação de dados e/ou conhecimentos entre AI, dentro ou fora do sistema de ISP.

3) Mensagem (Msg)

É o documento externo, padronizado, relacionado à comunicação de assuntos de interesse das AI.

4) Sumário

É o documento externo, padronizado, que expressa uma coletânea rotineira e periódica de fatos e situações ocorridas de interesse da Segurança Pública.

2.6.2 – Documentos internos

São documentos de circulação interna relacionados à atuação, solicitação de dados, resposta ou transmissão interna de dados ou *conhecimentos* no âmbito de cada AI, de acordo com seu objetivo, finalidade e estrutura.

2.6.3 - Requisitos do RELINT e PB

A padronização dos documentos é extremamente necessária para se obter unidade de entendimento e uniformidade de procedimentos entre os órgãos que integram o Sistema de Inteligência de Segurança Pública - SISP. Os documentos contêm um conjunto mínimo de itens sobre a sua classificação, conteúdo, destinatário e obrigatoriamente conterão:

a) logomarca do Estado Federado ou da União
b) designação e timbre da AI produtora e sua subordinação
c) classificação sigilosa
d) designação do tipo do documento
e) numeração seqüencial, por ano
f) cabeçalho contendo: Data; Assunto; Origem; Difusão; Difusão Anterior; Referência; Anexo; (Segundo regras

próprias de cada OI, o RELINT poderá conter avaliação sobre o documento de acordo com as tabelas de julgamento de fonte e conteúdo constantes desta normativa)
g) texto
h) numeração das folhas
i) autenticação
j) recomendação legal sobre quebra de sigilo.

2.6.4 - Classificação e Restrição ao uso dos documentos de ISP:

Os documentos de Inteligência receberão classificação de acordo com o assunto abordado, nos termos da legislação apropriada e somente poderão ser inseridos em procedimentos apuratórios nos casos e forma permitidos.

2.6.5 - Retransmissão

Consiste em uma AI transmitir a outra(s) um documento de Inteligência, cujo conteúdo expressa um conhecimento constante em documento originado de uma terceira agência. Como regra geral, a retransmissão deverá:

a) Manter a classificação sigilosa e anexos que possam existir.
b) Indicar a AI que produziu o conhecimento.
c) Indicar data em que foi produzido o texto que está sendo retransmitido, além do próprio conhecimento, mantendo a numeração do documento elaborado no processo de difusão original.
d) Formatar o conteúdo que está sendo retransmitido, de forma a não ser confundido com eventual novo conhecimento que possa ser agregado pela AI retransmissora, indicando a difusão anterior.

CAPÍTULO 3 – MÉTODOS PARA REUNIÃO DE DADOS

3.1 – CONCEITO DE REUNIÃO DE DADOS

Reunião de Dados é a fase do CPC na qual as AI procuram obter os dados necessários, realizando, metódica e sistematicamente, ações que lhes possibilitem produzir o *conhecimento*.

3.2 – AÇÕES DE INTELIGÊNCIA

São todos os procedimentos e medidas realizadas por uma AI para dispor dos dados necessários e suficientes para a produção do conhecimento, centrados, de um modo geral, em dois tipos de ações de Inteligência:

3.2.1- Ações de Coleta

São todos os procedimentos realizados por uma AI, ostensiva ou sigilosamente, a fim de obter dados depositados em fontes abertas, sejam elas originadas ou disponibilizadas por indivíduos e órgãos públicos ou privados.

Coleta Primária: envolve o desenvolvimento de ações de ISP para obtenção de dados e/ou conhecimentos disponíveis.

Coleta Secundária: envolve o desenvolvimento de ações de ISP, por meio de acesso autorizado, por se tratar de consulta a bancos de dados protegidos.

3.2.2 - Ações de Busca

São todos os procedimentos realizados pelo setor de operações de uma AI, envolvendo ambos os ramos da ISP, a fim de reunir dados protegidos ou negados, em um universo antagônico.

As ações de infiltração, entrada e interceptação de sinais ou comunicações em meios informáticos, de telecomunicações ou telemática devem ser previamente autorizadas judicialmente.

3.3 – OPERAÇÕES DE ISP

É o conjunto de *Ações de Busca,* podendo, eventualmente, envolver *Ações de Coleta,* executado para obtenção de dados protegidos e/ou negados de difícil acesso e que exige, pelas dificuldades e/ou riscos, um planejamento

minucioso, um esforço concentrado, e o emprego de pessoal, técnicas e material especializados.

3.3.1 - *Ambiente Operacional*

É o local onde se desenvolve uma *Operação de ISP* e que, normalmente, determina os recursos empregados.

3.3.2 - *Alvo*

É o objetivo principal das *Ações de Busca*. Pode ser um assunto, uma pessoa, uma organização, um local ou um objeto.

3.3.3 - *Elemento de Operações* (ELO)

É o setor de uma AI que planeja e executa as *Operações de ISP*.

3.3.4 - *Pessoal*

Agente é um funcionário orgânico da AI que possui treinamento especializado.

Colaborador é uma pessoa - recrutada operacionalmente ou não - que, por suas ligações e conhecimentos, cria facilidades para a AI até mesmo fora de sua área normal de atuação. Eventualmente pode transmitir dados obtidos em sua área de atuação. Não é orgânico da agência de ISP e não possui treinamento especializado.

Informante é uma pessoa recrutada operacionalmente, que trabalha em sua área normal de atuação. Existem dois tipos de informantes, os que não possuem treinamento e os que possuem, sendo esses últimos identificados como "Informante Especial (IE)."

3.3.5 - *Rede*

É a designação dada ao conjunto de pessoas não-orgânicos controlados pela AI.

3.3.6 - *Controlador*

É o agente responsável pelo controle de componentes da Rede.

3.4 – AÇÕES DE BUSCA

São Ações de Busca: reconhecimento, vigilância, recrutamento operacional, infiltração, desinformação, provocação, entrevista, entrada e interceptação de sinais e de dados.

Reconhecimento é a Ação de Busca realizada para obter dados sobre o ambiente operacional ou identificar visualmente uma pessoa. Normalmente é uma ação preparatória que subsidia o planejamento de uma Operação de Inteligência (Op Int).

Vigilância é a Ação de Busca que consiste em manter um ou mais alvos sob observação.

Recrutamento Operacional é a Ação de Busca realizada para convencer uma pessoa não pertencente à AI a trabalhar em benefício desta.

Infiltração é a Ação de Busca que consiste em colocar uma pessoa junto ao alvo.

Desinformação é a Ação de Busca - muito utilizada no ramo da Contra-Inteligência - realizada para, intencionalmente, confundir alvos (pessoas ou organizações), a fim de induzir esses alvos a cometerem erros de apreciação, levando-os a executar um comportamento pré-determinado.

Provocação é a Ação de Busca, com alto nível de especialização, realizada para fazer com que uma pessoa/alvo modifique seus procedimentos e execute algo desejado pela AI, sem que o alvo desconfie da ação.

Entrevista é a Ação de Busca realizada para obter dados por meio de uma conversação, mantida com propósitos definidos, planejada e controlada pelo entrevistador.

Entrada é a Ação de Busca realizada para obter dados em locais de acesso restrito e sem que seus responsáveis tenham conhecimento da ação realizada.

Interceptação de Sinais [eletromagnéticos, óticos e acústicos] *e de Dados* é a Ação de Busca realizada por meio de equipamentos adequados, operados por integrantes da Inteligência Eletrônica.

As Ações de Busca, *Infiltração*, *Entrada* e *Interceptação de Sinais e de Dados,* que necessitam de autorização judicial, são denominadas Ações de Inteligência Policial Judiciária (AIPJ). Tais ações são de natureza sigilosa e envolvem o emprego de técnicas especiais visando a obtenção de dados (indícios, evidências ou provas de autoria ou materialidade de um crime).

3.5 – TÉCNICAS OPERACIONAIS DE ISP (TOI)

São as habilidades desenvolvidas por meio de emprego de técnicas especializadas que viabilizam a execução das *Ações de Busca,* maximizando potencialidades, possibilidades e operacionalidades.

As principais TOI são: *Processos de Identificação de Pessoas; Observação, Memorização e Descrição (OMD); Estória-Cobertura; Disfarce; Comunicações Sigilosas; Leitura da Fala; Análise de Veracidade; Emprego de Meios Eletrônicos; e Foto-Interpretação.*

Processos de Identificação de Pessoas é conjunto de TOI, considerada a constante evolução tecnológica, destinado a identificar ou a reconhecer pessoas: fotografia, fotometria, retrato falado, datiloscopia, documentoscopia, DNA, arcada dentária, voz, íris, medidas corporais, descrição, dados de qualificação.

Observação, Memorização e Descrição é a TOI na qual os profissionais de ISP examinam, minuciosa e atentamente, pessoas, locais, fatos, ou objetos, por meio da máxima utilização dos sentidos, de modo a transmitir dados que possibilitem a identificação.

Estória-Cobertura é a TOI de dissimulação utilizada para encobrir as reais identidades dos agentes e das AI, a fim de facilitar a obtenção de dados (e dos propósitos), e preservar a segurança e o sigilo.

Disfarce é a TOI pela qual o agente, usando recursos naturais ou artificiais, modifica sua aparência física, a fim de evitar o seu reconhecimento, atual ou futuro, ou de adequar-se a uma *Estória-Cobertura.*

Comunicações Sigilosas é a TOI que consiste no emprego de formas e processos especiais, convencionados para a transmissão de mensagens, passar objetos, no decorrer de uma operação.

Leitura da Fala é a TOI na qual um agente, à distância, identifica diversos fatores relacionados a questões tratadas em uma conversação, que viabilizam a compreensão do assunto.

Análise de Veracidade é a TOI utilizada para verificar, por meio de recursos tecnológicos ou metodologia própria, se uma pessoa está falando a verdade sobre fatos ou situações.

Emprego de Meios Eletrônicos é a TOI que capacita os agentes integrantes da Inteligência Humana a utilizarem adequadamente os equipamentos de captação, gravação e reprodução de sons, imagens, sinais e dados.

Foto-interpretação é a TOI utilizada para identificar os significados das imagens obtidas.

3.6 – TIPOS DE OPERAÇÕES DE INTELIGÊNCIA

Existem dois tipos básicos de *Operações de Inteligência*: as exploratórias e as sistemáticas.

Operações Exploratórias

Visam atender as necessidades imediatas de dados específicos sobre determinado alvo. São utilizadas, normalmente, para cobrir eventos e levantar dados ou informações específicas em curto prazo. Prestam-se, particularmente, para a cobertura de reuniões em geral, para o reconhecimento e levantamento de áreas, para o levantamento das atividades e contatos das pessoas, para a obtenção de conhecimentos contidos em documentos guardados, para a avaliação da validade da abertura de outras operações, etc.

Operações Sistemáticas

São utilizadas normalmente para acompanhar, metodicamente, a incidência de determinado fenômeno ou aspecto da criminalidade, as atividades de pessoas, organizações, entidades e localidades. Prestam-se, principalmente, para o acompanhamento das facções criminosas, a neutralização de suas ações e a identificação de seus integrantes. Visam atualizar e aprofundar conhecimentos sobre suas estruturas, atividades e ligações, através da produção de um fluxo contínuo de dados.

São, particularmente, aptas para o levantamento das atividades futuras do alvo.

3.7 – PLANEJAMENTO DAS OPERAÇÕES DE INTELIGÊNCIA (Op Int)

É a formulação lógica e sistemática de ação ou ações que se pretende realizar, incluindo detalhamento e cronologia de desencadeamento (abertura, execução e encerramento). Tal planejamento é composto por um *Estudo de Situação* e um *Plano de* Op Int (mementos disponíveis nos anexos III e IV), além da previsão de ações alternativas.

No *Plano* são aplicadas cinco medidas indispensáveis à eficaz condução da Op Int: Controle, Coordenação, Avaliação, Orientação e Segurança.

É importante considerar que as Op Int estão sempre sujeitas ao dilema Efetividade *versus* Segurança. Ainda que a Segurança seja inerente e indispensável a qualquer ação ou operação, a primazia da Segurança sobre a Efetividade ou vice-versa, será determinada pelos aspectos conjunturais.

3.7.1 – Medidas de Controle

É o conjunto de procedimentos que tem por objetivo zelar por aspectos da operação em curso, fundamentalmente pela segurança e eficácia, inclusive por seu equilíbrio. Mais particularmente, as medidas de controle enfocam o desempenho do pessoal empregado, bem como a quantidade e a qualidade dos dados produzidos. São exemplos: prazos, códigos, relatórios, horários, reuniões periódicas etc.

3.7.2 – Medidas de Coordenação

É o conjunto de procedimentos que tem por meta promover a colaboração de distintos órgãos e evitar que haja interferências externas à Op Int.

3.7.3 – Medidas de Avaliação

É o conjunto de procedimentos, permanente e sistematicamente aplicado, que tem por objetivo verificar a efetividade da Op Int, permitindo estimar a eficácia e os riscos de segurança, realizar uma apreciação dos custos-benefícios acarretados pela operação, oferecer elementos que sirvam de base para a estimativa dos recursos a serem distribuídos e oferecer parâmetros de comparação para a abertura e o encerramento de outras operações.

3.7.4 – Medidas de Orientação

É o conjunto de procedimentos que tem por objetivo realizar alterações em prol da Op Int Essas medidas devem ser executadas como conseqüência das medidas de *Controle* e/ou da *Avaliação*.

3.7.5 – Medidas de Segurança

É o conjunto de procedimentos que tem por objetivo minimizar os riscos da Op Int, observando os aspectos relacionados à Segurança Orgânica e, particularmente, quanto ao aspecto do pessoal empregado.

CAPÍTULO 4 – CONTRA-INTELIGÊNCIA

4.1 – CONCEPÇÃO

Contra-Inteligência (CI) é o ramo da atividade de ISP que se destina a produzir conhecimentos para proteger a atividade de Inteligência e a instituição a que pertence, de modo a salvaguardar dados e conhecimentos sigilosos e identificar e neutralizar ações adversas de qualquer natureza. A CI assessora também em assuntos internos de desvios de conduta, relacionados à área de Segurança Pública.

4.2 - CONCEITOS BÁSICOS

4.2.1 - Responsabilidade

É a obrigação legal, individual e coletiva, em relação à preservação da segurança.

4.2.2 - Acesso

É a possibilidade e/ou a oportunidade de uma pessoa obter dados ou *conhecimentos* sigilosos, que devem ser protegidos. O *acesso*, em conseqüência, deriva de autorização oficial emanada de autoridade competente – o credenciamento – ou da superação das medidas de salvaguarda aplicadas aos documentos sigilosos.

4.2.3 - Comprometimento

É a perda da segurança de dados ou conhecimentos, provocada por fatores humanos, naturais e acidentais.

4.2.4 - Vazamento

É a divulgação não autorizada de dados ou conhecimentos sigilosos.

4.3 – SEGMENTOS

A Contra-Inteligência atua por meio de três segmentos: a Segurança Orgânica, a Segurança de Assuntos Internos e a Segurança Ativa.

4.3.1 – Segurança Orgânica (SEGOR)

A SEGOR é o conjunto de medidas de caráter eminentemente defensivo, destinado a garantir o funcionamento da instituição, de modo a prevenir e obstruir as ações adversas de qualquer natureza.

A SEGOR caracteriza-se pelo conjunto de medidas integradas e meticulosamente planejadas, destinadas a proteger o pessoal, a documentação, as instalações, o material, as operações de ISP, as comunicações e telemática, e a informática.

a. *Segurança de Pessoal*

É o conjunto de normas, medidas e procedimentos voltados para os recursos humanos, no sentido de assegurar comportamentos adequados à salvaguarda de dados e conhecimentos sigilosos. Uma das principais normas de Segurança de Pessoal é o Processo de Recrutamento Administrativo (PRA), que visa selecionar, acompanhar e desligar os recursos humanos orgânicos de uma AI.

b. *Segurança da Documentação*

É o conjunto de normas, medidas e procedimentos voltados para a proteção dos documentos de Inteligência, no sentido de evitar o comprometimento e/ou o vazamento. A *Segurança da Documentação* 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 sigilosos.

c. *Segurança das Instalações*

É o conjunto de normas, medidas e procedimentos voltados para os locais onde são elaborados, tratados, manuseados ou guardados dados e conhecimentos sigilosos, além de materiais sensíveis, com a finalidade de salvaguardá-los. A *Segurança das Instalações* é obtida pela adoção de medidas de proteção geral, fiscalização e controle do acesso.

d. *Segurança do Material*

É o conjunto de normas, medidas e procedimentos voltados para a guarda e a preservação do material.

e. *Segurança das Operações de ISP*

É o conjunto de normas, medidas e procedimentos adotados para proteger as ações operacionais realizadas pela AI. Essa proteção inclui, notadamente, os agentes, a instituição, a identidade do alvo e os objetivos da operação.

f. *Segurança das Comunicações e Telemática*

É o conjunto de normas, medidas e procedimentos voltados para os meios de comunicações, no sentido de salvaguardar dados e/ou conhecimentos, de modo a impedir ou a dificultar a interceptação e a análise da transmissão e do tráfego de dados e sinais.

g. *Segurança da Informática*

É o conjunto de normas, medidas e procedimentos destinados a preservar os sistemas de Tecnologia de Informação, de modo a garantir a continuidade do seu funcionamento, a integridade dos conhecimentos e o controle do acesso.

Plano de Segurança Orgânica (PLASEGOR)

O PLASEGOR é um documento que visa orientar os procedimentos de interesse da Segurança Orgânica. A adoção de medidas de segurança sem a necessária análise dos riscos e dos aspectos envolvidos poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação.

O PLASEGOR será resultado de um processo harmônico e integrado, após percorridas as seguintes fases: Estudo de Situação, Decisão, Elaboração do Plano, Implantação do Plano e Supervisão das Ações Planejadas. [o Modelo do PLASEGOR encontra-se no Anexo IV].

4.3.2 – Segurança de Assuntos Internos

A Segurança de Assuntos Internos (SAI) é o conjunto de medidas destinadas à produção de conhecimentos que visam assessorar as ações de correição das instituições de Segurança Pública.

5.4 – ORGANIZAÇÃO

5.4.1 – Sistema

A atividade de ISP, em nível nacional, é desenvolvida pelo Sistema de Inteligência de Segurança Pública (SISP), o qual, por sua vez, é um Subsistema do Sistema Brasileiro de Inteligência (SISBIN), cuja Agência Central é a Agência Brasileira de Inteligência (ABIN).

A Agência Central do SISP é o núcleo de inteligência da Secretaria Nacional de Segurança Pública (SENASP), do Ministério da Justiça.

5.4.2 – Subsistema

O SISP é integrado pelos subsistemas de ISP de cada estado da federação e do Distrito Federal. Esses subsistemas constituir-se-ão, por sua vez, nos sistemas de ISP das respectivas unidades federativas.

Em cada unidade federativa haverá, portanto, um Sistema de Inteligência de Segurança Pública do Estado respectivo, organizado de acordo com as normas, interesses e peculiaridades de cada um.

A Agência Central dos sistemas federados será o núcleo de ISP diretamente ligado ao secretário que trata dos assuntos de segurança pública.

5.4.3 - Tipos de AI

Poderão existir três tipos de AI: as efetivas, as especiais e as afins.

1) Efetivas: são as que pertencem à estrutura organizacional do Poder Executivo da Unidade Federativa e participam diretamente na produção de *conhecimentos* de interesse da Segurança Pública;

2) Especiais: são as que pertencem à estrutura organizacional do Poder Executivo da Unidade Federativa e participam direta ou indiretamente na produção de *conhecimentos* de interesse da Segurança Pública;

3) Afins: são as que não pertencem à estrutura organizacional do Poder Executivo da Unidade Federativa, mas que podem produzir *conhecimentos* do interesse da Segurança Pública. Essas Agências poderão integrar os Sistemas de ISP federados mediante o estabelecimento de Termos de Cooperação Técnica ou instrumentos congêneres, respeitando-se as prerrogativas constitucionais e o interesse da Segurança Pública.

5.4.4 - Classes de Agências de Inteligência

As AI podem ser divididas nas classes "A", "B" e "C", de acordo com os seguintes critérios:

a) nível hierárquico
b) estrutura organizacional
c) recursos humanos e materiais
d) CPC que realiza.

A classificação das AI, no âmbito de cada Subsistema que integra o SISP, é definida pelo titular da instituição a que pertence esse subsistema, observada a legislação vigente e ouvida a Agência Central de cada subsistema federado.

5.4.5 - Estruturas das AI

As estruturas das AI variam de sistema para sistema, conforme os objetivos estabelecidos e os recursos disponíveis. Entretanto, de um modo geral, são dispendiosas, complexas e de difícil organização.

As AI, em sua estruturação mais ampla, podem possuir, dentre outros, os seguintes setores de atuação: Inteligência, Contra-Inteligência, Operações de Inteligência, Arquivo, Informática, Inteligência Eletrônica, Comunicações e Apoio Administrativo.

5.4.5.1 – Comunidade de Inteligência de Segurança Pública

A Comunidade de Inteligência é composta pelo conjunto das Agências de Inteligência integrantes do território nacional, estabelecendo-se entre elas o compromisso pela troca de informações e a ajuda mútua, nos termos desta DNISP.

5.4.6 - Plano Nacional de Inteligência de Segurança Pública

Plano Nacional de ISP é o documento elaborado, no âmbito dos respectivos sistemas e subsistemas, a fim de orientar o exercício da atividade de Inteligência no SISP. É um conjunto ordenado de disposições e procedimentos que visa orientar a operacionalização das decisões governamentais no que se refere à atividade de ISP [o modelo do Plano de ISP encontra-se no Anexo IV].

A atividade de ISP será realizada pelas AI em consonância com a destinação constitucional de cada uma das instituições que compõem o SISP.

5.5 – PROFISSIONALISMO

a – Atributos

Os recursos humanos a serem empregados na atividade de ISP são fundamentais para funcionamento eficaz e eficiente do SISP.

O profissional de ISP, além da vocação para a atividade, terá que possuir perfil profissiográfico pré-estabelecido, vida pregressa compatível, observados os atributos, dentre outros, da voluntariedade, da ética e da moral, focados na lealdade, integridade, discrição e profissionalismo (capacidade de trabalho, dedicação, responsabilidade e cooperação).

Os analistas deverão destacar-se, ainda, pela objetividade e pela capacidade intelectual e analítica (curiosidade intelectual, capacidade de apreensão, imaginação criadora e disciplina intelectual).

Os que se dedicam às Operações de Inteligência, deverão possuir adaptabilidade, flexibilidade, dissimulação, habilidade no trato, iniciativa, criatividade, determinação, dinamismo, coragem, controle emocional, paciência e resistência à tensão.

b - Recrutamento Administrativo

Os candidatos deverão ser submetidos a Processo de Recrutamento Administrativo (PRA), conduzido pelo setor de Contra-Inteligência da respectiva agência de ISP, para avaliar o seu perfil e verificar se os seus antecedentes são compatíveis com a atividade.

c - Qualificação

A qualificação do profissional de ISP deverá ser realizada através de específicos e sistemáticos programas de formação, de especialização, de aperfeiçoamento, e de treinamento permanente.

d – Permanência

O profissionalismo da atividade de ISP depende diretamente da existência dos requisitos cognitivos próprios, de um sistema de educação continuada, da existência de um código de ética próprio e de critérios de cargos e gratificações, esses últimos, como incentivo à dedicação integral ao trabalho e sua relevância.

5.6 – DENÚNCIA

Denúncia é a acusação ostensiva ou sigilosa que se faz de algo ou alguém, sobre falta ou crime cometido ou na iminência de ser cometido, podendo ser realizada de maneira formal ou anônima.

As denúncias anônimas sejam por carta, pela internet ou pelo telefone (disque-denúncia) representam a participação da população no combate à criminalidade. Como tal, devem ser incentivadas e podem ser recebidas pelas AI, através de setores específicos, que processam e difundem junto aos órgãos competentes, responsáveis por investigar sua veracidade.

5.7 – INTELIGÊNCIA POLICIAL

A Inteligência Policial atua, principalmente, em duas esferas distintas e igualmente importantes: na prevenção e na repressão.

A Inteligência Policial atua na prevenção, principalmente, através da produção de *conhecimento* resultante da análise de padrões e tendências, visando antecipar situações futuras, com o objetivo de servir de base para a elaboração, por parte dos órgãos competentes, dos planos e ações de prevenção de atividades e fatos delitivos que vulnerem a Segurança Pública.

A Inteligência Policial atua em prol da repressão produzindo conhecimentos a fim de assessorar a investigação policial.

A diferenciação entre a atividade de Inteligência Policial e a Investigação Policial é, em regra, mais teórica do que prática, uma vez que ambas lidam, invariavelmente, com os mesmos objetos: crime, criminosos, criminalidade e questões conexas.

Aspecto diferenciador relevante é que enquanto a Investigação Policial está orientada pelo modelo de persecução penal previsto e regulamentado na norma processual própria, tendo como objetivo a produção de provas, a Inteligência Policial visa a produção de conhecimento e apenas eventualmente, subsidia na produção de provas.

Nesse sentido, o sigilo como princípio da atividade de ISP fica, em caráter excepcional mitigado, quando houver necessidade de emprestar aos procedimentos policiais e judiciais, elementos de provas. Neste caso, deverão os

chefes das AI valerem-se dos procedimentos e limites estabelecidos na legislação aplicável.

5.8 – RECURSOS MATERIAIS

5.8.1 - Equipamentos:

As Agências de ISP devem ser dotadas de equipamentos especializados para o desenvolvimento das atividades previstas pela ISP, observando-se sempre as normas e medidas administrativas para seu uso.

5.8.2 - Instalações:

A agência de ISP deverá ser estruturada fisicamente de forma a atender a segurança orgânica necessária, bem como, ambiente favorável para uso e manuseio dos equipamentos de ISP.

5.8.3 - Viaturas:

Serão destinadas äs agências de ISP viaturas diferenciadas , em cores comuns e variadas, com quatro portas e do tipo popular, com placas vinculadas e reservadas, possibilitando o desenvolvimento das atividades de acordo com as características que a ISP requer. Às agencias de ISP serão destinadas, ainda, viaturas técnicas equipadas com dispositivos necessários para o desenvolvimento de operações de inteligência.

5.8.4 - Equipamentos de comunicação:

A fim de atender aos princípios da ISP, deverão ser implementados equipamentos de telefonia e dispositivos de comunicação suficientes para serem utilizados proporcionando comunicação rápida e segura, sendo dotados inclusive de segurança criptográfica.

5.8.5-Equipamentos de Informática:

A rede de informática deve ser sigilosa e segura, exclusiva a seus participantes, dotada de equipamentos que atendam as modernas

idéias de telemática e as necessidades das operações de inteligência. Com a disponibilidade de equipamentos de informática deve se atrelar a segurança da informática, com medidas de segurança orgânica, com segurança de planejamento e segurança física, de modo a garantir a continuidade, integridade e confiabilidade dos conhecimentos ali produzidos.

5.9 – VERBA SECRETA

Deverão ser destinados, em legislação específica, recursos financeiros (VS), necessários ao desenvolvimento de ações de caráter sigiloso a cargo das AI .

ANEXO I - GLOSSÁRIO:

Ação Criminosa Complexa: São aquelas praticadas por indivíduos e/ou organizações criminosas que utilizam recursos tecnológicos, forma de execução planejada, dissimulada ou disfarçada, com emprego de ardil, poder econômico e sofisticados métodos para burlar a ação da justiça.

Ação Policial: Como regra geral, as equipes que realizam Ações de Inteligência de Segurança Pública não executam ações ostensivas, prisões ou flagrantes, visando preservar a segurança de seus integrantes e garantir o sigilo e a compartimentação. Tais ações ostensivas ficam a cargo de equipes policiais especialmente designadas para o seu cumprimento.

Agências de imposição da lei ou de provimento de ordem pública: órgãos polícias e forças constabulares (*e.g.* guarda costeira) de vários formatos em cada país.

Análise Criminal: é, genericamente, a coleta e análise da informação pertinente ao fenômeno da criminalidade. Sua finalidade é a produção de conhecimento relativo à identificação de parâmetros temporais e geográficos do crime e eventuais cifras obscuras, detecção da atividade e identidade da delinqüência correspondente, subsidiando as ações dos operadores diretos do sistema (análise criminal tática) bem como dos formuladores de políticas de controle (análise criminal estratégica e administrativa). As informações são utilizadas para o dimensionamento e posicionamento de recursos, bem como para a realização de ações gerais de gestão em relação ao patrulhamento e investigação policial.

Características: aspectos distintivos e particularidades que identificam e qualificam a DNISP.

Categorias de Inteligência: são utilizadas para direcionar o processo de aquisição de informação, organizar o trabalho de análise e classificar produtos.

Cifras e códigos: são recursos básicos para a transmissão de mensagens seguras e/ou abreviadas. A diferença básica entre uma cifra e um código, na (re)escrita de um "texto plano" enviado às claras é que uma cifra baseia-se no princípio da substituição de cada letra, enquanto um código substitui palavras ou frases inteiras por grupos arbitrários de símbolos. Nos dois casos, a segurança da comunicação depende de que somente os transmissores e os receptores possam "ler" as mensagens codificadas/cifradas, o que é feito utilizando-se uma "chave" de decifração ou dicionários de códigos.[Glossário Cepik]

Classificação: é a atribuição, pela autoridade competente, de grau de sigilo a dado, conhecimento, documento, material, área ou instalação.

Comunidade de ISP: é o conjunto de integrantes de AI que têm missões análogas ou que atuam em uma mesma área territorial. Através da Comunidade, aparam-se as arestas e quebra-se a rigidez do sistema, criando-se uma informalidade e uma confiança absolutamente necessária para as ligações entre as pessoas.

Conceitos: atribuição de significado emitida em função das características gerais de determinado objeto, ação ou de relações fundamentais previstas pela doutrina.

Credencial de Segurança: é o certificado que materializa o credenciamento.

Criptologia: abarca a criptografia (a arte de escrever em código ou cifradamente) e a cripto-análise (a arte de decifrar códigos ou cifras, conduzida por "quebradores de códigos").

Crise de Segurança Pública: é um evento ou situação crucial, que exige uma resposta especial da polícia, a fim de assegurar a melhor solução viável.

Desclassificação: é o cancelamento, pela autoridade competente ou pelo transcurso de prazo, da classificação, tornando ostensivos dados ou conhecimentos.

Disponibilidade: É a facilidade de recuperação ou acessibilidade de dados e conhecimentos.

Estratégia Policial: é a formulação planejada de diretrizes, processos, métodos e metas para o desempenho do trabalho policial, considerando o emprego dos recursos disponíveis para o desencadeamento de operações e/ou ações policiais conjuntas e/ou combinadas, delineando-se alternativas e avaliando-se a relação ação/resultado provável, visando a alcançar objetivos específicos ou múltiplos, norteada por preceitos legais e éticos.

Espionagem: é a ação clandestina voltada para a obtenção de informações relevantes, secretas ou pelo menos reservadas sobre determinado alvo, com o objetivo de beneficiar Estados, grupos de países, organizações, facções, empresas, personalidades ou indivíduos.[ver Cepik]

Grau de Sigilo: É a gradação atribuída a dados, conhecimentos, áreas ou instalações consideradas sigilosas em decorrência de sua natureza ou conteúdo.

Informática: é a ciência e a tecnologia que se ocupa do armazenamento e tratamento da informação, mediante a utilização de equipamentos e procedimentos da área de processamento de dados.

Integridade: é a incolumidade de dados ou conhecimentos na origem, no trânsito ou no destino.

Inteligência externa: está relacionada às capacidades, intenções e atividades de Estados, grupos ou indivíduos estrangeiros.

Inteligência Militar: é responsável por estudar, em particular, fatores do poder bélico dos países que potencialmente são considerados adversários, ou que neles podem se converter, a fim de satisfazer as necessidades da condução de estratégia militar. Nesse campo, contra-inteligência refere-se à toda inteligência sobre as capacidades, intenções e operações dos serviços de inteligência militares estrangeiros, o que envolve a implementação de medidas ativas no estrangeiro e a elaboração de mecanismos de proteção de informações e materiais sensíveis à defesa nacional.

Investigação para Credenciamento: É a averiguação sobre a existência dos requisitos indispensáveis para concessão de credencial de segurança.

Investigação Policial: Atividade de natureza sigilosa exercida por policial ou equipe de policiais, determinada por autoridade competente que, utilizando metodologia e técnicas próprias, visa a obtenção de evidências, indícios e provas da materialidade e autoria do crime e que podem desdobrar-se em ações policiais de controle, prevenção ou repressão.

Linguagem de Inteligência: A Doutrina de Inteligência preconiza o uso de uma linguagem especializada entre os profissionais da atividade e, em alguns casos, entre estes e os usuários de seus trabalhos. Essa linguagem singular é naturalmente construída com base na linguagem comum, mas os termos têm significado próprio, sem romper com o processo de comunicação utilizado pela sociedade, garantindo o entendimento essencial ao exercício da atividade de Inteligência, sem distorções ou incompressões.

Métodos: conjunto de procedimentos, medidas e ações para a produção e salvaguarda do conhecimento.

Missão Policial: Incumbência ou encargo determinado pela Autoridade Policial competente a um policial ou a uma equipe de policiais especialmente designados para o seu cumprimento.

Necessidade de Conhecer: É a condição inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou conhecimentos sigilosos. Dessa maneira, a necessidade de conhecer constitui fator restritivo do acesso, independentemente do grau hierárquico ou do nível da função exercida pela pessoa.

Normas: disposições que regulam os conceitos e procedimentos estabelecidos na doutrina.

Operação Policial: Conjunto de Ações Policiais que emprega técnicas de investigação, visando à obtenção de indícios, evidências ou provas da materialidade e autoria de um crime, para a instrução de um procedimento e/ou processo criminal,

Organização criminosa: é toda e qualquer associação estruturalmente organizada, caracterizada por hierarquia, divisão de tarefas e diversificação de áreas de atuação, com o objetivo precípuo de delinqüir, visando a obtenção de lucro financeiro e, eventualmente, vantagens político-econômicas e controle social, adquirindo dimensão e capacidade para ameaçar a sociedade e as instituições nacionais.

Ostensivo: É o documento sem classificação; o acesso pode ser franqueado, pois não há restrição.

Propaganda Adversa: Configura-se pela manipulação planejada de quaisquer informações, idéias ou doutrinas para influenciar grupos e indivíduos, com vistas a obter comportamentos pré-determinados que resultem em benefício de seu patrocinador.

Princípios: são diretrizes gerais, destinadas a orientar o desenvolvimento de um corpo doutrinário.

Procedimentos: conjunto de regras e diretrizes para intercâmbio de informações, entrada, gestão e exclusão de dados dos acervos informacionais do SISP.

Reclassificação: É a alteração do grau de sigilo atribuído a dado, conhecimento, material, área ou instalação.

Reconhecimento: entende-se como uma missão ou operação voltada para obter, seja através de contato visual ou outros meios de detecção, informações sobre atividades e recursos de um inimigo ou possível inimigo; utiliza-se também para missões designadas para a obtenção de dados confiáveis sobre relevo, aspectos meteorológicos, hidrográficos e outras características geográficas e morfológicas de uma área específica.

Sabotagem: É o ato deliberado, de efeitos físicos e/ou psicológicos, executado por agentes adversos, vinculados ou não a serviço de inteligência, com o objetivo de inutilizar ou de adulterar conhecimento, dado, material, equipamento e instalações. A sabotagem poder ser, ainda, empregada para a destruição de idéias ou a reputação de instituições e de pessoas.

Segredo: um saber de acesso particularizado a uma informação restrita, que cria alianças e divisões sociais e espaciais por aqueles que o compartilham.

Segredos estratégicos: são segredos retidos com uma motivação particular de alterar as ações e os pensamentos dos outros. Eles não são um fim em si mesmo, são meios realizados para alcançar outros fins e ocorrem quando os interesses dos atores envolvidos não são coincidentes, quando há uma assimetria de interesses relevantes.

Segredos Governamentais: informações reguladas e classificadas pelo Estado como sensíveis para a proteção individual e para os interesses da segurança institucional. Quando nos referimos a segredos governamentais estamos falando de informações que são retidas compulsoriamente e que acarretam algum tipo de punição a quem os deixar vazar.

Segurança: uma situação percebida como livre de ameaças ou de quaisquer outros fatores conflitivos. Na presença de ameaças ou conflitos identificáveis, a segurança, do ponto de vista institucional, é percebida como a possibilidade de articulação de mecanismos institucionais capazes de neutralizar essas ameaças ou conflitos, a fim de se alcançar determinado ordenamento e assegurar o conjunto de garantias e direitos constitucionais, bem como de assegurar o funcionamento integral das instituições políticas.

Segurança cidadã: é uma situação baseada no Direito Constitucional, no qual o cidadão comum encontra resguardada sua liberdade, sua vida, patrimônio, direitos e garantias, bem como a plena vigência das instituições do sistema constitucional.

A promoção da defesa destes valores e garantias é realizada através da ação integrada entre todos os segmentos sociais federais, estaduais e municipais e da indispensável participação comunitária, com a assunção das responsabilidades coletivas e individuais.

Segurança Institucional: A formulação de um certo ordenamento social, político e econômico; a identificação de um conjunto de fatos – percebidos como ameaças, riscos ou como fatores conflitivos; a articulação de um conjunto de mecanismos e procedimentos institucionais – tendentes a canalizar ações que apontem tanto para o conhecimento das ameaças, riscos ou conflitos identificados, como para sua prevenção e neutralização. Estar seguro significa viver em um Estado minimamente capaz de neutralizar ameaças através de negociações, de obter informações sobre capacidades e intenções dos interesses adversários através dos recursos que lhe estão disponíveis e legitimados pelo exercício soberano e exclusivo do monopólio da força física.

Terrorismo: É um tipo de uso ou ameaça de uso da força caracterizado pela indiscriminação dos alvos, pela centralidade do efeito psicológico que se busca causar e pela virtual irrelevância, para a correlação de forças entre as vontades antagônicas envolvidas no conflito, da destruição material e humana efetivada pela ação terrorista. Nesse sentido é que se pode dizer que o terrorismo configura um tipo específico de emprego da força: o terror.

Valores: disposições que visam fixar padrões de conduta adequados às normas impostas pela Doutrina.

Visitante: É a pessoa cuja entrada foi admitida, em caráter excepcional, em área ou instalação sigilosa.

ANEXO II - MODELO DE RELINT

CLASSIFICAÇÃO SIGILOSA

FL 01/01
LOGOMARCA DO ESTADO OU DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL OU GOVERNO DO ESTADO DO...
INSTITUIÇÃO OU SECRETARIA DE ESTADO DE...
ÓRGÃO DE INTELIGÊNCIA (OI)

RELATÓRIO DE INTELIGÊNCIA Nº [ ] DE [DATA]

1. DATA:
2. ASSUNTO:
3. ORIGEM:
4. DIFUSÃO:
5. DIFUSÃO ANTERIOR:
6. REFERÊNCIA:
7. ANEXO:
8. CLASSIFICAÇÃO:

TEXTO

Autenticação

Decreto Federal nº 4.553, de 27 Dez 2002
Art. 37 & 1º - "

Todo aquele que tiver conhecimento, nos termos deste Decreto, de assuntos sigilosos, fica sujeito às sanções administrativas, civis e penais decorrentes da eventual divulgação dos mesmos".

Art. 65 – "Toda e qualquer pessoa que tome conhecimento de documento sigiloso, nos termos deste Decreto, fica, automaticamente, responsável pela preservação de seu sigilo".

CLASSIFICAÇÃO SIGILOSA

ANEXO III – MEMENTO DE ESTUDO DE SITUAÇÃO

1. ANÁLISE DA MISSÃO

   a. Enunciado
   b. Finalidade
   c. Ações a realizar
   d. Outros dados julgados necessários

2. ANÁLISE DA SITUAÇÃO

   a. Elementos disponíveis
   b. Alvo
      1) Características
      2) Possibilidades e vulnerabilidades
      3) Outros dados julgados necessários
   c. Ambiente Operacional
      1) Descrição e características da área
      2) Aspectos que facilitam, dificultam ou impedem a ação
   d. Escolha das Técnicas Operacionais
   e. Meios em Pessoal e Material
   f. Órgãos Similares

3. LINHAS DE AÇÃO

   a. Linhas de Ação por Ação a Realizar
      1) Conceito da ação
      2) Composição dos Meios
   b. Análise das Linhas de Ação
   c. Comparação das Linhas de Ação

d. Seleção das Linhas de Ação

4. MEDIDAS ADMINISTRATIVAS

a. Recursos Financeiros
b. Segurança
Na Segurança, considerar:
1) Pessoal
a) Documentação
b) Vestuários e Disfarce
c) Armamento
d) Estória-Cobertura
2) Instalações
3) Compartimentação
c. Instrução e/ou Treinamento
d. Outras Medidas

5. COORDENAÇÃO E CONTROLE

a. Ligações
b. Prazos
c. Restrições e Imposições
d. Reuniões
e. Relatórios
f. Comunicações
1) Sistemas
2) Códigos
3) Horários
4) Prioridades

ANEXO IV – MEMENTO DO PLANO DE SEGURANÇA ORGÂNICA

Grau de Sigilo

Logomarca da organização

Cabeçalho da organização

1. Situação Geral
2. Finalidade
3. Objetivo
4. Competências
5. Legislação de Referências
6. Conceituações
7. Execução

7.1. Segurança do Pessoal

7.2. Segurança da Documentação e do Material

7.3. Segurança dos Sistemas de Telemática

7.3.1. Segurança das Comunicações

7.3.2. Segurança da Informática

7.4. Segurança das Áreas e das Instalações

7. Disposições Finais
8. Data
9. Assinatura

Grau de Sigilo

ANEXO V – MEMENTO DA DNISP

Ministério da Justiça

Secretaria Nacional de Segurança Pública

Sistema Brasileiro de Inteligência de Segurança Pública

Memento DNISP

FUNDAMENTOS DOUTRINÁRIOS

Características

- Produção de Conhecimento
- Assessoria
- Verdade com Significado
- Busca de Dados Protegidos
- Ações Especializadas
- Economia de Meios
- Iniciativa
- Abrangência
- Dinâmica
- Segurança

Princípios

- Amplitude
- Interação
- Objetividade
- Oportunidade
- Permanência
- Precisão
- Simplicidade
- Imparcialidade
- Compartimentação
- Controle
- Sigilo

Valores

- Vida
- Ética
- Direitos individuais e sociais
- Garantias Individuais e sociais
- Moralidade
- Legalidade
- Impessoalidade
- Eficiência
- Democracia

Ramos

- Inteligência
- Contra-Inteligência

Fontes

- Abertas
- Protegidas

Meios de Obtenção de dados

- Inteligência Humana
- Inteligência Eletrônica

Sinais
Imagens
Dados

CONHECIMENTO

Produção do Conhecimento - Dado - Conhecimento

- Estados da Mente
  Verdade
  Certeza
  Opinião
  Dúvida
  Ignorância

- Trabalhos Intelectuais
  Idéias
  Juízo
  Raciocínio

- Tipos de conhecimento
  Informe

Informação
Apreciação
Estimativa

Ciclo da Produção do Conhecimento

Planejamento
- Reunião de dados e/ou conhecimentos
- Processamento
  avaliação
  análise
  integração
  interpretação

- Difusão

Planejamento

- Assunto
- Faixa de tempo
- Usuário
- Finalidade
- Prazo
- Aspectos essenciais
  Verificação dos aspectos essenciais conhecidos
  Verificação dos aspectos essenciais a conhecer

Processamento

- Avaliação

Pertinência
Credibilidade

- Fonte
  Autenticidade
  Confiança
  Competência

- Conteúdo
  Coerência
  Compatibilidade

Semelhança

- Análise [Decomposição nas partes constitutivas]
  - Avaliadas
  - Relacionadas ao Assunto
  - Graduadas em importância ao assunto

- Integração [Montagem do conjunto das frações significativas]
  - Coerência
  - Ordenação lógica
  - Ordenação cronológica

- Interpretação [Significado Final]
  - Relações de Causa e Efeito
  - Tendências e padrões
  - Trajetória
  - Fatores de Influência

- Difusão
  - Formalização [Documentos de Inteligência]
    - Documentos Externos:
      - Relatório de Inteligência [RELINT]
      - Pedido de Busca [PB]
      - Mensagem [Msg]
      - Sumário
    - Documentos Internos
    - Requisitos do RELINT
    - Classificação e Restrição ao uso dos documentos de ISP
    - Retransmissão
  - Disponibilização
  - Arquivamento

- Avaliação de Resultados

MÉTODOS PARA REUNIÃO DE DADOS

Ações de Inteligência
- Ações de Coleta
  - Primária
  - Secundária
- Ações de Busca

Operações de ISP
- Ambiente Operacional
- Alvo
- Elementos de Operações
- Pessoal
  - Agente
  - Colaborador
  - Informante
- Rede
- Controlador

Ações de Busca
- reconhecimento
- vigilância
- recrutamento operacional
- infiltração
- desinformação
- provocação
- entrevista
- entrada
- interceptação de sinais e de dados.

Técnicas Operacionais de ISP
- Processos de Identificação de Pessoas
- Observação, Memorização e Descrição
- Estória-Cobertura
- Disfarce
- Comunicações Sigilosas
- Leitura da Fala
- Análise de Veracidade
- Emprego de Meios Eletrônicos
- Foto-interpretação

Tipos de Operações de Inteligência

Operações exploratórias
Operações sistemáticas

Planejamento das Operações de Inteligência

Estudo de Situação e Plano de Operação de Inteligência
Medidas de Controle
Medidas de Coordenação
Medidas de Avaliação
Medidas de Orientação
Medidas de Segurança

CONTRA-INTELIGÊNCIA

Responsabilidade

- Acesso
- Comprometimento
- Vazamento

Segmentos

Segurança Orgânica
Segurança de pessoal
Segurança de documentação
Segurança das instalações
Segurança do material
Segurança das Operações de ISP
Segurança das Comunicações e Telemática
Segurança da Informática

Segurança de Assuntos Internos

Segurança Ativa
Contrapropaganda
Contra-espionagem
Contrassabotagem
Contra-terrorismo

ORGANIZAÇÃO DA ISP

- Sistema
- Subsistema
- Canais
- Organização
  Sistema
  Subsistema
  Tipos de AI
  Classes de Agências de Inteligência
  Estruturas das AI
  Comunidade de Inteligência de Segurança Pública
  Plano Nacional de Inteligência de Segurança Pública

- Profissionalismo
  Atributos
  Recrutamento administrativo
  Qualificação
  Permanência

- Denúncia
- Inteligência Policial
- Recursos Materiais
  Equipamentos
  Instalações
  Viaturas
  Equipamentos de comunicação
  Equipamentos de Informática
- Verba Secreta

RESERVADO

RESERVADO