Universidade do Sul de Santa Catarina

Inteligência e Segurança Pública

UnisulVirtual

Universidade do Sul de Santa Catarina

Inteligência e Segurança Pública

UnisulVirtual
Palhoça, 2014

Créditos

Universidade do Sul de Santa Catarina – Unisul

Reitor
Sebastião Salésio Herdt
Vice-Reitor
Mauri Luiz Heerdt

Pró-Reitor de Ensino, de Pesquisa e de Extensão
Mauri Luiz Heerdt
Pró-Reitor de Desenvolvimento Institucional
Luciano Rodrigues Marcelino
Pró-Reitor de Operações e Serviços Acadêmicos
Valter Alves Schmitz Neto

Diretor do Campus Universitário de Tubarão
Heitor Wensing Júnior
Diretor do Campus Universitário da Grande Florianópolis
Hércules Nunes de Araújo
Diretor do Campus Universitário UnisulVirtual
Fabiano Ceretta

Campus Universitário UnisulVirtual

Diretor
Fabiano Ceretta

Unidade de Articulação Acadêmica (UnA) - Educação, Humanidades e Artes
Marciel Evangelista Cataneo *(articulador)*
Unidade de Articulação Acadêmica (UnA) – Ciências Sociais, Direito, Negócios e Serviços
Roberto Iunskovski *(articulador)*
Unidade de Articulação Acadêmica (UnA) – Produção, Construção e Agroindústria
Diva Marília Flemming *(articuladora)*
Unidade de Articulação Acadêmica (UnA) – Saúde e Bem-estar Social
Aureo dos Santos *(articulador)*

Gerente de Operações e Serviços Acadêmicos
Moacir Heerdt
Gerente de Ensino, Pesquisa e Extensão
Roberto Iunskovski
Gerente de Desenho, Desenvolvimento e Produção de Recursos Didáticos
Márcia Loch
Gerente de Prospecção Mercadológica
Eliza Bianchini Dallanhol

André Haydt Castello Branco
Fred Harry Schauffert
Luiz Otávio Botelho Lento

Inteligência e Segurança Pública

Livro didático

Designer instrucional
Marina Melhado Gomes da Silva

UnisulVirtual
Palhoça, 2014

Livro Didático

Professor conteudista
André Haydt Castello Branco
Fred Harry Schauffert
Luiz Otávio Botelho Lento

Designer instrucional
Marina Melhado Gomes da Silva

Projeto gráfico e capa
Equipe UnisulVirtual

Diagramador(a)
Noemia Mesquita

Revisor(a)
Perpétua Guimarães Prudêncio

ISBN
978-85-7817-612-9

658.4038
C34 Castello Branco, André Haydt
Inteligência e segurança pública: livro didático / André Haydt Castello Branco, Fred Harry Schauffer, Luiz Otávio Botelho Lento; design instrucional Marina Melhado Gomes da Silva. – Palhoça: UnisulVirtual, 2014.
160 p. : il. ; 28 cm.

Inclui bibliografia.
ISBN 978-85-7817-612-9

1. Gestão da informação. 2. Inteligência em negócios. 3. Segurança pública. I. Schauffer, Fred Harry. II. Lento, Luiz Otávio Botelho. III. Silva, Marina Melhado Gomes da. IV. Título.

Ficha catalográfica elaborada pela Biblioteca Universitária da Unisul

Sumário

Introdução

Caríssimos/as alunos/as:

Sejam bem-vindos ao estudo do livro didático **Inteligência e Segurança Pública**.

Na atualidade, a Inteligência tem demonstrado ser o sustentáculo das organizações policiais em todos os países do mundo. O crescimento exacerbado e desordenado das cidades tem oportunizado um aumento avassalador dos índices de violência e criminalidade, que só poderão ser contidos ou minimizados no campo preventivo ou repressivo através de um trabalho bem elaborado, desde o planejamento até a atuação das equipes de Inteligência das organizações policiais.

A produção de conhecimentos e a sua respectiva salvaguarda compreendem a atividade de Inteligência que o Estado tem interesse em preservar, utilizando metodologias e técnicas que permitam afastar a prática de ações meramente intuitivas e a adoção de procedimentos sem uma orientação racional.

A atividade de Inteligência, outrora denominada “Informações”, que sempre representou um tabu, ficando restrita aos seus especialistas, na atualidade do Estado Democrático de Direito abre as suas portas para que outros possam se abeberar dos seus conhecimentos e aplicá-los com equidade em prol de uma sociedade mais fraterna. Esta senda nos levará à preservação e manutenção da ordem pública, à segurança pública, à salubridade pública e, por derradeiro, à tão almejada tranquilidade pública, a paz social.

Conhecer os meandros da Inteligência é tarefa vital para o operador da área de preservação da ordem pública, com o intento de que seja o melhor no seu ofício.

Desejamos bom estudo!

Os professores.

Capítulo 1

História, definições e princípios básicos

Habilidades

Capacitar o estudante com saberes teóricos, práticos, e metodologia adequada para: descrever os sistemas de Inteligência dos órgãos de Segurança Pública; dominar técnicas de proteção aos dados e informações de cunho pessoal, evitando a exposição desnecessária de indivíduos; dominar técnicas de levantamento de informações, análise e proteção de dados; analisar e operar dados para realizar a gestão da informação atuando sobre os problemas relacionados à Segurança Pública e a questões correlatas; coletar a informação e analisá-la à luz da legislação e em articulação com os diferentes órgãos das esferas federais, estaduais e municipais e até internacionais; caracterizar as técnicas de Inteligência na gestão da Segurança Pública e suas potencialidades; conhecer e relacionar as Atividades de Inteligência e Contrainteligência; atuar com ética e imparcialidade, senso crítico e responsabilidade; trabalhar em equipe; conhecer e aplicar corretamente a legislação vigente na área de Inteligência, respeitando os direitos humanos.

Seções de estudo

Seção 1: Histórico da Atividade de Inteligência no Brasil

Seção 2: Definições e princípios básicos

Seção 1
Histórico da Atividade de Inteligência no Brasil

Ninguém vive sem passado, sem história. Como tudo na vida é escrito ao longo do espaço e do tempo, observamos que não é diferente com os estudos que estamos iniciando.

O primeiro contato transportará você a um passeio no túnel do tempo, retroagindo até a década de 20, e de lá para cá viajando na senda da história registrada por homens e mulheres que labutaram nos serviços de Inteligência do Brasil. Aprenderá um novo linguajar, navegará por um mundo diferente, com um jargão próprio que requer a familiarização com novos termos e conceitos que não podem ser desprezados.

Diante disto, iniciamos a nossa caminhada pelo campo da Atividade de Inteligência, navegando em meio a novas palavras e termos técnicos.

> *(...) a memória, com os anos, se apaga e o que não está escrito acaba não existindo.*
>
> *(Waldyr H. Neumann)*

Afirma Rodrigues (1999, p. 2) que

> Desde os primórdios da civilização a atividade de inteligência norteou a tomada de decisões buscando sempre uma avaliação precisa, quer no campo militar, quer no campo político, para um planejamento estratégico eficaz.

Perrenoud (1996 apud RODRIGUES, 1999, p. 2) cita alguns personagens que, ao longo da história, tornaram-se verdadeiros líderes, tais como: Moisés (*Êxodo*), Sun Tzu (*A Arte da Guerra*), Maquiavel (*O Príncipe*), Mao Tse Tung (Estrategista da guerra de guerrilha), e Napoleão Bonaparte (deu ênfase às informações de combate e é o precursor da criação do Estado-Maior).

No Brasil, a **Atividade de Inteligência**, outrora denominada **Atividade de Informações**, é detentora de uma história muito rica, povoada de mistérios e questões por vezes nebulosas, em razão das inúmeras crises governamentais a que fomos submetidos.

No início, sua ação era orientada para o assessoramento ao governo, o que ocorreu com o advento do Conselho de Defesa Nacional, mediante o Decreto n. 17999, de 29 de novembro de 1927, órgão diretamente subordinado ao Presidente da República e constituído por todos os ministros de estado e os chefes dos Estados-Maiores da Marinha e do Exército.

Antes daquele ano, a atividade era exercida apenas no âmbito dos dois ministérios militares então existentes (Ministério da Guerra e da Marinha), que se dedicavam exclusivamente às questões de defesa nacional e atuavam em proveito das respectivas forças. Nessa época, ainda não existia o Ministério da Aeronáutica (MAer) e a Força Aérea Brasileira (FAB), criados em 1941.

A Constituição outorgada em 1937, conhecida como Polaca, no seu artigo 162, passou a definir o Conselho Superior de Segurança Nacional apenas como "Conselho de Segurança Nacional".

Por que a denominação "de inteligência" e não "de informações"?

De acordo com a Agência Brasileira de Inteligência (ABIN), "porque no sentido de produção de conhecimentos voltados para a segurança do Estado e da sociedade, é consagrado o uso do termo Inteligência".

O que significa Constituição Outorgada? Qual a alcunha atribuída à Constituição de 1937? Você acabou de ver que a Atividade de Inteligência no Brasil deu os seus primeiros passos ligada às forças militares. Escreva abaixo os motivos que levaram Getúlio Vargas a impor uma Carta Magna autoritária.

Em 05 de outubro de 1942, o Conselho de Segurança Nacional teve a sua composição alterada pelo Decreto-Lei n. 4783, que instituiu e regulamentou como seus órgãos complementares a Comissão de Estudos, a Secretaria Geral, as Seções de Segurança Nacional e a Comissão Especial de Faixa de Fronteiras.

A Atividade de Inteligência passou a crescer em importância quando o Decreto n. 27583, de 14 de dezembro de 1949, aprovou o Regulamento para a Salvaguarda das Informações de Interesse da Segurança Nacional, e o Decreto n. 27930, de 27 de março de 1950, dispôs sobre a aplicação do Decreto n. 27583.

O Decreto n. 44489-A, de 15 de setembro de 1958, dispôs sobre o Serviço Federal de Informações e Contrainformações (SFICI), de que trata o Decreto-Lei n. 9975-A, tendo atribuído ao SFICI competência para superintender e coordenar as atividades de inteligência que interessassem à Segurança Nacional. Com a chegada dos militares ao poder, em 1964, o Estado brasileiro reformulou a sua gestão administrativa, ocasião em que reestruturou o organismo de informações do País, tendo o Presidente da República encaminhado Projeto de Lei ao Congresso Nacional, em 11 de maio, propondo a criação do Serviço Nacional de Informações (SNI). Em 13 de junho de 1964, através da Lei n. 4341, foi criado o Serviço Nacional de Informações. Como resultado disso, em 24 de setembro do mesmo ano, o Decreto n. 54303 alterou a redação do Regimento da Secretaria Geral do Conselho de Segurança Nacional, aprovado pelo Decreto n. 45040, e revogou o Decreto n. 44489-A.

A Circular n. 12, do Gabinete Civil da Presidência da República, datada de 06 de agosto de 1965, recomendou às Seções de Segurança Nacional dos Ministérios Civis que mantivessem estreita e permanente ligação com o SNI.O Decreto n. 60417, de 11 de março de 1967, aprovou e colocou em execução o Regulamento para a Salvaguarda de Assuntos Sigilosos (RSAS), que, em 06 de janeiro de 1977, foi revogado pelo Decreto n. 79099, que aprovou o novo RSAS.

Corria o ano de 1971, quando, em 31 de março, pelo Decreto n. 68488, foi criada a Escola Nacional de Informações (EsNI), diretamente subordinada ao Ministro Chefe do SNI, com a finalidade de preparar, atualizar e especializar o pessoal para exercer funções no Sistema Nacional de Informações (SISNI). A Escola Nacional de Informações passou a funcionar a partir do ano de 1972, quando formou a primeira turma, prosseguindo com as suas atividades nos anos seguintes, através da realização de cursos regulares e estágios de curta duração.

Em 12 de abril de 1990, a Lei n. 8.028 permitiu a fusão da Inteligência com o Planejamento Estratégico, durante o governo do Presidente Fernando Collor de Mello.

No governo de Itamar Franco, a Lei n. 8490, de 19 de novembro de 1992, criou a Secretaria Geral da Presidência da República.

Durante a gestão do Presidente Fernando Henrique Cardoso, a Medida Provisória n. 813, de 1º de janeiro de 1995, vincula a Subsecretaria de Inteligência (SSI/CMPR) à Secretaria Geral da Presidência da República (SG/PR). Ainda nesse governo, a Subsecretaria de Inteligência (SSI/CMPR) passou a ser subordinada

à Casa Militar através da Medida Provisória n.1384, e a Lei n. 9883, de 07 de dezembro de 1999, cria a Agência Brasileira de Inteligência (ABIN).

A atuação dos Órgãos de Inteligência na Polícia Militar teve origem na década de 50, com a reformulação da sua Organização Básica, que os colocou como integrantes do Estado-Maior Geral (EMG) e das Unidades Policiais. Desde aquela época, a sua atuação sempre foi voltada para o acompanhamento do público interno, deixando a produção de conhecimento sobre Segurança Pública em segundo plano. Com o advento da Revolução de 1964, a sua atuação, assim como a dos demais Órgãos de Inteligência do Brasil, foi direcionada para a defesa dos interesses do Estado revolucionário, passando a colaborar com os demais no acompanhamento da atuação dos integrantes de entidades e partidos políticos contrários ao regime.

Com a promulgação da Constituição de 1988, houve uma reformulação do trabalho executado pela maioria dos Órgãos de Inteligência, que tiveram seu foco de atuação alterado com base numa nova doutrina.

- *Antes de prosseguir com a leitura, que tal uma parada para fazer uma reflexão?*

Ao longo desta seção de estudos, você teve a oportunidade de conhecer o desenvolvimento histórico da Atividade de Inteligência no Brasil. Desde a década de 20 até meados dos anos 80, o povo brasileiro viveu a maior parte do tempo sob regime de exceção. Com o advento da Constituição Cidadã de 1988, verificamos que o artigo 5º constitui um monumento ao liberalismo e à democracia. Do ponto de vista da Atividade de Inteligência, emita sua opinião, traçando um comparativo entre aquele momento e o atual.

Seção 2
Definições e princípios básicos

> *Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas (...).*
>
> *(Sun Tzu – A Arte da Guerra).*

Para Álvares (1973, p. 345), "muitos são os modos de compreender e conceituar '**informações**'". No Dicionário Houaiss da Língua Portuguesa (2001), o verbete **informação** figura como "o ato ou efeito de informar (-se); comunicação ou recepção de um conhecimento ou juízo; o conhecimento obtido por meio de investigação ou instrução; esclarecimento, explicação; indicação".

Shermann Kent (1967, p. 17-153) afirma que a "Inteligência" pode ser entendida sob três aspectos: como "produto, organização e processo".

O que seria isso?

A Inteligência como **produto** é o resultado do processo desenvolvido na atividade, que é o conhecimento de Inteligência produzido; e que tem como cliente o tomador de decisão, em qualquer nível. Este conhecimento é expresso em documentos próprios da atividade: o informe, a informação, a apreciação e a estimativa.

A Inteligência como **organização** pode ser identificada nas estruturas que têm como missão produzir os conhecimentos de Inteligência. Como exemplo, temos a Agência Brasileira de Inteligência (ABIN), no nosso país.

A Inteligência como **processo** tem a ver com a metodologia empregada para produzir o conhecimento de Inteligência, a qual orienta as maneiras de se obter dados e outros conhecimentos para depois analisá-los e interpretá-los para sua posterior difusão aos interessados; abrangendo, também, as medidas de proteção de todo este ciclo de produção do conhecimento.

Álvares (1973, p. 345) prossegue afirmando que:

> [...] o manual escolar da ECEME (Escola de Comando e Estado-Maior do Exército) é já bem mais explícito, atribuindo às informações os significados de:
>
> • esclarecer, no sentido de troca de conhecimentos;

- prestar informações, no sentido de fornecer conhecimentos para o estudo de problemas de segurança nacional;
- divulgar informações, no sentido de conhecimento levado ao público; conhecimento, no sentido de atualização ou aprimoramento de cultura ou opinião.

Geraldo Knaack de Souza, então Coronel conferencista da ESG (Escola Superior de Guerra), esclarece que **informação** é conhecimento transmitido com uma ou diversas das seguintes finalidades: esclarecer, atualizar ou aprimorar cultura e formar opinião.

Outros conferencistas definem **informação** como o conhecimento objetivo necessário a uma decisão ou a um esclarecimento, apresentado precisa e oportunamente.

As diversas definições apresentadas possuem diferenças de estilo, levando à conclusão de que a **informação** é um tipo particular de conhecimento, pois exige um **agente** que o elabora e um **beneficiário** que nele se apoia, que é informado a respeito do fato. Na sequência, percebe-se que a transmissão desse tipo especial de conhecimento tem ampla finalidade: estudar problemas de segurança nacional; basear uma linha de ação bem sucedida; levar conhecimento ao público; aprimorar a cultura ou opinião etc.

A **informação** pode ser utilizada no campo do ensino e instrução, da propaganda ou da comunicação social, e, no nosso caso em particular, no campo da Segurança Pública.

No campo militar ou policial, as organizações destinadas à produção de Inteligência recebem diversas denominações: serviço, centro, agência, escritório, divisão, seção, unidade, dentre outras. O conjunto dessas organizações, estruturadas em um ou mais sistemas independentes, deve ser chamado de **Sistema de Inteligência**.

Segundo Rodrigues (1999, p. 08), “o desejo e a necessidade de **informações** são inerentes à natureza humana”.

O ser humano precisa estar informado antecipadamente, com vistas a permitir identificar comportamentos, diante de fatos ou situações futuras, nos âmbitos individual, grupal ou nacional. Todos os Estados organizados não desprezam o uso e a utilidade das **informações**, sob pena de pagar um preço alto pelo desconhecimento de fatos ou situações que estejam por ocorrer.

Para que os governos, em nível nacional e internacional, possam formular políticas e estabelecer estratégias, mister se faz a coleta, a posse e a constante obtenção de novos e complementares conhecimentos.

HUXLEY (1986 apud RODRIGUES, 1999, p. 9) registra que: “As pessoas nunca podem estar em segurança sem **informações**”.

A **Inteligência Policial** é arma poderosa contra a violência e a criminalidade, no momento em que une esforços da Polícia Militar com a Polícia Civil, para atuação nas áreas mais críticas dos aglomerados urbanos, acumulando **informações** necessárias para o combate aberto ao crime.

Conforme Rodrigues (1999), a Doutrina de Inteligência é recente no Brasil (aproximadamente 70 anos), sendo que, assim como nos países ocidentais, foi conhecida como Doutrina de Informações e inicialmente esteve voltada somente para assuntos militares.

Segundo DeLadurantey (1995 apud DANTAS; SOUZA, 2008, p. 01), a expressão **Inteligência** pode ser entendida da seguinte maneira:

> É o conhecimento das condições passadas, presentes e projetadas para o futuro de uma comunidade, em relação aos seus problemas potenciais e atividades criminais. Assim como a Inteligência pode não ser nada mais que uma informação confiável que alerta para um perigo potencial, também pode ser o produto de um processo complexo envolvendo um julgamento bem informado, um estado de coisas, ou um fato singular. O “processo de Inteligência” descreve o tratamento dado a uma informação para que ela passe a ser útil para a atividade policial.

A indústria cinematográfica e a mídia, formadores de opinião que são, quase sempre atribuem a conotação de **espionagem** para a **Atividade de Inteligência**. A primeira se constitui numa atividade ilegal, enquanto a segunda atende ao princípio da legalidade, sendo executada de acordo com a legislação que a regula e disciplina.

A **Atividade de Inteligência,** exercida pelas **Organizações Policiais,** está inserida na **Administração Pública**, mantendo-se sob a égide do **Direito Público**, onde só se pode fazer o que a lei permite, diferente da atividade no setor privado, que permite fazer tudo aquilo que a lei não proíbe.

2.1 Atividade de Inteligência

Segundo o Manual Básico da ESG (1986 apud RODRIGUES, 1999, p. 12), de acordo com a **Doutrina Nacional de Inteligência**, a Atividade de Inteligência "é o esforço organizado para colher dados, avaliá-los pouco a pouco e reuni-los até que formem configurações mais amplas e nítidas".

Tal esforço, recaindo sobre a **reunião** e o **processamento** dos dados e a **difusão** das informações, constituem o sustentáculo de todo o conjunto de ações que recebe a denominação genérica de **Atividades de Inteligência**.

Rodrigues (1999, p. 12) prossegue afirmando que a Atividade de Inteligência significa:

> O exercício sistemático de ações especializadas, orientadas para a **produção** e **salvaguarda** de conhecimentos, tendo em vista assessorar as autoridades governamentais, nos respectivos níveis e áreas de atribuição, para o **planejamento**, **execução** e **acompanhamento** de suas políticas.

Caracteriza-se pela prática contínua de ações especializadas, dirigidas para:

I – A obtenção de dados e a avaliação de situações externas que impliquem ameaças, veladas ou dissimuladas, capazes de dificultar ou impedir a consecução dos interesses estratégicos da Organização.

II – A identificação, a avaliação e a neutralização da espionagem promovida por serviços de inteligência ou outros organismos, vinculados ou não a governos.

III – A proteção dos conhecimentos científicos e tecnológicos que, no interesse da segurança da Organização e do Estado, sejam considerados sigilosos (ACI, 2005, p. 5).

2.2 Ramos da Atividade de Inteligência

A Atividade de Inteligência divide-se em dois ramos: **Inteligência** e **Contrainteligência**.

2.2.1 O que é Inteligência?

É o exercício permanente de ações especializadas orientadas para a obtenção de dados; a produção e a difusão de Conhecimentos, com vistas a assessorar o processo decisório de qualquer nível em suas áreas de atribuição.

De acordo com Dantas e Souza (2008), muito embora as atividades de Inteligência estejam presentes em quase todo o mundo, a percepção brasileira acerca da Inteligência é muito variável, causando reações que vão da simpatia ao total rechaço. De acordo com Gonçalves (2003 apud DANTAS; SOUZA, 2008, p.6), "Modernamente, não se pode cogitar a existência de Estado que não disponha de órgãos de inteligência em sua estrutura". A atividade de inteligência teve início com a civilização, claro que não com esse nome; e tendo sido percebida como essencial para a governabilidade e a garantia da segurança, não só em períodos de luta armada entre nações, mas também em tempos de paz e ordem institucional.

Dantas e Souza (2008) prosseguem enfatizando a relevância da inteligência no controle da criminalidade, através do fornecimento de dados para a contenção dos delitos, e a definição de cenários e estratégias de atuação na segurança pública e institucional.

Nos seus estudos, Dantas e Souza (2008, p.6) afirmam ainda que:

> É bastante sutil a diferenciação entre a Atividade de Inteligência e a de investigação policial. Ambas lidam, muitas vezes, com os mesmos objetos (crime, criminosos e questões conexas), com seus agentes atuando lado a lado. Enquanto a investigação policial tem como propósito direto instrumentar a persecução penal, a Inteligência Policial é um suporte básico para a execução das atividades de Segurança Pública, em seu esforço investigativo inclusive. A metodologia (de abordagem geral e de procedimentos específicos) da Inteligência Policial está essencialmente identificada com a da Inteligência de Estado.

O que é a "atividade policial guiada pela inteligência"?

Acerca do assunto, veja o que George Felipe de Lima Dantas expressa no texto:

A “atividade policial guiada pela inteligência” é um modelo de atividade policial em que a inteligência serve como guia para realização de atividades policiais, em lugar do reverso disso. O conceito é inovador, e de certa forma radical, já que está baseado na moderna premissa da gestão policial de que a principal tarefa da polícia é prevenir e detectar a criminalidade, em lugar de apenas reagir às ocorrências deste fenômeno social.

A gestão policial, no mundo inteiro, vem lidando com óbices a cada dia maiores. O velho “fazer” da atividade policial modernamente enfrenta situações em que forças econômicas, sociais e políticas produzem efeitos que permeiam todas as atividades humanas. Se considerarmos como fato positivo para o entendimento da criminalidade pela gestão policial a noção de que a motivação fundamental da delinquência continua sendo o velho conceito da ambição, o mesmo já não acontece em relação aos recursos e oportunidades dos criminosos. Os recursos e oportunidades da criminalidade aumentaram exponencialmente, bem como o tamanho dos ganhos potenciais da delinquência. A atividade policial precisa hoje lidar com modalidades do fenômeno da criminalidade que seriam irreconhecíveis por policiais da geração anterior. Some-se a isso o fato de que a gestão policial é cada vez mais tensionada por uma situação econômica em que os recursos de gestão são cada vez mais escassos.

O velho padrão de gestão reativa, conforme aponta a atual situação caótica da segurança pública brasileira, já não é mais viável. Também já não são mais tão aplicáveis velhos modelos de percepção do fenômeno da criminalidade e do comportamento criminal. A moderna gestão da inteligência policial, enquanto força propulsora dessa atividade essencial, pode ser um fator chave para a sobrevivência das atuais instituições policiais do Brasil.

Qualquer que seja o modelo específico de “atividade policial guiada pela inteligência”, tal paradigma de gestão demandará forte comprometimento institucional, capaz de superar velhas práticas e preconceitos. Seus gestores deverão estar preparados para distanciarem-se de velhos métodos e técnicas; terão de acreditar firmemente que as operações policiais podem e devem ser guiadas pela atividade de inteligência; terão ainda que pautar como princípio a ação, e não a reação, numa virada histórica em relação ao antigo paradigma reativo. Deverão, enfim, acreditar no processo de produção de conhecimento que a inteligência policial enseja, confiando em suas avaliações e recomendações. Tudo isso é bastante difícil e, de certa forma, doloroso, considerando que implica mudança.

DANTAS, George Felipe de Lima. **O quinto poder**. Disponível em: <http://www.oquintopoder.com.br>. Acesso em: 21 nov. 2006.

2.2.2 Contrainteligência

É o ramo da Atividade de Inteligência responsável pela proteção de dados, conhecimentos, áreas, pessoas e meios de interesse da sociedade, ou de qualquer organização.

2.2.3 Princípios básicos da Atividade de Inteligência

A nossa rotina de vida, na maioria das vezes, deve ser regida por um conjunto de princípios básicos, como forma de orientar os passos a serem seguidos na jornada evolutiva em todos os campos do relacionamento social. Os profissionais que participam da produção do conhecimento e, portanto, das Atividades de Inteligência, devem saber que elas são fundamentadas em princípios básicos, os quais você estudará na sequência.

Perrenoud (1996 apud RODRIGUES, 1999, p. 14) afirma que:

> [...] dentre os **princípios** que regem a **Atividade de Inteligência**, os relacionados a seguir devem ser observados harmonicamente de modo que a ênfase na aplicação de um deles não acarrete prejuízo no emprego dos demais.

Esse conjunto envolve os seguintes princípios: objetividade, segurança, oportunidade, controle, imparcialidade, simplicidade, amplitude e clareza.

a. **Objetividade**

Fundamenta-se em planejar e executar as ações de acordo com os objetivos a atingir e em perfeita harmonia com as finalidades da atividade. Em todas as fases, a produção do conhecimento de Inteligência deve se orientar pela utilidade, finalidade e objetivo específico da informação a ser produzida, e realizar-se com a maior precisão possível, através de uma linguagem clara e simples.

b. **Segurança**

Durante todas as fases da produção, a informação deve ser protegida por medidas de sigilo adequado, de maneira que o acesso a seus termos seja restrito apenas a pessoas credenciadas ao seu conhecimento. Requer a adoção de medidas de salvaguarda convenientes a cada caso.

c. **Oportunidade**

O valor da informação está em sua utilização oportuna, pois toda informação se deprecia com o passar do tempo, tendo um prazo final, após o que poderá até estar muito completa, porém totalmente inútil. Desta forma, o princípio da oportunidade estabelece que a informação deva ser produzida dentro de um período de tempo que garanta a sua utilização.

d. **Controle**

A produção do conhecimento deve obedecer a um planejamento que possibilite o adequado controle de cada uma das fases. Exige a supervisão e o acompanhamento adequado das ações.

e. **Imparcialidade**

A produção da informação requer equilíbrio. Toda informação deve ser isenta de ideias preconizadas, subjetivismos e outras influências que originem distorções. Levando em conta que, na produção da informação, existe a necessidade de serem verificados fatos que vão traduzir conhecimentos tão próximos da verdade quanto possível, é obrigatório que os operadores da organização **não se deixem dominar pela paixão ou quaisquer outros interesses ou influências** que possam modificar a informação produzida.

f. **Simplicidade**

As atividades ou ações complexas devem ser evitadas na produção do conhecimento. Os conhecimentos expressos devem ser simples, de forma a conter unicamente o que é essencial, isento de expressões e conceitos dispensáveis. A execução das ações deve evitar custos e riscos desnecessários.

g. **Amplitude**

O conhecimento sobre o fato, assunto ou situação deve ser o mais completo possível, utilizando-se de todas as fontes disponíveis. A amplitude deste princípio deve ser harmonizada com o da “oportunidade”, pois é necessário estabelecer um adequado equilíbrio entre a amplitude dos conhecimentos elaborados e a necessidade de difusão oportuna.

h. **Clareza**

Os usuários que entram em contato com os conhecimentos produzidos nas Atividades de Inteligência devem compreendê-los imediata e completamente. Este princípio prevê que o leitor deve ter a imediata e integral compreensão do significado do documento de Inteligência, assim como destacar-se pela evidência dos conhecimentos produzidos. Com o objetivo de atender a este princípio, o conhecimento deve ser redigido em linguagem correta e livre de literatura rebuscada e de floreios supérfluos. Na produção do conhecimento, a clareza vincula-se estreitamente à objetividade e simplicidade.

De maneira sucinta, até aqui você teve a oportunidade de estudar os diferentes momentos vividos pelo Serviço de Inteligência no país. A maior parte do tempo foi passada servindo a governos – e não ao Estado brasileiro – que conferiram à Atividade de Inteligência uma mácula que até hoje ainda empana o brilho de tão importante missão em prol do Estado e da sociedade.

Ainda foi oportunizado manter contato com as definições de Inteligência e Contrainteligência, bem como conhecer os princípios básicos da Atividade de Inteligência, condição elementar tão necessária para a perfeita produção do conhecimento. Vamos seguir adiante nos estudos da Inteligência na Segurança Pública.

Capítulo 2

Sistemas e subsistemas de Inteligência

Habilidades

Capacitar o estudante com saberes teóricos, práticos e metodologia adequada para descrever os sistemas de Inteligência dos órgãos de Segurança Pública, bem como caracterizar as técnicas de Inteligência na gestão da Segurança Pública e suas potencialidades.

Seções de estudo

Seção 1: O Sistema Brasileiro de Inteligência (SISBIN)

Seção 2: O Subsistema de Inteligência de Segurança Pública (SISP)

Seção 3: A Diretoria de Informação e Inteligência (DINI)

Seção 4: O Sistema de Inteligência da Polícia Militar (SIPOM)

Seção 1
O Sistema Brasileiro de Inteligência (SISBIN)

A Atividade de Inteligência remete-nos ao mundo da fantasia do cinema, permeado de mistérios, crimes e espiões. Toda esta magia foi quebrada ao longo da história com a derrocada de alguns impérios, de alguns mitos. O fim da Guerra Fria, a queda do muro de Berlim, o esfacelamento da União das Repúblicas Socialistas Soviéticas (URSS) e, mais precisamente no campo interno, a redemocratização do Brasil, oportunizaram mudanças radicais nesta área de atuação.

Muito embora ainda tenhamos legislação rigorosa sobre o assunto em tela, mais operadores da Segurança Pública passaram a ter acesso a essas informações. Para que as organizações policiais obtenham êxito no cumprimento da sua missão é importante que os seus colaboradores conheçam a estrutura e o funcionamento dos órgãos de Inteligência e Contrainteligência.

Neste capítulo, você vai conhecer os aspectos estruturais e de funcionamento do Sistema Brasileiro de Inteligência e da Agência Brasileira de Inteligência, e do Serviço de Inteligência da Secretaria de Segurança Pública e da Polícia Militar do estado de Santa Catarina.

1.1 Sistema Brasileiro de Inteligência (SISBIN)

> *Profundo sentimento de servir à causa pública e jamais a si mesmo.* (Valores e Princípios da ABIN).

O Sistema Brasileiro de Inteligência foi instituído e a Agência Brasileira de Inteligência (ABIN) foi criada por intermédio da Lei n. 9883, de 07 de dezembro de 1999, por intermédio dos Artigos citados a seguir:

> Art. 1º - Fica instituído o Sistema Brasileiro de Inteligência, que integra as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional.
>
> 1º O Sistema Brasileiro de Inteligência tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ainda cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária.

> 2º Para os efeitos de aplicação desta Lei, entende-se como inteligência 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.
>
> 3º Entende-se como contrainteligência a atividade que objetiva neutralizar a inteligência adversa.
>
> Art. 2º - Os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República.
>
> 1º O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
>
> 2º - Mediante ajustes específicos e convênios, ouvido o competente órgão de controle externo da atividade de inteligência, as Unidades da Federação poderão compor o Sistema Brasileiro de Inteligência.
>
> Art. 3º - Fica criada a Agência Brasileira de Inteligência - ABIN, órgão de assessoramento direto ao Presidente da República, que, na posição de órgão central do Sistema Brasileiro de Inteligência, terá a seu cargo planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes superiormente traçadas nos termos desta Lei.

Dantas e Souza (2008, p.7) informam-nos que “é digna de nota a preocupação do legislador, não só em criar um **Órgão Central de Inteligência**, mas também de instituir **o sistema** respectivo”.

De acordo com Chiavenato (1983 apud RODRIGUES, 1999, p. 12),

> **Sistema** é um conjunto de elementos interdependentes e interagentes; um grupo de unidades combinados que formam um todo organizado e cujo resultado é maior do que o resultado que as unidades poderiam ter se funcionassem independentemente.

Jhoson (1968 apud RODRIGUES, 1999, p.13) afirma que “**Sistema** é considerado como um todo organizado ou complexo; um conjunto ou combinação de coisas ou partes, formando um todo complexo ou unitário”.

O Decreto n. 4376, de 13 de setembro de 2002, dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n. 9883, de 07 de dezembro de 1999.

Compõem o SISBIN os seguintes órgãos:

Quadro 2.1 - Sistema Brasileiro de Inteligência

MINISTÉRIO	**ÓRGÃO**
Gabinete de Segurança Institucional da Presidência da República	- Gabinete de Segurança Institucional da Presidência da República - Agência Brasileira de Inteligência –ABIN
Ministério da Justiça	- Secretaria Nacional de Segurança Pública (SENASP) - Diretoria de Inteligência Policial do Departamento de Polícia Federal (DPF) - Departamento de Polícia Rodoviária Federal - Departamento Penitenciário Nacional (DEPEN) - Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI)
Ministério da Defesa	- Subchefia de Inteligência Estratégica (SCIE) - Assessoria de Inteligência Organizacional (AIOP) - Estado-Maior da Armada (EMA) - Centro de Inteligência da Marinha (CIM) - Centro de Inteligência do Exército (CIE) - Centro de Inteligência da Aeronáutica (CIAER) - Centro Gestor e Operacional do Sistema de Proteção da Amazônia (CENSIPAM)
Ministério das Relações Exteriores	- Coordenação geral de Combate aos Ilícitos Transnacionais (COCIT) - Secretaria geral
Ministério da Fazenda	- Secretaria Executiva do Conselho de Controle de Atividades Financeiras (SE/COAF) - Secretaria da Receita Federal (RFB) - Banco Central do Brasil (BCB)

Ministério do Trabalho e Emprego	- Secretaria executiva
Ministério da Saúde	- Gabinete do Ministro - Agência Nacional de Vigilância Sanitária (ANVISA)
Ministério da Previdência Social	- Secretaria-executiva
Ministério da Ciência e Tecnologia	- Gabinete do ministro
Ministério da Integração Nacional	- Secretaria Nacional de Defesa Civil (SEDEC)
Controladoria-Geral da União	- Secretaria-executiva
Ministério do Meio-Ambiente	- Secretaria-executiva - IBAMA
Secretaria de Aviação Civil	- Secretaria-executiva - Empresa Brasileira de Infraestrutura Aeroportuária (INFRAERO)
Casa Civil	- Secretaria-executiva
Ministério da Agricultura Pecuária e Abastecimento	- Secretaria-executiva

Fonte: Elaboração do autor, 2013.

1.2 Qual a finalidade da ABIN e sua subordinação?

A missão da ABIN é a de assessorar o Presidente da República através da produção de conhecimentos estratégicos sobre oportunidades, ameaças e antagonismos, reais ou potenciais, de interesses da sociedade e do país. Com fulcro na Carta Magna da Nação, calcado nos princípios éticos e de garantia dos direitos individuais, compete à ABIN planejar, executar, coordenar, supervisionar e controlar as Atividades de Inteligência do país, obedecendo à Política Nacional de Inteligência e às diretrizes baixadas pelos escalões superiores.

Suas atividades visam à defesa do Estado Democrático de Direito, da sociedade, da eficácia do poder público e, por derradeiro, da soberania nacional. Todas as análises e informações formalizadas através de documentos de Inteligência são remetidas para o gabinete de Segurança Institucional da Presidência da República (GSI/PR), em razão da sua vinculação direta a este órgão. Ao Presidente da República cabe orientar o uso dos conhecimentos como subsídio à ação governamental.

1.3 Onde e como atua?

A ABIN acompanha as questões nacionais e internacionais, através de análises de conjunturas, visando identificar possíveis obstáculos à integração, aplicação e consecução de objetivos governamentais, à ordem constitucional e à segurança do país. Atuando de forma isenta, a ABIN possui um caráter diferenciado para refletir a inter-relação de variáveis nacionais e internacionais. Em linhas gerais, a Agência opera em duas vertentes, a da Inteligência e a da Contrainteligência, que buscam atender tantos às necessidades rotineiras do processo de decisão da Presidência da República, quanto às que se referem ao acompanhamento de fatos emergentes, previsíveis ou não, objetivando antecipar possíveis ameaças ao Estado Democrático de Direito e à sociedade, bem como as oportunidades.

Então, guarde bem: a ABIN desempenha suas funções exercendo os dois ramos da Atividade de Inteligência, sejam eles:

a) Inteligência, por meio da produção de conhecimentos sobre fatos e situações de imediata ou potencial influência no processo decisório e na ação governamental.

b) Contrainteligência, pela adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que obstaculizem ações de Inteligência executadas em benefício de interesses estrangeiros.

1.4 Como são exercidos o controle e a fiscalização da Atividade de Inteligência?

A ABIN é fiscalizada internamente pelo Poder Executivo e externamente pelo Legislativo. Este mecanismo de controle e fiscalização está previsto na Lei nº 9883/99, em que o Executivo sofre a ação de dois órgãos:

a. a Câmara de Relações Exteriores e Defesa Nacional, que supervisiona a execução da Política Nacional de Inteligência;

b. a Secretaria de Controle Interno da Presidência da República (CISET), que inspeciona a aplicação de verbas orçamentárias.

Já o controle externo é executado pelo Tribunal de Contas da União (TCU), no tocante à gestão dos recursos orçamentários, e pela Comissão Mista do Congresso Nacional, sobre os atos decorrentes da execução da Política Nacional de Inteligência.

Integram a Comissão as lideranças majoritárias e minoritárias do Congresso Nacional e os presidentes das Comissões de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal.

Seção 2
O Subsistema de Inteligência de Segurança Pública (SISP)

2.1 Criação do SISP

Branco (2011, p.18) nos diz que, por causa das peculiaridades da Segurança Pública, houve a necessidade de se criar um subsistema de Inteligência, dentro do SISBIN, que reunisse todos aqueles que têm a Segurança Pública como missão principal.

Assim é que, a 21 de dezembro de 2000, **o Decreto Presidencial nº 3695 criou o Subsistema de Inteligência de Segurança Pública (SISP).**

Seu primeiro artigo diz:

> **Art. 1º** Fica criado, no âmbito do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, o Subsistema de Inteligência de Segurança Pública, com a finalidade de coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo.

Aqui, percebe-se a intenção do legislador em manter o recém-criado SISP em perfeita consonância com o SISBIN e também a ênfase na geração de conhecimentos que pudessem subsidiar o processo decisório na esfera da Segurança Pública.

Vemos também a preocupação em criar um subsistema de amplitude nacional, efetivamente integrando todos os órgãos que, de uma maneira ou outra, lidam com o tema Segurança Pública.

Já o segundo artigo do referido decreto trata da composição do SISP, principalmente no seu primeiro e segundo parágrafos:

> **Art. 2º** Integram o Subsistema de Inteligência de Segurança Pública os Ministérios da Justiça, da Fazenda, da Defesa e da Integração Nacional e o Gabinete de Segurança Institucional da Presidência da República. § 1º O órgão central do Subsistema de Inteligência de Segurança Pública é a Secretaria Nacional de Segurança Pública do Ministério da Justiça.§ 2º Nos termos do § 2ºdo art. 2ºda Lei nº 9.883, de 1999, poderão integrar o Subsistema de Inteligência de Segurança Pública os órgãos de Inteligência de Segurança Pública dos Estados e do Distrito Federal (Decreto Presidencial n3695, art. 2).

Esse artigo estabelece, portanto, quem integra a Comunidade de Inteligência de Segurança Pública (CISP).

Agora, acompanhe o parágrafo seguinte desse artigo para verificar qual o objetivo da CISP:

> § **3º** Cabe aos integrantes do Subsistema, no âmbito de suas competências, identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e **produzir conhecimentos** e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza. (grifo nosso).

O Diário Oficial da União, em 14 de agosto de 2009, publicou a **Resolução nº 1 de 15 de julho de 2009 da SENASP**, que regulamentava o Subsistema de Inteligência de Segurança Publica (SISP).

Para que entendamos perfeitamente o espírito daqueles que elaboraram a regulamentação do SISP, e é bom que notemos que isso ocorreu nove anos depois da criação do SISP, vamos percorrer seus artigos e parágrafos, entremeando o texto da Resolução com comentários.

Vamos a alguns pontos dessa resolução. Um deles é o seu primeiro artigo, que trata da estrutura e do objetivo do SISP. Acompanhemos, então, esse artigo:

> **Art. 1º** O Subsistema de Inteligência de Segurança Pública SISP, que compõe o Sistema Brasileiro de Inteligência – SISBIN, constituído de rede própria e responsável pelo processo de coordenação e integração das atividades de inteligência de segurança pública no âmbito do território nacional, tem por objetivo fornecer subsídios informacionais aos respectivos governos para a tomada de decisões no campo da segurança pública, mediante a obtenção, análise e disseminação da informação útil, e salvaguarda da informação contra acessos não autorizados.

> **Importante:** A grande meta do SISP é, portanto, propiciar aos governantes condições para a tomada de decisões com base em informações trabalhadas de maneira profissional, na área da Segurança Pública.

Buscava-se, com isso, mudar uma dura realidade ainda presente nas decisões tomadas na área de Segurança Pública, que afetam, diretamente, a segurança percebida pelos cidadãos, qual seja, a de as decisões serem tomadas unicamente baseadas em experiências individuais, privilegiando-se, muitas vezes, aspectos de cunho político, sem contar com outras informações trabalhadas de maneira isenta e profissional.

Seguindo, analisemos o primeiro parágrafo do referido artigo:

> § 1º O SISP tem como fundamentos a preservação e a defesa da sociedade e do Estado, das instituições, a responsabilidade social e ambiental, a dignidade da pessoa humana, a promoção dos direitos e garantias individuais e do Estado de Democrático de Direito.

Nesse parágrafo, verifica-se a **preocupação com o Estado de direito**. Há no SISP a busca pelo resgate da Atividade de Inteligência; de um sistema e de instituições muito desgastadas pelo seu passado de repressão, falta de profissionalismo, despreocupação com os direitos dos cidadãos e arbitrariedades com a população.

Prosseguindo na legislação aqui analisada, temos o terceiro parágrafo que apresenta a composição do SISP.

> § 3o São elementos constituintes do SISP, originariamente:
>
> I – Conselho Especial do Subsistema de Inteligência de Segurança Publica;
>
> II – a Rede Nacional de Inteligência de Segurança Pública RENISP;
>
> III – a Rede de Integração Nacional de Informações de Segurança Pública, Justiça e Fiscalização – INFOSEG;
>
> IV – o Sistema Nacional de Identificação de Veículos em Movimento – SINIVEM;
>
> V – os Organismos de Inteligência de Segurança Pública e suas agências, o respectivo pessoal e estrutura material;
>
> VI – a Doutrina Nacional de Inteligência de Segurança Publica – DNISP; e
>
> VII – os sistemas de informações, os bancos de dados de propriedade e/ou cedidos à SENASP;
>
> VIII – Conselho Nacional de Chefes de Organismos de Inteligência de Segurança Publica – CNCOI.
>
> IX – as Agências de Inteligência – AI – a ele vinculadas, respectivo pessoal e material.

Foram mantidos, portanto, os mesmos membros do **Decreto nº 3.695, de 21 de dezembro de 2000.**

2.1.1 A RENISP

A RENISP, um dos itens que compõe o SISP, é a forma de comunicação segura de voz, dados, imagens e demais tipos de arquivo, utilizada pelos órgãos integrantes do SISP. Tem como objetivo proporcionar o intercâmbio de informações entre os órgãos do SISP, contribuindo para a integração desses órgãos e para o combate sistemático à criminalidade.

Entre os **principais objetivos da RENISP**, como recurso da Atividade de Inteligência de Segurança Pública e meio comum de conversação entre os componentes do SISP, podemos elencar os seguintes:

- coordenar e integrar as atividades de Inteligência de Segurança Pública em todo o país;
- suprir os governos federal e estaduais com informações que subsidiem a tomada de decisões no âmbito da Segurança Pública;
- auxiliar os integrantes do SISP a identificar, acompanhar e avaliar ameaças reais ou potenciais à Segurança Pública, bem como produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza.

Seguindo, verifiquemos, então, o que apresenta o artigo 2º da Resolução nº 1 de 15 de julho de 2009 da SENASP. Segue seu texto:

> Art. 2º Ficam reconhecidas as Agências de Inteligência (AI) existentes e a serem criadas na estrutura dos Organismos de Inteligência integrantes do SISP, conforme as diretrizes contidas nesta Resolução.

2.2 O que são as Agências de Inteligência (AI)?

São as estruturas de inteligência existentes nos diversos setores da Administração Pública, federal ou estadual, de qualquer porte, que integram o SISBIN (e também subsistemas, como o SISP) e que produzem Inteligência para um cliente específico e para o SISBIN.

O segundo parágrafo do último artigo aqui citado trata do controle das AI pela SENASP:

> § 2º As AI comporão a Rede Nacional de Inteligência de Segurança Pública – RENISP, sob a gestão, responsabilidade e **controle direto** (grifo nosso) da Coordenação-Geral de Inteligência da SENASP, para fins táticos, estratégicos e normatização.

O texto desse parágrafo é um tanto quanto ambicioso, pois sabemos que as estruturas de Inteligência são criadas para servir, em primeiro lugar, a seu cliente preferencial, que pode ser o Presidente da República; Ministros; Governadores; Secretários de Segurança; Comandantes das Forças Armadas; Comandantes das Polícias Militares; Chefes de Polícia Civil etc.

Sabemos também que em Inteligência não existe subordinação entre agências de diversos órgãos, mesmo que componham um mesmo sistema. O que deve existir é a **cooperação**. Essa é a palavra-chave na Inteligência. Nenhuma agência consegue obrigar outra congênere a compartilhar informações se a outra assim não quiser.

E acrescentamos mais! Além da cooperação, devem existir laços indeléveis de confiança dentro de um Sistema de Inteligência.

Uma AI que, por exemplo, não pratica regras básicas de contrainteligência, sendo alvo de vazamentos constantes que fragilizam sua imagem, certamente não será incluída na lista de difusão de uma outra AI.

> Lembre-se: não existe subordinação dentro de um sistema de inteligência! Haverá, sempre, um órgão coordenador e agências que vão alimentar o sistema na medida em que ele se mostre, cada vez mais, confiável e profissional.

No artigo quarto da Resolução em comento, está exposto o objetivo maior das AI, qual seja, o de estabelecer canais de ligação entre todos os que pertencem ao SISP, permitindo o fluxo contínuo e seguro de informações entre os integrantes do subsistema.

> Art. 4º As AI têm por objetivo viabilizar a interoperacionalidade entre a CGI/SENASP e todas as unidades que compõem a estrutura do SISP.

O quinto artigo dessa Resolução trata, de maneira bem detalhada, da finalidade das AI, ou seja, o que se espera delas no desenvolvimento das tarefas pertinentes à Atividade de inteligência de Segurança Pública:

> Art. 5º Constitui finalidade das AI desenvolver, de forma rápida, eficaz, eficiente e conjunta, a execução de serviços compreendidos na atividade de inteligência de segurança pública em âmbito de cada instituição, para atendimento das demandas emergentes e [...] do planejamento de ações que impliquem na realização de serviços de natureza correlata, além de prover informações, observado o princípio da oportunidade, dentre outros, com vistas a subsidiar a adoção de providências adequadas em cada esfera de atuação.

Em fevereiro de 2002, os trabalhos de elaboração da Doutrina Nacional de Inteligência de Segurança Pública (DNISP) foram dados como concluídos. Neste documento orientador para a denominada Atividade de Inteligência de Segurança Pública (AISP) estão contidos todos os preceitos doutrinários para a produção do conhecimento de Inteligência de Segurança Pública.

A DNISP, em sua página 11, define a AISP dessa maneira:

> 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.

A **Atividade de Inteligência de Segurança Pública** tem-se apresentado como instrumento de resposta e apoio ao combate à violência em geral e, principalmente, aos crimes de alta complexidade, procurando identificar, entender e revelar os aspectos ocultos da atuação criminosa, que seriam de difícil detecção pelos meios tradicionais de investigação policial. Serve, ainda, para assessorar as autoridades governamentais na elaboração de planos e políticas públicas de Segurança Pública.

Seção 3
A Diretoria de Informação e Inteligência (DINI)

Vamos conhecer agora, a título de exemplo, o sistema utilizado pela Secretaria de Estado da Segurança Pública e Defesa do Cidadão de Santa Catarina.

A SSP/SC embasa suas ações em três pilares:

1. **policiamento ostensivo**, exercido pela Polícia Militar de Santa Catarina (PMSC), que está presente nos 293 municípios do Estado;
2. **policiamento repressivo e processual**, através da polícia judiciária, que é a Polícia Civil; e
3. a **Atividade de Inteligência** com a DINI, na qual são de suma importância os trabalhos desenvolvidos através da produção do conhecimento para proporcionar segurança à sociedade.

A DINI é uma das Diretorias da Secretaria de Estado de Segurança Pública do estado de Santa Catarina.

Além disso, existe também o **Sistema de Inteligência da Polícia Militar (SIPOM)**, que você conhecerá na Seção 4.

> **Segurança** é um estado de proteção em que uma pessoa ou a sociedade sente-se protegida contra ameaças ou agressões aos seus bens, interesses, valores e à própria vida. Na preservação desses direitos humanos, a SSPDC/SC desenvolve um conjunto de ações preventivas e repressivas que objetivam preservar a ordem pública e a segurança do cidadão.

O aumento desordenado das cidades, o crescimento da população e o avanço tecnológico, aliados a outros fatores, têm contribuído para o aumento dos índices de violência e criminalidade, que se apresentam com formas cada vez mais elaboradas e complexas de ações, principalmente em razão das novas tecnologias e de sofisticados métodos de operação, dificultando sobremaneira o trabalho policial preventivo e/ou repressivo.

Desta forma, os órgãos de Segurança Pública tiveram que desenvolver formas de investigação que tornam mais eficiente o combate à criminalidade, que com o passar do tempo dá mostras de estar mais bem organizada.

A Diretoria de Informação e Inteligência (DINI) da Secretaria de Estado da Segurança Pública de Santa Catarina (DINI/SSP/SC) iniciou seus trabalhos no dia 03 de dezembro de 2002, criada por convênio firmado entre os Governos Estadual e Federal, através do Ministério da Justiça (MJ) e da Secretaria Nacional de Segurança Pública (SENASP). A celebração do convênio SENASP/MJ, n. 06/2002, publicado no Diário Oficial da União em 24 de julho de 2002, teve como um de seus objetivos a **Integração ao Subsistema de Inteligência de Segurança Pública**, com fundamentação legal na Lei nº 9883/99 e no Decreto nº 3695/00, em consecução ao Compromisso nº 04 do Plano Nacional de Segurança Pública, citado a seguir.

Compromisso nº 4 - Implementação do Subsistema de Inteligência de Segurança Pública

O Subsistema de Inteligência de Segurança Pública será parte de um sistema maior, uma vez que integrará, quando formalizado, o Sistema Brasileiro de Inteligência – SISBIN, sob coordenação da Agência Brasileira de Inteligência - ABIN. O Subsistema de Inteligência é integrado por órgãos das esferas federal, estadual e municipal, tendo por objetivo identificar ameaças à segurança pública, subsidiar, com oportunidade, os órgãos governamentais, com conhecimentos necessários à adoção de providências para a manutenção da segurança pública. A integração de esforços permitirá sistematizar um fluxo de informações, propiciando cenários para a atuação das instituições envolvidas, favorecendo, em nível nacional, as ações de prevenção e repressão.

Fonte: Ministério da Justiça, 2011. Disponível em: <www.mj.gov.br>. Acesso em: 04 out. 2013.

O Núcleo de Gerenciamento do Subsistema de Inteligência e Estatística de Segurança Pública, como inicialmente intitulada a DINI, foi pioneiro em sua criação, pois **integrava o trabalho dos Policiais Militares e Civis de Santa Catarina**.

Conforme publicado no Diário Oficial nº 17050, de 09 de dezembro de 2002, na Portaria n. 0885/GEARH/DIAF/SSP, de 03 de dezembro de 2002, o Secretário de Segurança Pública e Defesa do Cidadão da época, no uso de suas atribuições, resolveu designar, com fundamento no artigo 8º, parágrafo único, da Resolução nº 014/2002/CSSP, de 11 de julho de 2002, e no artigo 6º do Decreto n. 2002, de 29 de dezembro de 2001, Policiais Civis e Militares. Estava criado o Núcleo de Gerenciamento do Subsistema de Inteligência e Estatística de Segurança Pública, sob a coordenação de um Delegado de Polícia.

No ano seguinte, a Lei Complementar nº 243, de 30 de janeiro de 2003, assinada pelo Governador de Santa Catarina, na Seção III, artigo 44, inciso XXII, cita o Combate ao Narcotráfico e ao Crime Organizado e, no Anexo VI, denomina a Diretoria de Combate ao Crime Organizado. Sua estrutura conta com um Diretor de Combate ao Crime Organizado, um Gerente de Inteligência e um Gerente de Estatística.

O titular da Diretoria de Combate ao Crime Organizado daquele período foi um Delegado de Polícia, e o Gerente de Inteligência, um Oficial Superior da Polícia Militar, mostrando o entrosamento existente entre as duas Instituições Estaduais - Polícia Civil e Militar - responsáveis pela preservação da ordem pública no território catarinensNa data de 28 de fevereiro de 2005, foi aprovada a

Lei Complementar nº 284, da reforma institucional do Estado, em que a Diretoria passa a ser chamada Diretoria de Informação e Inteligência (DINI), mantendo a Gerência de Inteligência e de Estatística em sua composição. (SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA, 2011).

A DINI é o órgão central do Subsistema de Inteligência e tem a missão de difundir no âmbito da SSP/SC os conhecimentos produzidos, também o fazendo junto às instituições policiais - **Polícia Militar**, **Polícia Civil**, **Polícia Federal**, **Polícia Rodoviária Federal** -, sempre respeitando as limitações legais.

A DINI realiza atividades de coleta de informações, bem como de análise criminal, estatística, geoprocessamento e operações de inteligência e contrainteligência.

Vamos dar uma olhada na Constituição Federal e na Estadual, a fim de conhecermos a missão constitucional, bem como o correto posicionamento dos órgãos de Segurança Pública do país e dos Estados-membros dentro da Carta Magna.

Constituição da República Federativa do Brasil de 1988

CAPÍTULO III

DA SEGURANÇA PÚBLICA

Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:

I - polícia federal;

II - polícia rodoviária federal;

III - polícia ferroviária federal;

IV - polícias civis;

V - polícias militares e corpos de bombeiros militares.

§ 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se a:(Redação dada pela Emenda Constitucional nº 19, de 1998)

I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;

II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência;

III - exercer as funções de polícia marítima, aeroportuária e de fronteiras; (Redação dada pela Emenda Constitucional nº 19, de 1998)

IV - exercer, com exclusividade, as funções de polícia judiciária da União.

§ 2º A polícia rodoviária federal, órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se, na forma da lei, ao patrulhamento ostensivo das rodovias federais. (Redação dada pela Emenda Constitucional nº 19, de 1998)

§ 3º A polícia ferroviária federal, órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se, na forma da lei, ao patrulhamento ostensivo das ferrovias federais. (Redação dada pela Emenda Constitucional nº 19, de 1998)

§ 4º Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.

§ 5º Às polícias militares cabem a polícia ostensiva e a preservação da ordem pública; aos corpos de bombeiros militares, além das atribuições definidas em lei, incumbe a execução de atividades de defesa civil.

§ 6º As polícias militares e corpos de bombeiros militares, forças auxiliares e reserva do Exército, subordinam-se, juntamente com as polícias civis, aos Governadores dos Estados, do Distrito Federal e dos Territórios.

§ 7º A lei disciplinará a organização e o funcionamento dos órgãos responsáveis pela segurança pública, de maneira a garantir a eficiência de suas atividades.

§ 8º Os Municípios poderão constituir guardas municipais destinadas à proteção de seus bens, serviços e instalações, conforme dispuser a lei.

§ 9º A remuneração dos servidores policiais integrantes dos órgãos relacionados neste artigo será fixada na forma do § 4º do art. 39. (Incluído pela Emenda Constitucional nº 19, de 1998).

A DINI também está sempre em sintonia com as Agências de Inteligência (AI) que atuam no âmbito do Conselho de Segurança Pública do **Conselho de Desenvolvimento do Sul (CODESUL)**, do qual são Estados-membros Santa Catarina, Rio Grande do Sul, Paraná e Mato Grosso do Sul, tendo completa integração com a SENASP/MJ, através da Coordenação Geral do Subsistema de Inteligência de Segurança Pública, com sede em Brasília, DF. (SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA, 2011).

Quais as divisões da DINI?

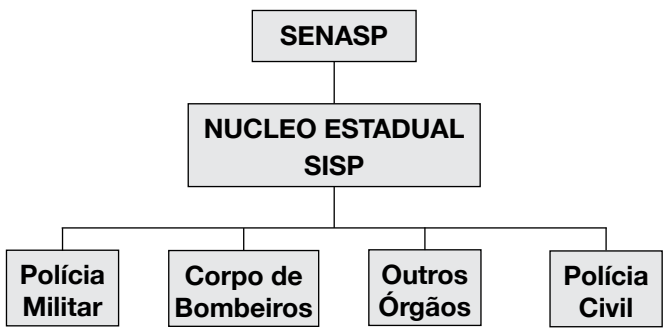
Desde 2002, a DINI atua na obtenção e análise de dados e informações e na produção e difusão de conhecimentos. Para isso, trabalha em parceria com instituições estaduais, nacionais e internacionais de Inteligência de Segurança Pública, realizando um intercâmbio de informações para o combate a atividades criminosas.

Outros objetivos do trabalho da DINI são: prevenir, detectar, obstruir e neutralizar ações que constituam ameaça à segurança da sociedade e do Estado. Seu corpo funcional congrega integrantes da Polícia Civil e da Polícia Militar do Estado, além de especialistas de outros órgãos públicos, divididos em cinco núcleos:

- Núcleo de Operações de Inteligência e de Contrainteligência (NOICI);
- Núcleo de Análise Criminal e Processamento da Informação (NAPI);
- Núcleo de Tecnologia da Informação (NUTI);
- Núcleo de Geoprocessamento e Estatística (NUGES);
- Núcleo de Repressão ao Crime Organizado (NURCOR).

Trouxemos à sua apreciação a maneira como a DINI, órgão central do Subsistema de Inteligência de Segurança Pública em Santa Catarina, está organizada. A mensagem que queremos deixar é que existe a necessidade primordial de que haja um órgão de Inteligência, em cada estado da Federação, que faça o papel que a DINI executa em Santa Catarina. A organização será a que melhor se apresentar, diante das necessidades e realidades de cada estado.

Figura 2.1 - Organograma do Núcleo Estadual de Inteligência de Segurança Pública (SISP)



Fonte: SENASP, 2010.

Seção 4
O Sistema de Inteligência da Polícia Militar (SIPOM)

Na seção 1, você ficou sabendo o que é um Sistema, e na seção anterior você conheceu os meandros da Diretoria de Informação e Inteligência (DINI) da Secretaria de Estado da Segurança Pública (SSP/SC). Agora, irá conhecer o Sistema de Inteligência da Polícia Militar (SIPOM).

Conforme Rodrigues (1999, p. 13), considerando o conceito de **Sistema** e fundamentado na **Doutrina Nacional de Inteligência de Segurança Pública (DNISP)**, pode-se conceituar o **Sistema de Inteligência da Polícia Militar (SIPOM)** como:

> O conjunto de órgãos de inteligência da Polícia Militar, estruturado hierárquica e harmonicamente com a organização funcional da Corporação, de modo a possibilitar a interação entre si de maneira eficiente e eficaz.

De acordo com Borges (1997 apud RODRIGUES, 1999, p.13), a missão do SIPOM é de assessoria do Comando Geral da Corporação e demais Comandos em todos os níveis, por intermédio da produção de conhecimento com relação aos índices de violência e criminalidade, bem como da operacionalidade da Polícia Ostensiva, a fim de subsidiar o planejamento estratégico e a tomada de decisões.

Dentro da Polícia Militar de Santa Catarina (PMSC) o Sistema de Inteligência da Polícia Militar (SIPOM) é formado por todas as Agências localizadas nos Batalhões Operacionais (Batalhão de Polícia Militar - BPM), suas Companhias Destacadas (Companhia de Polícia Militar - CPM), e em alguns Pelotões (Pel PM) sediados em cidades de médio porte. O Sistema é coordenado pela Agência Central de Inteligência (ACI), parte integrante do Estado-Maior Geral da Corporação (EMG), localizada no Quartel do Comando Geral (QCG), na cidade de Florianópolis, Santa Catarina, a quem compete o contato com os demais Órgãos e Sistemas de Inteligência existentes no Brasil.

A Atividade de Inteligência de Segurança Pública (AISP) prevista na DNISP constitui um mecanismo institucional de assessoria complementar, e atinge, por conseguinte, homens ou grupos, colocando-se à disposição dos sucessivos governantes, no sentido de auxiliá-los no planejamento, execução e acompanhamento de suas políticas públicas em favor da preservação da ordem pública e da defesa do Estado e da sociedade.

O Sistema de Inteligência de Segurança Pública da Polícia Militar de Santa Catarina (SIPOM) foi instituído através da **Portaria n. 156, de 18 de abril de 2001**, conforme prevê o seu artigo 1º: "Fica instituído o Sistema de Inteligência de Segurança Pública da PMSC - SIPOM, com a finalidade de integrar e otimizar as atividades de Inteligência de Segurança Pública no âmbito da Corporação".

4.1 As Agências de Inteligência

A Estrutura Organizacional da Agência Central de Inteligência (ACI) foi assim idealizada em seu nascedouro e está aqui apresentada como um exemplo para que agências que ainda estejam se estruturando possam avaliá-la.

- Chefia;
- Adjunto;
- Subseção Administrativa;
- Subseção de Inteligência;
- Subseção de Contrainteligência;
- Subseção de Operações.

Figura 2.2 - Organograma de Atividade de Inteligência

Secretaria ◄► Contrainteligência ◄► Setor Especial.
Fonte: ACI/PMSC, 2005.

4.2 Funções das Subseções

4.2.1 Subseção Administrativa

- Receber, protocolar e distribuir as **correspondências sigilosas** do Comando Geral.
- Expedir todas as correspondências da Agência.
- Controlar os meios de transportes da Agência.
- Controlar os documentos sigilosos expedidos pela Agência; Manter em dia o arquivo geral, ativo e inativo.
- Elaborar as correspondências ostensivas ordinárias da Agência; Organizar e manter as escalas de serviço.

4.2.2 Subseção de Inteligência

- Análise do crime organizado: Analisar o crime organizado, o sistema penitenciário e carcerário, organizações criminosas, o narcotráfico, o contrabando, armas, a lavagem de dinheiro, sequestros.
- Análise psicossocial: Acompanhamento dos fatos relativos à dinâmica social que possam afetar, de alguma maneira, a segurança pública.
- Análise de crimes contra pessoa: Analisar os crimes contra a pessoa, família, costumes, sentimento religioso, crianças e adolescentes, abandono de incapazes, corrupção e exploração de menores, grupos de extermínio, incolumidade pública, fé pública e administração pública.
- Análise de crimes contra patrimônio: Analisar os furtos, roubos, as depredações contra o meio ambiente, o patrimônio cultural, a organização do trabalho, calamidades, acidentes, catástrofes e sabotagens.

4.2.3 Subseção de Contrainteligência

- Setor de Controle do SIPOM: Trabalhar com pessoal, placas especiais para veículos descaracterizados, seleção/credenciamento, descaracterização de viaturas.
- Setor Especial: Atuar com o Poder Judiciário e auxiliares da Justiça, Ministério Público, Polícia Civil, Polícia Federal e Polícia Rodoviária Federal, empresas de vigilância, propaganda adversa e ameaças à Instituição.
- Segurança Orgânica: Manter a segurança do pessoal, da documentação e do material, da informática e das comunicações da Agência.

4.2.4 Subseção de Operações

- Planejar e executar as ações de busca de dados, atendendo às necessidades da chefia e das Subseções da Agência Central de Inteligência (ACI).
- Manter uma escala de serviço, ficando em condições de operar em situações de emergências.

Caminhar pelos corredores e pátios de um Batalhão de Polícia Militar (BPM) não significa encontrar somente policiais militares fardados em serviço administrativo ou operacional.

A Instituição também possui policiais militares que atuam em trajes civis, penetrando nos lugares onde existe maior probabilidade de ocorrência de crimes. A equipe recebe a denominação de P-2 no jargão Policial Militar.

O sucesso das atividades operacionais de um Batalhão de Polícia Militar normalmente é antecedido pelas ações discretas destes agentes. Este tipo de serviço criado pela Polícia Militar tem por objetivo antecipar-se ao fato, efetuando o levantamento dos locais onde existam problemas, a fim de descobrir se há pessoas planejando praticar algum delito tipificado na legislação penal vigente.

Os elementos de operações também podem atuar na condição de assuntos internos, ou seja, investigando a atuação dos próprios policiais militares. A designação de P-2 é utilizada por todas as Polícias Militares das Unidades Federativas, a exemplo da denominação empregada pelas Forças Armadas do Brasil (S2).

As forças policiais não podem ficar atreladas somente à prevenção executada pelo **Policiamento Ostensivo**, sendo necessário que a Atividade de Inteligência também seja forte.

Os policiais militares atuam nas operações conforme a necessidade, algumas vezes sozinhos e em outras acompanhados, mas sempre recebem a cobertura de outros companheiros de atividade. Os veículos que utilizam também são descaracterizados, ou seja, sem a pintura padrão da Polícia Militar, misturando-se com os veículos de propriedade particular para não despertar a atenção das pessoas. Além de motorizados, os elementos de operações podem utilizar outros meios de transporte ou mesmo atuar a pé.

Todo policial militar que atua em Operações deve ter cautela suficiente para que os seus colegas do Policiamento Ostensivo não o confundam com marginais, podendo prendê-lo ou até alvejá-lo num eventual confronto armado. A seleção e o recrutamento inicial para atuar na atividade operacional normalmente recaem sobre policiais militares que possuem maior experiência profissional e mais tempo de serviço.

Para firmar conceitos, leia a definição de Policiamento Ostensivo (SANTIAGO, 1993) e de Policiamento Velado (PMMG, 1990):

Policiamento Ostensivo:

> São ações de fiscalização de Polícia, no que diz respeito à Ordem Pública, em cujo emprego o homem ou a organização de Polícia Militar que estiver sendo empregada num determinado espaço geográfico, sejam identificados de pronto, quer pela farda, quer pelo equipamento e principalmente viatura. (SANTIAGO, 1993, p. 68).

Policiamento Velado:

É o tipo de policiamento voltado para a busca de informações operacionais, cujo objetivo é localizar e avaliar eventuais focos de risco a que estão sujeitas as comunidades, possibilitando o emprego racional do policiamento ostensivo (fardado). Constitui uma atividade de preservação da ordem pública, em apoio ao Policiamento Ostensivo, utilizando Policiais Militares em trajes civis (à paisana), e que possui características, variáveis e princípios próprios.

Sendo empregada de maneira conveniente, de acordo com as Diretrizes do Comando Geral da Corporação, a técnica produzirá os resultados que dela se espera e não se transformará em motivo de desvio da Polícia Militar de sua destinação constitucional. Este tipo de serviço não deve ser confundido com a Atividade de Inteligência e Contrainteligência. (Polícia Militar de Minas Gerais (PMMG) - Cartilha de Policiamento Velado – 1990).

Recomendação de segurança: Os agentes responsáveis pela custódia de documentos, conhecimentos, materiais, áreas, comunicações, operações e sistemas de informação de natureza sigilosa estão sujeitos às regras referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico.

Este capítulo demonstrou como a atividade de Inteligência está estruturada em nosso país e como atua para exercer sua grande finalidade: assessorar os processos decisórios. Ficou claro que os integrantes dos diversos sistemas, seja no âmbito federal, ou estadual, precisam estabelecer laços de confiança para que o conhecimento flua e esteja acessível a todos de um mesmo sistema, ou mesmo fora dele.

O que de mais importante fica é a mensagem de que, sem o concurso da atividade de Inteligência, gestores de qualquer escalão terão muita dificuldade para tomar as decisões que afetam o cotidiano das pessoas.

Capítulo 3

Documentos e legislação de Inteligência

Habilidades

Capacitar o aluno com saberes adequados ao domínio de técnicas de levantamento de informações, análise e proteção de dados, a fim de analisar e operar dados para realizar a gestão da informação atuando sobre os problemas relacionados à segurança e a questões correlatas, evitando a exposição desnecessária de indivíduos e dos assuntos de interesse da sociedade.

Seções de estudo

Seção 1: A proteção de assuntos sigilosos

Seção 2: Documentos de Inteligência, estrutura e sigilo

Seção 1
A proteção de assuntos sigilosos

Trabalhar na produção do conhecimento na Atividade de Inteligência de Segurança Pública (AISP) requer, por parte dos profissionais envolvidos, discrição fundamentada na ética profissional. Devemos buscar constantemente o aperfeiçoamento dentro de parâmetros éticos da Atividade de Inteligência, fundamentalmente porque o seu trabalho baseia-se no raciocínio e no argumento, portanto, na lógica dedicada à procura do conhecimento, e não apenas de uma opinião sem fundamento.

O analista ético não se desvia do seu compromisso com a verdade. Quem atua nesta área deve comprometer-se com os valores éticos e morais, dentro e fora da sua instituição.

Nesta seção, vamos estudar em detalhes a legislação de salvaguarda dos assuntos sigilosos.

> *Na paz, preparar-se para a guerra; na guerra, preparar-se para a paz. A arte da guerra é de importância vital para o Estado. É uma questão de vida ou morte, um caminho tanto para a segurança como a ruína. Assim, em nenhuma circunstância deve ser descuidada. (Sun Tzu)*

Para Dantas (2008, p.2), "o **sigilo** é uma das características comuns da Inteligência, bem como vários outros comportamentos típicos da cultura operacional da chamada **Atividade de Inteligência Humana"**.

1.1 Assuntos sigilosos

Consideremos, inicialmente, assuntos sigilosos aqueles que, por sua natureza, devam ser de conhecimento restrito e, por isso, merecem medidas de proteção para sua custódia e divulgação. Os assuntos sigilosos, no caso da ocorrência de um vazamento (acesso por pessoas não autorizadas), produzem risco à segurança da sociedade e do Estado, bem como podem afetar a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

Já um documento sigiloso é qualquer material redigido, impresso, gravado, desenhado, manuscrito ou fotografado e suas respectivas reproduções, que receba uma classificação sigilosa, de acordo com o previsto na legislação que a define, a ser apresentada a seguir.

A legislação que trata da proteção aos assuntos e documentos de natureza sigilosa, sejam de origem pública ou privada, é bastante completa, mas, infelizmente, de pouco conhecimento e aplicação.

Vamos conhecê-la?

Devemos começar pela Carta Magna de nosso país, a Constituição de 1988, que, em seu Artigo 5º, preocupa-se em proteger tudo que é relativo à **pessoa, ao cidadão e que, em consequência, para ele, trata-se de assuntos atinentes à sua privacidade:**

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

A Constituição, ainda no Artigo 5º, continua tratando da privacidade do cidadão fazendo menção à proteção de tudo que está contido no domicílio dos brasileiros:

> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo no caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.

E por fim, ainda no mesmo Artigo, a Constituição trata sobre os meios pelos quais o cidadão se comunica e sobre aquilo que ele veicula:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Já o Código Penal Brasileiro (CPB) trata dos crimes contra a inviolabilidade dos segredos, em seu Artigo 153:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
>
> § 1º-A - Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. (Incluído pela Lei 9.983/2000).

Prossegue este Diploma Legal, referindo-se, em seu Artigo 154, ao crime de revelação de segredos:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa.

Já no seu Artigo 297, o CPB protege a integridade de qualquer documento público, aí incluídos os conhecimentos de Inteligência:

> Art. 297 - Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:
>
> Pena - reclusão, de dois a seis anos, e multa.

E em seu Artigo 305, fala da tentativa de eliminação não autorizada de documentos públicos, aí também incluídos os documentos de Inteligência:

> Art. 305 - Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor.

Na seção que trata dos crimes praticados por funcionários públicos contra a administração em geral, o CPB foi modificado pela Lei nº 9.983, de 2000, sofrendo a inclusão dos Artigos 313-A e 313-B, que tratam da Segurança da Informação:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

E quando o CPB trata da violação do sigilo funcional, em seu Artigo 325, preconiza:

> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação.

Já a Lei 8.027, de 12 de abril de 1990, trata das normas de conduta dos servidores públicos civis da União, das autarquias e das fundações públicas, em seu Art 5º, inciso V:

> Art. 5º São faltas administrativas, puníveis com a pena de demissão, a bem do serviço público:
>
> V - revelação de segredo de que teve conhecimento em função do cargo ou emprego.

Nesse mesmo sentido, a Lei nº 8.112, de 11 de dezembro de 1990, dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais, em seu Artigo 116, inciso VIII:

> Art. 116
>
> São deveres do servidor:
>
> VIII - guardar sigilo sobre assunto da repartição

Esta mesma Lei, em seu Artigo 132, fala, sobre os casos de demissão do servidor:

> Art. 132 A demissão será aplicada nos seguintes casos:
>
> IX - revelação de segredo do qual se apropriou em razão do cargo.

Neste ponto, é necessário fazer uma observação importante. O Decreto nº 4.553 de 27 Dez 2002, que dispunha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, não está mais em vigor.

Foi revogado pelo Decreto 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento, assuntos tratados na nova **Lei de Acesso à Informação, a Lei 12.527, de 18 de novembro de 2.011.**

O Decreto 4.553 tratava o assunto da proteção dos assuntos sigilosos com muita profundidade, chegando ao detalhamento de medidas a serem aplicadas no cotidiano das organizações, coisa que a Lei de Acesso à Informação não o faz, pois que, pelo seu próprio nome, preocupou-se muito mais em propiciar ao cidadão o acesso à informação do que cerceá-la ou protegê-la. E, por isso, a cultura de proteção, que já não era exercida com muita atenção em todas as esferas da administração pública, tende a deteriorar-se cada vez mais.

Comentemos algumas prescrições da Lei 12.527, de 18 de novembro de 2.011, a Lei de Acesso à Informação, no pouco que trata da proteção dos assuntos sigilosos.

Em seu Artigo 4º, prescreve:

> Art. 4o Para os efeitos desta Lei, considera-se:
>
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Trata-se de um novo conceito, pois agrega um **tempo** obrigatório de restrição para toda informação que, porventura, receba alguma classificação sigilosa.

Prossegue dizendo, em seu Artigo 6º:

> Art. 6o Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
>
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Continua a Lei 12.527, no Artigo 23, que trata da classificação da informação quanto ao "grau" e "prazos de sigilo":

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
>
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

Então, pela nova Lei, somente os assuntos acima poderão receber algum grau de classificação sigilosa. E já dentro daquela alteração mencionada, sobre o tempo obrigatório em que uma informação poderá ficar classificada, a Lei prevê, em seu Artigo 24:

> Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ***ultrassecreta, secreta ou reservada***.
>
> § 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no **caput**, vigoram a partir da data de sua produção e são os seguintes:
>
> I - ultrassecreta: 25 (vinte e cinco) anos;
>
> II - secreta: 15 (quinze) anos; e
>
> III - reservada: 5 (cinco) anos.

Percebe-se, então, que a classificação sigilosa "confidencial", que era a mais utilizada nas Agências de Inteligência, não existe mais.

E quem pode, agora, classificar um documento com algum grau de sigilo? Vejamos o que diz a Lei:

> Art. 27. A classificação do sigilo de informações no âmbito da administração pública federal é de competência:
>
> I - no grau de ultrassecreto, das seguintes autoridades:
>
> a) Presidente da República;
>
> b) Vice-Presidente da República;
>
> c) Ministros de Estado e autoridades com as mesmas prerrogativas;
>
> d) Comandantes da Marinha, do Exército e da Aeronáutica; e
>
> e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
>
> II - no grau de secreto, das autoridades referidas no inciso I, dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista; e
>
> III - no grau de reservado, das autoridades referidas nos incisos I e II e das que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade, observado o disposto nesta Lei.

O que percebemos? Em uma Agência de Inteligência, não há mais como o analista, aquele que produz o documento, protegê-lo com uma classificação sigilosa, pois a Lei não lhe permite. Os órgãos de âmbito federal, pertencentes ou não ao SISBIN, deverão discutir como proceder para adaptarem-se à nova Lei, pois nem sempre os cargos de mais alto nível nas Superintendências Regionais são preenchidos pelo nível DAS 101.5.

E nos estados da federação, cada estado deve, à luz da **Lei 12.527, de 18 de novembro de 2011**, baixar seus decretos reguladores que adaptem as novas restrições da Lei às suas realidades, sem contrariar o que está previsto na Lei.

Sugerimos a consulta à nova Lei de Acesso à Informação na internet.

Para regulamentar a nova Lei, foi publicado o **Decreto 7.724, de 16 de maio de 2012**. Este decreto regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei no 12.527, de 18 de novembro de 2011.

Também sugerimos a leitura desse diploma legal na internet.

Para regulamentar procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispor sobre o Núcleo de Segurança e Credenciamento, foi promulgado o Decreto 7.845, de 14 de novembro de 2012, que define alguns termos de largo emprego na proteção de assuntos sigilosos, a saber:

- credencial de segurança - certificado que autoriza pessoa para o tratamento de informação classificada;
- credenciamento de segurança - processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada;
- gestor de segurança e credenciamento - responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle;
- Núcleo de Segurança e Credenciamento - órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, nos termos do art. 37 da Lei nº 12.527, de 2011;

- órgão de registro nível 1 - ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;
- órgão de registro nível 2 - órgão ou entidade pública vinculada a órgão de registro nível 1 e por este habilitado;
- tratamento da informação classificada - conjunto de ações referentes à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, ao transporte,à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada em qualquer grau de sigilo.

Credenciamento de segurança

Anteriormente à Lei nº 12.527, de 2011, a credencial de segurança para que o servidor pudesse tratar uma informação classificada era dada no seu próprio órgão. Agora, o procedimento mudou e é regulado pelo **Decreto 7.845 de 14 de novembro de 2012**.

Sugerimos, também, que você consulte este Decreto na internet..

Além da legislação vigente, cada órgão ou instituição operadora das Atividades de Inteligência deve, além de treinar o seu pessoal, possuir normas internas que detalhem o assunto.

Medidas especiais de segurança deverão ser observadas para a produção, o manuseio, a consulta, a transmissão, a manutenção e a guarda de dados ou informações sigilosas (Artigo 3º, *caput*). A autoridade responsável pelo tratamento de dados ou informações sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento (Artigo 3º, parágrafo único)

Seção 2
Documentos de Inteligência, estrutura e sigilo

> *(...) No ato comunicativo, há sempre um emissor ou remetente que envia a mensagem a um receptor ou destinatário.*
> (Samira Yousseff Campedelli et al*).*

Em todo **Sistema de Inteligência** circulam os documentos específicos da área, cujo emprego e competência de produção variam de acordo com os níveis das Agências Integradas, com as necessidades dos usuários e os objetivos do órgão.

O objetivo dos documentos de Inteligência é proporcionar um adequado fluxo de conhecimento entre as **Agências de Inteligência** que **integram** o **Sistema**, e atender às particularidades do exercício da Atividade de Inteligência. Por sua natureza sigilosa e pelas características próprias de como são produzidos, esses documentos não devem:

- ser utilizados como documentos integrantes de processos, inquéritos, sindicâncias, comunicações internas, ofícios, memorandos, dentre outras quaisquer ações estranhas à Atividade de Inteligência;
- possibilitar quaisquer atividades, mesmo regulamentares, que coloquem em risco o seu sigilo e a proteção de fonte;
- ser utilizados com finalidade disciplinar, administrativa ou de qualquer natureza diversa da Atividade de Inteligência.

2.1 Tipos de documentos de Inteligência

Nosso interesse está diretamente ligado aos documentos de Inteligência que circulam no Subsistema de Inteligência de Segurança Pública (SISP), preconizados na Doutrina Nacional de Inteligência de Segurança Pública (DNISP). Sabe-se que muitos sistemas de Inteligência de organismos policiais, em alguns estados brasileiros, ainda não estão atualizados, e que ainda utilizam documentos com características diversas do que vai ser aqui apresentado.

Existem vários documentos de Inteligência, sendo mais utilizados os seguintes: Informe, Informação, Apreciação, Estimativa, Pedido de Busca e Ordem de Busca. Os quatro primeiros são denominados de ˝Conhecimentos de Inteligência.˝

Em sua página 27, a DNISP define Documento de Inteligência como:

> (...) 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. (grifo nosso)

Os documentos chamados pela DNISP de “externos” são aqueles difundidos entre as Agências de Inteligência. São eles:

- Relatório de Inteligência (RELINT)
- Pedido de Busca (PB)
- Mensagem (Msg)
- Sumário

Nesta leitura, dos documentos citados pela DNISP só trataremos do RELINT e do PB, uma vez que a mensagem e o sumário servem apenas para tramitar, entre as AIs, os assuntos de rotina que sejam de interesse mútuo das agências, e não transmitem nem solicitam Conhecimentos de Inteligência. Comentaremos, também, sobre outro documento muito utilizado na Atividade de Inteligência e não tratado na DNISP, que se chama Ordem de Busca.

2.1.1 Relatório de Inteligência (RELINT)

Trata-se de um documento padronizado por meio do qual o analista transmite Conhecimentos de Inteligência para o usuário ou para outras AI pertencentes ou não ao SISP. Tal documento foi idealizado dentro Sistema Brasileiro de Inteligência (SISBIN) pela ABIN.

Em sua formalização, foi abolida a designação explícita do nome do Conhecimento de Inteligência (Informe, Informação, Apreciação ou Estimativa), que era colocada no cabeçalho dos documentos e que indicava claramente ao usuário o tipo de conhecimento que possuía em mãos. Extinguiu, também, o código alfanumérico identificador da avaliação da fonte e do conteúdo que acompanhava o Conhecimento do tipo “Informe”. Veremos isso mais adiante.

Com isso, o entendimento do conteúdo de qualquer tipo de Conhecimento de Inteligência, veiculado pelo RELINT, ficou restrito a quem sabe identificar os tempos verbais que apontam o estado da mente do analista ao produzir seu documento – opinião e certeza – e, principalmente, sabe interpretá-los.

Da mesma maneira, ficou a cargo do usuário perceber que determinados tipos de RELINT possuem conclusão, e outros não (como conhecimentos do tipo Informação, Apreciação e Estimativa). A existência da conclusão é uma nova pista para detectar o tipo de conhecimento presente num documento de Inteligência.

Se considerarmos que nem todos os usuários da ISP são pessoas que possuem formação na área de Inteligência, entenderemos que elas certamente sentirão dificuldade em entender o tipo de documento que recebem e a posição (estado de sua mente) do analista ao produzi-lo.

Pela falta de clareza desse tipo de documento, alguns órgãos integrantes do SISBIN não o adotaram, continuando a veicular os Conhecimentos de Inteligência por meio de documentos com seu próprio nome (Informe, Informação, Apreciação e Estimativa) no cabeçalho do documento.

Essa dificuldade no uso do documento RELINT deve ser considerada na sua difusão ao usuário, ou mesmo para outros interessados, dentro ou fora do SISP, cabendo ao analista tomar cuidados especiais para que sua redação seja a mais clara possível.

Os Sistemas de Inteligência que continuam a mencionar, em seus Conhecimentos do tipo Informe, o código alfanumérico de avaliação do conteúdo e da fonte dos dados usam tabelas, por meio dos quais o analista guia-se durante a aplicação da Metodologia da Produção do Conhecimento. Falaremos nestas tabelas mais à frente.

Estrutura do RELINT

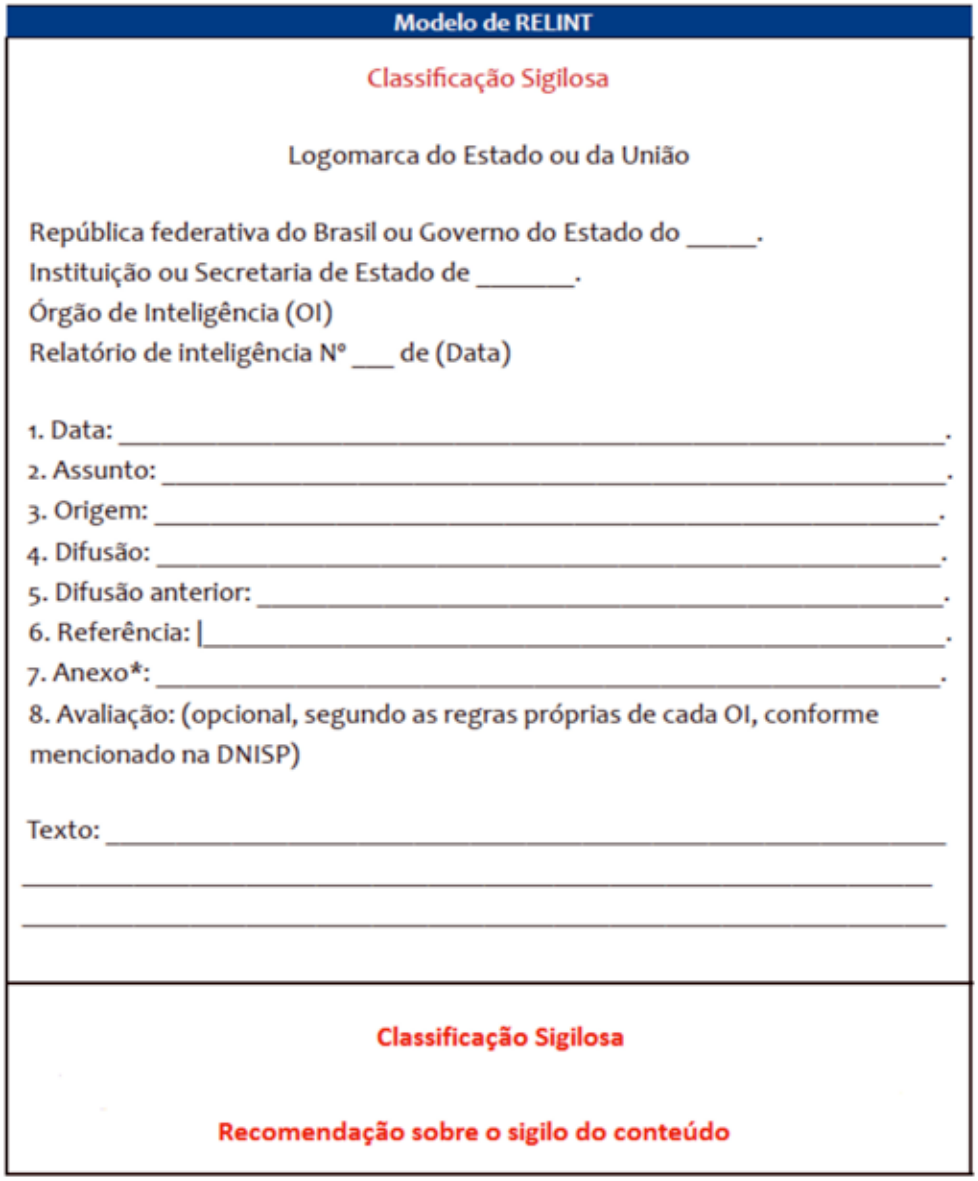
A padronização dos documentos de ISP é muito necessária para se obter unidade de entendimento e uniformidade de procedimentos entre os órgãos que integram o SISP. Por isso, os documentos contêm um conjunto mínimo de itens sobre a sua classificação, seu conteúdo, seu destinatário e, assim, obrigatoriamente conterão:

- **Classificação sigilosa –** a marcação do grau de sigilo deverá ser feita em todas as páginas do documento, em posição centralizada, em negrito, na primeira linha do cabeçalho e do rodapé, emoldurado por um retângulo, com um espaço entre as letras e na cor vermelha. Para que seja atribuído o grau de sigilo, deve-se seguir o que prescreve a **Lei nº 12.527, de 18 de novembro de 2011.**
- **Logomarca do Estado Federado ou da União** (conforme o caso) – deverá ser impressa na primeira página do documento, em posição centralizada, imediatamente abaixo da margem superior e nas cores originais ou em preto e branco.
- **Designação da AI** produtora e sua subordinação.
- **Designação do tipo do documento –** é composta pela especificação do tipo (RELINT) e do número do documento, pelo indicativo da AI que o produziu, e a data de sua elaboração.

- **Numeração sequencial** – por ano.
- **Cabeçalho** contendo:
  - » **Data** – a da **remessa do documento** (pode ser diferente da data da elaboração do documento). É escrita com dois algarismos para o dia, as três primeiras letras do mês (a primeira em caixa alta) e o ano com quatro algarismos. Ex: 15 Set 2012.
  - » **Assunto –** consiste em uma expressão que **sintetize** o conteúdo do texto, respondendo, pelo menos, às perguntas: O quê? Quando? Onde?
    Ex: Furto de veículos em Arapiraca/AL no primeiro semestre de 2001.
- **Origem –** unidade responsável pela sua produção.
  Ex: AI/14ºBPM
- **Difusão –** deverão ser indicados todos os destinatários do RELINT (cargo da autoridade ou AI).
- **Difusão anterior –** deverão ser relacionados os órgão(s) e autoridade(s) que já tenham tido conhecimento do conteúdo do texto do RELINT pelo fato de ele ter sido difundido anteriormente pela AI que o produziu, ou por qualquer outro órgão.
- **Referência –** deverão ser listados os documentos ou eventos que, de algum modo, relacionem-se com o assunto-objeto do RELINT. É obrigatório que eles já sejam conhecidos tanto pelo remetente como pelo destinatário do documento. Ex: PB nº 045/2006/14ºBPM, de 25 Set 2006.
- **Anexo –** quando for o caso, o RELINT poderá conter anexos, isto é, documentos ou objetos que o acompanharão a fim de oferecer compreensão mais ampla de algum ponto do texto. Exemplos:
  - » Anexo “A” – fotografia de Samir Asmed.
  - » Anexo “B” - Filmagem feita na “boca de fumo” de Samir Asmed.
- **Avaliação** – neste item, segundo regras próprias de cada Sistema de Inteligência, o RELINT poderá conter avaliação sobre o documento de acordo com as tabelas de julgamento de fonte e conteúdo. (somente no caso de um Conhecimento de Inteligência do tipo “Informe”).

- **Expressão - “Continuação do...”** – a partir da segunda página, a expressão deverá ser colocada no cabeçalho, abaixo da classificação sigilosa, se houver, seguida dos indicativos e separada do texto por uma linha. Exemplo: Continuação do Relatório de Inteligência nº 0112/DEIC/SSPRJ de 03 Jun. 2009.
- **Texto** - deve seguir o preconizado pela metodologia da Produção do Conhecimento em relação aos itens abaixo:
  - » ser simples e conciso, mas sem deixar hiatos que possam comprometer o entendimento;
  - » usar a norma culta de linguagem;
  - » usar frases e parágrafos curtos para melhor clareza e entendimento;
  - » usar vocábulos que não deixem dúvidas;
  - » expor os argumentos em sequência lógica;
  - » se usar termos técnicos de qualquer ordem, estes deverão ter seu significado esclarecido;
  - » na primeira vez que utilizar abreviaturas, ou siglas, deve ser expresso, por extenso, seu significado e a sigla/abreviatura vindos entre parênteses.
- **Numeração das folhas –** cada página deverá ser marcada com seu número sequencial seguido do total de páginas do documento e separados por barra. Exemplo: 1/3, 2/3, etc.
- **Autenticação –** marca própria da AI que confere autenticidade ao documento. Normalmente, trata-se de um carimbo, ou marca d’água com o símbolo da AI, colocado em um dos cantos das páginas (normalmente no inferior direito), onde será aposta a rubrica do chefe da AI. Atualmente, com a difusão feita de forma eletrônica, a autenticação será feita por medidas especiais de criptografia que garantam ao destinatário a autenticidade do documento.
- **Recomendação legal sobre quebra de sigilo** – deve ser inserida em quadro próprio dentro do rodapé (na segunda linha, após o grau de sigilo), na cor vermelha, alguma expressão que lembre a quem manipule o documento de suas responsabilidades no tocante ao sigilo do conteúdo.

Figura 3.1 – Modelo de RELINT



Modelo de RELINT

Classificação Sigilosa

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. Avaliação: (opcional, segundo as regras próprias de cada OI, conforme mencionado na DNISP)

Texto: _____
_____
_____

Classificação Sigilosa

Recomendação sobre o sigilo do conteúdo

Fonte: Elaboração dos autores, 2013.

2.1.2 O Pedido de Busca (PB)

Segundo a DNISP, é o documento externo, padronizado, utilizado para solicitação de dados e/ou Conhecimentos entre AI, dentro ou fora do sistema de ISP.

Cabe aqui um comentário. Apesar de esse documento ser o mais tradicional dentro da Inteligência brasileira, esse nome não é o mais apropriado para o que, normalmente, pretende-se solicitar por meio dele.

Sabemos que a busca implica a utilização do Elemento de Operações (ELO) de uma AI para obter um dado negado. Portanto, ao enviarmos um PB a uma AI, significaria dizer que nossa AI estaria pedindo que a outra usasse seu ELO para obter o dado solicitado.

É fato, entretanto, que os usos e costumes de todos que compõem a Inteligência brasileira acabam por absorver esse termo e entender que esse não é o objeto do PB.

Antes de elaborar um PB, deve-se ter o cuidado de definir o que pedir e avaliar, cuidadosamente, a quem pedir, ou seja, só se deve encaminhar um PB a quem tem reais possibilidades de atendê-lo.

Os PB são respondidos por meio de Conhecimentos de Inteligência, normalmente um Informe ou Informação.

Estrutura do PB

São os mesmos do RELINT, acrescentando-se o seguinte no seu texto:

I. Elementos disponíveis – nesse item, a fim de orientar o parceiro, deve ser relacionado tudo o que se sabe sobre o assunto que está sendo estudado, visando a orientar a execução dos procedimentos do órgão de Inteligência que vai receber o PB. Seus subitens deverão ser identificados por letras minúsculas seguidas de ponto (a., b., c., n.).

II. Necessidades – nesse item devem ser elencados, separados entre si por espaços iguais, e identificados por algarismos arábicos em ordem crescente e seguidos de ponto, os seguintes subitens:

1. necessidades de conhecimentos a serem atendidas (o que se quer saber);
2. outros conhecimentos julgados úteis, os quais propiciarão ao órgão de Inteligência destinatário do PB enviar conhecimentos não solicitados, mas que, a seu critério e inferidos do item Elementos disponíveis, são considerados potencialmente úteis; e
3. prazo para o recebimento das respostas.

III. Instruções especiais – serão transmitidas, quando necessário, orientações específicas, visando, principalmente, garantir a proteção do assunto tratado e possíveis fontes. Seus subitens deverão ser identificados por algarismos arábicos em ordem crescente e seguidos de ponto (1. Etc).

2.1.3 Ordem de Busca (OB)

Apesar de não preconizada pela DNISP, mas de tradicional e largo emprego dentro do Sistema Brasileiro de Inteligência, a OB é o documento utilizado pelas Agências de Inteligência para acionar seus Elementos de Operações (ELO). A OB é respondida pela Seção de Operações por meio do Conhecimento Informe.

Estrutura da OB

Os requisitos para sua elaboração são os mesmos do RELINT, com a diferença de que fazem parte do texto de uma OB os itens que seguem numerados com algarismos romanos, seus significados e suas respectivas subdivisões.

I. Elementos disponíveis – nesse item, a fim de orientar o ELO, deve ser relacionado o que se sabe sobre o assunto que está sendo estudado, visando orientar a execução dos procedimentos. Seus subitens deverão ser identificados por letras minúsculas seguidas de ponto (a., b. c., ...n.).

II. Missão – serão elencados os seguintes subitens, identificados por algarismos arábicos em ordem crescente e seguidos de ponto:

1. necessidades de conhecimento a serem atendidas; e
2. prazo para o recebimento das respostas.

III. Instruções especiais - serão transmitidas, quando necessário, orientações específicas, visando, principalmente, garantir o sigilo do assunto tratado, proteger possíveis fontes e o próprio ELO. Seus subitens deverão ser identificados por algarismos arábicos em ordem crescente e seguidos de ponto (1. Etc).

2.2 Conhecimentos de Inteligência

Os documentos produzidos pela Atividade de Inteligência são assim chamados por serem fruto do trabalho intelectual de um analista de Inteligência, após aplicada a Metodologia para a Produção do Conhecimento sobre os dados e conhecimentos recebidos sobre o assunto que está sendo desenvolvido.

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

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

É importante que tenhamos essas noções para que possamos entender como se processa a Metodologia para a Produção do Conhecimento, que transforma uma massa de dados e conhecimentos recebidos, de diversos parceiros, de dentro e de fora do Sistema de Inteligência, em Conhecimento de Inteligência, apresentados sob a forma daqueles documentos sobre os quais já lhes falamos: o Informe, a Informação, a Apreciação e a Estimativa.

2.2.1 Ideia, juízo e raciocínio

A **ideia** é a simples representação intelectual de um objeto. Nessa operação intelectual do espírito, o ser humano apreende (apanha, toma, captura), as características de um objeto. E essa apreensão é o ato pelo qual o espírito concebe uma ideia **sem nada afirmar ou negar** – é a simples concepção do objeto. Ex: flor; morro; carro; aglomeração de pessoas; etc.

Já o **juízo** é o procedimento intelectual pelo qual o espírito afirma alguma coisa de outra. O juízo relaciona duas ou mais ideias e afirma, ou nega algo sobre elas. Temos, como exemplo, as expressões do tipo: "Deus é bom"; o "homem não é imortal", "Maria, Pedro e João são gordos". Para expressarmos um juízo, de maneira verbal, ou escrita, temos o que se chama de **proposição** (**ou premissa**).

Por sua vez, o **raciocínio** é a operação intelectual do espírito na qual, partindo de duas ou mais premissas, podemos chegar a uma outra chegando-se a uma conclusão: uma ideia nova baseada nos argumentos expostos.

2.2.2 Ignorância, dúvida, opinião e certeza

A Atividade de Inteligência exige que o analista deixe fluir seu pensamento na direção da **busca da verdade**, ideal de todo profissional de Inteligência. E o que é a "verdade" para ele? Trata-se da exata correspondência daquilo que ele observa com a sua mente. Ou seja, a "verdade" será alcançada quando o analista conseguir apreender, captar tudo que o objeto lhe transmite.

E isso é fácil? Claro que não, pois nem sempre o analista terá condições de esmiuçar todas as características de um fato ou situação que esteja acompanhando.

Por isso, dizemos que, quando o analista tenta entender algo que se lhe apresenta, que ele julga ser interessante à Atividade de Inteligência, mas não consegue formar, em seu espírito, **nenhuma ideia** do que aquilo representa, dizemos que o estado de sua mente é de **ignorância**.

Esse estado pode perdurar indefinidamente e, assim, invalidar qualquer procedimento para a atividade de assessoria, pois **ninguém assessora uma autoridade sobre algo que nem ele sabe o que é,** não é mesmo?

Não se produzem conhecimentos de Inteligência no estado de ignorância!

Já o estado da mente chamado de **dúvida** acontece quando a verdade pode aparecer ao analista simplesmente como **possível.** Há aspectos que o levam a entender a imagem de uma maneira, mas há outros que o conduzem a formar a imagem de outra maneira. Existe, portanto, a dúvida.

Agora, vamos pensar. Se você está em dúvida, você acha que deve levar à apreciação de alguém a sua dúvida, conduzindo-o à mesma situação? Como uma autoridade, ou gestor, pode decidir sobre algo nessa condição? Então, você já percebeu que esse estado da mente não serve, também, para o analista produzir algum documento orientador.

Não se produzem conhecimentos de Inteligência no estado de dúvida.

Por outro lado, o estado da mente de **opinião** acontece quando a verdade parece ao analista como **provável**, ou seja, quando ele conseguiu **assimilar suficientes elementos** que o tiraram do estado de dúvida e o levaram a ter uma opinião (não chute!) sobre a imagem daquele objeto observado.

Dizemos que existe a **probabilidade** de que a imagem esteja, não totalmente certa, mas próxima disso. Você não está totalmente seguro sobre a imagem formada, mas reuniu **evidências** (essa é a palavra mágica) que o levaram a ter uma opinião formada sobre o objeto em estudo.

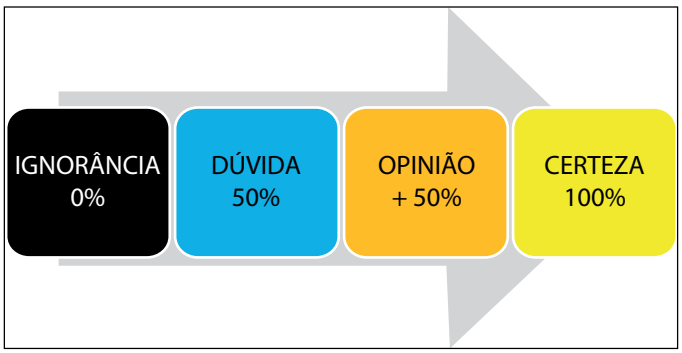
Surge, então, a **convicção do analista** sobre o fato ou situação observados. E quanto mais perto ele chegar do ideal, ou seja, do estado de **certeza**, onde **a verdade é evidente**, melhor para o trabalho.

Conhecimentos de inteligência podem e devem ser produzidos com a mente do analista em estado de opinião!

No estado de **certeza**, a mente do analista já conseguiu apreender **todas** as características do objeto, fato, ou situação em observação.

Portanto, se formos fazer uma relação desses estados da mente com a matemática, poderíamos dizer que a **ignorância** representaria **0% de imagem formada** e a **dúvida** estaria **em 50%.** Já na **opinião**, o analista **ultrapassou os 50%** e está em busca da certeza e já tem **convicção** sobre a imagem que se formou; passando a realizar todos os esforços possíveis para chegar à **certeza**, que corresponde aos **100%** de correspondência entre o que ele percebe no mundo real e o que se forma na sua mente sobre isso.

Figura 3.2 - A relação entre a formação da imagem e os estados da mente



Fonte: Elaboração dos autores, 2013.

2.2.3 Tipos de Conhecimento de Inteligência

Vamos ver, agora, os Conhecimentos de Inteligência em si:

a. Informe

É o conhecimento resultante de **juízos** formulados pelo profissional de Inteligência e que expressa os estados de **certeza** ou **opinião** em relação à verdade sobre fato ou situação **do passado** ou **do presente** de interesse para a Atividade de Inteligência.

O Informe não ultrapassa os limites do juízo, por não reunir evidências que permitam elaborar raciocínio.

Sua redação deve responder aos seguintes questionamentos: O quê? Quem? Onde? Como? Quando? Não deve conter conclusões, projeções ou sugestões.

Os tempos verbais utilizados para a redação de um informe, considerando o estado da mente do analista são:

- Estado de opinião: futuro do pretérito. Ex: A droga seria entregue na cidade de Quilombo.
- Estado de certeza: pretérito perfeito e presente do indicativo. Ex: A droga foi entregue na loja Damião, às 17:00h do dia 17 Set 2012; A milícia que controla o morro do Favelão é chefiada pelo Cabo PM João Trancoso, do 14º BPM, da cidade de Areia Roxa.

b. Informação

É o conhecimento resultante de raciocínio elaborado pelo profissional de Inteligência e que expressa o estado de **certeza** em relação à verdade, sobre fato ou situação **do passado** ou **do presente** de interesse para a Atividade de Inteligência.

Não contém expressões que indiquem a ideia de probabilidade, pois só contém frações (parágrafos) certas.

Os tempos verbais utilizados em uma Informação são o pretérito perfeito e o presente do indicativo.

A "informação" é um conhecimento normalmente confeccionado por Agências de Inteligência de mais alto escalão dentro do Sistema, desde que possuam analistas de Inteligência formados para produzir tal conhecimento.

c. Apreciação

É o conhecimento resultante de **raciocínio** elaborado pelo profissional de Inteligência e que expressa o estado de **opinião** em relação à verdade, sobre fato ou situação passado ou presente de interesse para a Atividade de Inteligência.

Ainda não estabelecido formalmente pela doutrina, a Apreciação tem sido usada com muita frequência para apontar tendências de evolução de determinados assuntos em um espaço temporal de pouco alcance, a partir do momento presente; ou seja, para descortinar um lapso temporal de futuro reduzido.

Quanto tempo seria isso? Seis meses? Duas semanas? Dois dias? Não existe um padrão. O que não pode é o analista tentar especular o futuro muito distante com a Apreciação. Nesse caso, é melhor utilizar o conhecimento exposto a seguir: a Estimativa.

A opinião do analista é resultante do emprego da metodologia para a produção do conhecimento sobre todos os dados e conhecimentos reunidos sobre o assunto "sob observação".

A “Apreciação” também é um conhecimento normalmente confeccionado por Agências de Inteligência de mais alto escalão dentro do Sistema, desde que possuam analistas de Inteligência formados para produzir tal conhecimento.

d. Estimativa

É o conhecimento resultante de **raciocínio** elaborado por um grupo de profissionais de Inteligência e que expressa o estado de opinião em relação à verdade, sobre a **evolução futura** de um fato ou de uma situação de interesse para a Atividade de Inteligência.

É elaborado com base na análise objetiva de todos os conhecimentos envolvidos e no estudo das possibilidades e probabilidades de sua evolução.

A “Estimativa” também é um conhecimento normalmente confeccionado pela Agência de Inteligência de mais alto escalão dentro do Sistema, desde que possuam analistas de Inteligência formados para produzir tal conhecimento.

2.3 O que é dado?

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 Inteligência, **à metodologia** de Produção de Conhecimento.

Os dados e os conhecimentos de Inteligência recebidos pelo analista de Inteligência constituem a matéria-prima da construção do conhecimento.

Mas como os dados não possuem qualquer tratamento, sendo uma informação em estado bruto, necessitam passar por uma avaliação. Sendo assim, não podem ser utilizados da maneira como chegam ao analista, por mais confiável que seja a fonte. Sempre que um dado estiver disponível, há que se aplicar sobre ele a chamada Técnica de Avaliação de Dados (TAD).

2.3.1 Avaliação de dados

É o processo a que são submetidos os dados de interesse para a prática da Atividade de Inteligência. A avaliação tem por objetivo mensurar a **credibilidade** que pode ser atribuída a um dado.

2.3.2 Fontes de dados

Para fins práticos de avaliação, são consideradas fontes: as pessoas, as organizações ou os documentos dos quais se obtém um dado, de acordo com a seguinte classificação:

1. **Pessoas como fonte:** Por terem percebido, memorizado e descrito um fato ou uma situação, são consideradas autoras do dado.
2. **Organizações como fonte:** São aquelas que detêm a responsabilidade pelo dado, por tê-lo difundido, tendo em vista a impossibilidade de identificação do autor.
3. **Documentos como fonte:** São aqueles que exprimem o dado, mas não contêm indicações que possibilitem a identificação do autor ou de uma organização por ele responsável.

2.3.3 Técnica de Avaliação de Dados (TAD)

Julgamento da fonte

Segundo esta técnica, é preciso julgar a fonte com o objetivo de estabelecer o seu grau de idoneidade, ocasião em que é considerada sob três aspectos: autenticidade, confiança e competência.

1. **Autenticidade**

   Sob o aspecto de autenticidade, procura-se primeiro averiguar se o dado provém realmente da fonte presumida. Este trabalho é desenvolvido por intermédio do estudo das particularidades e dos eventuais sinais indicativos que permitem caracterizar a fonte. Cuidados especiais devem ser tomados para distinguir fonte de canal de transmissão (fonte primária de fonte secundária), já que na maioria das vezes surge, entre a fonte e o avaliador, a figura do intermediário do dado. Este intermediário é considerado como canal de transmissão e não deve ser confundido com a fonte do dado, muito embora deva ser submetido aos mesmos critérios de avaliação da fonte primária.

2. **Confiança**

   Sob o aspecto da confiança, entre outros, são considerados os seguintes indicadores que a ela se relacionam:

   - antecedentes (criminais, políticos, de lealdade, de honestidade, dentre outros);
   - padrão de vida compatível ou não com o seu poder aquisitivo;
   - contribuição já prestada ao Órgão de Inteligência (precisão de dados, constância etc);
   - motivação (dinheiro, patriotismo, interesse pessoal, vingança, dentre outros).

3. **Competência**

   Sob o aspecto da competência, a fonte é julgada levando-se em conta essencialmente os seguintes indicadores:

   - **Habilitação -** Refere-se aos atributos pessoais da fonte presumida para perceber, memorizar e descrever especificamente o fato ou situação objeto do dado. Desta forma, a fonte é julgada com base no estudo da sua capacidade pessoal para perceber o fato ou a situação.
   - **Condições de obtenção do dado -** Diz respeito à possibilidade de a fonte (por si mesma) perceber o fato ou a situação que descreve.

Os indicadores aqui elencados são mais adequados para o julgamento de pessoas como fonte, podendo também ser adaptados para o julgamento de organizações.

Eventualmente, se o analista tiver que julgar um documento como fonte de dados, deverá valer-se de outros indicadores e técnicas específicas.

Com base na ACI (2005, p. 20 -22), o quadro abaixo apresenta, de forma resumida, os aspectos do **julgamento da fonte**:

Quadro 3.1 - Julgamento da fonte

ASPECTO	PERGUNTA-SE	VERIFICAM-SE
AUTENTICIDADE	- O dado provém realmente da fonte presumida? - Em caso positivo, foi dela que o dado se originou?	- Meios transmissores pelos quais passou o dado. - Processos utilizados para identificação e reconhecimento dos informantes. - Teve oportunidade de observar o dado?
CONFIANÇA	- Quem é a fonte? - Qual o envolvimento da fonte no episódio descrito? - Qual o interesse da fonte ao fornecer o dado?	- Antecedentes. - Padrão de vida. - Contribuição anterior. - Motivação.
COMPETÊNCIA	- A fonte está habilitada a perceber e transmitir o dado? - A localização da fonte permite perceber o fato ou a situação que descreve?	- Atributos pessoais. - Considerações sobre data, hora, local etc da observação.

Fonte: ACI/PMSC, 2005.

Julgamento do conteúdo

Na questão do julgamento do conteúdo, a ACI (2005, p. 20-21) informa que considera o dado sob os aspectos de: coerência, compatibilidade e semelhança.

- A **coerência** consiste em determinar se o dado em julgamento não apresenta contradições em seu conteúdo; busca-se, assim, verificar a harmonia interna do dado e o seu encadeamento lógico.
- A **compatibilidade** é aferida estabelecendo-se o relacionamento do dado com o que se sabe sobre o fato ou a situação que é objeto do mesmo; procura-se, deste modo, examinar o grau de harmonia com que o dado se relaciona com outros dados conhecidos anteriormente.
- A **semelhança** consiste em verificar se há outro dado, oriundo de fonte diferente, cujo conteúdo esteja conforme com o dado em julgamento.

O quadro abaixo resume os aspectos do **julgamento do conteúdo**:

Quadro 3.2 - Julgamento do conteúdo

ASPECTO	PERGUNTA-SE	VERIFICAM-SE
COERÊNCIA	- O dado em julgamento apresenta contradição lógica?	- A harmonia interna do dado. - O encadeamento lógico do dado.
COMPATIBILIDADE	- O dado se harmoniza com outros dados conhecidos?	- O relacionamento do dado com o que se sabe sobre o fato ou situação que é objeto do mesmo. - O grau de harmonia.
SEMELHANÇA	- Há outro dado, de fonte diferente, cujo conteúdo seja semelhante ao dado em julgamento?	- Há existência de dado semelhante gerado em outra fonte. - Há conformidade entre o dado em julgamento e o da outra fonte.

Fonte: ACI/PMSC, 2005

Determinação da credibilidade do dado

A ACI (2005, p. 21-22) dá conta de que, após julgados a fonte e o conteúdo, o analista terá condições de determinar o grau de credibilidade do dado.

A credibilidade das frações (parágrafos do documento) que comporão o conhecimento será traduzida, quando de sua formalização, por meio de recursos de linguagem que expressem o estado de certeza ou de opinião do analista.

Recordando:

- estado de certeza: uso dos tempos verbais presente do indicativo e pretérito perfeito;
- estado de opinião: uso do tempo verbal futuro do pretérito.

O grau de credibilidade, resultado final do que queremos, será expresso por meio da codificação alfanumérica abaixo:

Quadro 3.3 - Grau de credibilidade

JULGAMENTO DA FONTE	JULGAMENTO DO CONTEÚDO
A - Inteiramente idônea	1 - Confirmado por outras fontes
B - Normalmente idônea	2 - Provavelmente verdadeiro
C - Regularmente idônea	3 - Possivelmente verdadeiro
D - Normalmente inidônea	4 - Duvidoso
E - Inidônea	5 - Improvável
F - A idoneidade não pode ser avaliada	6 - A veracidade não pode ser avaliada

Fonte: ACI/PMSC, 2005.

Os **graus de idoneidade** da fonte são avaliados a partir dos seguintes critérios:

1. **Fonte "A"**: ao longo do tempo em que vem sendo utilizada atendeu sempre, de maneira positiva, aos aspectos considerados.
2. **Fonte "B"**: em algumas oportunidades deixou de atender a um ou mais parâmetros de avaliação.
3. **Fonte "C"**: coloca-se em uma situação intermediária entre o número de ocasiões em que se conduziu positivamente, ou não, em relação às avaliações.
4. **Fonte "D"**: na maioria das oportunidades deixou de atender aos parâmetros considerados.
5. **Fonte "E"**: deixou de atender sempre aos aspectos observados.
6. **Fonte "F"**: era desconhecida até o momento da avaliação.

Os **graus de veracidade** do conteúdo são avaliados a partir dos seguintes critérios:

1. **Avaliação "1":** nesta categoria inclui-se aquele dado que, de forma semelhante, foi difundido por outras fontes e apresenta um conteúdo coerente e compatível.
2. **Avaliação "2":** dado que apresenta coerência e compatibilidade, embora não tenha sido confirmado por outras fontes.
3. **Avaliação "3":** apesar de não ser confirmado, o dado apresenta coerência e compatibilidade.

4. **Avaliação “4”:** embora coerente, o dado não pôde ser confirmado e não é compatível com o que já se conhece sobre o fato ou situação considerada.
5. **Avaliação “5”:** o dado apresenta alguma compatibilidade, porém, não pôde ser confirmado e não apresenta coerência.
6. **Avaliação “6”:** o dado não apresenta nenhuma característica dos três parâmetros de avaliação. Em tese, assunto rotineiro não deve ser difundido até que seja possível atribuir-lhe um melhor grau de veracidade.

O profissional recrutado e selecionado para atuar no exercício da Atividade de Inteligência deve possuir discrição, dentre inúmeras outras qualidades que se fazem necessárias ao sucesso da missão.

Recomendação de segurança: Os agentes responsáveis pela custódia de documentos, conhecimentos, materiais, áreas, comunicações, operações e sistemas de informação de natureza sigilosa estão sujeitos às regras referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico.

Capítulo 4

Inteligência e Contrainteligência nas organizações policiais

Habilidades

Capacitar o estudante com conhecimentos adequados ao domínio de técnicas que permitam conhecer e relacionar as atividades de Inteligência e Contrainteligência, analisando e operando dados para realizar a gestão da informação com atuação sobre os problemas relacionados à segurança e a questões correlatas; bem como dar-lhe instrumentos para coletar, mapear a informação e analisá-la à luz da legislação e em articulação com os diferentes órgãos das esferas federais, estaduais e municipais e até internacionais.

Seções de estudo

Seção 1: Produção do conhecimento

Seção 2: Contrainteligência: segurança ativa e segurança de assuntos internos

Seção 3: Contrainteligência: segurança orgânica ou passiva

Seção 4: Operações de Inteligência

Seção 5: As polícias e as tecnologias de Inteligência

Seção 1
Produção do conhecimento

O exercício da Atividade de Inteligência de Segurança Pública – AISP - deve seguir o que está previsto na Doutrina Nacional de Inteligência de Segurança Pública – DNISP - a fim de padronizar a metodologia da produção do conhecimento, assim também como estabelecer normas, procedimentos e rotinas que servirão de base para organizar os diversos sistemas de Inteligência. Deve-se buscar a consolidação da DNISP, com o objetivo de impedir a prática de ações meramente intuitivas e a adoção de procedimentos sem uma orientação racional.

As Agências de Inteligência devem procurar sistematizar as rotinas de produção de conhecimentos, proporcionando subsídios para a elaboração dos documentos relativos à AISP. Lembrando que a AISP é a atividade que tem por objetivo a obtenção, análise e disseminação de conhecimentos sobre fatos e situações de imediata ou potencial influência sobre o processo decisório, planejamento e execução da política de Segurança Pública expressa pelos governos federal e estadual.

> *A informação só será útil se o usuário quiser compreendê-la.* (Perrenoud)

Antes de tudo, vamos lembrar o que é um "dado". Branco (2011, p. 137) nos diz que:

> **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 Inteligência, **à metodologia** de produção de conhecimento.

E **conhecimento**? Por que dizemos que o documento final, o produto da AISP, é um "Conhecimento de Inteligência"?

Branco (2012, p. 49) lembra-nos que o **conhecimento humano** é uma expressão usada para definir toda a experiência gerada pelo ser humano adquirida até o presente momento em que vivemos. Acrescenta que podemos dizer, também, que o conhecimento humano é a soma de todos os pensamentos, criações e invenções da mente humana. Ou seja, tudo que nos cerca e que foi produto da **mente criativa** do ser humano pode ser chamado conhecimento humano.

O Conhecimento de Inteligência é um produto da mente humana. Dessa maneira, podemos dizer que é **científico,** uma vez que também utiliza uma metodologia muito semelhante à aplicada na produção do conhecimento científico e é fruto da mente humana – a do analista de Inteligência.

Assim, a **produção do conhecimento** é o conjunto de procedimentos realizados pelo profissional de Inteligência do qual resulta determinado Conhecimento de Inteligência (Informe, Informação, Apreciação e Estimativa).

De acordo com a ESG (1986 apud RODRIGUES, 1999, p. 16),

> Toda a produção do conhecimento na Atividade de Inteligência envolve órgãos de planejamento e decisão, que representam os **usuários,** e os órgãos de inteligência que representam o **produtor**.

Em consequência, existe um terceiro elemento que, apesar de não participar da produção do conhecimento, é seu **beneficiário**.

Rodrigues (1999, p.16) prossegue afirmando que:

> **Usuários do conhecimento**: são as autoridades governamentais em todos os níveis, que dele se valem para a tomada de decisão.
>
> **Produtores do conhecimento**: são os órgãos de inteligência formados por profissionais especializados para cumprir este tipo de missão.
>
> **Beneficiários do conhecimento**: são as pessoas beneficiadas pelas decisões acertadas adotadas pelas autoridades.

O **conhecimento** seria, portanto, o produto acabado da Atividade de Inteligência, decorrente do estudo de um assunto levado a efeito por um analista de Inteligência.

Conhecimento: É o ato ou a atividade de conhecer, realizado por meio da razão e/ou da experiência. Ato ou efeito de apreender intelectualmente, de perceber um fato ou uma verdade. Percepção de algo ou de alguma coisa.

Conforme Possebom (1996 apud RODRIGUES, 1999, p. 13), conhecimento na Atividade de Inteligência é "a representação de um fato ou situação, reais ou hipotéticos, de interesse para a Atividade de Inteligência, elaborada em um órgão de inteligência".

Borges (1997 apud RODRIGUES, 1999, p. 14) afirma que o **conhecimento na Atividade de Inteligência** é apresentado em quatro tipos, assim definidos como:

- INFORME: elaborado pelo profissional de inteligência, expressa seu estado de certeza ou de opinião frente à verdade sobre fatos ou situação passados e/ou presentes; não ultrapassa os limites do juízo; requer do profissional de inteligência capacidade de julgamento, análise e síntese; requer metodologia específica, em especial da técnica de avaliação de dados; elaborado com o uso de

linguagem apropriada, o que definirá o grau de verdade em relação à certeza ou opinião; requer narrativa apenas no pretérito ou no presente, sem traduzir qualquer tipo de evolução futura.

- INFORMAÇÃO: elaborado por profissional de inteligência e resultante de raciocínio, expressa estado de certeza frente à verdade sobre fato ou situação passados e/ou presentes; consequência da operação mais apurada da mente que é o raciocínio; contém o desdobramento dos fatos ou situações, não se limitando à simples narrativa; não admite a gradação da verdade, porque expressa unicamente o estado de certeza, não comporta qualquer tipo de projeção dos fatos ou situações futuras.
- APRECIAÇÃO: resultante de raciocínio elaborado pelo profissional de inteligência, expressa opinião sobre fato ou situação passados e/ou presentes; difere-se da informação pelo fato de expressar uma opinião e não o estado da certeza como é na informação.
- ESTIMATIVA: resultante de raciocínio elaborado pelo profissional de inteligência, expressa seu estado de opinião frente à verdade, sobre a evolução futura de um fato ou de uma situação; requer raciocínio prospectivo e conhecimento compatível com a complexidade da técnica de previsão.

Lembremos aqui, em complemento a Borges (1997 apud RODRIGUES, 1999, p. 14), que o Conhecimento denominado “Apreciação” tem sido usado como um Conhecimento de Inteligência que aponta tendências futuras, dentro de um espaço temporal reduzido, de evolução de um fato, ou situação de interesse da AISP.

1.1 Por que se produz um conhecimento de Inteligência?

Um Conhecimento de Inteligência, em princípio, é produzido para atender às necessidades especificadas pelo chefe/diretor, comandante da organização/instituição, gestor, etc, nos diversos níveis em sua área de responsabilidade. No jargão da Atividade de Inteligência, o destinatário maior dos conhecimentos produzidos é chamado de “cliente”.

Um Conhecimento de Inteligência pode ainda ser produzido nas seguintes situações:

- Em atendimento a um **Plano de Inteligência ou Plano de Operações** do escalão superior.
- Em atendimento a um pedido ou ordem específica.
- Por iniciativa da própria da Agência de Inteligência.
- Em atendimento à **solicitação de uma agência congênere.**

1.2 Ciclo de produção do conhecimento

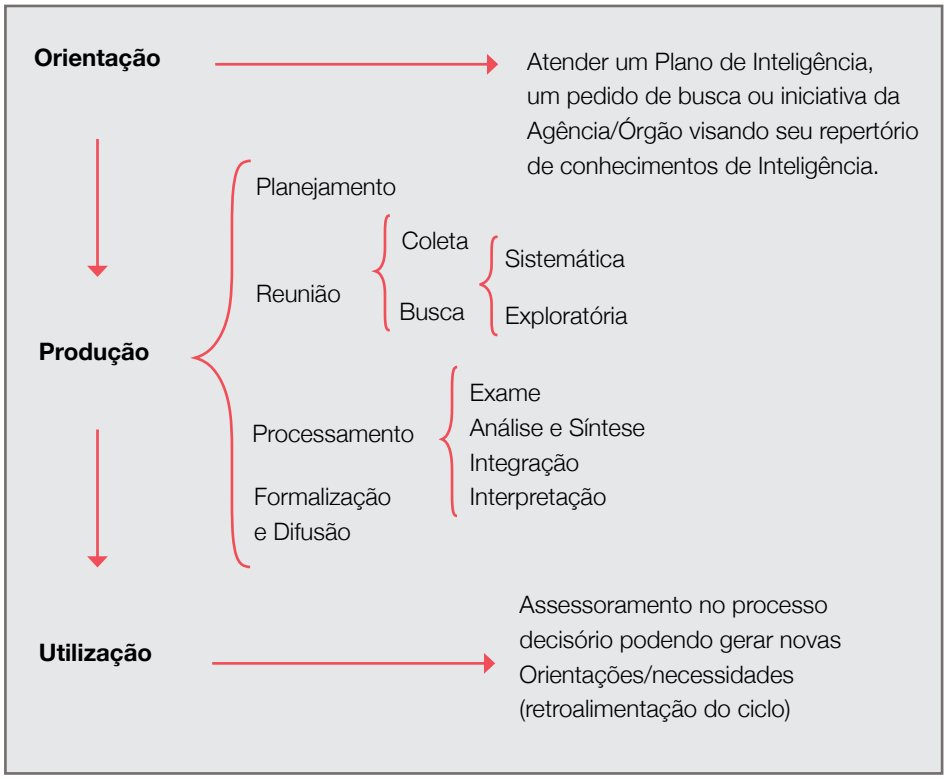
Branco (2012, P.50) nos ensina que o **Ciclo de Produção de Conhecimento** (CPC) é um processo intelectual em que a **capacidade humana**, auxiliada por **metodologia própria**, possibilita a elaboração de um conhecimento especializado e estruturado a partir de **dados**, devidamente avaliados e analisados, para atender àss demandas do processo decisório em qualquer dos seus níveis.

O Ciclo de Produção do Conhecimento (CPC) é uma sequência de ações em que, inicialmente, as necessidades de conhecimentos são reveladas para, em seguida, os conhecimentos de Inteligência serem produzidos e, finalmente, colocados à disposição do usuário (o cliente).

Assim, dentro do CPC, inicialmente, existe a fase da **orientação**, que se fundamenta por intermédio das necessidades de Conhecimentos da autoridade ou do gestor, as quais estão consubstanciadas no Plano de Inteligência de Segurança Pública.

Uma vez entendidas perfeitamente essas necessidades, dá-se a fase da **produção** do conhecimento, que culmina com a sua **utilização** pelo interessado, sendo que este pode realimentar o sistema com novas necessidades.

Figura 4.1 - Ciclo de Produção do Conhecimento



Fonte: Adaptação da ESG, 1986, p. 235.

1.3 Metodologia para a produção do conhecimento

Branco (2011, p. 141) nos ensina que a metodologia consiste na sequência ordenada de procedimentos executados pelo analista que visa à produção de um conhecimento de Inteligência de forma racional e com melhores resultados.

O emprego da metodologia, entretanto, não garante o êxito no trabalho, pois outros fatores concorrem para o sucesso, tais como: a experiência pessoal, os atributos pessoais, a preparação profissional, a experiência e o embasamento cultural do analista de inteligência.

Tal metodologia, entretanto, garante que o analista:

- considere todos os aspectos do problema;
- produza um conhecimento com bases científicas;
- uniformize os procedimentos no âmbito do SISP; e
- ofereça ao usuário um trabalho pleno de credibilidade.

A metodologia para a produção do conhecimento de Inteligência obedece a 04 (quatro) fases: planejamento, reunião, processamento (exame, análise e síntese, integração e interpretação) e formalização e difusão.

Habitualmente, as fases de produção do conhecimento se superpõem, permitindo que na prática as fases do **planejamento**, **reunião** e **processamento** tenham estreita relação entre si e algumas vezes se interpenetrem.

1.3.1 Planejamento

Alguém faz alguma coisa sem realizar um planejamento?

Essa fase da Metodologia é muito importante para o analista, uma vez que, se no início do trabalho, não houver uma percepção clara do que deve ser feito podem permanecer lacunas, que só serão vistas muito mais à frente e, talvez, não haja tempo de preenchê-las, resultando em um trabalho incompleto, ou mesmo impossibilitando sua realização.

Branco (2011, p 142) nos fala dessa fase, dizendo serem ordenadas nela, de forma sistematizada e lógica, as etapas do trabalho a ser desenvolvido. É a fase em que são estabelecidos os objetivos, as necessidades, os prazos, as prioridades e a cronologia, definindo os parâmetros e as técnicas a serem utilizadas a partir dos procedimentos mais simples para os mais complexos. Complementa dizendo que “planejar deve constituir-se em uma ação rotineira do profissional de Inteligência”.

Para o autor, essa fase deve seguir algumas etapas para que, ao final, o analista esteja seguro de que realizou todos os estudos preliminares e estabeleceu todos os procedimentos para cumprir a tarefa. Assim, as etapas seriam:

- A **determinação do assunto** a ser estudado – consiste em especificar o fato ou a situação, objeto do conhecimento a ser produzido, por intermédio de uma expressão escrita. O assunto deve ser preciso, determinado e específico e, para isso, o analista deve responder, se possível, às perguntas: O quê? Quem? Onde? Ex: Contrabando de remédios, por quadrilhas brasileiras, na fronteira do Brasil com o Paraguai.
- A **determinação da faixa de tempo a ser considerada –** consiste em estabelecer marcos temporais para o desenvolvimento do estudo considerado. Ex: no primeiro semestre de 2001; de 20 a 30 Set; nos últimos cinco anos.
- A **determinação do usuário do conhecimento –** identifica a autoridade governamental ou o órgão congênere que, pelo menos potencialmente, utilizará o conhecimento que está sendo produzido. Identificando isso, o analista pode ter uma ideia do nível de profundidade do conhecimento a ser produzido.
- A **determinação da finalidade do conhecimento** – diz respeito à possível 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. Nesse caso, o planejamento é orientado para esgotar o assunto tratado de tal modo que o usuário venha a encontrar, em algum ponto do conhecimento produzido, os subsídios úteis a sua atuação.
- A **determinação do prazo disponível para a produção** – 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.

- A **determinação dos aspectos essenciais do assunto** – consiste em fazer uma lista do que o analista **precisa saber** para elaborar um documento o mais completo possível. Tal lista poderá ser ampliada ou sofrer supressões em decorrência da evolução do estudo. Ainda nesta fase, para melhor orientar a fase seguinte – a da reunião – o analista separa os aspectos essenciais a conhecer em "conhecidos", porque, de alguma maneira, já tem a resposta para eles dentro de sua própria AI, dos aspectos "a conhecer, ou complementar", que necessitarão ser buscados.
- A **atribuição de medidas de proteção para o documento.** Se for possível, atribuir um grau de sigilo preliminar. E de qualquer maneira, adotar todas as medidas de proteção a documentos existentes, durante sua elaboração.

1.3.2 Reunião

Segundo Rodrigues (1999, p. 17), nesta fase o analista de Inteligência "procura reunir conhecimentos ou dados que respondam ou completem os aspectos essenciais a conhecer".

Esta menção à complementação dos aspectos essenciais a conhecer, levantados na fase do planejamento, tem a ver com o fato de o analista já possuir, em seus arquivos algumas respostas para eles. E, então, podem existir aspectos que estejam incompletos; e por isso necessitam ser completados. Também podem existir aspectos sobre os quais o analista nada conhece; e assim precisam ser totalmente respondidos.

Pode acontecer, entretanto, que o analista parta para começar seu trabalho sem conhecer absolutamente nada sobre um determinado assunto (estado de ignorância de sua mente, lembra disso?). E, assim, ele só terá aspectos essenciais a serem respondidos.

Outro aspecto a ser comentado na citação de Rodrigues, acima, é o fato de o analista reunir conhecimentos. Como vamos observar mais adiante, quando o analista precisa preencher as lacunas de seu conhecimento sobre o assunto, ele poderá perguntar, por intermédio de um Pedido de Busca, a uma AI do próprio sistema a que pertence, ou mesmo de outro, o que necessita saber. Assim, a AI questionada responderá o PB com um Conhecimento de Inteligência. Daí então o motivo de, na fase da reunião, o analista receber conhecimentos e dados.

Branco (2011, p 144) explica como o analista deve proceder à reunião daquilo que precisa. A **reunião de dados** pode ser assim esquematizada:

- Consulta aos arquivos e bancos de dados da própria AI, em primeiro lugar – tais arquivos podem oferecer dados ou conhecimentos sobre o assunto, que não serão perguntados aos parceiros, caso esgotem a necessidade do analista.
- Pesquisa – contatos com pessoas, estudos em bibliotecas, ligações formais e informais com organizações fora do SISP. Como resultado da pesquisa, o analista só reunirá dados.
- Ligações com órgãos congêneres – consiste na solicitação do apoio de outras AIs pertencentes ou não ao SISP. Esse contato fornecerá conhecimentos ao analista.
- Acionamento do Elemento de Operações (ELO) – o analista deverá saber se o ELO tem a capacidade de atendê-lo antes de emitir a Ordem de Busca de dados necessários ou mesmo avaliar a real necessidade desses dados que faltam, pois acionar o ELO sempre significa risco à AI e ao próprio ELO.
- Autorização judicial em hipótese de sigilo legal e investigação criminal.

O analista de Inteligência, portanto, obtém e reúne conhecimentos ou dados, processados ou não, pertinentes ao assunto do conhecimento a ser produzido. Além disso, desenvolve dois tipos de atividades nesta fase: a coleta e a busca.

1.3.3 Coleta

É a pesquisa ostensiva sobre um assunto. São aqueles assuntos que estão disponíveis nos arquivos, bibliotecas etc; conhecimentos e/ou dados de livre acesso a quem procura obtê-los.

1.3.4 Busca

É a procura de conhecimento de obtenção mais difícil, pelo fato de os dados possuírem algum tipo de proteção que impeça, ao analista, obtê-lo com a coleta. Na busca, o órgão de Inteligência procura ocultar ao máximo a sua participação. Quem executa uma busca é o Elemento de Operações (ELO) da AI.

Além disso, a **busca** pode ser classificada de **sistemática** e **exploratória**. A busca sistemática caracteriza-se por ser contínua, produzindo um fluxo constante de conhecimentos, e acompanha a evolução de um assunto. Trata-se de uma atualização e/ou aprofundamento de conhecimento sobre um assunto em questão. A busca exploratória tem por objetivo atender às necessidades imediatas de um conhecimento específico sobre determinado assunto. Usualmente é realizada por intermédio de uma operação de inteligência, planejada com o fim específico de obter o conhecimento almejado.

1.3.5 Processamento

Para Rodrigues (1999, p. 17), a terceira etapa ou fase da produção do conhecimento é chamada de **processamento**. Nesta etapa acontece o **exame**, a **análise**, a **integração** e a **interpretação** das informações.

A DNISP denomina a fase do exame, de Rodrigues, como “avaliação”. As demais são iguais.

1.3.6 (“Avaliação” para a DNISP)

Rodrigues trata, aqui, o termo “informações” referindo-se aos “dados e conhecimentos reunidos”.

Rodrigues (1999, p. 17) afirma que “o **exame** consiste na verificação inicial do grau de credibilidade das **informações** obtidas e da pertinência dos mesmos com o assunto do conhecimento a ser produzido”.

Branco (2011, p.145) nos diz que o analista, nessa fase, busca conhecer o **valor** daquilo que ele conseguiu reunir (dados e conhecimentos) para seu trabalho.

Prossegue dizendo que o trabalho agora é saber se os dados e conhecimentos reunidos são **coerentes e compatíveis** com o objeto do conhecimento a ser produzido. Isto é, vamos verificar sua **pertinência**, ou seja, se realmente interessa para o trabalho pretendido.

Inicia-se por um exame preliminar da relação entre o que foi obtido (dados e conhecimentos) e o desejado (aspectos essenciais a conhecer), e termina-se com a seleção das frações significativas, isto é, as parcelas de dados e/ou conhecimentos que **interessam** aos aspectos essenciais determinados na fase do planejamento. Ou seja, extrairemos dos dados e conhecimentos os fragmentos (parágrafos) que são pertinentes ao assunto estudado. Os demais serão abandonados.

Perguntas a serem feitas para verificar a pertinência das frações de dados e conhecimentos obtidos em relação ao objeto em pesquisa:

- A fração do dado ou o conhecimento tem relação com meu assunto? Sim? Passa-se à pergunta seguinte. Não? Descarta-se o dado ou o conhecimento.
- Quais frações respondem aos aspectos a conhecer? Pronto: agora o analista só tem frações pertinentes ao assunto que está sendo tratado, tanto obtidas de dados, quanto de conhecimentos.

Em seguida, vamos verificar a **credibilidade da fonte e do conteúdo somente dos dados** recebidos, pois as frações dos conhecimentos já foram submetidas a esse processo em sua origem. Serão estabelecidos julgamentos sobre a fonte e o conteúdo dos dados recebidos, aplicando-se a Técnica de Avaliação de Dados (TAD), que você já conhece.

1.3.7 Resultado da avaliação

Após o trabalho de avaliação dos dados e dos conhecimentos reunidos, a **credibilidade** das frações significativas 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.

1.3.8 Análise e síntese

Branco (2011, p 149) diz que esta é a etapa da fase do processamento na qual o analista decompõe os dados e/ou conhecimentos reunidos e pertinentes em suas partes constitutivas, já devidamente avaliadas e agora chamadas de frações significativas, relacionadas aos aspectos essenciais levantados, e examina cada uma delas a fim de estabelecer sua importância em relação ao assunto que está sendo estudado.

Ou seja: o analista já separou tudo que é pertinente e, agora, verifica qual a capacidade de cada fração em responder aos aspectos essenciais a conhecer.

1.3.9 Integração

De acordo com Rodrigues (1999, p. 18), “consiste em formar conjuntos coerentes, relacionados aos aspectos essenciais, a partir dos fatos significativos selecionados e confirmados”. É a montagem de um grande quebra-cabeça, onde as peças são as frações significativas já selecionadas nas fases anteriores.

1.3.10 Interpretação

Constitui a fase em que o analista de Inteligência revela o valor do assunto tratado, definindo o significado final dos conhecimentos integrados. Na base da interpretação, os processos desenvolvidos misturam-se de tal maneira que qualquer tentativa de ordenação e delimitação torna-se difícil. Nos casos de pouca complexidade, não são necessariamente cumpridos todos os processos da interpretação. Desta forma, é possível passar da integração para o significado final.

O que normalmente acontece é que o analista, ao integrar as frações significativas, já começa a formar em seu espírito o real significado de tudo que fez até agora: é a etapa da interpretação acontecendo!

Rodrigues (1999, p. 18) esclarece que:

> As conclusões devem ser objetivas e restritas aos fatos analisados e integrados, eliminando-se as apreciações de caráter subjetivo ou fantasioso, que poderiam levar o usuário a erros graves na avaliação do problema.

Branco (2011, p.150) nos diz que esta é a etapa da fase do processamento, na qual o profissional esclarece o **significado final** do assunto tratado. Após os processos de avaliação, análise e integração, busca-se estabelecer as relações de causa e efeito, apontar tendências e padrões e fazer previsões baseadas no raciocínio.

1.3.11 Formalização e difusão

Nesta fase é necessário que o conhecimento seja organizado de forma a ser levado ao usuário. Esta preparação refere-se à formalização, na qual se admitem as seguintes opções:

- mediante a elaboração de um **conhecimento de Inteligência**;
- mentalmente, para, quando necessário, transmitir **verbalmente** o conhecimento.

Qualquer que seja a opção escolhida, é indispensável que a **formalização** possua todos os elementos necessários ao entendimento e à utilização do conhecimento pelo usuário. Tais elementos são, normalmente, os que formam a estrutura padrão dos **Documentos de Inteligência**.

A **difusão** é a remessa do conhecimento formalizado para o competente usuário.

Conforme Rodrigues (1999, p. 19),

> A **difusão** deve obedecer ao prazo estabelecido pelo usuário, para que não perca sua **oportunidade**. Do mesmo modo, o grau de sigilo e os meios de comunicação a adotar devem ser compatíveis com a natureza do conhecimento.

Na fase que completa o ciclo de produção do conhecimento, chamada de **utilização**, o usuário do conhecimento está localizado no ponto extremo de uma cadeia. Como cliente em potencial, torna-se o destinatário de um produto acabado, chamado de **Conhecimento de Inteligência**.

Seção 2
Contrainteligência: segurança ativa e segurança de assuntos internos

2.1 Contrainteligência

A atividade de Inteligência tem por objetivo a produção de conhecimento e a salvaguarda dos assuntos sigilosos e dos assuntos de interesse do Estado e da sociedade. Subdivide-se em dois ramos: **Inteligência e Contrainteligência**.

A Contrainteligência é colocada em prática através da adoção de ações voltadas para a prevenção, obstrução, detecção e neutralização de ações adversas de qualquer natureza. Ela se divide em três segmentos: Segurança Ativa (SEGAT), Segurança de Assuntos Internos (SAI) e a Segurança Orgânica (SEGOR).

Tendo como base os termos acima, a ContraInteligência (CI) aplicada na Inteligência de Segurança Pública (ISP) assumiu a seguinte definição, segundo consta na página 37 da Doutrina Nacional de Inteligência (DNISP):

> é o ramo da atividade que se destina a produzir conhecimentos para proteger a atividade de ISP e a instituição a que esta pertence, de modo a salvaguardar dados e conhecimentos sigilosos e identificar e neutralizar ações adversas de qualquer natureza.

2.1.1 Ameaças a um sistema

A Contrainteligência (CI) é o ramo da Atividade de Inteligência responsável pela proteção de um determinado sistema em face das ameaças e ações antagônicas provenientes de atores de qualquer natureza.

E quais seriam estas ameaças?

Podemos citar, segundo Branco (2013, p.80 a 83):

- Vazamentos: acesso não autorizado a determinado dado ou conhecimento sensível/sigiloso.
- Engenharia Social: é a arte de induzir pessoas a agirem de acordo com seus próprios desejos. Explora os medos, as vaidades, as ambições, a cobiça e a raiva, dentre outras fraquezas das pessoas.
- Ataques a sistemas informatizados: no mundo atual, praticamente tudo o que fazemos, ou a maneira como nos relacionamos, está baseado em sistemas informatizados, o que nos traz muitas vulnerabilidades.
- Furto: Normalmente praticado por elementos infiltrados em nossa organização, muitas vezes esse tipo de ocorrência acaba sendo dissimulado pelo funcionário responsável pela guarda daqueles dados, informações, ou materiais, com receio de sanções.
- Desinformação: emprego de relatos falsos e boatos, combinados com matérias verdadeiras, com a intenção de enganar e manipular a opinião dos adversários, a fim de comprometer a imagem da instituição, ou influenciar o centro de poder adversário a tomar decisões equivocadas.
- Espionagem: ato caracterizado pela busca ilegal e antiética de informações sigilosas, visando beneficiar Estados ou corporações. Entretanto, esta barreira legal está longe de afastar esta ameaça das instituições, públicas, ou privadas.
- Sabotagem: conjunto de ações, normalmente conduzidas no anonimato, que ocasionam graves danos às instalações, ou ao que nelas é produzido ou guardado. Tem como finalidade afetar setor ou atividade essencial para o funcionamento de uma instituição/empresa, para paralisar suas atividades e/ou desestruturar ou desorganizar a consecução de seus objetivos.

- Corrupção (suborno): a oferta de vantagens indevidas a agentes públicos, ou funcionários de empresas privadas, em troca de facilidades de trânsito na instituição; do acesso aos ativos sensíveis; e da cessão de informações privilegiadas. É uma das ameaças mais corriqueiras de se concretizar, pela própria facilidade que o ser humano, alvo da ação adversa, proporciona.
- Terrorismo: segundo a Agência Brasileira de Inteligência – ABIN, é o uso intencional – ou ameaça de uso – de violência por um grupo político organizado contra "populações não-combatentes", de forma a se alcançar objetivos político-ideológicos.
- Desastres naturais de origem humana.
- Acidentes.
- Atos escusos de funcionários mal intencionados.
- Crime organizado.
- Ilícitos transnacionais.
- Grupos que possam comprometer o estado democrático de direito.
- Tráfico de armas, munições e explosivos.
- Atos contra tecnologias sensíveis.
- Atos para obtenção de bens de uso dual.
- Produção e comércio ilícitos de substâncias psicotrópicas.
- Tráfico de órgãos e seres humanos.
- Agressões ao meio ambiente.
- Concorrência desleal (na área privada).
- outras.

2.2 Ações de Contrainteligência

Visam salvaguardar conhecimentos e dados sigilosos oriundos:

- da estrutura de Inteligência ou por ela manuseados ou custodiados;
- de outras entidades nacionais, públicas ou privadas.

Visam identificar e neutralizar:

- as ações adversas realizadas por organismos ou por grupos de pessoas, vinculados aos governos ou não;

- a espionagem realizada por serviços de Inteligência adversos (estrangeiros ou não), ou de quaisquer grupos que tenham intenção de obter informações da organização;
- as ações cometidas por aqueles que desejam prejudicar, ou impedir o funcionamento, ou a consecução dos objetivos de uma instituição, pública, ou privada.

2.2.1 Segurança ativa

Branco (2011, p. 108) nos diz que **Segurança Ativa (SEGAT) é** um conjunto de medidas de caráter eminentemente **ofensivo** destinadas a detectar, identificar, avaliar, analisar e neutralizar as ações adversas de elementos ou grupos de qualquer natureza dirigidas contra a sociedade e o Estado. Essas medidas são desenvolvidas por meio da contrapropaganda, da contraespionagem, da contrassabotagem e do contraterrorismo.

Vamos entender os conceitos?

Branco (2011, p. 108) refere-se às medidas de SEGAT da seguinte maneira:

- **Contraespionagem -** Conjunto de medidas implantadas que oportunizem detectar e neutralizar as ações adversas de busca de conhecimento e/ou dados sigilosos por meio da espionagem.
- **Contraterrorismo -** É o conjunto de medidas destinado a detectar, identificar, avaliar e neutralizar ações e ameaças terroristas.
- **Contrapropaganda -** Ocorre através da desinformação, que consiste na manipulação planejada de conhecimentos e/ou dados, com o objetivo de iludir ou confundir determinado alvo que possa apresentar risco à salvaguarda de conhecimentos e/ou dados sigilosos, ou a interesse do Estado.
- **Contrassabotagem -** É o conjunto de medidas colocadas em prática visando detectar, identificar e neutralizar atos ou atividades de sabotagem contra a organização, seu pessoal, bens, materiais e informações e que possam causar impacto e danos.

2.2.2 Segurança de Assuntos Internos (SAI)

Caracteriza-se por um conjunto de medidas destinadas à produção de conhecimentos que visam assessorar as ações de correição das instituições de Segurança Pública (DNISP, 2009).

Seção 3
Contrainteligência: segurança orgânica ou passiva

A Segurança Orgânica (SEGOR) é uma medida adotada para proteger a organização como um todo. Acontece por meio de medidas simultâneas de **segurança de pessoal**, de **segurança da documentação e do material**, de **segurança das comunicações e** da **informática (sistemas de informações), de segurança das operações de ISP,** e de **segurança das áreas** e **instalações**.

3.1 Segurança das áreas e instalações

É assegurada por intermédio da proteção de áreas, edificações, instalações e serviços essenciais; e conseguida através de adoção de medidas de proteção geral, fiscalização e controle do acesso àqueles locais, sobre o pessoal orgânico ou estranho aos mesmos, bem como pela demarcação, bloqueio e permanente controle de áreas sigilosas ou restritas, de acordo com regulamentação específica de cada órgão.

As diversas áreas selecionadas para serem protegidas, por conterem algum tipo de conhecimento, dado, ou material sigiloso, são denominadas de **áreas sigilosas.**

Por sua vez, as áreas que contenham materiais sensíveis que possam representar perigo às pessoas ou à organização, se acessadas indevidamente, e que sejam consideradas vitais para o pleno funcionamento da organização, são chamadas de **áreas restritas.**

Toda a área da instituição deve ser protegida, fisicamente, adotando-se o princípio da proteção em profundidade que indica que os obstáculos de maior dificuldade de transposição, para o invasor, devem ser instalados mais próximos dos alvos a serem protegidos.

Exemplos de medidas de proteção: avaliação e demarcação das áreas e instalações; implantação de barreiras; implantação de sistema de detecção, identificação e monitoramento de ocorrência; formação e capacitação de força de resposta; contramedidas eletrônicas; plano de prevenção de acidentes; e plano de prevenção e combate a incêndios.

3.2 Segurança da documentação e do material

É o conjunto de normas, medidas e procedimentos voltados para a proteção dos documentos de Inteligência, desde a produção até a eliminação, em suporte físico ou lógico, e dos materiais sigilosos, para evitar seu vazamento e/ou comprometimento.

As principais ameaças a serem prevenidas e obstruídas pela segurança da documentação e do material são:

- a **espionagem** – que ocorre por meio de furto, cópias não autorizadas, fotografias, leituras de documentos etc; e
- a **sabotagem** – que visa a empreender ações de destruição, de adulteração ou mesmo de interrupção do processo de difusão e recepção dos documentos, retirando-lhes a possibilidade de utilização em tempo hábil.

O comprometimento de documentos ou materiais poderá ser motivado também por fenômenos naturais. Devem-se considerar, ainda, as ocorrências motivadas por causas humanas, com ou sem intenção.

Para que tais ameaças sejam eliminadas ou minimizadas existe a necessidade da adoção de procedimentos rígidos. O primeiro trata-se da **segurança durante a produção de um conhecimento de Inteligência** ou de um documento de cunho sensível, que estudaremos a seguir.

3.2.1 Segurança da documentação

Os documentos sigilosos devem ser protegidos por conterem assuntos que não devam ser do conhecimento das pessoas em geral; tanto os que são produzidos na organização, quanto os que chegam a ela. Para isso, algumas medidas de segurança devem ser tomadas para garantir a proteção da documentação, desde a produção até o arquivamento e mesmo a destruição de um documento. São elas:

a. **Proteção na produção de um documento**

- Atribuir um grau de sigilo preliminar, dentro do que prescreve a legislação em vigor.
- Controlar os recursos utilizados, tais como: manuscritos, rascunhos, carbonos etc.
- Classificar e marcar todas as páginas do documento com o grau de sigilo.
- Autenticar o documento.

b. **Proteção na difusão e na recepção**

- Acondicionar adequadamente o documento (dois envelopes, com o envelope externo sem indicações de seu conteúdo).
- Controlar por meio do protocolo a saída, averiguando o correto endereçamento.
- Controlar através do protocolo a entrada, verificando e registrando, se for o caso, indícios de violação.

c. **Proteção no manuseio**

- Controlar a reprodução.
- Elaborar termo de custódia.
- Proceder à reclassificação ou desclassificação de grau de sigilo, de acordo com a legislação em vigor.
- Selecionar os documentos a serem arquivados ou destruídos, considerando o conteúdo e a oportunidade/ necessidade de aproveitamento.

d. **Proteção no arquivamento**

- Escolher o local adequado.
- Manter controle no arquivamento e na recuperação.

e. **Proteção na destruição**

- Escolher adequadamente os meios e os locais para a destruição.
- Elaborar o Termo de Destruição, a fim de exercer o perfeito controle neste momento.
- Estabelecer procedimentos de rotinas para a destruição em situações de emergência.

Observar, ainda, como medidas de proteção da documentação e do material que o contém:

- Não jogar na cesta de papéis materiais como rascunhos, manuscritos, notas, cópias de documentos sigilosos, fotos, disquetes etc.
- Ao final do expediente administrativo, retirar de sua mesa de trabalho toda a documentação, que deve ser guardada sob chave.
- Criar a rotina de cobrir toda documentação que estiver exposta quando se aproxima alguém.

- Somente fornecer informações sobre o teor e o trâmite dos documentos às pessoas que estiverem devidamente credenciadas.
- Verificar se os arquivos, gavetas e portas ficaram devidamente fechadas e trancadas ao final do expediente administrativo.
- Lembrar sempre que o conhecimento de assuntos sigilosos está condicionado à função desempenhada, e não ao grau hierárquico.
- Não deixar documentos sigilosos nas gavetas e mesas, todo documento deve ser guardado no arquivo do Órgão de Inteligência ao término do expediente administrativo.
- Não portar documento sigiloso, nem guardá-lo em sua casa ou outro lugar fora do Órgão de Inteligência.
- Conhecer somente o que é necessário ao cumprimento das suas missões.
- O manuseio de documentos fica restrito aos credenciados para tal.

3.2.2 Segurança do material

A **segurança do material** trata de procedimentos expressos em regulamentos, instruções ou normas que servem para proteger a informação contida nos materiais, com destaque para aqueles onde se processam o recebimento, o registro, a produção, a classificação, a expedição, o manuseio, a guarda, o arquivamento e a destruição de documentos sigilosos.

Para a segurança do material, o que deve ser protegida é toda matéria, substância ou artefato que contenha, utilize e/ou veicule informações, que, de posse de ator(es) de qualquer natureza, possam beneficiá-lo(s) ou atentar, de forma direta ou indireta, contra qualquer segmento do Sistema de Inteligência ao qual pertencemos.

Também deve ser considerado como material a ser protegido toda a matéria, substância ou artefato imprescindível ao funcionamento da organização, que, diante da ação danosa de ator(es) de qualquer natureza, possa interromper os trabalhos da organização, de forma direta ou indireta.

As principais ameaças a serem prevenidas e obstruídas pela segurança do material são a **espionagem**, por meio de furto de equipamentos, acessos indevidos na forma de leituras de documentos, entre outros; e a **sabotagem,** que visa empreender ações de destruição, de adulteração ou mesmo de interrupção do processo de difusão e recepção de documentos, ou mesmo retirando dos materiais a possibilidade de utilização para o fim a que se destina a Agência de Inteligência.

As medidas de proteção dos materiais sensíveis ou sigilosos estarão intimamente ligadas às medidas de segurança de áreas e instalações e à consequente sinalização de áreas sigilosas e restritas, considerando-se, logicamente, a natureza, o tamanho, a forma e, principalmente, o fim a que se destinam os materiais dentro do sistema da instituição.

3.3 Segurança do pessoal

Comporta normas, medidas e procedimentos voltados para o pessoal que trabalha em todo o sistema de Inteligência, em qualquer escalão, a fim 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 a selecionar, acompanhar e desligar os recursos humanos orgânicos de uma Agência de Inteligência.

As medidas de **segurança no processo seletivo de recursos humanos para trabalhar na Atividade de Inteligência** visam a dificultar as ações adversas de infiltração em órgãos que tratam de assuntos sigilosos e a admissão de indivíduos com características e antecedentes pessoais que possam causar, futuramente, comprometimento das informações desses órgãos.

3.3.1 Segurança no processo seletivo

a) Determinação de sensibilidade da função

Antes de designar alguém para alguma função, precisamos determinar a sensibilidade do cargo atrelado à mesma, ou seja, saber que tipo de conhecimento estará acessível ao funcionário que ocupar tal cargo. Com isso, pode-se escolher o candidato adequado mediante observação de seu perfil. Essa providência não exime a investigação de segurança que deve ser feita sobre os antecedentes do candidato.

Tais medidas aplicam-se, também, ao pessoal contratado para suprir necessidades da organização em serviços de manutenção e outros, necessários ao perfeito funcionamento das instalações, dos materiais e equipamentos sensíveis.

Deve ser procedida uma avaliação criteriosa, observando os dados abaixo:

- Grau de sensibilidade do cargo que o candidate vai ocupar.
- Características pessoais (perfil).
- Lealdade, honestidade e discrição.

b) Investigação de segurança

É a ação administrativa para suprir as necessidades de pessoal de um órgão que trata de assuntos sigilosos/sensíveis. Deve ser realizada a **pesquisa dos antecedentes** objetivando evitar a infiltração e o comprometimento, em que o entrevistador deve:

- observar a vida pregressa do candidato e sua atuação em funções, ou empregos anteriores;
- obter atestados e certidões de idoneidade moral e "nada consta" sobre dívidas, processos, etc.

c) Controle de segurança na consulta ao candidato

O entrevistador deve:

- Adotar medidas cautelosas, pois não sabe com quem está tratando.
- Evitar o comprometimento do órgão, restringindo-se a dar informações superficiais sobre o trabalho a ser realizado.

d) Aplicação de testes seletivos

Visa:

- Confirmar potencialidades.
- Instruir o parecer final de aquisição.

3.3.2 Segurança no desempenho da função

Durante a execução das funções do servidor, algumas providências relativas à segurança devem ser tomadas, dentre elas:

- Efetivar o credenciamento para a função, de acordo como que prescreve a legislação em vigor.
- Proceder à educação de segurança.
- Confirmar as características pessoais exigidas.
- Acompanhar o desempenho do servidor, com respeito ao cumprimento das normas de segurança.

Com relação à **educação de segurança**, vista acima, cabe esclarecer que deve ser executada de forma contínua de forma a ensinar e a rememorar o compromisso de todos com a segurança da organização.

São tipos de educação de segurança:

- Orientação Inicial - explicar a importância das medidas de segurança, antes da assunção do cargo.
- Orientação Específica - especificar as medidas de segurança e seu cumprimento em uma determinada função.
- Orientação Periódica - manutenção das medidas de segurança feita para todos.
- Sinalização de Advertência - serve para criar mentalidade de segurança.

3.3.3 Segurança no desligamento

Serve para:

- Assegurar comportamento adequado posterior ao desligamento.
- Prevenir e obstruir as ações adversas sobre o ex-funcionário.

Quadro 4.1 - Procedimentos e objetivos no desligamento de pessoal

PROCEDIMENTOS	OBJETIVOS
Entrevista final	Orientar e cientificar da responsabilidade na preservação do segredo de assuntos sigilosos aos quais tenham tido acesso.
Controle após o desligamento	Verificar se o ex-agente mantém um comportamento adequado.

Fonte: Agência Brasileira de Inteligência (ABIN), 2006.

3.4 Segurança das comunicações e da informática (Sistemas de Informações)

A segurança nos Sistemas de Informações é mantida pela observância de normas especiais de exploração e regras operacionais, com o objetivo de impedir que assuntos sigilosos cheguem ao conhecimento de pessoas ou órgãos desautorizados para tal.

3.4.1 Segurança das comunicações

Quais as medidas de segurança nas comunicações?

a. **Segurança da transmissão**

Visa proteger fisicamente os meios de informática que farão as comunicações e dificultar a interceptação de mensagens e a consequente análise do fluxo das mesmas.

Será feita por intermédio de:

- processos de **gerência** capazes de **monitorar e registrar os eventos** relativos ao funcionamento dos serviços, de forma a permitir que o fiel cumprimento das regras seja verificado.
- procedimentos de **manutenção** rotineira dos serviços.
- mecanismos de **defesa contra ataques** aos sistemas.
- **medidas de contingência** em condições de ativação imediata.

b. **Segurança no tráfego**

- Utilizar código para as organizações e assinantes.
- Utilizar código de autenticação.
- Manter tráfego falso – simulação de mensagens e variação proposital do número rotineiro de mensagens transmitidas.
- Utilizar recursos criptográficos.

3.4.2 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.

Envolve um conjunto de elementos direcionados para a informática com o intuito de garantir a segurança e integridade do *hardware*, do *software* e dos Sistemas de Gerenciamento de todos os dados e dos próprios bancos de dados.

> Serão em vão os gastos derivados da produção de informações e conhecimentos, se não forem adotadas as providências devidas para a sua proteção, de sorte a evitar que caiam nas mãos dos inimigos ou de concorrentes.

3.5 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.

Seção 4
Operações de Inteligência

É a ação levada a efeito, por uma fração do Órgão de Inteligência, mediante a aplicação de técnicas operacionais, objetivando a busca de dados negados e a neutralização de ações adversas.

Toda operação de Inteligência deve ser meticulosamente planejada e executada, visando a:

- garantir a obtenção do dado não disponível;
- proteger a identidade do órgão de Inteligência que a executa;
- proteger a identidade e a atuação da equipe envolvida na operação.

Do planejamento até a execução de uma operação de Inteligência, devem ser seguidos os princípios básicos abaixo elencados:

Objetividade

O motivo da busca, o objetivo de uma operação de Inteligência, desde o planejamento até a execução, é a obtenção do conhecimento (conhecimentos).

Oportunidade

O instante exato para o início de cada uma das ações de uma operação de Inteligência forma um dos principais aspectos do planejamento e da execução da mesma. Desencadeá-la antes ou depois do momento ideal pode ser fatal para o sucesso da missão.

Segurança

Uma operação de Inteligência, desde o seu planejamento até a execução, deve garantir em todos os seus detalhes a proteção e o sigilo da missão; a proteção da identidade do órgão de Inteligência e da equipe para ela escalada; a proteção física da equipe e do material utilizado, bem como das instalações ou locais onde se realizam e, quiçá, a proteção do alvo da busca.

Clareza

As ordens dadas para as equipes de busca e aos agentes devem ser transmitidas de maneira clara, não deixando qualquer dúvida sobre o desempenho de cada membro do grupo. Deve-se definir, portanto, com a mais absoluta precisão, aquilo que se deseja fazer, como fazer, quando fazer e quem vai executar a ação.

Simplicidade

Cumpridos os requisitos necessários à segurança e à flexibilidade a que deve obedecer uma operação de Inteligência, esta deve ser planejada e executada da maneira mais simples possível.

Com certeza, todas as ações planejadas com simplicidade são executadas com facilidade, culminando em maior segurança e economia na utilização dos recursos humanos e materiais.

Flexibilidade

Quando se planeja uma operação de Inteligência não se deve subestimar a ocorrência de eventualidades antes ou durante a sua execução. Desta forma, deve-se ter linhas de ação alternativa, bem como oportunizar às equipes executantes uma razoável margem de iniciativa.

Economia

Ao planejar e executar uma operação de Inteligência, deve-se ter em mente a maior economia possível no emprego dos recursos humanos e materiais, sem que ocorram prejuízos para os demais requisitos fundamentais.

4.1 Objetivo de uma operação de Inteligência

O objetivo de uma operação de Inteligência é, normalmente, a busca do dado negado, aquele que não está disponível pelas fontes ostensivas.

Branco (2011, p.153) nos fala sobre o conceito de “dado negado”.

> Dado negado é aquele que está sob proteção de seu detentor e cuja obtenção, pelo órgão de Inteligência, exige o emprego de técnicas operacionais.

O mais comum é que as operações de ISP sejam desenvolvidas em favor do ramo tático de ISP, em que o setor de operações ficará em condições de ser acionado pelo setor de análise da Agência de Inteligência.

Os alvos de uma operação podem ser: uma pessoa, um documento, objetos, locais, uma foto, croqui etc. Esse alvo poderá ser alcançado através de ações de busca e técnicas operacionais.

Branco (2011, p.158) nos lembra que as seguintes modalidades são consideradas, pela DNISP, como ações de busca: o reconhecimento, a vigilância, o recrutamento operacional, a infiltração, a desinformação, a provocação, a entrevista, a entrada e a interceptação de sinais e de dados.

Branco diz também (p.161) que “técnicas operacionais” 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 técnicas operacionais são instrumentos necessários à superação de obstáculos para obter dados negados e neutralizar ações adversas.

E, como exemplo, cita: Processos de Identificação de Pessoas (PIP); Observação, Memorização e Descrição (OMD); Estória-Cobertura (EC); Disfarce; Comunicações Sigilosas (ComSig); Emprego de Meios Eletrônicos (EME*)*, dentre outras.

4.2 Planejamento de operações

É a elaboração lógica do raciocínio, empregando método determinado, que objetiva orientar a execução de uma operação de Inteligência.

Objetivos

- Orientar e assegurar a execução.
- Proteger a identidade do Órgão de Inteligência.
- Proteger a identidade e a atuação da equipe de serviço.

Elementos essenciais

- Missão de acordo com as necessidades do Órgão de Inteligência.
- Alvo.
- Ambiente Operacional.
- Meios:
  - » Pessoal
  - » Material

4.3 Relatório do agente ou da missão

É a exposição dos fatos ocorridos, observados ou obtidos pelo agente no decorrer das suas atividades. Trata-se de um documento de caráter interno que é usado nas ligações do agente ou da equipe de agentes com o Encarregado de Caso (EC), que é o responsável pela operação. Pode ser apresentado tanto oralmente como por escrito; individualmente ou em grupo.

Seção 5
A polícia e as tecnologias da Inteligência

> *O rádio-comunicador, a viatura operacional e, mais recentemente, o computador, têm cultivado a ideia de que a tecnologia vai livrar as organizações policiais do peso de ter que lidar diretamente com a confusa condição humana.*
> (Peter K. Manning)

Para Manning (2003, p. 375), as organizações policiais vêm almejando de longa data que a **tecnologia** possa tornar mais fácil a sua árdua missão, principalmente nos pontos que mais as incomodam. Os mais recentes *hardwares* e *softwares* despontam como os componentes mais inovadores em tecnologia. Para o perfeito cumprimento da missão, as organizações policiais necessitam de **informações**, tendo na população a sua fonte básica. Compreender como as organizações policiais obtêm, processam, codificam, decodificam e usam as informações possibilita compreender as suas funções.

Manning (2003, p. 375) prossegue afirmando que:

Teoria geral e/ou estudo sistemático sobre técnicas, processos, métodos, meios e instrumentos de um ou mais ofícios ou domínios da atividade humana, tais como indústria, ciência, informática etc. O Webster's Collegiate Dictionary apud Manning (2003, p. 379), "define tecnologia como uma linguagem técnica, uma ciência aplicada e como meios técnicos para se chegar a um objetivo prático. E explica o conceito associando à tecnologia a totalidade de meios empregados para fornecer os objetos necessários ao sustento e ao conforto humanos".

Há pelo menos três tipos de informações policiais (primária, secundária e terciária), inteligência (prospectiva, retrospectiva e aplicada) e estratégias operacionais (preventiva, proativa e reativa), cada uma das quais interage de forma complexa com a tecnologia.

A atividade policial, em especial a desenvolvida pelo policial que atua nas ruas, aliada às **culturas ocupacionais do policiamento**, modela este processo de modo significativo. A **tecnologia** dá forma às organizações e por elas é moldada em virtude de estar arraigada na organização social.

5.1 Fontes de informação

Segundo Manning (2003, p. 384-385), a informação passa a ter sentido por intermédio das atividades desenvolvidas pela organização policial. "Os quatro tipos principais de fontes de informações são: o público em geral; os sistemas de organização e de alarme; outras fontes policiais; e as elites externas".

Manning (2003, p. 385) prossegue:

> A maior parte das informações vem do público em geral (Reiss, 1971; Goldstein, 1990, pp.8-10). A tendência do público em geral para relatar é geralmente limitada pela sua disposição em relatar, pelas condições que determinam o acesso ao telefone, ao número de telefones *per capita*, à propensão em usá-los e à natureza do evento que vai ser relatado ((SPELMAN; BROWN, 1981). Acredita-se menos na informação originada no cidadão, que é mais diversificada, cuja triagem e avaliação – pela "linha de frente final" da organização policial, pelos operadores e encarregados do despacho – é mais rigorosa. Dadas as condições sociais que ipificam o chamado, o objetivo maior dos sistemas de comunicação da polícia é reduzir o potencial de sobrecarga dos chamados dos cidadãos (MANNING, 1989).
> O negócio interno da polícia constitui uma grande parte da carga total de informação da polícia.
> Os chamados dos sistemas de alarmes – dos quais 90% são alarmes falsos – permanecem um importante fator na carga de trabalho e uma fonte de informação potencial. Pouco se sabe sobre as influências da elite ou sobre os padrões de comunicação com a administração da polícia.

Quais os tipos de informação?

De acordo com Manning (2003, p. 385-387), “a informação recebida (e trabalhada) pela polícia pode ser dividida em três tipos”:

> A **informação primária** é aquela que primeiro chega à atenção da polícia ou a que foi processada por uma única unidade. Um exemplo é um material que um patrulheiro escreve no relatório do carro, sobre uma resposta a um pedido de serviço. Fala sobre isso com outro policial, mesmo um detetive, mantém essa informação primária, até que tenha sido alterada ou transformada em seu formato e mudado de lugar dentro da organização. A informação primária domina quase todas as funções da polícia. Unidades como as de patrulha e trânsito são mais dependentes de informações provenientes dos cidadãos e fornecem a maior parte das “novas informações”, como um resultado de seus bloqueios, inquirições e observações e de quaisquer enfretamentos que eles tenham iniciado por conta própria. De acordo com várias fontes, cerca de 86% da carga de trabalho da polícia, um índice geral de informações, surge dos chamados dos cidadãos (Reiss, 1971, p. 11). Outras divisões funcionais da polícia recebem menos informações primárias do que as patrulhas. Não se sabe a diferença total, pois não são mantidos relatórios dos chamados feitos às unidades de detetives, drogas ou juvenis, a não ser que o chamado resulte em uma investigação.

Manning (2003, p. 401) afirma que “as modificações no processamento da informação primária tem sido o enfoque de muitos sistemas de comunicação da polícia”. Isso inclui a coleta de chamadas por meio de uma central com número único, como, por exemplo, o popular telefone 190 da Central de Emergência ou Central de Operações Policiais Militares (COPOM), ou o telefone 193 do Corpo de Bombeiros, dentre outros mais utilizados para emergências. Neste campo, incluem-se os despachos efetuados com o auxílio do computador, o sistema de rastreamento de chamadas e o acesso mais amplo a dados ou à rede.

> A **informação secundária** é a que foi processada uma ou mais vezes por duas unidades quaisquer dentro da polícia e mudou tanto de lugar como de formato. Um exemplo é o movimento do relatório de um crime, de um policial para o escritório dos detetives. Esta informação muda sua localização e seu formato. Se um detetive trabalha com a informação falada, dada por um patrulheiro, ela permanece uma informação primária porque está sendo processada a partir do ponto de vista oficial da organização e não mudou de formato. As variações sobre este tema se tornam muito complexas. Quando a informação dá uma volta, indo do trabalho do patrulheiro para o trabalho do detetive e voltando, é uma informação secundária, pois foi processada.

> Na teoria, essas voltas podem ser infinitas, produzindo múltiplas informações processadas secundárias. As informações secundárias estão presentes em todas as áreas funcionais do policiamento, tanto do pessoal interno como dos que estão nas ruas, mas se concentram no trabalho com os detetives, com adolescentes e com drogas, pois uma grande parte dele é baseado em informações recebidas e passadas adiante pelos patrulheiros ou policiais de trânsito.

Referente às **informações secundárias**, Manning (2003, p. 407) diz que "um sistema de informações baseado em computadores pode fornecer dados analiticamente reduzidos e ordenados, que informem as modificações nas operações da polícia".

O emprego do computador permitirá a aplicação de técnicas a fim de auxiliar na administração da polícia no tocante aos dados secundários e terciários.

Manning (2003, p. 407) registra, ainda, que

> Inovações significativas na criação e uso de informações secundárias incluem uma série de softwares que, além da patrulha e das respostas aos pedidos de serviços dos cidadãos, afetam outras funções da polícia.
>
> **Informações terciárias** são aquelas processadas por duas unidades quaisquer e que mudaram de formato pelo menos uma vez. Quando a informação mudou de formato mais de uma vez, e de lugar mais de uma vez, ela permanece informação terciária processada. Por exemplo, a informação processada por uma única unidade, como a informação que se move da divisão de patrulha para a unidade de detetives, segue para a unidade de assuntos internos e volta para a patrulha, permanece uma informação terciária depois de processada pelos assuntos internos, embora agora esteja localizada em uma divisão de patrulha. Desta perspectiva, a informação não pode voltar à forma anterior. A informação terciária é o território da administração da polícia (os sargentos e os que estão acima deles). A administração da polícia exerce autoridade baseada nas informações terciárias que foram processadas duas vezes, pelas unidades que tal administração reinvidica, ou pretende dirigir, comandar e controlar.

Conforme Manning (2003, p. 408), "raramente são encontradas informações terciárias no policiamento e, quando disponíveis, raramente são usadas". Usa-se no controle dos escalões inferiores da hierarquia da organização policial.

O gerenciamento de tecnologia da informação tem sido empregado na administração da organização policial; na administração de informações; na manutenção de registros e na administração interna; no fluxo rotineiro de trabalho ou nos sistemas de controle dos procedimentos; e no armazenamento e recuperação de dados.

O dia 16 de dezembro de 2004 foi marcado com o lançamento oficial da nova REDE INFOSEG, que passou a integrar as Informações de Segurança Pública, Justiça e de Fiscalização em todo o Brasil. A rede, formada pela integração de um conjunto de bases de dados distribuídos pelos Estados da Federação e por órgãos do governo federal, tem por finalidade a disponibilização das informações contidas em qualquer base integrante ao usuário. O sistema, em seu projeto inicial, possuía uma arquitetura que dificultava a integração das bases de dados devido à utilização de tecnologias proprietárias que acarretavam um alto custo de implantação para as Unidades da Federação e impossibilitavam a difusão de acessos em outros dispositivos, como também somente poderia ser acessada através de intranet, além de ter uma infraestrutura precária tanto de lógica como de força (elétrica).

Outro fator determinante para o insucesso do projeto inicial era a forma de alimentação do Índice Nacional, que abastecia a atualização dos dados manualmente, ficando a cargo dos Estados-Membros o envio das informações por meio de um processo altamente precário.

O antigo sistema INFOSEG acabava tendo um Índice Nacional quase que totalmente desatualizado, longe de refletir as informações contidas nas bases estaduais, provocando total descrédito.

Em razão dos problemas encontrados, a administração da SENASP/MJ decidiu por reestruturar totalmente o projeto, adotando uma nova arquitetura dentro de padrões de interoperabilidade do governo eletrônico (*E-ping*) e objetivando a difusão de acesso em outros dispositivos, tais como viaturas policiais, *palmtops* e celulares. Foram também desenvolvidas soluções para os módulos de atualização e consulta em tempo real (online), de forma a tornar o sistema flexível, fácil de integrar e, principalmente, confiável.

A partir de 2004, a SENASP/MJ passou a trabalhar com a filosofia de **rede***,* e todas as ações necessárias para o desenvolvimento das novas soluções definidas no projeto de arquitetura e concepção foram executadas em conjunto com os Estados, Distrito Federal e os órgãos federais conveniados, de forma a integrar os módulos da nova rede em todo o país.

Foi desenvolvido o módulo central do sistema na nova plataforma, denominado módulo integrador, permitindo a consulta aos dados básicos de indivíduos e utilizando a pesquisa fonética, que possibilita uma maior precisão no retorno das consultas.

O módulo de administração e auditoria também foi todo reformulado.

O módulo de atualização em tempo real foi liberado para os Estados a fim de que se iniciasse a integração da nova forma de atualização nos 27 Estados da Federação a partir de junho de 2004.

As Unidades da Federação iniciaram as atividades para a integração de suas bases no módulo de atualização em tempo real, e no início de dezembro de 2004, 15 Estados já estavam integrados, atualizando-se de forma online. O Poder Judiciário já iniciou os trabalhos de integração ao módulo de atualização e consulta, e hoje já é possível visualizar na consulta de indivíduos dados da base da Justiça Federal.

Os Estados já começaram a integração com o módulo de consulta, permitindo a visualização do detalhamento das informações nas bases das Unidades da Federação e a consulta via aplicações estaduais.

> **!** Os módulos de consulta aos sistemas Registro Nacional de Chassi (RENACH), Registro Nacional de Veículos Automotores (RENAVAM) e Sistema Nacional de Armas (SINARM) também foram migrados para a nova plataforma, fortalecendo o conceito da nova REDE INFOSEG.

Foram também adquiridos novos servidores, links e infraestrutura para o novo CPD da REDE INFOSEG, além de ser instalado um moderno sistema de segurança física que utiliza câmeras, vídeofone, e autenticação biométrica.

Este resultado só está sendo possível por conta do apoio de todos os Estados, do Distrito Federal, da Polícia Federal, da Polícia Rodoviária Federal e da Receita Federal do Brasil.

O processo de recadastramento dos usuários da nova REDE e a integração do módulo de consultas nas 27 Unidades da Federação também já está em andamento. Outros sistemas de interesse da Segurança Pública, Justiça e de órgão de fiscalização também estão sendo integrados à nova REDE INFOSEG, além do Exército Brasileiro (SIGMA), da Receita Federal (CPF e CNPJ) e do Superior Tribunal de Justiça e da Justiça Federal (ENCLA).

Por derradeiro, é importante ressaltar que a nova REDE INFOSEG já está funcionando via internet, permitindo uma maior acessibilidade a qualquer Operador da Segurança Pública, da Justiça ou da Fiscalização, em qualquer parte do mundo onde consiga acesso à internet. (INFOSEG, 2010).

Quais as estratégias operacionais da polícia e da inteligência?

Prosseguindo na sua obra, Manning (2003, p. 391) afirma que: “a organização das polícias urbanas anglo-americanas resulta de práticas tradicionais e da capacidade diferencial da polícia, de forma seletiva, para conhecer ou encontrar a informação”.

Tal modelo de organização, juntamente com a forma e o conteúdo da tomada de decisões e do fluxo de informações, dá forma à interação entre o processamento de informações e as estratégias operacionais da polícia.

Polícias urbanas anglo-americanas ou anglo-saxônicas

Segundo Brewer (apud MARCINEIRO et al, 2005, p. 63-64), “o modelo da polícia anglo-saxônica é o mais comum de ser encontrado nas democracias liberais” e parte de uma filosofia reativa, limitando-se a atender às situações de emergência quando for acionada para atender a uma ocorrência policial. Seus integrantes podem até participar do cotidiano da comunidade, porém, isto não seria objeto da organização; não existiria uma interação, permitindo detectar sinais de anormalidade e agir com antecipação. Desta forma, a polícia acaba tornando-se uma agência da administração pública, fundamentada mais na autoridade legal que na moral.

Ainda segundo Manning (2003, p. 392), “a inteligência policial – ou a informação sistematizada, classificada e analisada, que foi codificada em categorias relevantes para a polícia – adquire três formas”:

> A ***inteligência prospectiva*** é a informação coletada antes de um crime ou problema, com base na identificação de alvos selecionados e com o desenvolvimento de alguma “teoria” de base social, ou pela compreensão da natureza, da aparência e da freqüência do fenômeno a ser controlado. Um exemplo é a estratégia de identificação de criminosos profissionais pela polícia de Washington, DC. Muito pouco deste tipo de evidência é coletado sistematicamente, de modo que possa ser considerada como “inteligência prospectiva”.
>
> A ***inteligência retrospectiva*** é a informação que resulta do curso normal do trabalho policial; por exemplo, dos arquivos de prisões, das violações de trânsito e dos mandados de prisão pendentes. Após um assalto ou furto em que os suspeitos foram pegos, pode-se procurar informações nas atividades anteriores, com o objetivo de investigar ou de juntar dados de apoio. Pode ser difícil juntar dados relevantes para um determinado crime. Apesar de qualquer departamento de polícia estar inundado por arquivos, registros, evidências e papéis, não existe um ***“sistema de metainformações”*** central para guardar, recuperar ou cruzar todos esses dados. O uso é dependente da boa memória individual de policiais, do julgamento perspicaz e da paciência.

Por exemplo, nenhum sistema articula os casos dos detetives, os registros dos adolescentes, os arquivos das unidades de vício e narcóticos (p. ex. alcunhas, *modus operandi* , informantes, casos atuais e passados), os registros de prisões dos departamentos, acusações atuais e passadas, fitas gravadas do setor de despacho, arquivos de mensagens telefônicas e arquivos da inteligência.

A ***inteligência aplicada*** é significativa quando há evidências sobre os suspeitos. A inteligência aplicada busca associar nomes de suspeitos já anteriormente conhecidos com atos conhecidos, ou é usada para conectá-los. O uso da inteligência aplicada pode exigir dados processados analiticamente, tais como material forense e trabalho de inferência ligando suspeitos a hora, lugar, oportunidade, motivo e outros. ***O uso criativo da inteligência aplicada é a base para os grandes filmes de detetives***, mas é surpreendentemente ausente no dia-a-dia do trabalho dos detetives.

5.2 Sistema de metainformações, metaconhecimento, ou Inteligência Artificial

Alguns estudiosos acham promissores os Sistemas de Informações mais sofisticados e complexos – baseados em aplicações da inteligência artificial ou 'metaconhecimento' (conhecimento sobre o conhecimento). Hernandez (1989 apud MANNING, 2003, p. 409) sugere que a inteligência artificial pode ser usada para criar perfis de vilões e de redes de associações criminosas em caso de drogas, mas observa que nenhum sistema desse tipo estava em uso quando escreveu a respeito.

Continuando seus estudos, Manning (2003, p. 393) esclarece que "As estratégias operacionais da polícia interagem com as necessidades da inteligência e moldam os tipos de informações de inteligência que são desenvolvidas e preservadas".

Quando emprega **estratégias preventivas**, a polícia necessita de inteligência considerável, baseada no comportamento passado e potencial de indivíduos ou grupos. Isso significa coletar e analisar tanto a inteligência prospectiva como a retrospectiva. Entretanto, tal tipo de informação de inteligência é quase sempre considerado irrelevante para os objetivos tácitos e inespecíficos do policiamento. Como resultado, as unidades responsáveis pelas funções de inteligência prospectiva, tais como as unidades de relações da comunidade com a polícia e as de prevenção do crime, são vistas como tendo um *status* inferior e sendo marginais e subordinadas ao policiamento tradicional, baseado nas patrulhas, para interromper o crime.

Quando a polícia usa **estratégias proativas**, em teoria, confia na inteligência prospectiva que lhe permite predizer eventos ou planejar-se para eles. Entretanto, as organizações policiais como um todo não fazem planos de longo prazo. Isso tem mudado, e o crescimento de "operações usando disfarce" [*sting operations*] é certamente uma sugestão das tendências no desenvolvimento de estratégias proativas.

As estratégias reativas criam inteligência retrospectiva e surgem dela. Alguma inteligência aplicada pode ser usada quando o incidente está sujeito a verificações por meio de históricos criminais automáticos, registros de automóveis e mandados de prisão pendentes. É claro que, na ausência de mudanças na política ou no comando, a predominância de estratégias reativas e de inteligência retrospectiva significa que cada policial cria seu próprio banco de dados, ou capacidade de inteligência, e trabalha autonomamente.

> **!** Manning (2003) realizou os seus estudos com base nas unidades de polícia dos Estados Unidos. Mesmo retratando outra realidade, estes estudos relevantes e atuais no campo da Segurança Pública devem ser trazidos ao âmbito dos debates das diversas polícias existentes no Brasil. Inúmeros autores têm, através dos seus estudos, demonstrado que a formação do policial brasileiro é voltada essencialmente para a área jurídica. Devemos, portanto, voltar-nos também para outras áreas tão importantes para a Segurança Pública, tais como a administração policial, a polícia comunitária, as técnicas de investigação e de avaliação do trabalho policial, a Inteligência e a Contrainteligência policial, dentre outras.

Neste capítulo, você conheceu a metodologia para a produção do conhecimento utilizado pelas Agências de Inteligência. Conheceu a Contrainteligência e as medidas necessárias para a segurança plena do exercício da Atividade de Inteligência. Por último, manteve contato com as Tecnologias da Inteligência que são utilizadas pelas organizações policiais.

Recomendação de segurança: Os agentes responsáveis pela custódia de documentos, conhecimentos, materiais, áreas, comunicações, operações e sistemas de informação de natureza sigilosa estão sujeitos às regras referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico.

Capítulo 5

Segurança da informação: uma visão macro de projeto

Habilidades

Capacitar o aluno com ensinamentos teóricos e metodologia adequada para dominar técnicas de proteção da informação, trabalhando em equipe, com senso crítico e responsabilidade.

Seções de estudo

Seção 1: A importância da segurança da informação

Seção 2: Solução de segurança (ISO 27001)

Seção 3: Seleção de controles para uma política de segurança

Seção 4: Auditoria na Informática

Seção 1
A importância da segurança na informação

No capítulo 4, você estudou sobre segurança da informação, e neste capítulo você vai aprofundar um pouco mais os conhecimentos estudando sua importância, soluções e seleção de controle para uma política de segurança. Comecemos estudando a história.

No decorrer dos anos, a informação vem aumentando cada vez mais o seu valor. A gerência, a velocidade da troca e a segurança de informações são fatores preponderantes no sucesso de uma organização. Este capítulo visa conceituar segurança da informação e apresentar como uma solução para esse problema.

A segurança em sistemas computacionais não é formada somente por dispositivos que objetivam proteger as suas informações ou recursos, mas também de metodologias e técnicas que tentam manter as propriedades de um sistema. Ela é obtida a partir da implementação de um conjunto adequado de processos (ex: políticas, práticas, procedimentos, estruturas organizacionais e funções de software), que garante que os objetivos específicos de segurança de uma organização sejam obtidos.

Várias definições de segurança podem ser achadas na literatura, mas, segundo Landwehr (2001), segurança pode ser vista como uma disciplina de procedimentos e políticas que torna livre o sistema computacional de ameaças.

Segundo Russel, Gangemi (1992), e Bishop (2003), a segurança possui três propriedades fundamentais:

- **confidencialidade** - a segurança de um sistema computacional não deve admitir que informações sejam descobertas por qualquer pessoa não autorizada. A confidencialidade garante a privacidade das informações sensíveis em ambientes computacionais;
- **integridade** – a segurança de informação deve sempre manter a integridade da informação armazenada. Logo, manter a integridade dos dados de um sistema significa que estes não terão as suas informações corrompidas, seja de forma acidental ou intencional, via pessoas não autorizadas. A autenticação consiste numa forma de verificar a origem do dado (quem enviou ou quem introduziu o dado no sistema); e
- **disponibilidade** – consiste na capacidade de manter disponível para os usuários do sistema os dispositivos de software e hardware. O oposto da disponibilidade é o DoS (*Denial of Service*).

Além dessas três propriedades, alguns autores acrescentam a **autenticidade** (LANDWEHR, 2001), que procura garantir que as informações provenientes de uma fonte sejam genuínas.

> Então, para nosso estudo adotaremos as quatro propriedades da informação: disponibilidade, integridade, confidencialidade e autenticidade.

Nesta primeira seção, serão apresentados alguns aspectos que podem justificar o uso da segurança da informação em organizações. A informação e os seus processos de suporte, os sistemas e as redes são importantes bens do negócio. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para a linha de negócio competitiva, o fluxo de capital, a utilidade, a conformidade legal e a imagem comercial. (FRASER, 1997).

Outro aspecto relevante é a dependência das organizações dos sistemas de informações e serviços, deixando-as mais vulneráveis às ameaças de segurança. A interconexão de redes públicas e privadas e o compartilhamento dos recursos de informação aumentam a dificuldade de se ter um controle de acesso realmente eficiente. A tendência da computação distribuída tem enfraquecido a eficiência do controle central especializado. Muitos sistemas de informação não foram projetados para implementar segurança. Sendo assim, a segurança que se pode ter através de meios técnicos é limitada, e deve ser suportada com procedimentos e gerenciamento apropriado.

Outros aspectos poderiam ser citados, mas deve-se ter em mente que não existem sistemas totalmente seguros; a segurança da informação possibilita apenas minimizar os riscos existentes.

1.1 Aspectos conceituais

Corresponde em burlar de alguma forma a segurança de sistemas computacionais.

As **violações de segurança** são em decorrência das vulnerabilidades, ameaças e ataques em sistemas computacionais. (BISHOP, 2003; RUSSEL e GANGEMI, 1992).

1.2 Vulnerabilidade

Todo sistema computacional é vulnerável a ataques. Políticas e produtos de segurança podem reduzir a probabilidade de que um ataque seja capaz de penetrar nas defesas do seu sistema ou podem gastar o tempo de intrusos que tentam investir contra o seu sistema.

Os seguintes pontos de vulnerabilidades podem ser citados:

- **físicos** - acessos indevidos a compartimentos que guardam computadores com informações sensíveis do seu sistema;
- **naturais** - computares são vulneráveis a desastres naturais (fogo, enchentes etc);
- **de hardware e software** - certos tipos de hardware falham e podem comprometer a segurança de um sistema computacional por inteiro (alguns sistemas oferecem segurança via estrutura da memória - acesso privilegiado ou não - se esta proteção falha, o sistema é todo comprometido). Falhas de desenvolvimento de sistemas, deixando portas de entrada abertas, podem afetar a segurança do sistema como um todo;
- **de emanação** - equipamentos eletrônicos podem emitir radiação elétrica e eletromagnética, interceptando os sinais provenientes de enlaces existentes em redes de computadores;
- **de comunicações** - se o computador está fisicamente conectado a uma rede, ou conectado a uma rede telefônica, existe grande probabilidade de ele sofrer um ataque; e
- **humanas** - as pessoas que administram ou usam o seu sistema. A segurança do sistema está quase sempre nas mãos do seu administrador.

A ameaça, segundo Bishop (2003), pode ser definida como uma violação potencial da segurança. As ameaças podem ser apresentadas de três formas:

- **naturais e físicas** – estas ameaças colocam em perigo a estrutura física e parte dos equipamentos. São exemplos desses tipos de ameaças: incêndio, enchente, falhas de energia, entre outros. Não se podem sempre prevenir esses tipos de acidentes, mas pode-se ter conhecimento do acidente de forma rápida, evitando danos ainda maiores (ex: alarmes contra incêndio). Dentro da política de segurança pode existir um plano para desastres (replicação da planta fisicamente posicionada remotamente);
- **não intencionais** – são as ameaças provenientes por ignorância de operacionalidade do sistema (ex: um administrador de sistema não bem treinado pode executar uma operação que afete a disponibilidade de um recurso de rede);

- **intencionais** – são as ameaças provenientes de atos programados por pessoas (intrusos) ou produtos utilizados. Estes intrusos podem ser classificados em: agentes inimigos, terroristas, *crackers*, criminosos e corporações criminosas.

1.3 Ataques

Ataques, segundo Bishop (2003), são ações que concretizam as ameaças a um sistema computacional. Alguns tipos de ataques podem ser apresentados, conforme McGlure (2000), e classificados em:

1.3.1 Tipo físico

- **Investigação do lixo** (*Dumpster diving, Trashing*) – é um tipo de ataque à segurança bastante simples, que consiste em procurar nas latas de lixo das organizações papéis ou outras fontes, jogadas fora, sem um devido tratamento quanto à segurança. É um tipo de ataque considerado legal, pois parte-se da premissa que coisas encontradas num repositório de lixo não possuem mais utilização. É um método utilizado há muitos anos para se conseguir informações importantes.
- **Escuta telefônica** (*Wiretapping*) e emanações eletromagnéticas – consiste em ataques que realizam escutas em meios físicos. Existem dois tipos de escuta:
  - » passiva - este tipo de escuta ameaça a confidencialidade da informação. Utiliza normalmente tecnologia de grampo com fio ou interceptação via rádio, em que as informações coletadas são analisadas via software ou outra tecnologia. Tem como objetivo somente a coleta, não alterando o conteúdo das informações; e
  - » ativa - este tipo de escuta ameaça a autenticidade da informação transmitida. Esta metodologia envolve a quebra da comunicação, modificando de forma deliberada a informação. O intruso pode alterar a origem da mensagem ou então o destino da mensagem, substituindo o conteúdo da mesma.

1.3.2 Tipo pessoal

Este tipo de ataque envolve basicamente o fator humano, isto é, as diversas falhas apresentadas pelo ser humano. Pode-se dividir em:

- **Engenharia social** - é a forma de ataque que consiste em obter informações importantes que possibilitem ataques, utilizando a comunicação oral ou escrita como sua principal arma. Este ataque está diretamente ligado à capacidade do elemento em coletar as informações de alvos preestabelecidos (padrões de comportamento de pessoas, preferências sexuais, insatisfação com a atividade exercida etc).
- **Mascaramento** (*Masquerading*) - este tipo de quebra de segurança ocorre quando uma pessoa usa a identidade de outra para ter acesso a um computador, podendo ser feito no próprio local ou de modo remoto.

1.3.3 Ataques a comunicações e dados

Chamados de ataques de **Negação de Serviço** (*Denial of Service – DoS*), são ataques realizados a provedores de acesso ou redes corporativas, que têm como objetivo paralisar a rede inteira por um período de tempo ou determinados serviços que dependam de dispositivos específicos da rede. Logo, o objetivo é bastante claro: tirar os *hosts* de ação na internet.

Este tipo de ataque pode ser classificado em:

- ***Syn Flooding*** (Inundação Syn) – é um ataque de *flood* que usa a característica de conexão do protocolo TCP como uma arma.
- ***TearDrop I, II, NewTear, Bonk e Boink*** – consiste em enviar um par de fragmentos de IP maliciosos que são recebidos como um datagrama UDP inválido pelo computador da vítima, causando um estado de instabilidade na mesma.

1.3.4 Ataques a textos cifrados

- **Texto cifrado** - o atacante possui uma grande quantidade de mensagens cifradas, não conhece as mensagens originais e nem as chaves utilizadas.
- **Texto conhecido** (*Known-Plain/text*) - o atacante possui grande quantidade de mensagens cifradas e conhece as mensagens originais equivalentes.

Seção 2
Solução de segurança (ISO 27001)

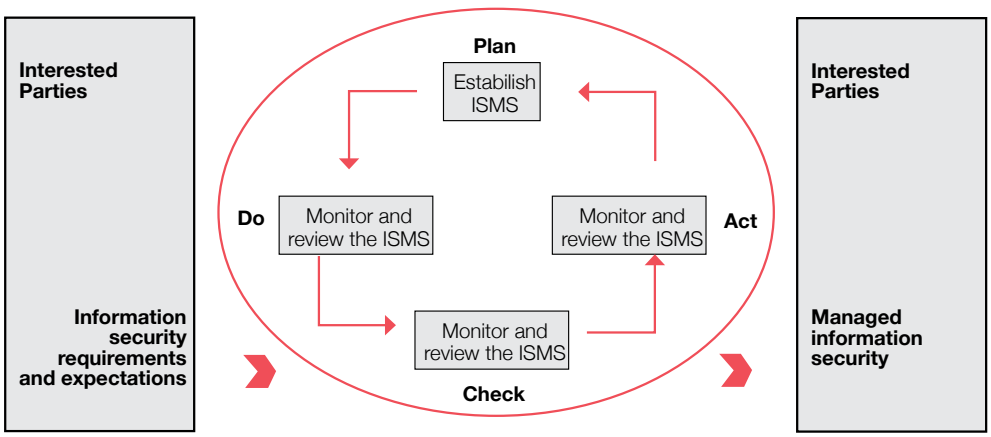
A ISO 27001 é um padrão internacional que provê um modelo para estabelecer, implementar, operar, monitorar, revisar e melhorar o SGSI (Sistema de Gerenciamento de Segurança da Informação).

O **SGSI** consiste em uma parte do sistema global de gerenciamento, baseado no risco do negócio (ou da atividade da organização), para estabelecer, implementar, operar, monitorar, revisar e melhorar a segurança da informação.

O sistema inclui a estrutura organizacional, políticas, atividades de planejamento, procedimentos, processos e recursos.

Veja abaixo a estrutura do modelo PDCA e as explicações sobre suas fases a seguir:

Figura 5.1 – Modelo PDCA



Fonte: ISO/IEC 27001.

- ***Plan*** (estabelecer o SGSI) – estabelecer a política, os objetivos, os processos e os procedimentos relevantes ao gerenciamento de risco, melhorando assim a segurança da informação, provendo resultados em concordância com os objetivos e as políticas globais da organização;
- ***Do*** (implementar e operar) – implementa e opera a política, os controles, os processos e os procedimentos do SGSI;
- ***Check*** (monitorar e rever o SGSI) – avaliar o desempenho dos processos, da política, dos objetivos e da experiência prática e reportar os resultados ao gerenciamento para a revisão; e
- ***Act*** (preservar e melhorar) – realizar ações preventivas e corretivas com base nos resultados da auditoria do SGSI e rever o gerenciamento ou outra informação relevante para manter uma melhora contínua do SGSI.

Pode-se constatar que a segurança é uma tarefa complexa, composta de várias partes, em que erros são fáceis de acontecer, impedindo de se ter um ambiente computacional seguro. Estes erros podem ocasionar grandes perdas para uma instituição, sendo então necessária uma verificação da infraestrutura de segurança, e um dos métodos para essa verificação é a auditoria da segurança. O item que segue apresenta uma visão do que é uma política de segurança da informação, como planejá-la, projetá-la e auditá-la.

2.1 Política de segurança

2.1.1 Conceitos básicos

Política de segurança da informação pode ser definida como um conjunto de regras de segurança de acesso físico e lógico às informações contidas em um sistema de computação. O objetivo de uma política de segurança da informação é fornecer as diretivas de gerenciamento e suporte à segurança da informação.

As regras são estabelecidas de acordo com as possíveis ameaças que o sistema de computação possa vir a sofrer. Com a política implantada, tem-se condição de saber o quanto a sua rede é segura ou não, o quanto de funcionalidade essa rede oferece e o quanto é fácil operá-la.

Para que as regras de segurança sejam bem estabelecidas, necessita-se conhecer os objetivos da segurança, pois, de posse dessa informação, pode-se definir, por exemplo, quais ferramentas serão utilizadas.

Os objetivos do administrador de segurança são diferentes do utilizador do sistema, pois não há como negar que aquele estará sempre mais preocupado e empenhado no cumprimento das normas do que os últimos, os servidores.

Logo, os objetivos da segurança estarão baseados nos seguintes aspectos (FRASE, 1997):

- serviços oferecidos *versus* segurança – para cada serviço oferecido ao usuário, deve-se analisar o risco de segurança. Realiza-se uma análise para se saber se vale a pena ou não manter o serviço;
- facilidade de uso *versus* segurança – o quanto a segurança atrapalhará a vida do usuário? Pode-se citar como exemplo o uso de senhas. Torna o sistema, talvez, menos conveniente para o usuário, porém, mais seguro. O equilíbrio é o segredo;
- custo da segurança *versus* risco de perda – os custos financeiros, de desempenho e de facilidade de uso, devem ser analisados quanto ao risco de perda de privacidade e de serviço, por exemplo.

2.1.2 Pessoal envolvido na política de segurança

Para que uma política de segurança torne-se apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de servidores dentro da organização. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança; caso contrário, haverá pouca chance que ela tenha o impacto desejado. Durante a criação da política de segurança, as seguintes pessoas devem ser envolvidas:

- administrador de segurança do site;
- pessoal de desenvolvimento;
- gestores de diferentes níveis;
- gerente da rede/segurança;
- usuários afetos à política;
- pessoal jurídico.

2.1.3 Uma boa política de segurança

Uma boa política de segurança:

- deve ser capaz de ser implementada tecnicamente;
- deve ser capaz de ser implementada organizacionalmente;
- deve definir, claramente, as áreas de responsabilidade dos usuários, administradores de sistemas e gerentes de sistemas e negócios;
- deve ser rígida, fazendo uso de ferramentas de segurança onde forem necessárias e de ações punitivas onde não se puder aplicar a tecnologia;
- deve ser flexível e adaptável às mudanças de ambientes;
- deve ser implementada via procedimentos, descritos em manual.

Os componentes de uma boa política de segurança incluem:

- **normas para aquisição de tecnologia computacional** – especificam as características de segurança necessárias ou ideais, assessorando na aquisição de dispositivos de hardware e software;
- **política de privacidade** – define as expectativas em relação à privacidade do tráfego de e-mails, arquivos *logs* e arquivos dos usuários;

- **política de responsabilidade** – define as responsabilidades dos usuários, as operações, servidores e gestores. Pode especificar a forma de auditoria e normas para agir no caso de incidentes de invasão (o que fazer e quem chamar no caso de intrusos detectados);
- **política de acesso** – define os direitos de acesso e privilégios para proteger as informações de perdas ou revelações, especificando as normas de uso para os usuários, para as operações de funcionários e gerentes. Estabelece as normas para conexões externas, comunicações de dados, dispositivos vivos da rede e a instalação de softwares em rede;
- **política de autenticação** – estabelece a confiança do sistema via uma efetiva política de senhas, normas de autenticação de usuários ou dispositivos remotos e a utilização de dispositivos de autenticação;
- **parâmetros de disponibilidade** – estabelecem aos usuários qual a disponibilidade de recursos. Incluem as horas de operação, períodos fora do ar, informações sobre falhas no sistema etc;
- **política de manutenção** – estabelece normas para o pessoal de suporte (interno ou externo) no acesso e na execução das tarefas de manutenção (corretiva ou preventiva) do sistema. Um dos itens a ser abordado é a possibilidade de realizar ou não manutenção no sistema remotamente (ex: COMPAQ acessar o seu ambiente para a realização de manutenção);
- **política de invasões** – define quais tipos de invasão (interna ou externa) são informadas e quem deve conhecer;
- **divulgação de informação** – informa aos servidores de qualquer nível como agir quando questionados por pessoas extra-empresa sobre: incidentes de segurança, informações consideradas confidenciais ou de propriedade de alguém, procedimentos de segurança, entre outras.

Durante a criação de uma política de segurança, não se pode esquecer de trabalhar em paralelo com o setor jurídico da organização, estabelecendo quais os parâmetros legais que podem ser utilizados na implantação da política.

2.1.4 Como validar a política de segurança

- O documento de uma política de segurança somente é válido se houver concordância com os seguintes princípios éticos e condutas padrão (acordo de cavalheiros):
- **responsabilidade profissional** – todos os servidores têm a obrigação de cumprir com as suas metas profissionais dentro da organização sem afetar suas normas de segurança;
- **autoridade legal** – todos os servidores devem respeitar e reconhecer toda a autoridade legal.
- **conflito de interesses** – os servidores devem evitar praticar interesses particulares, obrigações e transações que irão de encontro com os interesses, metas e regulamentos da empresa;
- **confidencialidade** – os servidores devem assegurar que o segredo será mantido com respeito às diversas informações confidenciais tratadas ou manipuladas em relação à organização ou qualquer fato/ato relativo a ela.

2.1.5 Análise de riscos de segurança

Para implementar uma política de segurança faz-se necessário determinar quais riscos a organização está sofrendo para que existam condições de se determinar o que tratar e o que assumir.

O primeiro conceito a ser introduzido é o de **risco**. Ele pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências. Por conseguinte, a gestão de riscos é um elemento central na gestão da estratégia de qualquer organização. Ela consiste no processo em que as organizações analisam os riscos inerentes às respectivas atividades, com o objetivo de atingir uma vantagem sustentada em cada atividade individual bem como em seu conjunto. Uma boa gestão de riscos consiste na identificação e tratamento dos mesmos, acrescentando uma maior sustentabilidade de todas as atividades executadas pela organização. (FERMA, 2002).

A análise de riscos pode ser definida como a combinação da identificação dos itens críticos do sistema, colocando um valor da criticidade em cada item, e da determinação da probabilidade de ocorrer quebras (falhas) na segurança. Ela é dividida nas seguintes fases:

- **identificação dos riscos** - tem como objetivo identificar a exposição de uma organização ao elemento de incerteza, isto é, identificar todos os riscos associados a todas as atividades (estratégicas, operacionais, financeiras, etc) executadas pela organização. Esta identificação exige um conhecimento profundo da organização, do **ambiente** no qual desenvolve a sua atividade, do ambiente jurídico, social, político e cultural em que está inserida, assim como o desenvolvimento de uma sólida interpretação das suas estratégias e objetivos operacionais, incluindo os fatores fundamentais para o seu êxito e as ameaças e oportunidades relativas à obtenção dos referidos objetivos;
- **descrição dos riscos** - o objetivo da descrição dos riscos é apresentar os riscos que foram identificados num formato estruturado;
- **estimativa dos riscos** - a estimativa dos riscos pode ser quantitativa, semi-quantitativa ou qualitativa em termos de probabilidade de ocorrência e possível consequência.

O resultado da análise de risco servirá para estabelecer um **perfil dos riscos**, pois classifica-os quanto a sua importância, e passa a ser uma ferramenta fundamental para as tomadas de decisão quanto aos riscos que serão ou não assumidos, estabelecendo prioridades no seu tratamento. Com base neste resultado, pode-se obter uma avaliação em relação à continuidade do negócio, determinando os diversos segmentos críticos e como eles estão estruturados.

Após determinar os riscos e sua estimativa, existe a necessidade de tratá-los. Este processo consiste na escolha e implementação de medidas para modificar um risco, tendo como principal elemento o controle e/ou diminuição dos riscos.

Seção 3
Seleção de controles para uma política de segurança

Uma vez tendo sido identificados os requisitos de segurança, os controles devem ser selecionados e implementados de forma a garantir que os riscos sejam reduzidos a um nível aceitável. Sua seleção baseia-se em seus custos de implementação, mas levando-se sempre em consideração a redução dos riscos, minimizando, assim, as perdas potenciais no caso de falhas de segurança ocorrerem. Todas as diretivas para o estabelecimento dos controles estão baseadas na ISO 17799.

3.1 Segurança organizacional

A estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação da política de segurança da informação dentro da organização. Um gerenciamento apropriado, com um gerente de projeto, deverá:

- aprovar a política de segurança da informação;
- estabelecer as normas de segurança; e
- coordenar a implementação da segurança através da organização.

Todas as recomendações quanto à segurança devem ser de conhecimento do público interno via publicação de comunicações internas ou afixadas em locais de fácil acesso (ex: quadros de aviso ou Intranet) aos funcionários da organização.

3.1.1 A equipe de gerenciamento da segurança da informação

Uma equipe de gerenciamento de risco deve ser formada para garantir que exista um conjunto claro de normas de segurança e um suporte de gerenciamento necessário à execução destas normas. A equipe possuirá um único gerente que será o responsável por todas as atividades relacionadas com a segurança. A equipe de segurança trata basicamente dos seguintes pontos:

- aprovação e revisão da política de segurança da informação e todas as responsabilidades envolvidas;
- monitoramento das mudanças significativas na exposição dos bens de informação às principais ameaças;
- revisão e monitoramento dos incidentes de segurança;
- aprovação das iniciativas superiores para melhorar a segurança da informação.

3.1.2 A coordenação da segurança da informação

Em uma grande organização a equipe de segurança possui coordenadores em diversos setores e níveis da instituição, com a finalidade de ajudar a coordenar a implementação dos controles de segurança da informação. Algumas atividades estão relacionadas com estes coordenadores, como:

- identificar-se com as regras específicas e responsabilidades para a segurança da informação através da organização;
- dar aval às metodologias específicas e aos processos para a segurança da informação (ex: análise de risco, sistema de classificação seguro);
- respaldar e dar suporte às iniciativas da segurança da informação em toda organização (ex: programa conscientização de segurança).

3.1.3 As atribuições de responsabilidades na segurança da informação

As responsabilidades pela proteção dos bens individuais e a condução dos processos específicos de segurança devem ser claramente definidas. A política de segurança da informação deve ser um guia geral sobre a alocação de regras de segurança e responsabilidades na organização. Esta atividade deve ser suplementada, quando necessário, com normas mais detalhadas para locais específicos, sistemas ou serviços. Uma destas normas chama-se Plano de Segurança Orgânica, que consubstancia todas as medidas dessa subárea da Contrainteligência. Pode, também, ser feito um Plano de Segurança Ativa.

3.2 Segurança de acesso por terceiros

3.2.1 Identificação dos riscos de acesso

Em primeiro lugar, devem-se especificar sempre quais os tipos de acesso que são autorizados. Posteriormente, especificar quais são os componentes referentes a cada tipo.

Os tipos de acesso são:

- **Acesso físico** - escritórios, sala de servidores, estruturas de cabeamento etc.
- **Acesso lógico** - acesso ao banco de dados da organização, sistemas de informação etc.

O acesso à informação e aos recursos de processamento da informação ao pessoal terceirizado não deve ser permitido até que os controles apropriados sejam implementados e os contratos relacionados sejam assinados definindo os termos da conexão ou do acesso.

3.2.2 Requisitos de segurança dos contratos com terceiros

Acordos envolvendo o acesso de terceiros aos recursos de processamento de informação da organização devem ser baseados em contratos formais que contenham ou façam referência a todos os requisitos de segurança, de forma a garantir a conformidade com os padrões e políticas de segurança da organização. O contrato deve garantir que não existam mal-entendidos entre a organização e as empresas contratadas.

3.2.3 Requisitos de segurança para a contratação de empresas terceirizadas

O planejamento para terceirizar serviços dentro de uma organização deve levar em consideração riscos, controles de segurança e procedimentos para os sistemas de informação, rede e/ou ambientes de *desktop* no contrato entre as partes.

Os requisitos de segurança que uma organização especifica na terceirização de serviços, como o gerenciamento e o controle de todo ou de parte dos seus sistemas de informação, redes e/ou *desktop*, devem constar no contrato entre as partes.

3.3 Formas de segurança

3.3.1 Segurança de pessoal

a. A política de seleção de pessoal

Um aspecto importante é a verificação constante do grupo que deve ter acesso, executar e implementar durante o período contratado. Devem ser incluídos os seguintes itens:

- disponibilidade de uma referência satisfatória (bancária ou uma pessoa);
- verificação exata do currículo do candidato;
- confirmação das qualificações acadêmicas e profissionais;
- verificação independente da identidade (ex: CPF ou carteira de motorista).

No caso de funcionários exercerem funções que manipulem informações sensíveis (informações financeiras ou informações extremamente confidenciais), a organização deve também fazer outras checagens como de crédito e idoneidade. Para funcionários com autoridade considerável, este procedimento deve ser revisto periodicamente. Um processo de seleção semelhante deve ser feito para funcionários temporários, bem como nas empresas que os fornecem.

Os acordos de confidencialidade e de não divulgação são usados como advertência de que a informação é confidencial ou secreta. Funcionários devem normalmente assinar tais acordos como parte dos termos iniciais e das condições de contratação.

b. Os termos e condições de trabalho

Os termos e condições de trabalho devem estabelecer as responsabilidades dos funcionários no tocante à segurança da informação.

Quando apropriado, estas responsabilidades devem continuar por um determinado período de tempo, após terminar o contrato de trabalho. As ações que poderão ser impetradas nos casos de descumprimento ao acordo também devem ser incluídas no contrato.

Os usuários devem ser treinados nos procedimentos de segurança e no uso correto dos sistemas de processamento da informação de forma a minimizar os possíveis riscos à segurança.

c. Resposta aos incidentes de segurança

Os incidentes que afetam a segurança devem ser informados por meio dos canais apropriados de comunicação gerencial tão logo quanto possível.

Todos os servidores e contratados devem ter conhecimento dos procedimentos para a informação de diversos tipos de incidentes (violação da segurança, ameaças, fragilidades ou mal funcionamento) que podem ter um impacto na segurança dos bens da organização. Deve ser solicitado que qualquer incidente observado ou suspeito seja informado tão logo quanto possível ao ponto de contato previamente designado.

A organização deve estabelecer um processo disciplinar formal para tratar os servidores que tenham provocado violações na segurança. Para que se possam solucionar os incidentes de forma apropriada, devem-se coletar evidências o mais rapidamente possível após a sua ocorrência.

Os incidentes de segurança devem ser informados por meio dos canais apropriados o mais rapidamente possível. O procedimento de relatar formalmente o ocorrido deve ser estabelecido, juntamente com o procedimento de solução do incidente, estabelecendo as ações a serem tomadas nos casos de recepção de um relato de incidente.

d. Procedimentos para o gerenciamento de incidentes

Devem ser estabelecidos procedimentos que cubram todos os tipos potenciais de incidentes de segurança. Para tal, é essencial a existência de planos de contingência, projetados para recuperação de sistemas e serviços com a maior brevidade possível.

Uma das primeiras providências é a análise e identificação das causas do incidente. A comunicação com os afetados, para a coleta de dados é muito importante nesta fase.

Existe, também, a necessidade de comunicação constante com os responsáveis pela solução do problema, assim como o fornecimento das informações necessárias às autoridades que devam acompanhar a solução do incidente.

São ainda, medidas de prevenção a futuros incidentes:

- planejamento e implementação de medidas para prevenir a recorrência, se necessário;
- coleta de trilhas de auditoria e evidências similares, mantendo-as seguras.

3.3.2 Segurança física

As facilidades de processamento de informações críticas ou sensíveis do negócio devem ser mantidas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

a. Delimitação do perímetro de segurança física

A proteção física pode ser alcançada por meio da criação de diversas barreiras ao longo da propriedade física do negócio e das facilidades de processamento da informação. Cada barreira estabelece um perímetro de segurança, cada uma contribuindo para o aumento da proteção total fornecida. As organizações devem usar os perímetros de segurança para proteger as áreas que contêm as facilidades de processamento de informação. Um perímetro de segurança é qualquer coisa que permita implantar uma barreira de acesso às áreas sigilosas, isto é, um conjunto de medidas como a instalação de uma parede, um portal com controle de entrada baseado em cartão ou mesmo um balcão de controle de acesso com registro manual. A localização e a resistência de cada barreira dependem dos resultados da análise de risco.

b. Função dos controles de entrada física

As áreas seguras devem ser protegidas por controles de entrada apropriados para garantir que apenas as pessoas autorizadas tenham permissão de acesso.

3.4 Trabalhando em áreas protegidas

Manuais e controles adicionais podem ser necessários para melhorar a segurança de uma área. Incluem controles tanto para o pessoal da organização como para aqueles terceirizados que trabalham em áreas seguras, assim como para atividades terceirizadas que possam ocorrer nesta área.

3.4.1 Segurança de equipamento

Os equipamentos devem ser fisicamente protegidos contra ameaças da segurança e perigos ambientais. A proteção de equipamentos (incluindo aqueles utilizados fora do local) é necessária para reduzir o risco de acesso não autorizado a dados e para proteção contra perda ou dano.

3.4.2 Instalação e proteção de equipamentos

Os equipamentos devem ser localizados ou protegidos para reduzir o risco de ameaças ambientais e perigos, além de oportunidades de acesso não autorizado.

3.4.3 Fornecimento elétrico

Os equipamentos devem ser protegidos contra falhas e outras anomalias na alimentação elétrica. Um fornecimento elétrico apropriado deve ocorrer em conformidade com as especificações do fabricante.

3.4.4 Segurança do cabeamento

O cabeamento elétrico e de telecomunicação que transmite dados ou suporta os serviços de informação deve ser protegido contra intercepção ou dano.

3.4.5 Manutenção de equipamentos

A manutenção correta dos equipamentos deve garantir a continuidade da disponibilidade e integridade.

3.4.6 Segurança de equipamentos fora da organização

O uso de qualquer equipamento (PC, telefones, documentos etc) fora da propriedade da organização para o processamento da informação deve ser autorizado por quem de direito. A segurança fornecida deve ser semelhante àquela oferecida a equipamentos no local usado com o mesmo propósito, levando-se em consideração os riscos do trabalho externo à propriedade da organização.

3.4.7 Política de utilização da mesa de trabalho e monitor de vídeo

A organização deve considerar a política para utilização de mesa de trabalho que abranja a utilização de papéis e meios magnéticos removíveis, assim como a utilização de uma política de monitor para as facilidades de processamento de informação, de forma a reduzir os riscos de acesso não autorizados, a perda e os danos à informação durante e fora do horário normal de trabalho. A política deve levar em consideração a classificação segura da informação, os riscos correspondentes e os aspectos culturais da organização.

3.4.8 Gerenciamento das operações e comunicações

Para garantir uma operação segura e correta das facilidades de processamento da informação, devem ser estabelecidas responsabilidades e procedimentos pelo gerenciamento e operação de todas as facilidades de processamento da informação. Isto inclui o desenvolvimento de instruções apropriadas de operação e procedimentos de resposta a incidentes.

3.4.9 Documentação dos procedimentos de operação

Os procedimentos de operação identificados pela política de segurança devem ser mantidos e documentados. Modificações podem ocorrer apenas com autorização de quem de direito.

3.4.10 Mudança de controle operacional

As modificações nos sistemas e facilidades de processamento da informação devem ser controladas. O controle inadequado das modificações nos sistemas e facilidades de processamento da informação são causas comuns de falhas de segurança ou de sistemas.

As responsabilidades pelo gerenciamento formal e os procedimentos devem ser estabelecidos de forma a garantir um controle satisfatório de todas as modificações em equipamentos, software ou procedimentos. Programas que estão operacionais devem ser submetidos a um controle estrito de modificações. Quando programas são modificados, um *log* de auditoria contendo todas as informações relevantes deve ser mantido. Modificações no ambiente operacional podem causar impacto em aplicações.

3.4.11 Segregação das obrigações e responsabilidades

A segregação das obrigações é um método utilizado para reduzir o risco da má utilização deliberada dos sistemas. Deve ser considerada a separação do gerenciamento ou execução de certas obrigações ou áreas de responsabilidade, de forma a reduzir as oportunidades de modificação não autorizada ou o mau uso da informação ou serviços.

3.4.12 Desenvolvimento, testes e operação

Separar as facilidades de desenvolvimento, teste e operação é importante para se adquirir segregação das funções envolvidas. As regras para a transferência de software do estado de desenvolvimento para o estado operacional devem ser bem definidas e documentadas.

3.4.13 Planejamento e aprovação dos sistemas

São necessários planejamento e preparação avançada para garantir a disponibilidade de recursos e capacidade adequada.

As projeções de requisitos de capacidades futuras devem ser feitas para reduzir o risco de sobrecarga dos sistemas. Os requisitos operacionais dos novos sistemas devem ser estabelecidos, documentados e testados antes da sua aceitação e do seu uso.

3.4.14 Planejamento de capacidade

As demandas de capacidade devem ser monitoradas e as projeções de requisitos de capacidades futuras devem ser feitas de forma a garantir que um poder de processamento e armazenamento adequado esteja disponível. Estas projeções devem levar em consideração os requisitos de sistemas e de novas tarefas da organização e as tendências atuais e projetadas de processamento de informação da organização.

3.4.15 Homologação de sistema

Devem ser estabelecidos critérios de aprovação e aceitação de novos sistemas, atualizações e novas versões; bem como devem ser efetuados testes apropriados dos sistemas antes da sua aceitação. Os gerentes devem garantir que os requisitos e critérios para aceitação de novos sistemas estejam claramente definidos, acordados, documentados e testados.

3.4.16 Proteção contra softwares maliciosos

São necessárias precauções para prevenir e detectar a introdução de softwares maliciosos. As facilidades de processamento da informação e do software são vulneráveis à introdução de softwares maliciosos, tais como vírus de computador, cavalos de Tróia e bombas lógicas. Os usuários devem ser informados sobre os perigos do uso de software não autorizado ou malicioso, e os gerentes devem, quando for apropriado, introduzir os controles especiais para detecção ou prevenção contra a sua introdução. Em particular, é essencial que sejam tomadas precauções para detecção e prevenção de vírus em computadores pessoais.

3.4.17 Manutenção

Devem ser estabelecidos procedimentos de rotina para implementação da estratégia de *backup* definida, executando cópias *backup* de dados e reavaliação do tempo de restauração, *log* de eventos e falhas; e, se for apropriado, monitorar o ambiente do equipamento.

3.4.18 *Backup* de informação

Cópias de *backup* das informações essenciais dos trabalhos e software devem ser feitas regularmente. Facilidades de *backup* adequadas devem estar disponíveis, de forma a garantir que toda informação essencial ao negócio e todo software possam ser recuperados após um desastre ou problemas nos meios magnéticos que estão operacionais. Acordos de *backups* para sistemas individuais devem ser regularmente testados para garantir que eles satisfaçam os requisitos dos planos de continuidade de negócios.

3.4.19 *Log* de operador e falhas

Deve ser mantido um *log* das atividades do grupo de operação. Qualquer tipo de falha deve ser informado e devem ser tomadas as ações apropriadas para corrigi-las. Todas as falhas informadas pelos usuários e relacionadas com o processamento de informações ou sistemas de comunicação devem ser guardadas em *log*.

3.4.20 Gerenciamento da rede

O gerenciamento de segurança de redes deve se estender até os limites da organização. Pode ser necessária a utilização de controles adicionais para proteção de dados sensíveis que transitem sobre redes públicas.

É necessária a utilização de um conjunto de controles buscando garantir a segurança nas redes de computadores. Os gerentes das redes devem implementar controles para garantir a segurança de dados na redes, assim como a proteção dos serviços conectados contra acessos não autorizados.

3.4.21 Segurança e manipulação do meio magnético

Os procedimentos operacionais apropriados devem ser estabelecidos para proteger documentos, meios magnéticos de computadores (fitas, discos, cassetes), dados de entrada e saída e documentação do sistema relacionada a danos, roubos e acessos não autorizados.

3.4.22 Gerenciamento de meio magnético removível

Devem existir procedimentos para o gerenciamento de meios magnéticos removíveis, como fitas, discos, cassetes e formulários impressos.

3.4.23 Destruição de meios magnéticos

Os meios magnéticos devem ser dispensados de cofres e dos ambientes seguros quando não forem mais necessários. As informações sensíveis podem vazar para pessoas externas à organização através de procedimentos descuidados no processo de inutilização dos meios magnéticos.

3.4.24 Procedimentos para manipulação de informação

Devem ser estabelecidos procedimentos para a manipulação e o armazenamento de informação com o objetivo de proteger as informações contra a divulgação não autorizada ou o seu uso indevido. Os procedimentos para a manipulação da informação devem ser definidos de acordo com a classificação da informação usada para cada documento, sistemas de computadores, redes de computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços e facilidades postais, uso de máquinas de fax e qualquer outro item sensível (cheques em branco, solicitações de compras).

3.4.25 Segurança da documentação dos sistemas

A documentação dos sistemas pode conter um grupo de informações sensíveis (descrições de processos de aplicação, procedimentos, estruturas de dados, processos de autorização).

Os seguintes controles devem ser considerados para proteger a documentação dos sistemas contra acessos não autorizados:

- a documentação dos sistemas deve ser guardada em local seguro;
- a lista de acesso à documentação dos sistemas deve ser mantida no mínimo possível e as pessoas devem ser autorizadas pelo dono ou responsável pela aplicação;
- a documentação de sistema obtida ou fornecida por meio de uma rede pública deve ser protegida de forma apropriada.

3.4.26 Segurança do comércio eletrônico

O comércio eletrônico é vulnerável a um número de ameaças de rede, que pode resultar em atividades fraudulentas, disputas de contratos e divulgação ou modificação de informação. Devem ser aplicados controles para proteger o comércio eletrônico de tais ameaças.

Os acordos de comércio eletrônico entre parceiros comerciais devem ser amparados em um contrato documentado que relaciona ambas as partes com os termos do acordo comercial, incluindo detalhes de autorização. Outros acordos com serviço de informação e provedores de rede de valores agregados podem também se tornar necessários.

Os sistemas de comércio público devem publicar termos de negócio para seus clientes. Devem ser consideradas as flexibilidades de ataques que podem ocorrer nos *hosts* utilizados para o comércio eletrônico, e as implicações de segurança de qualquer interconexão de rede necessária para este tipo de implementação.

3.4.27 Segurança do correio eletrônico

O correio eletrônico é utilizado para as comunicações do negócio, substituindo formulários tradicionais de comunicação, como telex e cartas. O correio eletrônico difere das formas tradicionais de comunicação de negócio pela sua velocidade, estrutura da mensagem, grau de informação e vulnerabilidade a ações não autorizadas.

As organizações devem definir uma política clara para a utilização do correio eletrônico, incluindo:

- ataques a correios eletrônicos (vírus, interceptação indevida);
- proteção dos anexos das mensagens;
- orientações de quando não se devem utilizar correios eletrônicos;

- responsabilidades dos empregados no não comprometimento da companhia (envio de mensagens difamatórias, uso do correio eletrônico para atormentar pessoas ou fazer compras não autorizadas);
- uso de técnicas de criptografia para proteger a confidencialidade e integridade das mensagens eletrônicas;
- armazenamento de mensagens que podem ser descobertas em casos de litígio;
- controles adicionais para verificação de mensagens que não podem ser autenticadas.

3.4.28 Sistemas de disponibilidade pública

Deve-se tomar cuidado para proteger a integridade da informação publicada eletronicamente de forma a prevenir modificações não autorizadas que possam vir a prejudicar a reputação da publicação da organização. Informação em sistemas disponíveis para o público (informações em um servidor web acessível através da internet) pode necessitar estar em conformidade com as leis, regras e regulamentações na jurisdição na qual o sistema está localizado, ou onde o negócio está ocorrendo. Deve existir um processo de autorização formal antes da informação tornar-se publicamente disponível.

Softwares, dados e outras informações que requerem um alto nível de integridade, expostos em um sistema disponível publicamente, devem ser protegidos por mecanismos apropriados (ex: assinaturas digitais).

Sistemas de publicação eletrônica, especialmente aqueles que permitem realimentação e entrada direta de informações, devem ser cuidadosamente controlados, de forma que:

- a informação seja obtida em conformidade com qualquer legislação relacionada à proteção de dados;
- as informações sensíveis sejam protegidas durante o processo de captação e quando forem armazenadas;
- o acesso a sistemas de publicação de informações não permita acesso indevido a redes nas quais estes sistemas estão conectados.

3.5 Controle de acesso

3.5.1 Política de controle de acesso

Os requisitos para controle de acesso devem ser definidos e documentados. As regras de controle de acesso e direitos para cada usuário ou grupo de usuários devem ser claramente estabelecidas em concordância com a política de acesso. Aos usuários e aos provedores de serviço é fornecido um documento contendo os requisitos do negócio a serem satisfeitos pelos controles de acesso.

Na especificação de regras para controle de acesso, alguns cuidados devem ser seguidos:

- diferenciar as regras que devem sempre ser incentivadas das regras que são opcionais ou condicionais;
- estabelecer regras seguindo a premissa de que tudo deve ser proibido, a menos que seja expressamente permitido. Não utilize a regra de que tudo deve ser permitido a menos que expressamente proibido;
- diferenciar os rótulos de informação que são atribuídos automaticamente pelas facilidades de processamento da informação e aqueles atribuídos sob juízo de um usuário;
- diferenciar as permissões de usuários que não são atribuídas automaticamente pelo sistema de informação daquelas que são atribuídas pelo administrador;
- diferenciar as regras que necessitam da aprovação do administrador ou de outro funcionário antes de ser tornarem operacionais daquelas que não necessitam de tal aprovação.

3.5.2 Gerenciamento dos acessos de usuário

Devem ser estabelecidos procedimentos formais para controlar a alocação de direitos de acesso aos serviços e sistemas de informação.

Os procedimentos devem cobrir todos os estágios no ciclo de vida de acesso de usuário, do registro inicial de novos usuários até a sua desabilitação de uso do sistema e serviços (quando o usuário não mais necessitar de tais serviços e sistemas). Deve ser dada a atenção especial para a necessidade de controle da alocação de direitos de acesso privilegiado, que permite aos usuários o poder de sobrepor os controles do sistema.

3.5.3 Gerenciamento de privilégios

A alocação e o uso de privilégios (qualquer característica ou facilidade de um sistema de informação multiusuário que permita ao usuário sobrepor controles dos sistemas ou das aplicações) devem ser restritos e controlados. O uso inadequado dos privilégios do sistema é frequentemente considerado como sendo o fator que mais contribui para a violação dos mesmos.

3.5.4 Gerenciamento das senhas de usuários

As senhas são um meio comum de validação das identidades dos usuários para acessar um sistema ou serviço de informação.

As senhas de usuário nunca deverão ser guardadas em sistemas computacionais de forma desprotegida. Outras tecnologias para a identificação de usuário e autenticação, tais como identificação biométrica (verificação de impressão digital, verificação de assinatura) e utilização de fichas de hardware (*smart cards*) já estão disponíveis para este fim e devem ser utilizadas quando apropriado.

3.5.5 Responsabilidades dos usuários

A cooperação dos usuários é essencial para a eficácia da segurança. Os usuários devem ser mantidos informados das suas responsabilidades sobre a manutenção da eficiência dos controles de acesso, considerando-se particularmente o uso de senhas e a segurança dos equipamentos dos mesmos.

Os usuários devem seguir as boas práticas de segurança na seleção e uso de senhas. As senhas fornecem um meio de validar a identidade do usuário, e assim, o estabelecimento de direitos de acesso às facilidades e serviços de processamento da informação.

Caso os usuários não necessitem de acesso a múltiplos serviços ou às plataformas e necessitem manter múltiplas senhas, eles devem ser informados de que podem usar uma única senha de qualidade para todos os serviços que proverem um nível razoável de proteção para os arquivos de senhas.

3.5.6 Controle de acesso à rede

O acesso aos serviços da rede interna assim como aos da rede externa deve ser controlado. Isso é necessário para se garantir que os usuários que possuem acesso a redes e serviços de rede não comprometam a segurança desses serviços. Para este tipo de proteção é necessário garantir que:

- sejam utilizadas interfaces apropriadas entre a rede da organização e as redes de outras organizações, ou redes públicas;
- sejam utilizados mecanismos de autenticação apropriados para usuários e equipamentos;
- conexões a serviços de rede sejam seguras, pois conexões inseguras podem afetar toda a organização.

Os usuários só devem possuir acesso àqueles serviços para os quais eles possuem autorização específica de uso. Este controle é particularmente importante para as conexões de rede com aplicações sensíveis ou críticas do negócio ou para usuários que estão em locais de alto risco (áreas públicas ou externas que se encontram fora do controle e da gerência de segurança da organização).

3.5.7 Autenticação de usuário para conexão externa

As conexões externas fornecem um potencial para acesso não autorizado às informações do negócio (acessos via métodos *dial-up*). Consequentemente, o acesso de usuários remotos deve estar sujeito à autenticação.

Existem diferentes tipos de métodos de autenticação. Alguns desses métodos fornecem um maior nível de proteção que os outros (os métodos baseados no uso de técnicas de criptografia podem fornecer autenticação forte). É importante determinar-se a partir de uma análise de risco o nível de proteção mais adequada. Isto é necessário para a seleção apropriada de um método de autenticação.

3.5.8 Controle de acesso ao sistema operacional

Facilidades de segurança em sistemas operacionais devem ser usadas para restringir o acesso aos recursos computacionais. Estas facilidades devem incluir a possibilidade de:

- identificar e verificar a identidade e, quando necessário, a estação de trabalho e a localização de cada usuário autorizado;
- registrar os acessos e as falhas de acesso ao sistema;
- prover meios apropriados para a autenticação, caso um sistema de gerenciamento de senhas seja utilizado. É necessário garantir que senhas de qualidade sejam utilizadas;
- quando for apropriado, restringir as conexões momentâneas (em determinados momentos do dia) de usuários.

3.5.9 Procedimentos de *logon*

O acesso aos serviços de informação deve ser realizado via um processo seguro de *logon*. O procedimento para *logging* no sistema de computador deve ser projetado para minimizar a oportunidade de acessos não autorizados. Deve, consequentemente, divulgar o mínimo de informações sobre o sistema, de forma a evitar fornecer a um usuário não autorizado a assistência e informações desnecessárias.

3.5.10 Identificação e autenticação de usuário

Todos os usuários (incluindo o pessoal de suporte, como operadores, administradores de rede, programadores de sistema e administradores de base de dados) devem ter um único identificador (ID de usuário) para o seu uso pessoal e único, de forma que suas atividades possam subsequentemente permitir a localização do indivíduo responsável.

3.5.11 Isolamento de sistemas sensíveis

Os sistemas sensíveis podem requerer um ambiente computacional dedicado (isolado). Alguns sistemas de aplicação são suficientemente sensíveis à perda potencial de informações, requerendo desta maneira manipulação especial. A sensibilidade pode indicar que o sistema de aplicação deve rodar em um computador dedicado, deve compartilhar recursos apenas com sistemas de aplicação confiáveis, ou não possuir limitações.

3.5.12 Procedimentos e áreas de risco

Devem ser estabelecidos procedimentos para a monitoração do uso das facilidades de processamento da informação. Tais procedimentos são necessários para garantir aos usuários que estão executando apenas as atividades para as quais eles foram explicitamente autorizados. O nível de monitoração necessária para as facilidades individuais deve ser determinado através de uma análise de riscos.

3.6 Computação móvel

Quando se utilizam as facilidades da computação móvel (notebooks*, palmtops,* laptops) e que requerem proteção física, controles de acesso, técnicas criptográficas, backups e proteção contra vírus são necessários. Esta política deve, também, incluir regras e avisos nas facilidades de computação móvel para redes e manuais, e procedimentos sobre o uso desta ferramenta em locais públicos.

Devem ser tomadas certas precauções quando se utilizarem facilidades de computação móvel em locais públicos, salas de reuniões e outras áreas desprotegidas fora dos limites da organização. Devem ser estabelecidas certas proteções para se evitar o acesso não autorizado ou a divulgação de informações que se encontram armazenadas e que são processadas por estas ferramentas, por meio da utilização de técnicas de criptografia, por exemplo.

É importante lembrar que, quando tais facilidades forem utilizadas em locais públicos, certos parâmetros devem ser considerados para se evitar o risco de terem as informações espreitadas por pessoas não autorizadas. Também devem ser estabelecidos procedimentos contra softwares maliciosos, mantendo-os sempre atualizados.

O equipamento deve estar disponível para possibilitar um *backup* rápido e fácil das informações. Estes *backups* devem fornecer uma proteção adequada contra a perda ou roubo de informação.

Uma proteção adequada deve ser dada ao uso das facilidades de computação móvel conectadas às redes. O acesso remoto às informações do negócio por meio de redes públicas usando as facilidades de computação móvel apenas deve ocorrer após o sucesso da identificação e da autenticação, e da implantação de mecanismos de controle de acesso apropriado.

As facilidades de computação móvel devem também ser protegidas fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião. Os equipamentos que contêm informações sensíveis e importantes e/ou críticas ao negócio nunca devem ser deixados sem a observação e, quando possível, devem ficar guardados; ou travas especiais devem ser utilizadas com o intuito de manter o equipamento seguro.

Seção 4
Auditoria da Informática

Auditoria pode ser definida como uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de verificar a sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões. (DORA, 2001).

Outra forma de se vivenciar uma auditoria consiste em estabelecer e executar procedimentos para a coleta de dados gerados pela atividade de um sistema computacional (uma rede, sistema de informação ou qualquer dispositivo de hardware ou software). Estes dados podem ser utilizados na análise de segurança do sistema computacional em questão, visando detectar as falhas ocorridas para que possam ser corrigidas e responder aos incidentes de segurança ocorridos. (DIAS, 2000).

Toda auditoria é dividida em três fases:

1. **Planejamento** – identifica os instrumentos indispensáveis à sua realização.
2. **Execução** – reúne as evidências teoricamente confiáveis, relevantes e úteis para a realização dos objetivos da auditoria.
3. **Relatório** – são apresentados os resultados, análises e conclusões por escrito.

4.1 Auditoria da Tecnologia da Informação (Auditoria de Sistemas ou de Informática)

A auditoria analisa a gestão de recursos, enfocando os aspectos de:

- **Eficiência** – é a relação entre os produtos, bens e serviços produzidos ou outros resultados atingidos por uma unidade ou entidade, tendo em conta a quantidade e qualidade apropriada e os recursos utilizados para produzi-los ou atingi-los, menor custo, maior velocidade, melhor qualidade.
- **Eficácia** – é o grau em que uma organização, programa, processo, projeto, operação, atividade, função ou sistema atinge os objetivos da política, as metas operativas estabelecidas e outros resultados e efeitos previstos.

- **Economia** – é o grau em que uma organização, programa, processo, projeto, operação, atividade, função ou sistema minimiza o custo dos recursos humanos, financeiros e materiais, adquiridos ou utilizados, tendo em conta a quantidade e qualidade apropriada, ou seja, é a prática por parte da gerência das virtudes de poupança e boa economia doméstica (gastando menos).

Segundo Dias (2000), pode-se dividir a auditoria de tecnologia da informação nas seguintes subáreas:

Auditoria da segurança da informação – determina como a Instituição se comporta em relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança. Ela abrange:

- avaliação da política de segurança;
- controles de acesso lógico;
- controle de acesso físico;
- controles ambientais;
- plano de contingências e continuidade de serviços.

Auditoria da tecnologia da informação – além dos aspectos relacionados com a auditoria da segurança, ela também abrange outros controles que podem influenciar a segurança de informações e o bom funcionamento dos sistemas de toda a organização. Estes controles são:

- organizacionais;
- sobre operação dos sistemas;
- sobre banco de dados;
- sobre microcomputadores;
- sobre ambientes cliente-servidor.

Auditoria de aplicativos – aplica-se à segurança e ao controle de aplicativos, conforme os aspectos de orçamento, contabilidade, estoque etc. Este tipo de auditoria compreende:

- controle sobre o desenvolvimento de sistemas aplicativos;
- controle de entrada, processamento e saída de dados;
- controle sobre conteúdo e funcionamento do aplicativo, com relação à área por ele atendida.

4.1.1 Planejamento de uma auditoria de tecnologia da informação

Pesquisa das fontes de informação

É adquirida a maior quantidade de informações sobre a instituição a ser auditada e também sobre o seu ambiente computacional, possibilitando estabelecer os aspectos iniciais do plano de auditoria. Todo este conhecimento inicial possibilita à equipe de auditoria ter uma visão básica do grau de complexidade de todo ambiente computacional (hardware e software) que irá encontrar, possibilitando que essa auditoria prepare-se tecnicamente (estudando o ambiente) e providencie os dispositivos necessários (ex: ferramentas de software) para a realização da tarefa.

O que/onde coletar

Os principais dados a serem coletados são: tipo do hardware, sistemas operacionais, SGBD, recursos de segurança, componentes das áreas a serem auditadas.

Algumas destas informações podem ser obtidas via entrevistas com os componentes das áreas. Mas vale a pena ler relatórios anteriores de auditoria, documentos que abordem os aspectos operacionais dos dispositivos de software e hardware, documentos sobre a segurança da empresa (política de segurança) etc.

Campo, âmbito e subáreas

Com o conhecimento da empresa a ser auditada, é definido o:

a. Campo - o campo é composto pelo:
   - » objeto - ele pode ser um sistema de informação, uma área do setor (ex: banco de dados, redes etc), a segurança da informação etc;
   - » período - este varia conforme a abrangência e a profundidade das tarefas a serem executadas na auditoria;
   - » natureza - tecnologia da informação.

b. Âmbito - avaliação da eficácia dos controles (prevenção, detecção ou correção).

c. Subáreas - estas estão em concordância com o objeto a ser auditado (ex: segurança da informação - pode-se ter as subáreas de controle de acesso lógico, controles de desenvolvimento de sistemas por terceiros, segurança de pessoal etc).

4.2 Recursos necessários

Recursos humanos - a escolha da equipe está diretamente relacionada ao grau de complexidade do escopo da auditoria, dos componentes existentes no ambiente computacional (ex: sistemas operacionais, hardware etc), das ferramentas a serem utilizadas e da disponibilidade da equipe.

Recursos econômicos - realizar uma previsão de gastos (ex: viagens, pessoal terceirizado).

Recursos técnicos - quais dispositivos de hardware (ex: notebooks), software (ex: ferramentas para coleta de dados) e documentos técnicos serão utilizados.

4.3 Metodologia

4.3.1 Entrevistas

- Apresentação - realizada no início dos trabalhos para a apresentação da equipe, do cronograma de atividades, das áreas a serem auditadas, do período da auditoria e das metodologias utilizadas.
- Coleta de dados - são obtidos dados sobre os sistemas, sobre o ambiente computacional, entre outros, junto aos gerentes de área e/ou funcionários. Durante essa entrevista, são identificados pontos falhos e fortes, bem como irregularidades.
- Discussão - são apresentadas as deficiências encontradas e discutidas com os seus respectivos responsáveis.
- Encerramento - é apresentado um resumo dos resultados da auditoria (pontos positivos e negativos), e são feitos comentários de cada componente (caso seja solicitado).

4.3.2 Técnicas ou ferramentas de apoio

- Análise de dados - os dados podem ser coletados e analisados com auxílio de softwares, por amostragem, arquivos *logs* etc.
- Verificação de controles de sistemas - testa se os controles do sistema são realmente confiáveis e se operam de acordo com o esperado.

4.3.3 Execução

Durante a execução da auditoria, evidências úteis à auditoria são coletadas, interpretadas e analisadas, possibilitando uma conclusão adequada.

Dividem-se as evidências em 4 tipos:

- **física** - podem-se citar como exemplo observações de atividades de sistemas, gerentes e administradores de rede e segurança etc;
- documentária - podem ser obtidos via registros *logs*, relatórios emitidos pelo sistema etc;
- **fornecida pela entidade que está sofrendo a auditoria** - documentos sobre sistemas, faturas etc;
- **analítica** - comparações, cálculos e interpretações de documentos fornecidos em diferentes períodos.

A inclusão ou não de uma determinada evidência é baseada na sua importância para os objetivos da auditoria, do tempo e do esforço necessário para esclarecer os pontos que não estão claros. Porém, qualquer evidência incompatível com a auditoria que está sendo realizada pode ser um início para outra auditoria.

4.3.4 Relatório

O relatório contém todas as evidências, conclusões e normalmente recomendações e/ou determinações. Para a geração do relatório final, as diversas áreas de auditoria apresentam os seus relatórios parciais. Estes relatórios são analisados pela equipe como um todo, e um relatório final é gerado e normalmente entregue a quem solicitou a auditoria.

4.3.5 Plano de contingência - gerenciamento da continuidade do negócio

Todo sistema computacional, por mais protegido, possui vulnerabilidades. Estas vulnerabilidades podem ocasionar desastres de forma inesperada, proporcionando uma grande perda para empresas que dependem da informática para manter a continuidade de seus serviços.

O processo de gerenciamento da contingência é implementado com o objetivo de reduzir a possibilidade de interrupção das atividades de negócio, causada por um desastre ou falha de segurança (ex: desastres naturais, acidentes, falhas de equipamentos e ações intencionais - terrorismo), reduzindo-a para um nível aceitável de funcionamento via a combinação de controles preventivos e de recuperação.

Este processo deve incluir controles que identificam e reduzem os riscos, limitam as consequências dos danos causados por incidentes e garantem um reinício na hora certa das operações essenciais.

Todas as consequências de desastres, falhas de segurança e perda de serviço devem ser analisadas. De posse desta análise, têm-se parâmetros para se desenvolver um plano de contingência adequado às necessidades de uma empresa. A partir dessas informações, portanto, os planos de contingência são desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados dentro de um período de tempo previsto e adequado às necessidades da empresa.

4.3.6 Processo de planejamento de contingências

Normalmente existe um processo de gerência instalado para o desenvolvimento e a manutenção da continuidade do negócio da empresa. Este processo está baseado nos seguintes elementos-chave do gerenciamento da continuidade do negócio:

a) Comprometimento da diretoria da empresa - é bom esclarecer que o planejamento da continuidade dos negócios é responsabilidade da diretoria da empresa. Membros da empresa (auditores internos, equipe de segurança das informações) podem auxiliar no seu desenvolvimento, mas cabe à diretoria garantir a sua eficiência. Para tornar o plano exequível, existe a necessidade de se definir um orçamento prevendo gastos como treinamento, testes e manutenção do plano.

Também é necessário:

- Compreender os riscos que a organização enfrenta em termos da probabilidade de ocorrência de eventos danosos e o seu impacto, incluindo a identificação e priorização dos processos críticos do negócio.
- Ter conhecimento do impacto que as interrupções terão sobre os negócios, e o estabelecimento dos objetivos do negócio relacionados com as facilidades de processamento da informação (análise de impacto). As soluções encontradas para minimizar o impacto devem tratar tanto os pequenos incidentes, quanto os mais sérios, que podem pôr em risco a funcionalidade da empresa.
- Formular e documentar uma estratégia consistente de continuidade do negócio com acordos, considerando as prioridades e objetivos do negócio. Logo, devem-se estudar as diversas alternativas de recuperação dos serviços computacionais (leve em consideração a relação custo/benefício). Entre elas podem-se citar:

- estabelecer uma política de *backup*;
- estabelecer uma forma de armazenar os dados do sistema (*backup* identificado);
- estabelecer procedimentos para a recuperação de dados;
- providenciar o seguro dos equipamentos, entre outros itens;
- estabelecer contratos comerciais, como contratos de manutenção e fornecimento de dispositivos de hardware e software;
- desenvolver um plano de contingência;
- realizar treinamento para garantir a eficiência do plano;
- testar e atualizar regularmente os planos e processos estabelecidos.

b) Continuidade do negócio e análises de impacto

O impacto consiste no dano que uma ameaça pode causar. Geralmente, os impactos são classificados como:

- Diretos - envolvem perdas financeiras (ex: reposição de equipamentos) e diminuição de receita (ex: site fora do ar).
- Indiretos - não envolvem diretamente perdas financeiras, mas podem provocá-las (ex: perda de credibilidade em transações eletrônicas).

A continuidade do negócio deve começar pela identificação dos eventos (identificação das possíveis ameaças) que podem causar interrupções nos processos do negócio (ex: incêndios, roubos, quedas de link etc), seguida por uma análise de risco para se determinar o impacto destas interrupções (tanto em termos de escala de dano quanto em relação ao período de recuperação). Ambas as atividades devem ser executadas com o total envolvimento dos responsáveis pelos processos e recursos do negócio. Essa análise deve considerar todos os processos do negócio, e não deve estar limitada somente às facilidades de processamento da informação. Deve, ainda, classificar os recursos, funções e sistemas críticos conforme a sua importância: alta, média e baixa.

Dependendo dos resultados da análise de risco, um planejamento estratégico deve ser desenvolvido para se determinar uma estratégia a ser usada para alcançar a continuidade de todo o negócio, em que um dos parâmetros é o tempo máximo tolerável de indisponibilidade de cada recurso ou sistema (minutos, horas, dias etc), definido pela gerência da empresa. Com isso, têm-se condições de decidir como e onde investir em medidas de segurança, protegendo os bens e mantendo as atividades dentro de sua maior normalidade. Uma vez que o plano é desenvolvido, ele deve ser validado e implementado pela gerência da empresa.

Todo impacto gera a necessidade de um relatório, o qual deve conter os seguintes itens:

- identificação dos recursos, sistemas e funções críticas por ordem de importância;
- descrição de cada um dos elementos acima citados, que tipo de perda ou dano poderá ser ocasionado, qual o tempo máximo de indisponibilidade e quais as condições mínimas de adestramento e conhecimento de pessoal, instalações e serviços necessários para a recuperação do sistema.

c) Desenvolvendo planos de contingência: o que se deve abordar?

Os planos de contingência devem ser desenvolvidos para manter ou restaurar as operações do negócio, em uma escala de tempo definida para interrupções ou falhas dos processos críticos do negócio. O plano de contingência deve abordar duas fases:

- **resposta imediata a um desastre** - envolve decisões gerenciais, isto é, tomar medidas corretivas para restaurar os sistemas e funções do segmento de rede inoperante, por exemplo;
- **processo de restauração** - reestruturação do serviço **d**anificado (ex: subir um servidor em outro servidor).

O processo de planejamento do plano de contingência deve considerar os seguintes itens:

- **designação de um grupo de recuperação de contingências** - este grupo é o responsável em colocar na prática o plano de contingência. O grupo pode ser dividido em equipes conforme a sua área de atuação (ex: equipe para resposta a incidentes de segurança);
- **identificação** e entendimento de todas as responsabilidades e procedimentos de emergência;
- **implementação** dos procedimentos de emergência para permitir a recuperação e restauração na escala de tempo necessária;
- **documentação** dos processos e procedimentos acordados.

O plano deve conter procedimentos quanto:

- à retirada de pessoal;
- aos procedimentos com os documentos em papel;
- aos procedimentos com os documentos em meio magnético;
- à educação e instrução apropriada do grupo de trabalho nos procedimentos de emergência acordados e nos processos relacionados, incluindo a gerência da crise;
- à testagem do plano de contingência;
- à manutenção e atualização do plano de contingência.

Apresentaram-se neste capítulo conceitos e alguns aspectos básicos e necessários para a segurança da informação.

Todo o conteúdo apresentado aqui não esgota o assunto, sendo que a busca sem fim pelo conhecimento faz-se necessária. Além das referências apresentadas, a internet é uma fonte inesgotável do assunto. A segurança da informação é um processo contínuo e árduo. É uma luta sem fim, na qual restará sempre muito o que fazer. Quem trabalha com segurança estará buscando eternamente novos caminhos para minimizar as vulnerabilidades que sempre existirão.

Recomendação de segurança: Os agentes responsáveis pela custódia de documentos, conhecimentos, materiais, áreas, comunicações, operações e sistemas de informação de natureza sigilosa estão sujeitos às regras referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico.

Considerações Finais

Prezado/a estudante,

Você concluiu o estudo do livro didático “**Inteligência e Segurança Pública**”. Missão cumprida!

Nesta caminhada, você travou contato com algo que, para grande parte das pessoas, sempre esteve envolto em mistérios e que, com o advento da Constituição Cidadã e do restabelecimento do Estado Democrático de Direito no país, “deitou” por terra toda a mística que cercava este campo do conhecimento.

O objetivo desta viagem era o de, efetivamente, romper as portas do secreto que até então pareciam estar acessível apenas a alguns poucos especialistas privilegiados.

Hoje, compreende-se efetivamente que para prestar um serviço de Segurança Pública de qualidade é necessário que os seus operadores estejam preparados de forma multidisciplinar. A Inteligência Policial se constitui na viga mestra das ações de polícia preventiva ou reativa, sem a qual será inexitosa, trazendo prejuízos incalculáveis para a sociedade.

Por derradeiro, sugerimos que continue se interessando pelo tema tão relevante, mas pouco explorado pelos estudiosos. Que você possa ser um baluarte no campo da Inteligência nas missões de Segurança Pública.

Sucesso!

Os professores.

Glossário

Dados Operacionais

São dados que auxiliam no planejamento das Operações de Inteligência.

Encarregado de caso

É a função desenvolvida por um profissional de Inteligência que tem como atribuições planejar, dirigir, coordenar e controlar a execução das Operações de Inteligência.

Agente Principal

É o profissional com a função de auxiliar o encarregado de caso no controle de agentes e na condução de Operações de Inteligência.

Chefe de Equipe

É o membro de uma equipe de busca, com a função de coordenar as ações no ambiente operacional.

Equipe de Busca

É o grupo de agentes envolvidos na busca.

Turma de Busca

É o conjunto de equipes envolvidas na busca.

Agente

É o profissional de inteligência ou não, com a responsabilidade de obter dados negados ou de criar facilidades para a execução de Operações de Inteligência.

Agente Operacional

É o profissional com a função de aplicar técnicas operacionais.

Contato

É o profissional não pertencente ao órgão de Inteligência que, conscientemente ou não, colabora com o profissional de Inteligência, criando facilidades e/ou fornecendo dados.

Dado Negado

Qualquer dado de interesse do Órgão de Inteligência que esteja sendo protegido pela pessoa ou organização que o detém.

Operação Exploratória

Compreende a execução de ações operacionais de ISP que se caracterizam por serem eventuais, proporcionando resultados específicos em um determinado momento.

Operação Sistemática

Compreende a execução de ações operacionais que se caracterizam por serem contínuas, produzindo um fluxo constante de dados em um determinado período de tempo.

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 de Segurança Pública.

Vigilância

É a Ação de Busca que consiste em manter um ou mais alvos sob observação. A Vigilância é uma técnica operacional que possui um modus operandi específico e de execução complexa que emprega muitos meios humanos e materiais e, dependendo do alvo, pode tornar-se perigosa, exigindo, assim, muito controle em sua execução.

Recrutamento Operacional

Trata-se da Ação de Busca realizada para convencer uma pessoa que não seja pertencente ao órgão de Inteligência a trabalhar em benefício deste. Todavia, se de um lado o Recrutamento pode proporcionar excelentes resultados, de outro é uma das técnicas mais sensíveis e comprometedoras caso a abordagem seja mal sucedida.

Infiltração

Consiste na Ação de Busca que coloca uma pessoa junto a um alvo, ou em uma organização-alvo, por meio de um processo natural de ingresso, ou admissão.

Desinformação

Essa é uma Ação de Busca muito utilizada no ramo da Contrainteligência. É realizada para, intencionalmente, confundir alvos (pessoas ou organizações) a fim de induzi-los a cometer erros de apreciação e levando-os a executar um comportamento pré-determinado.

Provocação

Consiste na Ação de Busca com alto nível de especialização realizada para fazer com que uma pessoa ou um alvo modifique seus procedimentos e execute algo desejado pela AI sem que esse 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. Ou seja, a entrevista visa a criar uma empatia entre os comunicantes e um envolvimento de tal forma que o entrevistador conduza a conversa no sentido de extrair o dado sem levantar suspeita.

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 e de Dados

É a Ação de Busca realizada por meio de equipamentos adequados, operados por integrantes da Inteligência Eletrônica.

Processos de Identificação de Pessoas (PIP)

É um conjunto de técnicas que deve considerar, sempre, a constante evolução tecnológica destinada a identificar ou a reconhecer pessoas. Fazem parte dos PIP a fotografia; a fotometria; o retrato falado; a datiloscopia; os exames de DNA, da arcada dentária, da voz e da íris; a tomada de medidas corporais; a descrição; os dados de qualificação, entre outras.

Observação, Memorização e Descrição (OMD)

Na execução das Operações de Inteligência, o profissional depara-se com a necessidade de observar atentamente e de memorizar o que foi observado, visto que, dependendo da operação, nem sempre é possível a utilização de equipamentos como filmadora, gravador, máquina fotográfica ou até mesmo de papel e caneta.

Estória-Cobertura (EC)

É a Técnica Operacional de Inteligência – TOI - de dissimulação utilizada para encobrir as reais identidades dos agentes das AI, bem como a realização das ações sigilosas operacionais de ISP, a fim de facilitar a obtenção de dados 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.

Compartimentação

É a limitação de acesso.

Vazamento

É a divulgação não autorizada de documento.

Comprometimento

Perda de segurança resultante de acesso não autorizado.

Referências

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **ABIN.** Disponível em: <http://abin.gov.br>. Acesso em: 05 nov. 2006.

ÁLVARES, Obino Lacerda. **Estudos de Estratégia.** Brasília: Biblioteca do Exército Editora, 1973.

AGÊNCIA CENTRAL DE INTELIGÊNCIA DA POLÍCIA MILITAR DE SANTA CATARINA (ACI – PMSC). **Nota de Aula da ACI para Treinamento Básico para Agentes de Inteligência.** 2005.

BRANCO. André Haydt Castello. **Doutrina Nacional de Inteligência de Segurança Pública.** Unisul. 2011.

BRANCO, André Haydt Castello. **Guia de estudo** – Análise de Inteligência – A Produção do Conhecimento, Nível Básico. 2012 – Centro Universitário UNIS.

BRANCO, André Haydt Castello. **Inteligência, Estratégia de Segurança Privada**: livro didático. UNISUL, 2013.

AGÊNCIA CENTRAL DE INTELIGÊNCIA DA POLÍCIA MILITAR DE SANTA CATARINA (ACI – PMSC). **Nota de Aula.** 2005.

AGÊNCIA CENTRAL DE INTELIGÊNCIA DA POLÍCIA MILITAR DE SANTA CATARINA (ACI/PMSC). **Salvaguarda de assuntos sigilosos**. 2005.

AGÊNCIA CENTRAL DE INTELIGÊNCIA DA POLÍCIA MILITAR DE SANTA CATARINA (ACI/PMSC). Salvaguarda de assuntos sigilosos: proteção ao conhecimento – legislação vigente. Coletânea de legislação. Brasília: Coordenação Geral de Biblioteca e Memorial de Inteligência, 2004.

ANDRADE, Gladston Gonçalves Vilela. **Atividade de informações/inteligência no Brasil: perspectivas e propostas.** Rio de Janeiro: Escola Superior de Guerra, 1998.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 17799.** Tecnologia da informação – Código de Prática para Gestão da Segurança de Informações. Rio de Janeiro, 2000.

_____. **ISO/IEC 27001.** Tecnologia da informação – Técnicas de Segurança – Sistemas de Gerenciamento de Segurança da Informação. Rio de Janeiro, 2005

BARBEIRO, Heródoto. **O relatório da CIA – Como será o mundo em 2020.** Rio de Janeiro: Ediouro, 2006.

BISHOP, M. **Computer Security Art and Sciense.** Boston:Addison Wesley, 2003.

BORGES, Celso Gonçalves. **Curso de inteligência policial militar** – nível "b". Goiânia: Polícia Militar de Goiás – PMGO, 1997, mimeo.

BRASIL. **Constituição Federal.** Brasília, DF, 2000.

CAMPEDELLI, Samira Yousseff et al. P**rodução de textos e usos da linguagem:** curso de redação. 2 ed. São Paulo: Editora Saraiva, 1999.

CEPIK, Marco A. C. **Espionagem e democracia.** Rio de Janeiro: Ed FGV, 2003.

_____. Inteligência, política e poder no Estado contemporâneo. **Revista de Sociologia e Política,** Curitiba, n.9, p.193-196, nov.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração.** 3. ed. São Paulo: McGraw-Hill do Brasil, 1983.

CONSELHO DE DESENVOLVIMENTO E INTEGRAÇÃO SUL. **CODESUL.** Disponível em: <http://www.codesul.com.br>. Acesso em: 13 dez. 2010.

DANTAS, George Felipe de Lima; SOUZA, Nelson Gonçalves de. **As bases introdutórias da análise criminal na inteligência policial.** Disponível em: <http://mj.gov.br/senasp/biblioteca/bibliot_artigos.htm>. Acesso em: 13 dez. 2010.

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

DOLABELLA, Rodrigo Paulo de Ulhôa. **Informação e Contra Informação:** a guerra de cérebros. Belo Horizonte: Editora Lastro Egl, 2009.

DORA, D. S. **Tutorial sobre Auditoria de Segurança.** Universidade Católica de Pelotas, 2001.

ESCOLA SUPERIOR DE GUERRA. **Manual Básico.** Rio de Janeiro: ESG, 1986.

FERMA – FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS. **Norma de gestão de riscos.** Airmic, Alarm, Irm: 2002.

FRASER, B. **RFC 2196** – Site Security Handbook, ISO/IEC, 1997.

GOMES, Rodrigo Carneiro. A repressão à criminalidade organizada e os instrumentos legais: sistemas de inteligência. **Jus Navigandi**, Teresina, ano 10, n. 1114, 20 jul. 2006. Disponível em: <http://jus2.uol.com.br/doutrina/texto.

asp?id=8669>. Acesso em: 12 nov. 2006.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata.** Niterói, RJ: Impetus, 2009.

GRUPO DE REDES, RFC 2196 - Site Security Handbook, 1997.

HOUAISS, Antônio. **Dicionário da Língua Portuguesa.** Rio de Janeiro: Objetiva, 2001.

JAMUNDÁ, Theobaldo. **O barriga-verde: versões e versões.** Florianópolis: IOESC, 1989.

JORNAL "A Notícia". Joinville, SC. Edição n. 23.958. 11 nov. 06. **Caderno AN Capital.** p. 05.

LANDWEHR, Carl E. **Computer security.** Springer-Verlag, 2001.

MAGALHÃES, Luiz Carlos. **A inteligência policial como ferramenta de análise do fenômeno: roubo de cargas no Brasil.** Disponível em: <http://www.infoseg.gov.br/infoseg/arquivos/a-inteligencia-policial-como-ferramenta-de-analise-do-fenomeno-roubo-de-cargas-no-brasil>. Acesso em: 10 dez. 2010.

MAGNOLI, Demétrio Martinelli. **O Mundo Contemporâneo.** São Paulo: Editora Ática, 1990.

MARCINEIRO, Nazareno. **Polícia Comunitária: evoluindo para a Polícia do século XXI.** Florianópolis: Insular, 2005.

McCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos.** Makron Books, 2000.

MELHOR: Gestão de Pessoas. Revista da Associação Brasileira de Recursos Humanos (ABRH-Nacional), out.2002.

MELLO, A. O. - Instituto dos Auditores Internos do Brasil. **Organização Básica da Auditoria Interna,** Biblioteca Técnica de Auditoria Interna.

MINISTÉRIO DA JUSTIÇA. **MJ.** Disponível em: <www.mj.gov.br/senasp/seat>. Acesso em: 05 nov. 2006.

MORAIS, Fernando. **Olga.** São Paulo: O Círculo do Livro, 1989.

NOSSO SÉCULO. Vol. 9 e 10. São Paulo: Editora Abril, 1980. **O Quinto Poder.** Disponível em: <http://www.oquintopoder.com.br>. Acesso em: 21 nov. 06.

PERRENOUD, Renato Penteado. **A análise de inteligência para o trabalho**

policial. São Paulo: PMSP/CSP-II, 1996.

PIRES, José Herculano. **Parapsicologia hoje e amanhã.** 9. ed. São Paulo: Edicel, 1987.

POLÍCIA MILITAR DE MINAS GERAIS (PMMG). **Cartilha de Policiamento Velado.** 1990.

POSEBOM, Francisco. **Redação de documentos de informação.** São Paulo: Polícia Militar do Estado de São Paulo, 1996, mimeo.

REVISTA UNIDADE: Revista de assuntos técnicos de Polícia Militar. n.48. Brigada Militar. Porto Alegre, 2001.

RODRIGUES, Lázaro Arruda. **O emprego do policial no sistema de inteligência Polícia Militar.** Monografia. Florianópolis, 1999.

RUSSEL, D., GANGEMI SR., G. T. **Computer security basics.** Nova Iorque: O'Reilly, 1992.

SANTA CATARINA. Constituição Estadual. Disponível em: <http://www.sc.gov.br>. Acesso em: 13 dez. 2010.

SANTIAGO, Carlos Alberto. **Apostila de Doutrina Geral de Polícia.** CEPM: Florianópolis, 1993.

SARTI, Antônio Carlos França. Organismos de Inteligência Policial no Mundo. **Revista Unidade.** n. 31. Brigada Militar. Porto Alegre: 1997. 92 p.

SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA E DEFESA DO CIDADÃO DO ESTADO DE SANTA CATARINA. **SSP/SC.** Disponível em: <http://ssp.sc.gov.br>. Acesso em: 13 dez. 2010.

SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. **SENASP.** Disponível em: <http://www.infoseg.gov.br>. Acesso em: 16 nov. 06.

SEGURANÇA MÁXIMA: o guia de um hacker para proteger seu site na internet e sua rede. Rio de Janeiro: Campus, 2002.

TONRY, Michael; MORRIS, Norval (orgs.). **Policiamento moderno.** São Paulo: EDUSP, 2003.

Sobre os professores conteudistas

André Haydt Castello Branco

Graduado Oficial do Exército pela Academia Militar das agulhas Negras – 1977; mestre pela Escola de Aperfeiçoamento de Oficiais – 1987; especialista em Análise de Inteligência pela Escola Nacional de Inteligência, em 1989; Chefe da Divisão de Inteligência do Centro de Inteligência do Exército – 2004; pós-graduado em Inteligência Estratégica pela Universidade Gama Filho – 2008 e 2009; Doutor em Curso de Altos Estudos Militares pela Escola de Comando e Estado Maior do Exército - 1992 e 1993; assessor na Agência Brasileira de Inteligência (ABIN) – 2008 a 2012; professor universitário em cursos de graduação e pós-graduação da Unisul Virtual.

Fred Harry Schauffert

É Coronel da Polícia Militar de Santa Catarina, graduado em Segurança Pública pela Academia de Polícia Militar da Trindade (APMT/PMSC), pós-graduado em Administração em Segurança Pública pela UNISUL. Ciclo de Estudos de Segurança Orgânica da Agência Brasileira de Inteligência (ABIN), membro do Fórum Permanente de Segurança Pública da Unisul.

Professor do Centro de Ensino da Polícia Militar nas áreas de Polícia Ostensiva, Ética e Cidadania e Gerenciamento do Estresse Profissional. Professor de Educação a Distância da Secretaria Nacional de Segurança Pública do Ministério da Justiça (SENASP/ MJ) e da Secretaria de Estado da Segurança Pública e Defesa do Cidadão de Santa Catarina (SSPDC/SC), nas áreas de Violência, Criminalidade e Prevenção; Mulher Vítima de Violência; Uso Legal da Força e Busca e Apreensão. Atuou como chefe da Agência de Inteligência (AI/P-2) do 8º Batalhão de Polícia Militar em Joinville/SC e como chefe da Agência Central de Inteligência (ACI) da Polícia Militar de Santa Catarina. Comandante da 1ª Região de Polícia Militar (Policiamento Metropolitano da Grande Florianópolis). Diretor de Saúde e Promoção Social da PMSC.

Luiz Otávio Botelho Lento

Oficial da Marinha da reserva, mestre em Ciência da Computação pela UNICAMP (Sistemas Distribuídos) e doutorando na UFSC no curso de Engenharia Elétrica, Departamento de Automação de Sistemas, com concentração na área de Segurança. Atuou no governo na área de segurança da informação; consultor de treinamento da Aker Security Solutions; consultor na área de redes e segurança da Empresa Immerson; gerente de rede e de segurança da Rede Acadêmica do UNICEUB; professor de disciplinas de rede de computadores e na área de segurança na graduação do UNICEUB, bem como orientações de projetos finais; professor de graduação e pós-graduação na área de redes de computadores e segurança na Universidade Católica de Brasília, bem como orientações de projetos finais.

Atualmente é professor de graduação da UNISUL nos cursos de Tecnologia de Redes de Computadores, Sistemas de Informação, Ciência da Computação e Engenharia Elétrica e Telemática, e coordenador do curso de pós-graduação de Implantação de Software Livre; professor do Senai Santa Catarina (CTAI) no curso superior de Tecnologia de Redes de Computadores e pós-graduação no curso de Gestão de Segurança da Informação em Redes de Computadores; consultor da FIESC (TIC) na área de redes de computadores e segurança; e consultor de segurança do CTAI.

Inteligência e Segurança Pública

Neste livro, são apresentados os meandros da Atividade de Inteligência e desvendados seus mistérios. Os assuntos abordam a utilidade da atividade da produção de conhecimentos que embasará processos decisórios de interesse da sociedade e sua importância na proteção de tudo que é sensível para o Estado brasileiro, assim como para qualquer organização, com destaque para as organizações policiais. Veremos a utilização de metodologias e técnicas que permitirão afastar a prática de ações pouco profissionais no trato com a atividade.

UNISUL

ISBN 9788578176129

9 788578 176129

www.unisul.br