

#VemPraFamart
famart.edu.br

PÓS-GRADUAÇÃO

INTELIGÊNCIA DE SEGURANÇA



famart
GRUPO EDUCACIONAL

INTELIGÊNCIA DE SEGURANÇA

DÚVIDAS E ORIENTAÇÕES

Segunda a Sexta das 09:00 as 18:00

ATENDIMENTO AO ALUNO

editorafamart@famart.edu.br



famart
GRUPO EDUCACIONAL

Sumário

Introdução	4
Origem da Atividade de Inteligência	4
A Atividade de Inteligência no Mundo Atual	8
Atividade de Inteligência no Brasil	15
Outros Organismos de Inteligência no Brasil	17
Características da Sociedade Contemporânea	18
Conceito de Inteligência	22
Conceito: Atividade de Inteligência de Segurança Pública	26
Inteligência Policial X Investigação	26
Conceito e diferença: Dado, Informação e Conhecimento	28
Conceitos e definições fundamentais da Atividade de Inteligência	29
Finalidades da Atividade de Inteligência	30
Características da Atividade de Inteligência	31
Legislação pertinente à Atividade de Inteligência	32
Classificação Sigilosa	60
Ramos da Atividade de Inteligência	62
Produção de Conhecimento	62
Princípios da Atividade de Inteligência	62
Valores da Atividade de Inteligência	64
Termos e Expressões usadas na Atividade de Inteligência	64
Técnicas utilizadas na Atividade de Inteligência	65
Procedimentos do Policiamento Ostensivo ao identificar um Agente de Inteligência	67
Procedimentos do Policiamento Ostensivo ao chegar no local da ocorrência	68
A Importância do Boletim de Ocorrência para o Serviço de Inteligência	68
Análise de Inteligência	72
Contra inteligência	76
Segurança Orgânica	77
Ameaças a Atividade de Inteligência	91
Referências	95

Introdução

O ser humano, há séculos procurou aliar a força do poderio militar, a qual representava a defesa e conquista, com o tratamento e valor da “**Informação**”, como elemento imprescindível à concretização de seus objetivos.

Na era do conhecimento, quando as informações circulam numa velocidade extraordinária e o crime se organiza de forma cada vez mais sofisticada, dispondo de modernas tecnologias e operando em plano internacional, não há mais lugar para uma polícia reativa, calcada em métodos superados, no empirismo e na intuição, impulsionada apenas pela dedicação e força de vontade dos seus agentes.

A atividade de Inteligência Policial passou a integrar o cotidiano das grandes corporações policiais, substituindo o poder da força, pelas vantagens do conhecimento. Não são mais os fortes que abatem, mas os ágeis e informados que superam os desinformados e lentos.

A inteligência consiste na produção de conhecimentos para tomada da melhor decisão, tendo como princípios básicos a **objetividade**, a **imparcialidade** e a **oportunidade**. É conceituada como processo informacional proativo que conduz à melhor tomada de decisão, seja ela estratégica ou operacional.

Origem da Atividade de Inteligência

Com sua origem remontando aos primórdios das civilizações, a atividade de inteligência sempre foi percebida como essencial para a governabilidade e garantia de segurança, não só em contextos de guerra, mas também em períodos de paz e ordem institucional. Modernamente, não se pode cogitar a existência de Estado que não disponha de órgãos de inteligência em sua estrutura.

Os relatos mais antigos sobre a origem da Atividade de Inteligência são encontrados na Bíblia Sagrada, no Velho Testamento, há 1.300 anos a.C., nos livros de Números, Josué e São Lucas, conforme podemos constatar nos trechos abaixo:

a. 1.300 a.C. – Israel - Bíblia Sagrada – Velho Testamento

Números, 13

1. O Senhor disse a Moisés:
 2. **“Envia homens para explorar a terra de Canaã, que eu hei de dar aos filhos de Israel. Enviarás um homem de cada tribo patriarcal, tomados todos entre os príncipes.”**
 3. Enviou-os Moisés do deserto de Farã segundo as ordens do Senhor; todos esses homens eram príncipes em Israel.
 4. Eis os seus nomes: da tribo de Rubem, Samua, filho de Zecur;
 5. da tribo de Simeão, Safat, filho de Huri;
 6. da tribo de Judá, Caleb, filho de Jefoné;
 7. da tribo de Issacar, Igal, filho de José;
 8. da tribo de Efraim, Oséias, filho de Nun;
 9. da tribo de Benjamim, Falti, filho de Rafu;
 10. da tribo de Zabulon, Gediel, filho de Sodi;
 11. da tribo de José, na tribo de Manassés, Gadi, filho de Susi;
 12. da tribo de Dã, Amiel, filho de Gemali;
 13. da tribo de Aser, Stur, filho de Miguel;
 14. da tribo de Neftali, Naabi, filho de Vapsi;
 15. da tribo de Gad, Guel, filho de Maqui.
 16. Estes são os nomes dos homens que Moisés enviou como exploradores a Canaã.
- Moisés deu a Oséias, filho de Nun, o nome de Josué.
17. Enviando-os a explorar a terra de Canaã, Moisés disse-lhes: “Ide pelo Negeb e subi a montanha.
 18. Examinai que terra é essa, e o povo que a habita, se é forte ou fraco, pequeno ou numeroso.
 19. Vede como é a terra onde habita, se é boa ou má, e como são as suas cidades, se muradas ou sem muros;

20. examinai igualmente se o terreno é fértil ou estéril, e se há árvores ou não. Coragem! E trazei-nos dos frutos da terra.” Era então a época das primeiras uvas.

21. Partiram, pois, e exploraram a terra desde o deserto de Sin até Roob, no caminho de Emat.

22. Subiram ao Negeb e foram a Hebron, onde se encontravam Aquimã, Sisai e Tolmai, filhos de Enac. Hebron fora construída sete anos antes de Tânis, no Egito.

23. Chegaram ao vale de Escol, onde cortaram um ramo de vide com um cacho de uvas, que dois homens levaram numa vara; tomaram também consigo romãs e figos.

24. Chamou-se a esse lugar vale de Escol, por causa do cacho que nele haviam cortado os israelitas.

25. Tendo voltado os exploradores, passados quarenta dias,

26. foram ter com Moisés e Aarão e toda a assembléia dos israelitas em Cades, no deserto de Farã. Diante deles e de toda a multidão relataram a sua expedição e mostraram os frutos da terra.

27. Eis como narraram a Moisés a sua exploração: “Fomos à terra aonde nos enviaste. É verdadeiramente uma terra onde corre leite e mel, como se pode ver por esses frutos.

28. Mas os habitantes dessa terra são robustos, suas cidades grandes e bem muradas; vimos ali até mesmo filhos de Enac.

29. Os amalecitas habitam na terra do Negeb; os hiteus, os jebuseus e os amorreus habitam nas montanhas, e os cananeus habitam junto ao mar e ao longo do Jordão.”

30. Caleb fez calar o povo que começava a murmurar contra Moisés, e disse: “Vamos e apoderemo-nos da terra, porque podemos conquistá-la.”

31. Mas os outros, que tinham ido com ele, diziam: “Não somos capazes de atacar esse povo; é mais forte do que nós.”

32. E diante dos filhos de Israel depreciaram a terra que tinham explorado: “A terra, disseram eles, que exploramos, devora os seus habitantes: os homens que vimos ali são de uma grande estatura;

33. vimos até mesmo gigantes, filhos de Enac, da raça dos gigantes; parecíamos gafanhotos comparados com eles.”

Josué, 2

1. Josué, filho de Nun, despachou de Setim secretamente dois espiões: Ide, disse-lhes ele, e examinai a terra e a cidade de Jericó. Em caminho, entraram em casa de uma prostituta chamada Raab, onde se alojaram.

São Lucas, 20

20. Puseram-se então a observá-lo e mandaram espiões que se disfarçassem em homens de bem, para armar-lhe ciladas e surpreendê-lo no que dizia, a fim de o entregarem à autoridade e ao poder do governador.

Nos trechos Bíblicos supracitados, podemos perceber o quanto a Atividade de Inteligência é antiga e o quão era e é essencial para as tomadas de decisões das autoridades, ou seja, quebrando barreiras do tempo e espaço entre os povos e nações até os dias atuais.

b. 500 a.C. – China - Sun Tzu – A Arte da Guerra

“Os espiões são os elementos mais importantes de uma guerra, porque neles repousa a capacidade de movimentação de um exército”.

c. 44 a.C. – Roma Antiga – Cifra de Júlio César

“Se ele tinha qualquer coisa confidencial a dizer, ele escrevia cifrado, isto é, mudando a ordem das letras do alfabeto, para que nenhuma palavra pudesse ser compreendida. Se alguém deseja decifrar a mensagem e entender seu significado, deve substituir a quarta letra do alfabeto, a saber 'D', por 'A', e assim por diante com as outras.”(Suetônio, A Vida de Júlio César).

A Atividade de Inteligência no Mundo Atual

O fato é que o mundo mudou, a produção do conhecimento se tornou cada vez mais importante, exigindo do indivíduo e da organização ações voltadas para a antecipação e prevenção. Tornou-se um elemento estratégico e sua gestão e utilização para produção de Inteligência é elemento básico para o desenvolvimento estratégico das organizações, contribuindo para que a organização responda mais rapidamente às ameaças e oportunidades. Chefes tomam decisões muitas vezes errôneas e equivocadas, com consequente prejuízo, por falta de informações seguras.

Foi nas guerras que a Inteligência se desenvolveu, particularmente, na Segunda Guerra Mundial e durante a Guerra Fria. Nas últimas décadas, surgiram diversas denominações, tais como: Business Intelligence, Inteligência Organizacional, Inteligência de Estado, Inteligência Militar, Inteligência de Segurança Pública, Tecnologia da Informação, Inteligência de Compras, Inteligência Competitiva, Inteligência Empresarial, etc. Porém, tudo é uma adaptação da atividade de Inteligência “clássica” à atividade de Inteligência específica.

O Presidente Barack Obama reforçou a segurança virtual dos Estados Unidos. Ele anunciou em Washington a criação da agência federal de prevenção de ataques contra redes de computadores do governo e de empresas. “De agora em diante, as redes e os computadores dos quais dependemos todos os dias, serão tratados como deveriam: como recurso nacional estratégico”, afirmou Obama.

Vivemos novos tempos e uma nova ordem mundial. O conhecimento tecnológico é cada vez mais um produto comercial entre os Estados, as empresas e organizações. Não há dúvida de que, na atual conjuntura deste mundo globalizado, com rápidas mudanças, esses atores procuram mais eficiência para a proteção do conhecimento por eles produzidos e guardados.

A todo o momento a mídia noticia casos de espionagem e sabotagem. Assim, torna-se interessante saber que o ato de sabotagem pode variar desde uma pequena ação individual até uma de grande porte, integrando um plano de caráter estratégico. Pode ser ainda um ato deliberado para destruir ideias e/ou a reputação de organizações e de pessoas, praticado por motivos variados.

A espionagem utiliza práticas ilegais para acessar dados, informações e conhecimentos. Porém, cabe ressaltar, que em torno de 90% do que se precisa pode ser coletado na Internet, em documentos públicos ou em entrevistas.

Um dos mais conhecidos exemplos de captação de dados é o sistema **Echelon**. Acredita-se que a NSA14 com a cooperação das agências equivalentes no Reino Unido

(Government Communications Headquarters), Canadá (Communications Security Establishment), Austrália (Defence Signals Directorate) e Nova Zelândia (Government Communications Security Bureau) sejam os responsáveis pelo Sistema. Suspeita-se, que façam interceptação das transmissões telefônicas, de fax e até tráfico de dados da Internet, com o objetivo de procurar ameaças à segurança mundial.

a. Agências de Inteligência do Mundo

ASIS – Austrália

Formado 13 de maio de 1952

Sede Canberra, Australian Capital Territory, Austrália

O Serviço Secreto Australiano de Inteligência, mais conhecido como ASIS (Australian Secret Intelligence Service), é a agência de inteligência do governo australiano, responsável pela coleta de inteligência externa, a realização de contraespionagem e atividades de cooperação com outras agências de inteligência no exterior. Por mais de vinte anos, a existência da agência era um segredo até mesmo de seu próprio governo. Sua responsabilidade principal é reunir informações de interesse, principalmente da Ásia e do Pacífico, utilizando agentes estacionados em uma ampla variedade de áreas. Seu principal objetivo, como a maioria das agências, é para proteger os interesses políticos e econômicos do país, garantindo segurança para o povo da Austrália contra ameaças nacionais.



RAW – Índia

Formado 21 de setembro de 1968

Sede Nova Deli, Índia

Asa de Pesquisa e Análise é a agência de inteligência externa da Índia. Ela foi formada em setembro de 1968, após a recém independente República da Índia foi confrontada com 2 guerras consecutivas, a guerra sino-indiana de 1962 e a guerra da Índia-paquistanesa de 1965, como era evidente que uma configuração de coleta de inteligência credível estava faltando. Sua função principal é a coleta de inteligência externa, contra-terrorismo e operações encobertas. Além disso, é responsável pela obtenção e análise de informações sobre governos estrangeiros, corporações e pessoas, a fim de aconselhar os políticos indianos estrangeiros.



DGSE – França

Formado 02 de abril de 1982

Precedendo agência Documentação Externa e Contra-Espionagem

Direção-geral da Segurança Externa é a agência France de inteligência externa. Operando sob a direção do ministério francês da Defesa, a agência trabalha com a DCRI (Direção Central de Inteligência Interior) no fornecimento de inteligência e segurança nacional, nomeadamente através da realização de operações paramilitares e contra-inteligência no exterior. A Direção-geral da Segurança Externa (DGSE), da França tem uma história bastante curta em comparação com outras agências de inteligência na região. Foi fundada oficialmente em 1982



a partir de uma infinidade de agências de inteligência anteriores no país. Seu principal foco é reunir informações de fontes estrangeiras para auxiliar nas decisões militares e estratégicas para o país. A agência emprega mais de cinco mil pessoas.

FSB – Rússia

Formado 03 de abril de 1995

Sede Praça Lubianka

Precedendo agência KGB

O Serviço de Segurança Federal da Federação Russa (FSB) é a agência de segurança nacional principal da Federação Russa e da agência principal sucessora da Cheka da era soviética, NKVD e KGB. O FSB está envolvido em contra-espionagem, segurança interna e de fronteiras, combate ao terrorismo, e de vigilância. Sua sede fica em Lubyanka Square, centro de Moscou, o mesmo local da antiga sede da KGB. O FSB é responsável pela segurança interna do Estado russo, contra-espionagem e a luta contra o crime organizado, terrorismo e tráfico de drogas. O número de pessoal do FSB e seu orçamento permanecem segredos de estado.



BND – Alemanha

Formado: 01 de abril de 1956

Agência Executiva: Gehlen Organização

Agência-mãe: Grupo Central de Inteligência

O Bundesnachrichtendienst é a agência de inteligência externa do governo alemão, sob o controle do



Gabinete do chanceler. O BND atua como um sistema de alerta precoce para subsidiar o governo alemão acerca de ameaças aos interesses alemães no exterior. Depende muito de vigilância e escutas eletrônicas de comunicações internacionais. Ele coleta e avalia as informações em uma variedade de áreas como o terrorismo internacional, proliferação de ADM e transferência ilegal de tecnologia, o crime organizado, tráfico de armas e de drogas, lavagem de dinheiro, imigração ilegal e guerra de informação. O serviço de inteligência da Alemanha no exterior, reúne militares e de inteligência civil.

MSS – China Jurisdição: República Popular da China

Sede: Pequim

Agência Executiva: Geng Huichang, Ministro de Estado de Segurança

Agência-mãe: Conselho de Estado

O Ministério da Segurança do Estado é o órgão de segurança da República Popular da China. O Artigo 4º da Lei de Processo Penal do país dá a MSS a mesma autoridade para prender ou deter pessoas que a polícia, nos crimes que envolvam a segurança do Estado, com supervisão das procuradorias e tribunais. Ela está sediada perto do Ministério da Segurança Pública da República Popular da China em Pequim. De acordo com Liu Fuzhi, Secretário-geral da Comissão de Política e Direito no âmbito do Comitê Central do Partido Comunista da



China e o ministro da Segurança Pública, a missão do MSS é garantir “a segurança do Estado, através de medidas eficazes contra o inimigo agentes, espiões e contra-revolucionárias atividades destinadas a sabotar ou derrubar o sistema Socialista da China. Muitos agentes do MSS dizem ter operado na região da Grande China (Hong Kong, Macau e Taiwan) e integraram-se com numerosas comunidades chinesas ultramarinas. Cerca de 120 agentes que operavam em condições não oficiais nos EUA, Canadá, Europa Ocidental, Norte da Europa e Japão, como empresários, banqueiros, acadêmicos e jornalistas foram convocados para a China, fato que demonstra a ampla cobertura do MSS.

CIA – América**Formado:** 18 de setembro de 1947**Agência-mãe:** Grupo Central de Inteligência

A CIA é a maior das agências de inteligência e é responsável por coletar dados de outros países que poderiam afetar a política dos EUA. É uma agência de inteligência civil do governo dos Estados Unidos, responsável pelo fornecimento de informações de segurança nacional a altos responsáveis políticos dos Estados Unidos. A CIA também se engaja em atividades secretas a pedido do presidente dos Estados Unidos da América. A função principal da CIA é coletar informações sobre governos estrangeiros, corporações e indivíduos, assim como aconselhar políticas públicas. A agência realiza operações clandestinas e ações paramilitares e exerce influência política externa através da sua Divisão de Atividades Especiais. No 50º aniversário da CIA, o presidente Clinton disse: “Por necessidade, o povo americano nunca vai saber a história completa de sua coragem. Na verdade, ninguém sabe”. Altamente financiada, é tecnologicamente, a mais avançada Inteligência set-up do mundo.

**M1-6 – Reino Unido****Formado:** 1909 como o Bureau Serviço Secreto**Jurisdição:** Governo do Reino Unido**Sede:** Vauxhall Cross, London**Ministro responsável:** Secretário de Relações Exteriores**Agência-mãe:** Foreign and Commonwealth Office

Os britânicos tiveram uma percepção pública de uma agência de inteligência eficaz (devido ao sucesso dos filmes de James Bond, apesar do glamour cinematográfico). Esta percepção corresponde a realidade MI6, o equivalente britânico para a CIA. Algumas histórias surgiram na Guerra Fria, o MI6 recrutou Oleg Penkovsky, que desempenhou um papel chave na resolução favorável da Crise dos Mísseis Cubanos, e Oleg Gordievski, que operou durante uma década antes do MI6. Existem também rumores de que o MI6 teria sabotado o Tu-144 supersônico, programa aeronáutico, através da alteração de documentos, afim de certificar-se de o projeto não cairia nas mãos da KGB.

Mossad – Israel

Formado: 13 de dezembro de 1949 como o Instituto Central de Coordenação

Agência-mãe: Gabinete do Primeiro-Ministro



O Mossad é responsável pela coleta de inteligência e operações encobertas, incluindo atividades paramilitares. É uma das principais entidades na comunidade de inteligência israelense, juntamente com Aman (inteligência militar) e do Shin Bet (segurança interna). A lista de seus sucessos é longa. A Agência de inteligência de Israel é a mais famosa por ter capturado agentes da OLP em retaliação pelo ataque que matou onze atletas israelenses nas Olimpíadas de 1972 em Munique. Esta agência tem outro sucesso relacionado ao seu nome, incluindo a aquisição de um MiG-21 antes da guerra dos Seis Dias de 1967 e do roubo dos planos para o Mirage 5, após o negócio com a França ter sido frustrado. O Mossad também ajudou os Estados Unidos no apoio à Polônia durante a década de 1980.

ISI – Paquistão

Formado: 1948

Jurisdição: Governo do Paquistão

Sede: Islamabad, Paquistão



Com o registro mais longo de sucessos, O Paquistão tem a melhor Inteligência da qual se tem conhecimento até agora. O Inter-Services Intelligence foi criado como uma unidade independente em 1948, a fim de fortalecer o desempenho da Inteligência Militar do Paquistão, durante a guerra indopaquistanesa de 1947. Seu sucesso em evitar uma invasão de longa escala do Paquistão, por parte dos soviéticos, é um feito não igualado por qualquer outro meio fora do mundo da inteligência. KGB, o melhor de seu tempo, não conseguiu contrariar a ISI e proteger os interesses soviéticos da Ásia Central. Em sua história não existem registros de agentes duplos ou desertores. Ela tem protegido suas armas nucleares desde formada e tem frustrado tentativas da Índia para alcançar a supremacia, através da desestabilização interna da Índia. Está acima de todas as leis em seu país. Suas políticas são feitas “fora” de todas as outras instituições, com exceção do Exército. Acredita que esta é a agência de inteligência com o maior número de agentes de todo o mundo, perto de 10.000.

Atividade de Inteligência no Brasil

A história da Atividade de Inteligência no Brasil teve origem em 1927, quando foi criado o Conselho de Defesa Nacional, órgão diretamente subordinado ao Presidente da República. Até então, a atividade era exercida apenas no âmbito dos ministérios militares. Diversas foram as reformulações introduzidas na então atividade de Informações ao longo do processo político nacional. Entre elas, cabe citar a criação, ocorrida em 6 de setembro de 1946, do **Serviço Federal de Informações e Contra-Inteligência** (SFICI).

O Brasil, no início da década de 60, apresentou um cenário interno bastante conturbado, gerando manifestações de segmentos da sociedade. O quadro evoluiu para uma intervenção militar no processo político nacional, a partir de março de 1964. Na ocasião, foi extinto o SFICI e criado o **Serviço Nacional de Informações (SNI)**.

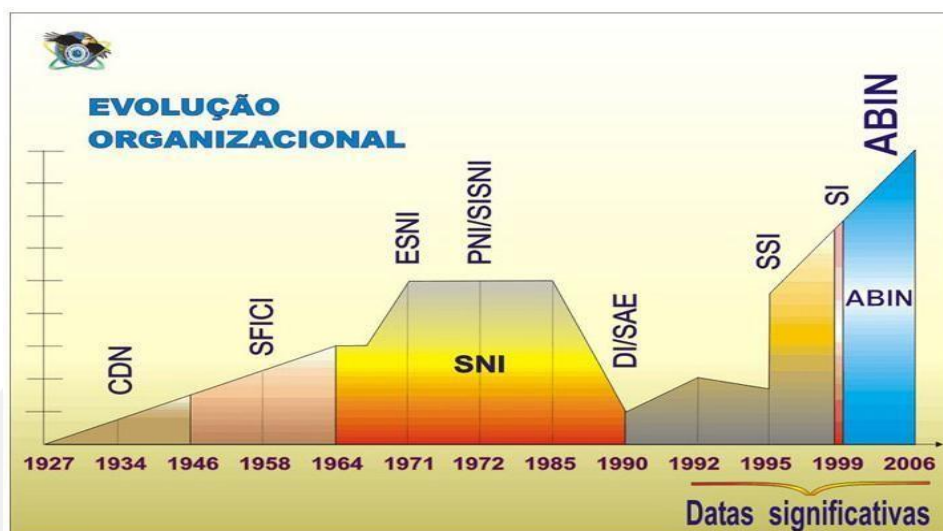
Foi criado, em 1970, o **Sistema Nacional de Informações (SISNI)**, integrado por todos os órgãos de informações dos ministérios civis e militares. O SNI era o órgão central desse sistema.

A partir de 1979, procurou-se ajustar as estruturas de Informações aos novos tempos, pois já estava em andamento o processo de redemocratização do país. Os governos da época buscaram alternativas no sentido de reposicionar a atividade de Informações em seu correto espaço e devido limite.

Em 1990, no contexto de ampla reforma da Administração Pública Federal, o SNI foi extinto. O exercício perene da atividade, todavia, foi preservado com a criação da Secretaria de Assuntos Estratégicos (SAE), que absorveu as atribuições do SNI.

Em 7 de dezembro de 1999, o Presidente da República instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência (ABIN). A criação da Agência proporcionou ao Estado brasileiro institucionalizar a atividade de Inteligência, mediante ações de coordenação do fluxo de informações necessárias às decisões de Governo, no que diz respeito ao aproveitamento de oportunidades, aos antagonismos e às ameaças, reais ou potenciais, para os mais altos interesses da sociedade e do país.

Linha do Tempo



Fonte: Site da ABIN, acesso em 9 nov. 2012.

Outros Organismos de Inteligência no Brasil

A comunidade de inteligência é formada, portanto, por unidades de inteligência nos mais variados setores da Administração Pública e, também, em empresas privadas. Em termos de Executivo Federal, os órgãos com poder de polícia ou com atribuições que envolvam fiscalização e controle dispõem – ou deveriam dispor – de setores de inteligência.

Além da ABIN, que é o órgão federal, por excelência responsável pelas ações de inteligência, destacam-se:

- a. Os setores de inteligência dos Comandos Militares – do Exército, da Marinha e da Aeronáutica – e do Ministério da Defesa, voltados, preponderantemente, à inteligência militar;
- b. As áreas de inteligência de órgãos de fiscalização, como a da Receita Federal, do INSS e do IBAMA;
- c. Os setores de inteligência direcionados à área financeira – do Banco Central do Brasil ou de bancos estatais, como a Caixa Econômica Federal;

d. A unidade de inteligência financeira encarregada da coordenação das atividades de combate à lavagem de dinheiro – o COAF;

e. Unidades de inteligência policial – na Polícia Federal, na Polícia Rodoviária Federal e nas polícias estaduais civis e militares.

A maior parte desses órgãos mantém relações com seus congêneres de outros países, alguns inclusive com "adidos" em representações brasileiras no estrangeiro, que atuam na área de inteligência policial e militar. Assim, os órgãos de inteligência governamental e policial brasileiros encontram-se conectados com serviços de inteligência das nações hemisféricas e de outros continentes, o que constitui importante alicerce para a cooperação internacional na prevenção e no combate a organizações criminosas e terroristas.

Características da Sociedade Contemporânea

Borges (2008, p. 179) não faz distinção entre Sociedade da Informação e Sociedade do Conhecimento, ao dizer que: “A Sociedade da Informação e do conhecimento é reconhecida pelo uso intenso da informação e do conhecimento e das tecnologias de informação e da comunicação, na vida do indivíduo e da sociedade, em suas diversas atividades.” Demonstrando a relação existente entre: informação, conhecimento e tecnologia, categorias intrínsecas a toda tentativa de conceituação da nova sociedade. Não se pode discutir Sociedade da Informação e Sociedade do Conhecimento sem mencionar a Cúpula Mundial da Sociedade da Informação. Evento promovido pela Organização das Nações Unidas (ONU) que ocorreu em 2003 em Genebra e em 2005 na Tunísia, o qual contou com a participação de diversas entidades e organismos interessados na temática e no desenvolvimento da sociedade.

Segundo Ambrosi, Pimenta e Peugeot (2005) esse evento serviria para pensar a respeito da diminuição da exclusão digital global, que separa países periféricos dos ditos centrais, alargando o acesso à Internet. O mesmo possuía objetivos claros,

porém para alguns, esses objetivos estavam ligados diretamente à preocupação do: “impacto da informação nos sistemas de produção”, em, “Escolher o modo de produção como a característica fundamental de uma sociedade [o que] não é uma atitude neutra.” (Ambrosi, Pimenta e Peugeot, 2005).

A importância da informação e do conhecimento, como molas propulsoras do desenvolvimento da Sociedade do Conhecimento. Nesse contexto, a informação é considerada o insumo básico para o desenvolvimento do conhecimento, ou seja, não são sinônimos. O conhecimento vem a ser o valor agregado à informação, é o „o que se faz com ela”; o diferencial que culminará na tomada de decisões acertadas, no saber fazer.

Desse modo, se de um lado tem-se a informação como mola propulsora do crescimento do capitalismo e, com isso o aumento de desigualdades sociais, de outro lado, tem-se o desenvolvimento de uma consciência maior, plural, que escapa ao mando das grandes potências econômicas, haja vista às potencialidades ofertadas pelo próprio desenvolvimento das tecnologias da informação e comunicação, através das quais a informação parece adquirir força própria e se dissipar ciberespaço afora, sem possibilidades de controle.

Segundo Lucci (2000): “Essa nova sociedade que está se formando, e que tem por base o capital humano ou intelectual, é chamada de Sociedade do Conhecimento. Nessa sociedade onde as ideias, portanto, passam a ter grande importância, estão surgindo em várias partes do mundo os Think Thanks, que nada mais são do que grupos ou centros de pensamento para a discussão de ideias. Esses centros têm por objetivo a construção de um mundo, de uma sociedade mais saudável do ponto de vista econômico e social, que possa desfrutar de uma melhor qualidade de vida. ”

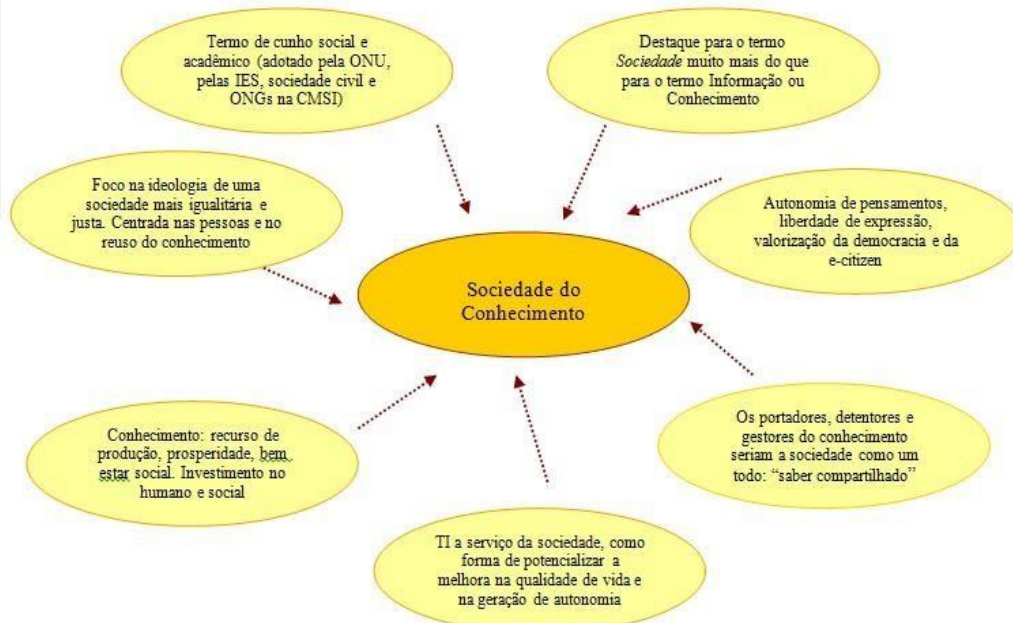
Sendo assim, o que por vezes parece se experimentar em alguns momentos na história da sociedade contemporânea, mesmo que ainda de modo tímido, é a frutificação da semente da liberdade, adquirida pela tomada de consciência, promovida pelo acesso à informação, a qual, mesmo nos países periféricos, consegue, ainda que heterogeneamente, chegar de forma mais efetiva do que outrora e, de certo modo, mobilizar e se constituir.

De acordo com Burch (2005) é perceptível a existência de duas realidades distintas. A que apresenta uma sociedade existente (Sociedade da Informação) e a que é desejada (Sociedade do Conhecimento) por organismos que se importam com o desenvolvimento social, como as universidades, alguns braços da ONU, Organizações não governamentais (ONGs), mas que, infelizmente, ainda é uma sociedade em potencial e não uma realidade circunscrita.

Dado o teor da sua importância, procura-se identificar aspectos positivos da aplicação das tecnologias da informação e comunicação nas sociedades contemporâneas, uma vez que as mesmas têm um caráter que transcende qualquer projeto de comunicação anterior; elas podem auxiliar a potencializar o poder da comunicação, podem auxiliar a romper barreiras geográficas, podem auxiliar a pôr em contato diversas culturas, unir através de fóruns cidadãos que jamais se encontrariam se não fosse via aparato tecnológico, dada a distância geográfica e a diversidade econômica e social, as quais indivíduos de sociedades distantes vivenciam. As tecnologias da informação e comunicação podem auxiliar, quanto aos governos possibilitarem espaços públicos que se transformem em cenários de pleitos, onde cidadãos comuns passam a ter voz e voto, destituindo muitas vezes o caráter representativo existente na contemporaneidade. Uma nova forma de organização político-social emerge conjuntamente com as mazelas sociais que o mau planejamento da incorporação das tecnologias da informação e comunicação pelas sociedades traz. Sendo assim, os aspectos positivos precisam ser pensados e bem administrados pelos governos e sociedades, para que se tire proveito do que elas (tecnologias) têm de melhor a oferecer e, para que, se dirimam os aspectos negativos e tendenciosos.



Fonte: Disponível em: <http://www.dgz.org.br/out11/Art_01.htm>.



Fonte: Disponível em: <http://www.dgz.org.br/out11/Art_01.htm>.

Conceito de Inteligência

Segundo Veronezzi (Artigo: Os 7 Tipos de Inteligência: de que Tipo é o seu Cérebro?

“Durante grande parte dos séculos 19 e 20, acreditou-se que a inteligência era algo que podia ser facilmente medido, determinado e comparado através de testes, como o famoso teste de QI, por exemplo, que dava a inteligência da pessoa em números. No entanto, com o tempo, o teste de QI foi caindo em descrédito, pois pouco a pouco foi se notando que nem sempre as pessoas mais inteligentes e bem-sucedidas obtinham os melhores resultados.

Os psicólogos e pesquisadores começaram a notar que existiam inúmeros casos de pessoas que obtinham resultados medíocres nos testes de QI, mas que tinham um excelente desempenho na vida, pois eram pessoas determinadas, disciplinadas, persistentes e carismáticas.

Como pessoas consideradas “burras” pelo teste de QI poderiam ter tanto sucesso? A resposta é simples: existem vários tipos de inteligência !!

Segundo **Howard Gardner**, psicólogo e autor desta teoria, existem ao todo 7 tipos de inteligência e todas as pessoas tem um pouco das 7 combinadas dentro de si. No entanto, cada pessoa tem uma delas desenvolvida de modo mais forte e que se sobrepõe sobre as outras.

Os 7 Tipos de Inteligência

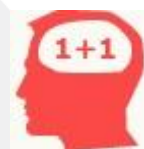
Os 7 tipos de inteligência identificados no trabalho de Howard Gardner são:

Inteligência Linguística



As pessoas que possuem este tipo de inteligência têm grande facilidade de se expressar, tanto oralmente quanto na forma escrita. Além de possuírem grande expressividade, elas também têm um alto grau de atenção e uma alta sensibilidade para entender pontos de vista alheios. É uma inteligência fortemente relacionada ao lado esquerdo do cérebro e uma das inteligências mais comuns.

Inteligência Lógica



Pessoas com esse perfil de inteligência tem uma alta capacidade de memória e um grande talento para lidar com matemática e lógica em geral. Elas tem facilidade para encontrar solução de problemas complexos, tendo a capacidade de dividir estes problemas em problemas menores e ir resolvendo-os até chegar a resposta final. São pessoas organizadas e disciplinadas. É uma inteligência fortemente relacionada ao lado direito do cérebro.



Inteligência Motora

Pessoas com este tipo de inteligência possuem um grande talento em expressão corporal e tem uma noção espantosa de espaço, distância e profundidade. Tem um controle sobre o corpo, maior que o normal, sendo capazes de realizar movimentos complexos, graciosos ou então fortes com enorme precisão e facilidade. É uma inteligência relacionada a porção do cérebro que controla os movimentos voluntários do corpo. Presente em esportistas olímpicos e de alta performance. É um dos tipos de inteligência diretamente relacionado a coordenação e capacidade motora.



Inteligência Espacial

Pessoas com este perfil de inteligência tem uma enorme facilidade para criar, imaginar e desenhar imagens 2D e 3D. Elas tem uma grande capacidade de criação em geral, mas, principalmente, tem um enorme talento para a arte gráfica. Pessoas com este perfil de inteligência tem como principais características a criatividade e a sensibilidade, sendo capazes de imaginar, criar e enxergar coisas que, aqueles que não têm este tipo de inteligência desenvolvido, em geral, não consegue.

Inteligência Musical



É um dos tipo raros de inteligência. Pessoas com este perfil tem uma grande facilidade para escutar músicas ou sons em geral e identificar diferentes padrões e notas musicais. Eles conseguem ouvir e processar sons, além do que a maioria das pessoas consegue, sendo capazes também de criar novas músicas e harmonias inéditas. Pessoas que têm este perfil, sentem como se conseguissem “enxergar” através dos sons. Algumas pessoas tem esta inteligência tão evoluída que são capazes de aprender a tocar instrumentos musicais sozinhas. Assim como a inteligência espacial, este é um dos tipos de inteligência fortemente relacionados a criatividade.

Inteligência Interpessoal



Inteligência interpessoal é um tipo de inteligência ligada a capacidade natural de liderança. Pessoas com este perfil de inteligência são extremamente ativas e em geral causam uma grande admiração nas outras pessoas. São os líderes práticos, aqueles que chamam a responsabilidade para si. Eles são calmos, diretos e tem uma enorme capacidade para convencer as pessoas a fazer tudo o que ele achar conveniente. São capazes também de identificar as qualidades das pessoas e extrair o melhor delas, organizando equipes e coordenando trabalhos em conjunto.

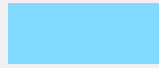
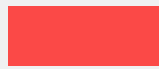
Inteligência Intrapessoal



É um tipo raro de inteligência, também relacionado a liderança. Quem desenvolve a inteligência interpessoal tem uma enorme facilidade em entender o que as pessoas pensam, sentem e desejam. Ao contrário dos líderes interpessoais que são ativos, os líderes intrapessoais são mais reservados, exercendo a liderança de um modo mais indireto, através do carisma e influenciando as pessoas através de ideias e não de ações. Entre os tipos de inteligência, este é considerado o mais raro.

As Inteligências Predominantes:

Cálculo percentual quanto a predominância dos tipos de inteligência, em relação a população geral:

Inteligência Linguística *	29 %	
Inteligência Lógica *	29 %	
Inteligência Motora	16 %	
Inteligência Espacial	14 %	
Inteligência Musical	6 %	
Inteligência Interpessoal	4 %	

Inteligência Intrapessoal	2 %	
----------------------------------	-----	--

Segundo Cepik (2001, p. 24) “Há dois usos principais do termo inteligência fora do âmbito das ciências cognitivas. Uma definição ampla, diz que inteligência é toda informação coletada, organizada ou analisada para atender às demandas de um tomador de decisões qualquer. Para a ciência da informação, inteligência é uma camada específica de agregação e tratamento analítico em uma pirâmide informacional, formada, na base, por dados brutos e, no vértice, por conhecimentos reflexivos. A sofisticação tecnológica crescente dos sistemas de informação que apóiam a tomada de decisões, tornou corrente o uso do termo inteligência para designar essa função de suporte, seja na rotina dos governos, no meio empresarial ou mesmo em organizações sociais. Nesta acepção ampla, inteligência é o mesmo que conhecimento ou informação analisada.”

Conceito: Atividade de Inteligência de Segurança Pública

Segundo a Doutrina Nacional de Inteligência e Segurança Pública – DNISP (2009, p. 11) “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 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.”

Inteligência Policial X Investigação

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

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

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

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

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

Nesse sentido, o sigilo como princípio da atividade de ISP fica, em caráter excepcional mitigado, quando houver necessidade de emprestar aos procedimentos policiais e judiciais elementos de provas. Neste caso, deverão os chefes das AI valerem-se dos procedimentos e limites estabelecidos na legislação aplicável.

Enquanto a investigação policial tem como propósito básico instrumentar a persecução penal, a inteligência policial pode ser percebida como um instrumento de apoio e assessoria da atividade fim policial (inteligência tática) e da gestão da segurança pública e da defesa social (inteligência estratégica).

Veremos abaixo outras definições e diferenças:

a. **Atividade de Inteligência** - 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.

b. **A inteligência policial** - atua na prevenção, obstrução, identificação e neutralização das ações criminosas.

c. **Investigação Criminal** - é o conjunto de procedimentos interdisciplinares, de natureza inquisitiva, que busca, de forma sistematizada, a produção da prova de um delito penal.

d. **A investigação policial** - é uma pesquisa sobre pessoas e coisas úteis para a reconstrução das circunstâncias de um fato legal ou ilegal e sobre a ideia que se tem a respeito deste.

Conceito e diferença: Dado, Informação e Conhecimento

Para SANTIAGO Jr, dados podem ser considerados: “Uma sequência de números e palavras, sob nenhum contexto específico. Entretanto, quando os dados são organizados com a devida contextualização, há a informação. Já o conhecimento é a informação organizada, com o entendimento de seu significado.” (SANTIAGO Jr., 2004, p. 27)

Portanto, veremos agora os conceitos e diferenças entre dado, informação e conhecimento:

a. **Dados** – São informações fora de um contexto, sem valor suficiente para compreensão de um fenômeno, ou seja, o meio pelo qual a informação e o conhecimento são transferidos.

Exemplos: Data, local, hora do crime, perfil da vítima e do suspeito, etc.

b. **Informação** – São dados organizados, manipulados e tratados dentro de um contexto, contendo algum significado como explicação de um determinado fato.

Exemplos: A notícia de que alguém foi visto, pouco antes do crime, saindo da casa onde foi encontrado o cadáver da vítima. A significação dada às gotículas de sangue encontradas na cena do crime, como indicativas de que a vítima teria sido conduzida para aquele ambiente já ferida ou de que o autor teria saído da cena do crime com alguma lesão.

c. **Conhecimento** é a informação organizada, contextualizada e com o entendimento de todos seus significados. É resultado da interpretação da informação e de sua aplicação em algum fim, especificamente para gerar novas hipóteses, resolver problemas ou tomar decisões.

Exemplo: A pessoa que foi vista saindo da casa onde foi encontrado o cadáver da vítima era seu ex-marido, que, enciumado, deu-lhe dois tiros no peito e depois fugiu para Madri levando as duas filhas menores.

Conceitos e definições fundamentais da Atividade de Inteligência

A Atividade de Inteligência de Segurança Pública, balizada por sua Doutrina, procura **conhecer, estudar, interpretar, difundir e orientar** os valores de uma nação, baseados no modo próprio de pensar, agir e sentir de seu povo, que abranjam os interesses nacionais e do mundo em que vive e do qual são atores. É formulada para orientar o pensamento crítico e permitir contribuições para o enriquecimento da produção de conhecimentos, orientando-a num sentido tático e estratégico. Seu esquema, voltado para a aplicação do método, é formulado a partir desses valores.

A Doutrina de Inteligência é o conjunto de princípios, conceitos, normas, métodos e valores que orientam e disciplinam a Atividade de Inteligência de Segurança Pública.

A Doutrina de Inteligência de Segurança Pública embasa-se nos princípios da Constituição Brasileira, com ênfase no respeito aos direitos sociais e individuais, no pluralismo político, na harmonia social e na ordem interna, objetivando alicerçar e dar eficácia à Atividade de Inteligência de Segurança Pública. Assim sendo, todas as suas ações serão sempre exercidas em proveito dos mais elevados interesses da Justiça e em defesa permanente da Sociedade e do Estado.

A Atividade de Inteligência de Segurança Pública é o exercício permanente e sistemático de ações especializadas para **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 federais e estaduais na tomada de decisões, para o **planejamento** e a **execução** de uma política de Segurança Pública e das ações para **prever**, **prevenir**, **neutralizar** e **reprimir** atos criminosos de qualquer natureza ou atentatórios a ordem pública

O emprego da Atividade de inteligência Policial é utilizado com o objetivo de coletar dados e informações não disponíveis, na produção e difusão de conhecimentos, relativos a fatos e situações de imediata ou potencial influência sobre o processo decisório. A ação governamental, a salvaguarda e a segurança da sociedade e do Estado. A inteligência deve ser utilizada em submissão a autoridade legítima da nossa Carta Magna, protegendo o direito e as garantias individuais. As ações devem ser desenvolvidas com caráter preventivo e ofensivo. A atividade de inteligência não pode ser vista ou utilizada apenas como repressão, mas também como prevenção. Devendo ser uma ferramenta utilizada pelas autoridades no planejamento de combate ao crime. Reunir dados e informações precisas que possam subsidiar o fornecimento de provas nos processos judiciais e/ou no simples flagrante delito executado pelo Policial Militar.

Finalidades da Atividade de Inteligência

- a. **Proporcionar** diagnósticos e prognósticos sobre a evolução de situações do interesse da segurança Pública, subsidiando seus usuários no processo decisório;
- b. **Contribuir** para que o processo interativo entre usuários e profissionais de Inteligência produza efeitos cumulativos, aumentando o nível de efetividade desses usuários e de suas respectivas organizações;
- c. **Subsidiar** o planejamento estratégico integrado do sistema e a elaboração de planos específicos para as diversas organizações do Sistema de Segurança Pública;
- d. **Apoiar** diretamente com informações relevantes as operações policiais de prevenção, repressão, patrulhamento ostensivo e de investigação criminal;

- e. **Prover** alerta avançado para os responsáveis civis e militares contra crises, grave perturbação da ordem pública, ataques surpresa e outras intercorrências;
- f. **Auxiliar** na investigação de delitos;
- g. **Preservar** o segredo governamental sobre as necessidades informacionais, as fontes, fluxos, métodos, técnicas e capacidades de Inteligência das agências encarregadas da gestão da segurança pública.

Características da Atividade de Inteligência

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

Suas principais características são:

- a. **Produção de Conhecimento:** é a característica da Atividade de Inteligência de Segurança Pública- ISP, que qualifica como uma atividade de inteligência, na medida em que coleta e busca dados e, por meio de metodologia específica, transforma-os em conhecimento preciso, com a finalidade de assessorar os usuários no processo decisório;
- b. **Assessoria** é a característica da ISP que qualifica como órgão de assessoramento, produzindo conhecimento para o processo decisório e para auxiliar as polícias em suas atividades.
- c. **Verdade como Significado** é a característica da ISP que torna uma produtora de conhecimento precisos, claros e imparciais, de tal modo que consiga expressar as intenções, óbvias ou subentendidas, das pessoas envolvidas ou mesmo as possíveis ou prováveis consequências dos fatos relatados.
- d. **Busca de dados Protegidos** é a características da ISP de obter dados não disponíveis e protegidos, em um universo antagônico, uma vez que os dados relevantes do ambiente criminal encontram-se, invariavelmente, protegidos.
- e. **Ações Especializadas** é a característica da ISP que, em face da metodologia, técnica e linguagem próprias e padronizadas, exige dos seus integrantes formação acadêmica, permanente, complementada por treinamento e experiência.

- f. **Economia de Meios** é a característica da ISP que permite otimizar os recursos disponíveis, proporcionada pela produção de conhecimento objetivos, precisos e oportunos.
- g. **Iniciativa**: é a características da ISP que induz a produção constante de conhecimentos antecipados em atitude pró-ativa.
- h. **Abrangência**: é a característica da ISP que, em razão dos métodos e sistematização peculiares, permite-lhe ser empregada em qualquer campo do conhecimento de interesse da segurança pública.
- i. **Segurança** é a característica da ISP que visa garantir sua existência, protegidos de ameaças.

Legislação pertinente à Atividade de Inteligência

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. (**Art. 2º Lei nº 9.883 de 07 de Dezembro de 1999**).

a. Lei nº 9.883, 7 de dezembro de 1999

Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.

O PRESIDENTE DA REPÚBLICA. Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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 contra-inteligência 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. (Vide Medida Provisória nº 2.216-37, de 2001)

Parágrafo único. As atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado.

Art. 4º À ABIN, além do que lhe prescreve o artigo anterior, compete:

- I - planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;
- II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;
- III - avaliar as ameaças, internas e externas, à ordem constitucional;
- IV - promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

Parágrafo único. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

Art. 5º A execução da Política Nacional de Inteligência, fixada pelo Presidente da República, será levada a efeito pela ABIN, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo.

Parágrafo único. Antes de ser fixada pelo Presidente da República, a Política Nacional de Inteligência será remetida ao exame e sugestões do competente órgão de controle externo da atividade de inteligência.

Art. 6º O controle e fiscalização externos da atividade de inteligência serão exercidos pelo Poder Legislativo na forma a ser estabelecida em ato do Congresso Nacional.

§ 1º Integrarão o órgão de controle externo da atividade de inteligência os líderes da maioria e da minoria na Câmara dos Deputados e no Senado Federal, assim como os Presidentes das Comissões de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal.

§ 2º O ato a que se refere o caput deste artigo definirá o funcionamento do órgão de controle e a forma de desenvolvimento dos seus trabalhos com vistas ao controle e fiscalização dos atos decorrentes da execução da Política Nacional de Inteligência.

Art. 7º A ABIN, observada a legislação e normas pertinentes, e objetivando o desempenho de suas atribuições, poderá firmar convênios, acordos, contratos e quaisquer outros ajustes.

Art. 8º A ABIN será dirigida por um Diretor-Geral, cujas funções serão estabelecidas no decreto que aprovar a sua estrutura organizacional.

§ 1º O regimento interno da ABIN disporá sobre a competência e o funcionamento de suas unidades, assim como as atribuições dos titulares e demais integrantes destas.

§ 2º A elaboração e edição do regimento interno da ABIN serão de responsabilidade de seu Diretor-Geral, que o submeterá à aprovação do Presidente da República.

Art. 9º Os atos da ABIN, cuja publicidade possa comprometer o êxito de suas atividades sigilosas, deverão ser publicados em extrato.

§ 1º Incluem-se entre os atos objeto deste artigo os referentes ao seu peculiar funcionamento, como às atribuições, à atuação e às especificações dos respectivos cargos, e à movimentação dos seus titulares.

§ 2º A obrigatoriedade de publicação dos atos em extrato independe de serem de caráter ostensivo ou sigiloso os recursos utilizados, em cada caso.

Art. 9º A - (Vide Medida Provisória nº 2.216-37, de 2001)

Art. 10º A ABIN somente poderá comunicar-se com os demais órgãos da administração pública direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, com o conhecimento prévio da autoridade competente de maior hierarquia do respectivo órgão, ou um seu delegado.

Art. 11º Ficam criados os cargos de Diretor-Geral e de Diretor-Adjunto da ABIN, de natureza especial, e os em comissão, de que trata o Anexo a esta Lei.

Parágrafo único. São privativas do Presidente da República a escolha e a nomeação do Diretor-Geral da ABIN, após aprovação de seu nome pelo Senado Federal.

Art. 12º A unidade técnica encarregada das ações de inteligência, hoje vinculada à Casa Militar da Presidência da República, fica absorvida pela ABIN.

§ 1º Fica o Poder Executivo autorizado a transferir para a ABIN, mediante alteração de denominação e especificação, os cargos e funções de confiança do Grupo-Direção e Assessoramento Superiores, as Funções Gratificadas e as Gratificações de Representação, da unidade técnica encarregada das ações de inteligência, alocados na Casa Militar da Presidência da República.

§ 2º O Poder Executivo disporá sobre a transferência, para a ABIN, do acervo patrimonial alocado à unidade técnica encarregada das ações de inteligência.

§ 3º Fica o Poder Executivo autorizado a remanejar ou transferir para a ABIN os saldos das dotações orçamentárias consignadas para as atividades de inteligência nos orçamentos da Secretaria de Assuntos Estratégicos e do Gabinete da Presidência da República.

Art. 13º As despesas decorrentes desta Lei correrão à conta das dotações orçamentárias próprias.

Parágrafo único. O Orçamento Geral da União contemplará, anualmente, em rubrica específica, os recursos necessários ao desenvolvimento das ações de caráter sigiloso a cargo da ABIN.

Art. 14º As atividades de controle interno da ABIN, inclusive as de contabilidade analítica, serão exercidas pela Secretaria de Controle Interno da Presidência da República.

Art. 15º Esta Lei entra em vigor na data de sua publicação.

Brasília, 7 de dezembro de 1999; 178º da Independência e 111º da República.

FERNANDO HENRIQUE CARDOSO

Amaury Guilherme Bier Martus Tavares
Alberto Mendes Cardoso

b. Lei nº 12.527, 18 de novembro de 2011

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

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no [inciso XXXIII do art. 5º](#), no [inciso II do § 3º do art. 37](#) e no [§ 2º do art. 216 da Constituição Federal](#).

Parágrafo único. Subordinam-se ao regime desta Lei:

- I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
- II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Art. 2º Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções

sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.

Parágrafo único. A publicidade a que estão submetidas as entidades citadas no **caput** refere-se à parcela dos recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas.

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

- I - observância da publicidade como preceito geral e do sigilo como exceção;
- II - divulgação de informações de interesse público, independentemente de solicitações;
- III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
- IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
- V - desenvolvimento do controle social da administração pública.

Art. 4º Para os efeitos desta Lei, considera-se:

- I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
- III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
- IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
- V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão,

distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Art. 5º É dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

CAPÍTULO II

DO ACESSO A INFORMAÇÕES E DA SUA DIVULGAÇÃO

Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter:

I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;

III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;

IV - informação primária, íntegra, autêntica e atualizada;

V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;

VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e VII - informação relativa:

a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;

b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

§ 1º O acesso à informação previsto no **caput** não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

§ 2º Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

§ 3º O direito de acesso aos documentos ou às informações neles contidas utilizados como fundamento da tomada de decisão e do ato administrativo será assegurado com a edição do ato decisório respectivo.

§ 4º A negativa de acesso às informações objeto de pedido formulado aos órgãos e entidades referidas no art. 1º, quando não fundamentada, sujeitará o responsável a medidas disciplinares, nos termos do art. 32 desta Lei.

§ 5º Informado do extravio da informação solicitada, poderá o interessado requerer à autoridade competente a imediata abertura de sindicância para apurar o desaparecimento da respectiva documentação.

§ 6º Verificada a hipótese prevista no § 5º deste artigo, o responsável pela guarda da informação extraviada deverá, no prazo de 10 (dez) dias, justificar o fato e indicar testemunhas que comprovem sua alegação.

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

§ 1º Na divulgação das informações a que se refere o **caput**, deverão constar, no mínimo:

- I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;
- II - registros de quaisquer repasses ou transferências de recursos financeiros;
- III - registros das despesas;
- IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;
- V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e
- VI - respostas a perguntas mais frequentes da sociedade.

§ 2º Para cumprimento do disposto no **caput**, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

§ 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:

- I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
- II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e

VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do [art. 17 da Lei nº 10.098, de 19 de dezembro de 2000](#), e do [art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008](#).

§ 4º Os Municípios com população de até 10.000 (dez mil) habitantes ficam dispensados da divulgação obrigatória na internet a que se refere o § 2º, mantida a obrigatoriedade de divulgação, em tempo real, de informações relativas à execução orçamentária e financeira, nos critérios e prazos previstos no [art. 73-B da Lei Complementar nº 101, de 4 de maio de 2000](#) (Lei de Responsabilidade Fiscal).

Art. 9º O acesso a informações públicas será assegurado mediante:

I - criação de serviço de informações ao cidadão, nos órgãos e entidades do poder público, em local com condições apropriadas para:

a) atender e orientar o público quanto ao acesso a informações;

b) informar sobre a tramitação de documentos nas suas respectivas unidades;

c) protocolizar documentos e requerimentos de acesso a informações; e

II - realização de audiências ou consultas públicas, incentivo à participação popular ou a outras formas de divulgação.

CAPÍTULO III

DO PROCEDIMENTO DE ACESSO À INFORMAÇÃO

Seção I

Do Pedido de Acesso

Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

§ 1º Para o acesso a informações de interesse público, a identificação do requerente não pode conter exigências que inviabilizem a solicitação.

§ 2º Os órgãos e entidades do poder público devem viabilizar alternativa de encaminhamento de pedidos de acesso por meio de seus sítios oficiais na internet.

§ 3º São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público.

Art. 11. O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível.

§ 1º Não sendo possível conceder o acesso imediato, na forma disposta no **caput**, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias:

- I - comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;
- II - indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou
- III - comunicar que não possui a informação, indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

§ 2º O prazo referido no § 1º poderá ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente.

§ 3º Sem prejuízo da segurança e da proteção das informações e do cumprimento da legislação aplicável, o órgão ou entidade poderá oferecer meios para que o próprio requerente possa pesquisar a informação de que necessitar.

§ 4º Quando não for autorizado o acesso por se tratar de informação total ou parcialmente sigilosa, o requerente deverá ser informado sobre a possibilidade de recurso, prazos e condições para sua interposição, devendo, ainda, ser-lhe indicada a autoridade competente para sua apreciação.

§ 5º A informação armazenada em formato digital será fornecida nesse formato, caso haja anuência do requerente.

§ 6º Caso a informação solicitada esteja disponível ao público em formato impresso, eletrônico ou em qualquer outro meio de acesso universal, serão informados ao requerente, por escrito, o lugar e a forma pela qual se poderá consultar, obter ou reproduzir a referida informação, procedimento esse que desonerará o órgão ou entidade pública da obrigação de seu fornecimento direto, salvo se o requerente declarar não dispor de meios para realizar por si mesmo tais procedimentos.

Art. 12. O serviço de busca e fornecimento da informação é gratuito, salvo nas hipóteses de reprodução de documentos pelo órgão ou entidade pública consultada, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

Parágrafo único. Estará isento de ressarcir os custos previstos no **caput** todo aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da [Lei nº 7.115, de 29 de agosto de 1983](#).

Art. 13. Quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade, deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original.

Parágrafo único. Na impossibilidade de obtenção de cópias, o interessado poderá solicitar que, a suas expensas e sob supervisão de servidor público, a reprodução seja feita por outro meio que não ponha em risco a conservação do documento original.

Art. 14. É direito do requerente obter o inteiro teor de decisão de negativa de acesso, por certidão ou cópia.

Seção II

Dos Recursos

Art. 15. No caso de indeferimento de acesso a informações ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da sua ciência.

Parágrafo único. O recurso será dirigido à autoridade hierarquicamente superior à que exarou a decisão impugnada, que deverá se manifestar no prazo de 5 (cinco) dias.

Art. 16. Negado o acesso a informação pelos órgãos ou entidades do Poder Executivo Federal, o requerente poderá recorrer à Controladoria-Geral da União, que deliberará no prazo de 5 (cinco) dias se:

- I - o acesso à informação não classificada como sigilosa for negado;
- II - a decisão de negativa de acesso à informação total ou parcialmente classificada como sigilosa não indicar a autoridade classificadora ou a hierarquicamente superior a quem possa ser dirigido pedido de acesso ou desclassificação;
- III - os procedimentos de classificação de informação sigilosa estabelecidos nesta Lei não tiverem sido observados; e
- IV - estiverem sendo descumpridos prazos ou outros procedimentos previstos nesta Lei.

§ 1º O recurso previsto neste artigo somente poderá ser dirigido à Controladoria-Geral da União depois de submetido à apreciação de pelo menos uma autoridade hierarquicamente superior àquela que exarou a decisão impugnada, que deliberará no prazo de 5 (cinco) dias.

§ 2º Verificada a procedência das razões do recurso, a Controladoria-Geral da União determinará ao órgão ou entidade que adote as providências necessárias para dar cumprimento ao disposto nesta Lei.

§ 3º Negado o acesso à informação pela Controladoria-Geral da União, poderá ser interposto recurso à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35.

Art. 17. No caso de indeferimento de pedido de desclassificação de informação protocolado em órgão da administração pública federal, poderá o requerente recorrer ao Ministro de Estado da área, sem prejuízo das competências da Comissão Mista de Reavaliação de Informações, previstas no art. 35, e do disposto no art. 16.

§ 1º O recurso previsto neste artigo somente poderá ser dirigido às autoridades mencionadas depois de submetido à apreciação de pelo menos uma autoridade hierarquicamente superior à autoridade que exarou a decisão impugnada e, no caso das Forças Armadas, ao respectivo Comando.

§ 2º Indeferido o recurso previsto no **caput** que tenha como objeto a desclassificação de informação secreta ou ultrassecreta, caberá recurso à Comissão Mista de Reavaliação de Informações prevista no art. 35.

Art. 18. Os procedimentos de revisão de decisões denegatórias proferidas no recurso previsto no art. 15 e de revisão de classificação de documentos sigilosos serão objeto de regulamentação própria dos Poderes Legislativo e Judiciário e do Ministério Público, em seus respectivos âmbitos, assegurado ao solicitante, em qualquer caso, o direito de ser informado sobre o andamento de seu pedido.

Art. 19. (VETADO).

§ 1º (VETADO).

§ 2º Os órgãos do Poder Judiciário e do Ministério Público informarão ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público, respectivamente, as decisões que, em grau de recurso, negarem acesso a informações de interesse público.

Art. 20. Aplica-se subsidiariamente, no que couber, a [Lei nº 9.784, de 29 de janeiro de 1999](#), ao procedimento de que trata este Capítulo.

CAPÍTULO IV

DAS RESTRIÇÕES DE ACESSO À INFORMAÇÃO

Seção I

Disposições Gerais

Art. 21. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.

Parágrafo único. As informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso.

Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

Seção II

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.

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.

§ 2º As informações que puderem colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as) serão classificadas como reservadas e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

§ 3º Alternativamente aos prazos previstos no § 1º, poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, desde que este ocorra antes do transcurso do prazo máximo de classificação.

§ 4º Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação tornar-se-á, automaticamente, de acesso público.

§ 5º Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I - a gravidade do risco ou dano à segurança da sociedade e do Estado;
e

II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

Seção III

Da Proteção e do Controle de Informações Sigilosas

Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.

§ 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.

§ 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.

§ 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.

Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas.

Parágrafo único. A pessoa física ou entidade privada que, em razão de qualquer vínculo com o poder público, executar atividades de tratamento de informações sigilosas adotarás providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Lei.

Seção IV

Dos Procedimentos de Classificação, Reclassificação e Desclassificação

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.

§ 1º A competência prevista nos incisos I e II, no que se refere à classificação como ultrassecreta e secreta, poderá ser delegada pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação.

§ 2º A classificação de informação no grau de sigilo ultrassecreto pelas autoridades previstas nas alíneas “d” e “e” do inciso I deverá ser ratificada pelos respectivos Ministros de Estado, no prazo previsto em regulamento.

§ 3º A autoridade ou outro agente público que classificar informação como ultrassecreta deverá encaminhar a decisão de que trata o art. 28 à Comissão Mista de Reavaliação de Informações, a que se refere o art. 35, no prazo previsto em regulamento.

Art. 28. A classificação de informação em qualquer grau de sigilo deverá ser formalizada em decisão que conterá, no mínimo, os seguintes elementos:

- I - assunto sobre o qual versa a informação;
- II - fundamento da classificação, observados os critérios estabelecidos no art. 24;
- III - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, conforme limites previstos no art. 24; e
- IV - identificação da autoridade que a classificou.

Parágrafo único. A decisão referida no **caput** será mantida no mesmo grau de sigilo da informação classificada.

Art. 29. A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou

de ofício, nos termos e prazos previstos em regulamento, com vistas à sua desclassificação ou à redução do prazo de sigilo, observado o disposto no art. 24.

§ 1º O regulamento a que se refere o **caput** deverá considerar as peculiaridades das informações produzidas no exterior por autoridades ou agentes públicos.

§ 2º Na reavaliação a que se refere o **caput**, deverão ser examinadas a permanência dos motivos do sigilo e a possibilidade de danos decorrentes do acesso ou da divulgação da informação.

§ 3º Na hipótese de redução do prazo de sigilo da informação, o novo prazo de restrição manterá como termo inicial a data da sua produção.

Art. 30. A autoridade máxima de cada órgão ou entidade publicará, anualmente, em sítio à disposição na internet e destinado à veiculação de dados e informações administrativas, nos termos de regulamento:

- I - rol das informações que tenham sido desclassificadas nos últimos 12 (doze) meses;
- II - rol de documentos classificados em cada grau de sigilo, com identificação para referência futura;
- III - relatório estatístico contendo a quantidade de pedidos de informação recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes.

§ 1º Os órgãos e entidades deverão manter exemplar da publicação prevista no **caput** para consulta pública em suas sedes.

§ 2º Os órgãos e entidades manterão extrato com a lista de informações classificadas, acompanhadas da data, do grau de sigilo e dos fundamentos da classificação.

Seção V

Das Informações Pessoais

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:

I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;

IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;

V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;

VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e

VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

§ 1º Atendido o princípio do contraditório, da ampla defesa e do devido processo legal, as condutas descritas no **caput** serão consideradas:

I - para fins dos regulamentos disciplinares das Forças Armadas, transgressões militares médias ou graves, segundo os critérios neles estabelecidos, desde que não tipificadas em lei como crime ou contravenção penal; ou

II - para fins do disposto na [Lei nº 8.112, de 11 de dezembro de 1990](#), e suas alterações, infrações administrativas, que deverão ser apenadas, no mínimo, com suspensão, segundo os critérios nela estabelecidos.

§ 2º Pelas condutas descritas no **caput**, poderá o militar ou agente público responder, também, por improbidade administrativa, conforme o disposto nas [Leis nºs 1.079, de 10 de abril de 1950](#), e [8.429, de 2 de junho de 1992](#).

Art. 33. A pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto nesta Lei estará sujeita às seguintes sanções:

- I - advertência;
- II - multa;
- III - rescisão do vínculo com o poder público;
- IV - suspensão temporária de participar em licitação e impedimento de contratar com a administração pública por prazo não superior a 2 (dois) anos; e
- V - declaração de inidoneidade para licitar ou contratar com a administração pública, até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

§ 1º As sanções previstas nos incisos I, III e IV poderão ser aplicadas juntamente com a do inciso II, assegurado o direito de defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias.

§ 2º A reabilitação referida no inciso V será autorizada somente quando o interessado efetivar o ressarcimento ao órgão ou entidade dos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso IV.

§ 3º A aplicação da sanção prevista no inciso V é de competência exclusiva da autoridade máxima do órgão ou entidade pública, facultada a defesa do interessado, no respectivo processo, no prazo de 10 (dez) dias da abertura de vista.

Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

Parágrafo único. O disposto neste artigo aplica-se à pessoa física ou entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.

CAPÍTULO VI

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 35. (VETADO).

§ 1º É instituída a Comissão Mista de Reavaliação de Informações, que decidirá, no âmbito da administração pública federal, sobre o tratamento e a classificação de informações sigilosas e terá competência para:

I - requisitar da autoridade que classificar informação como ultrassecreta e secreta esclarecimento ou conteúdo, parcial ou integral da informação;

II - rever a classificação de informações ultrassecretas ou secretas, de ofício ou mediante provocação de pessoa interessada, observado o disposto no art. 7º e demais dispositivos desta Lei; e

III - prorrogar o prazo de sigilo de informação classificada como ultrassecreta, sempre por prazo determinado, enquanto o seu acesso ou divulgação puder ocasionar ameaça externa à soberania nacional ou à integridade do território nacional ou grave risco às relações internacionais do País, observado o prazo previsto no § 1º do art. 24.

§ 2º O prazo referido no inciso III é limitado a uma única renovação.

§ 3º A revisão de ofício a que se refere o inciso II do § 1º deverá ocorrer, no máximo, a cada 4 (quatro) anos, após a reavaliação prevista no art. 39, quando se tratar de documentos ultrassecretos ou secretos.

§ 4º A não deliberação sobre a revisão pela Comissão Mista de Reavaliação de Informações nos prazos previstos no § 3º implicará a desclassificação automática das informações.

§ 5º Regulamento disporá sobre a composição, organização e funcionamento da Comissão Mista de Reavaliação de Informações, observado o mandato de 2 (dois) anos para seus integrantes e demais disposições desta Lei.

Art. 36. O tratamento de informação sigilosa resultante de tratados, acordos ou atos internacionais atenderá às normas e recomendações constantes desses instrumentos.

Art. 37. É instituído, no âmbito do Gabinete de Segurança Institucional da Presidência da República, o Núcleo de Segurança e Credenciamento (NSC), que tem por objetivos:

I - promover e propor a regulamentação do credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações sigilosas; e

II - garantir a segurança de informações sigilosas, inclusive aquelas provenientes de países ou organizações internacionais com os quais a República Federativa do Brasil tenha firmado tratado, acordo, contrato ou qualquer outro ato internacional, sem prejuízo das atribuições do Ministério das Relações Exteriores e dos demais órgãos competentes.

Parágrafo único. Regulamento disporá sobre a composição, organização e funcionamento do NSC.

Art. 38. Aplica-se, no que couber, a [Lei nº 9.507, de 12 de novembro de 1997](#), em relação à informação de pessoa, física ou jurídica, constante de registro ou banco de dados de entidades governamentais ou de caráter público.

Art. 39. Os órgãos e entidades públicas deverão proceder à reavaliação das informações classificadas como ultrassecretas e secretas no prazo máximo de 2 (dois) anos, contado do termo inicial de vigência desta Lei.

§ 1º A restrição de acesso a informações, em razão da reavaliação prevista no **caput**, deverá observar os prazos e condições previstos nesta Lei.

§ 2º No âmbito da administração pública federal, a reavaliação prevista no **caput** poderá ser revista, a qualquer tempo, pela Comissão Mista de Reavaliação de Informações, observados os termos desta Lei.

§ 3º Enquanto não transcorrido o prazo de reavaliação previsto no **caput**, será mantida a classificação da informação nos termos da legislação precedente.

§ 4º As informações classificadas como secretas e ultrassecretas não reavaliadas no prazo previsto no **caput** serão consideradas, automaticamente, de acesso público.

Art. 40. No prazo de 60 (sessenta) dias, a contar da vigência desta Lei, o dirigente máximo de cada órgão ou entidade da administração pública federal direta e indireta designará autoridade que lhe seja diretamente subordinada para, no âmbito do respectivo órgão ou entidade, exercer as seguintes atribuições:

- I - assegurar o cumprimento das normas relativas ao acesso a informação, de forma eficiente e adequada aos objetivos desta Lei;
- II - monitorar a implementação do disposto nesta Lei e apresentar relatórios periódicos sobre o seu cumprimento;
- III - recomendar as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto nesta Lei; e
- IV - orientar as respectivas unidades no que se refere ao cumprimento do disposto nesta Lei e seus regulamentos.

Art. 41. O Poder Executivo Federal designará órgão da administração pública federal responsável:

- I - pela promoção de campanha de abrangência nacional de fomento à cultura da transparência na administração pública e conscientização do direito fundamental de acesso à informação;
- II - pelo treinamento de agentes públicos no que se refere ao desenvolvimento de práticas relacionadas à transparência na administração pública;
- III - pelo monitoramento da aplicação da lei no âmbito da administração pública federal, concentrando e consolidando a publicação de informações estatísticas relacionadas no art. 30;
- IV - pelo encaminhamento ao Congresso Nacional de relatório anual com informações atinentes à implementação desta Lei.

Art. 42. O Poder Executivo regulamentará o disposto nesta Lei no prazo de 180 (cento e oitenta) dias a contar da data de sua publicação.

Art. 43. O inciso VI do art. 116 da Lei nº 8.112, de 11 de dezembro de 1990, passa a vigorar com a seguinte redação:

“Art. 116.

.....

VI - levar as irregularidades de que tiver ciência em razão do cargo ao conhecimento da autoridade superior ou, quando houver suspeita de envolvimento desta, ao conhecimento de outra autoridade competente para apuração;

.....” (NR)

Art. 44. O Capítulo IV do Título IV da Lei nº 8.112, de 1990, passa a vigorar acrescido do seguinte art. 126-A:

“**Art. 126-A.** Nenhum servidor poderá ser responsabilizado civil, penal ou administrativamente por dar ciência à autoridade superior ou, quando houver suspeita de envolvimento desta, a outra autoridade competente para apuração de informação concernente à prática de crimes ou improbidade de que tenha conhecimento, ainda que em decorrência do exercício de cargo, emprego ou função pública.”

Art. 45. Cabe aos Estados, ao Distrito Federal e aos Municípios, em legislação própria, obedecidas as normas gerais estabelecidas nesta Lei, definir regras específicas, especialmente quanto ao disposto no art. 9º e na Seção II do Capítulo III.

Art. 46. Revogam-se:

I - a **Lei nº 11.111, de 5 de maio de 2005**; e

II - os **arts. 22 a 24 da Lei nº 8.159, de 8 de janeiro de 1991**.

Art. 47. Esta Lei entra em vigor 180 (cento e oitenta) dias após a data de sua publicação. Brasília, 18 de novembro de 2011; 190º da Independência e 123º da República.

DILMA ROUSSEFF

José Eduardo Cardoso

Celso Luiz Nunes Amorim

Antonio de Aguiar Patriota

Miriam Belchior

Paulo Bernardo Silva

Gleisi Hoffmann
José Elito Carvalho Siqueira
Helena Chagas
Luís Inácio Lucena Adams
Jorge Hage Sobrinho
Maria do Rosário Nunes

Classificação Sigilosa

É a marcação do documento com o grau de sigilo que lhe for atribuído, de acordo com o previsto pela legislação (**Lei Federal nº 12.527, de 18 de novembro de 2011**) pertinente e, eventualmente, pelas normas internas da Agência de Inteligência que está elaborando:

a. ULTRASECRETO: Classificação de sigilo, cujo prazo máximo de restrição de acesso a informação é de 25 (vinte e cinco) anos, e sua competência refere-se às seguintes autoridades: Presidente da República, Vice-Presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas, Comandantes da

Marinha, do Exército e da Aeronáutica, Chefes de Missões Diplomáticas e Consulares permanentes no exterior;

b. SECRETO: Classificação de sigilo, cujo prazo máximo de restrição de acesso a informação é de 15 (quinze) anos, e sua competência refere-se às autoridades citadas no item “a”(Presidente da República, Vice-Presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas, Comandantes da Marinha, do Exército e da Aeronáutica, Chefes de Missões Diplomáticas e Consulares permanentes no exterior), além dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista;

c. RESERVADO: Classificação de sigilo, cujo prazo máximo de restrição de acesso a informação é de 5 (cinco) anos, e sua competência refere-se às autoridades citadas no item “a” e “b” (Presidente da República, Vice-Presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas, Comandantes da Marinha, do Exército e da Aeronáutica, Chefes de Missões Diplomáticas e Consulares permanentes no exterior, titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista), além das que exercem funções de direção, comando ou chefia.

As classificações de sigilo - **Ultrasecreta, Secreta e Reservada** - das informações em poder dos órgãos e entidades públicas, visam assegurar à segurança da sociedade e/ou do Estado.

Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerando:

- I - a gravidade do risco ou dano à segurança da sociedade e do Estado;
- e
- II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

Os prazos máximos de restrição de acesso a informação passam a vigorar a partir da data de sua produção, e transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação tornar-se-á, automaticamente, de acesso público.

OBSERVAÇÃO:

As informações que puderem colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as) serão classificadas como reservadas e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição (**§2º, art. 24 da Lei nº 12.527, de 18 de novembro de 2011**).

Ramos da Atividade de Inteligência

A atividade da ISP possui dois ramos: a Inteligência e a ContraInteligencia.

- a. **Inteligência** é o ramo da ISP que se destina à produção de conhecimentos de interesse da segurança pública;
- b. **ContraInteligencia** é o ramo da ISP que se destina a produzir conhecimentos para neutralizar a inteligência adversa, a proteção da atividade e da instituição a que pertence.

Produção de Conhecimento

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

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

- a. **Dado** é toda e qualquer representação de fato, situação, comunicação, notícia documento, extrato de documento, fotografia, gravação, relato, denúncia, etc., ainda não submetida, pelo profissional de ISP, a metodologia de Produção de conhecimento;
- b. **Conhecimento** é o resultado final - expresso por escrito ou oralmente pelo profissional de ISP – da utilização da metodologia de Produção de Conhecimento sobre dados e/ou conhecimentos anteriores.

Princípios da Atividade de Inteligência

São compostos de 16 (dezesseis) princípios:

- a) **Objetividade** é o princípio que norteia a ISP para que cumpra suas funções de forma organizada, direta e completa, planejando e executando ações de acordo com os objetivos previamente definidos.
- b) **Oportunidade** é o princípio da ISP que orienta a produção de conhecimentos, a qual deve realizar-se em prazo que permita seu aproveitamento.
- c) **Simplicidade** é o princípio da ISP que orienta a sua atividade de forma clara e concisa, planejando e executando ações com o mínimo de custos e riscos.
- d) **Imparcialidade** é o princípio da ISP que norteia a atividade de modo a ser isenta de ideias preconcebidas e/ou tendenciosas, subjetivismos e distorções.
- e) **Compartimentação** é o princípio da ISP que objetiva, a fim de evitar riscos e comprometimentos, restringir o acesso ao conhecimento sigiloso somente para aqueles que tenham real necessidade de conhecê-lo.
- f) **Controle** é o princípio da ISP que recomenda a supervisão e o acompanhamento sistemático de todas as suas ações, de forma a assegurar a não interferência de variáveis adversas no trabalho desenvolvido.
- g) **Sigilo** é o princípio que visa preservar o órgão, seus integrantes e ações.
- h) **Segurança:** em todas as fases da produção, a informação deve ser protegida.
- i) **Clareza:** as informações devem ser repassadas de maneira que sejam facilmente compreendidas por aqueles que terão acesso a elas.
- j) **Amplitude:** as informações devem ser produzidas com o máximo de dados disponíveis, na busca de facilitar o seu entendimento de forma completa.
- k) **Utilidade:** as informação obtidas devem ser úteis e, se possível, utilizadas nas ações.
- l) **Exclusividade:** as informações devem ser exclusivas, mesmo quando a informação for de conhecimento de todos. Devem ser interpretadas por uma ótica diferente, de modo a oferecer à autoridade algo novo.
- m) **Legalidade:** todas as ações de inteligência são desenvolvidas dentro da legalidade, para isto existe uma legislação específica.

n) **Atualidade:** pressupõe a busca constante do aperfeiçoamento de conceitos, técnicas, métodos e processos para atender os desafios impostos pelas transformações do mundo.

o) **Cooperação:** implica estabelecer relacionamentos e ligações que possibilitem maximizar esforços para consecução dos objetivos.

p) **Ética:** a Atividade de Inteligência de Segurança Pública está alicerçada em preceitos éticos e valores morais, sociais e cívicos, estando compromissada com a verdade, a honra, a integridade de caráter, a família, a solidariedade, o respeito aos direitos humanos, o patriotismo, o respeito às leis, à autoridade constituída e a democracia.

Valores da Atividade de Inteligência

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

Termos e Expressões usadas na Atividade de Inteligência

a. **Agência de Inteligência:** é o órgão responsável pela coleta de informações, que atua a fim de avaliar e correlacionar as informações relativas à segurança do Estado e da sociedade, divulgando-as de forma apropriada para os tomadores de decisão.

b. **Alvo:** é o objetivo ao qual estão voltadas as ações de inteligência.

c. **Dado Negado:** são as informações que não são de conhecimento da agência de inteligência.

d. **Ações de Inteligência:** são as técnicas operacionais utilizadas legalmente pelos agentes de inteligência.

- e. **Agente:** funcionário da agência de inteligência, o qual é utilizado na coleta de informações.
- f. **Missão:** são as ações desenvolvidas pelo o agente de inteligência na busca do dado negado.
- g. **Busca:** são as ações voltadas a procura, pesquisa e exame de pessoas, lugares ou objetos.
- h. **Ambiente Operacional:** espaço físico onde se desenvolvem as ações de inteligência.
- i. **Informante:** pessoas que não fazem parte da agência de inteligência, porém são utilizados na busca de informações. Geralmente recebe orientações, treinamento e recompensa pelo serviço prestado.
- j. **Colaborador:** pessoas que não fazem parte da agência de inteligência, porém cooperam, repassando informações ou dados. Normalmente não estão buscando recompensas materiais.

Técnicas utilizadas na Atividade de Inteligência

a. Observação, Memorização e Descrição (OMD)

Observação: é a capacidade que o agente tem de examinar e analisar tudo que esta a sua vista e ao alcance dos seu sentidos. Técnica que pode ser inata no agente, assim como pode ser desenvolvida e treinada para utilização nas ações policiais. Normalmente o Policial Militar começa a desenvolver a técnica durante o curso de formação. Tal recurso tem grande importância e é de muita utilidade para a atividade policial militar. É essencial que o policial em seu serviço ordinário (Guarnição, POG, Guarda, etc) utilize a **observação** para analisar os fatos no seu ambiente operacional.

Memorização: é o ato de fixar na mente fatos e objetos observados. Muitos policiais acreditam apenas na memorização visual e descartam a memorização auditiva, enquanto a grande queixa da população é justamente o fato de o policial não

escutar as vítimas. Em muitos casos, a maior assimilação e memorização ocorre a partir de informações repassadas de forma oral. Informações que podem ser expostas através da fala por vítimas, testemunhas, suspeitos, curiosos, outros, que poderão ser de suma importância posteriormente.

Descrição: é a capacidade de enumerar partes essenciais de caracteres, de fatos ou de imagens com máximo de precisão possível. A descrição precisa ser simples, clara, imparcial, ampla e objetiva.

Alguns aspectos que podem ser observados:

- **ASPECTOS FÍSICOS GERAIS:** cor, altura, sexo, peso, idade, etc.
- **ASPECTOS FÍSICOS ESPECÍFICOS:** tatuagens, sinais, cabelos, olhos, voz, etc.
- **CARACTERES DISTINTIVOS:** algo incomum que seja de fácil percepção.
- **DADOS QUALIFICATIVOS:** são dados que não são visíveis, necessitando uma coleta aprofundada para serem conhecidos (ex.: dados individuais).
- **INDUMENTÁRIAS:** tipo de vestimentas.

b. Recrutamento

Ação desenvolvida com objetivo de persuadir uma pessoa, através de argumentos, a fim de que aquela execute alguma ação, de forma consciente ou inconsciente.

c. Entrevista

Técnica através da qual o policial mantém uma conversa com o entrevistado, buscando informações. Bastante utilizada pelo Policial Militar, visando detectar

mentiras e a correta aferição da verdade. Ferramenta que pode ser utilizada tanto com testemunhas, quanto com suspeitos.

d. Estória de Cobertura

É a técnica de dissimular, a fim de ocultar o objetivo que se desejar alcançar. Visa cuidar, de forma a impedir o conhecimento operacional da atividade policial, do policial e até mesmo da instituição.

e. Fotografia

Processo de obtenção de imagens, no qual se registra posição do objeto e o retrato de pessoas, de modo que no futuro, seja possível a identificação do alvo. Técnica e meio bastante desenvolvido na última década (principalmente em celulares), que vem sendo cotidianamente empregado na atividade policial.

f. Vigilância

É um conjunto de métodos empregados na observação de todos os movimentos praticados pelo o alvo, que devem ser devidamente registrados, sem que a gente seja percebido.

Procedimentos do Policiamento Ostensivo ao identificar um Agente de Inteligência

- a. Cumprimentar apenas quando couber, discretamente, sem formalidades militares, mas com respeito e cordialidade dispensados a um cidadão comum (o AI pode estar buscando dados);
- b. Evitar palavras que identifiquem o Agente como policial;

- c. Atentar para detalhes que ele possa estar repassando, a fim de facilitar ou concluir o serviço ostensivo (nome, pessoa envolvida no delito, dados em geral, etc.);
- d. Após uma abordagem na qual o policial identifique uma Equipe de Busca, este não deve gesticular, indicar, comentar e/ou mencionar que se tratava de uma EB.

Procedimentos do Policiamento Ostensivo ao chegar no local da ocorrência

- a. Não divulgar a presença dos Agentes de Inteligência, seja antes, durante ou depois da chegada da Equipe de Busca;
- b. Coletar informes ou informações que possam auxiliar o serviço de inteligência na busca do dado;
- c. Preservar o local de crime;
- d. Ao tomar conhecimento de informes ou informações sobre criminalidade, ou ainda de fatos relativos à segurança pública, repassar ao serviço de inteligência, de forma discreta, para que levantamentos possam ser providenciados, respeitando o princípio da legalidade.

A Importância do Boletim de Ocorrência para o Serviço de Inteligência

A ampliação das atribuições da Polícia Militar e a evolução das organizações criminosas requerem que a Inteligência ganhe espaço na instituição policial (GONÇALVES, 2010, p. 27). Essa doutrina deve estar inserida em um planejamento no qual receba a devida importância, deixando de ser apenas uma função operacional, para ser um passo estratégico essencial nas missões a serem designadas (CHIROLI; ARAÚJO, 2009, p. 48).

A utilização da Inteligência Policial no combate a criminalidade, requer um sistema efetivo, tal como sugerido por Ratcliffe (2005), para o qual um sistema de inteligência vitorioso é, então, um que esteja apto a interpretar o ambiente criminal,

conduzir esse conhecimento aos tomadores de decisão e influenciar o pensamento deles, para que esses tomadores de decisão modelem uma criativa política de redução criminal que tenha impacto no contexto criminal.

Neste contexto, enxerga-se como uma ferramenta importante para a atividade de inteligência de segurança pública, a confecção dos boletins de ocorrência na Polícia Militar. Mas o que vem a ser BO? Podemos definir como o documento, por meio do qual o policial militar registra, de maneira detalhada, os acontecimentos e circunstâncias relacionados às ocorrências policiais, ou seja, a todo fato que, de qualquer forma, afete ou possa afetar a ordem pública e que exija a intervenção policial, por meio de ações e/ou operações. Todas as vezes que ocorrer um fato definido como ocorrência policial e que teve a intervenção policial, o Boletim de Ocorrência deve ser produzido.

Os boletins de ocorrências confeccionados pela Polícia Militar, constituem-se em fonte primária para geração de bases de informações criminais, refletindo as concentrações de delitos, distribuídos ao longo de um período considerado. Estas informações são de grande utilidade, como suporte ao planejamento estratégico, bem como às ações táticas específicas ostensivas.

Os boletins de ocorrência, quando bem confeccionados, através de uma linguagem natural e apresentando narrativas ricas de fatos, objetos e instrumentos utilizados, podem apresentar um elo entre o autor e o delito cometido, o crime e suas particularidades, o autor e seus comparsas, fornecendo continuamente informações essenciais à inteligência policial militar e às investigações policiais em andamento.

Pontos importantes a serem observados pelos policiais militares em serviço, no momento do preenchimento dos boletins de ocorrência:

- 1) O que aconteceu?
- 2) Quem foi o possível autor do fato?
- 3) Quando tal fato se deu?
- 4) Onde ele aconteceu?
- 5) Por que ele veio à tona?
- 6) Como foi o ato criminoso praticado?
- 7) Com quais instrumentos o autor levou a termo a sua perpetração?

Os dados coletados, certamente contribuirão para a produção do conhecimento necessário, a uma intervenção mais eficaz e efetiva da Polícia Militar. Preencher um boletim de ocorrência sem explicitar de forma adequada, os detalhes verificados durante o acompanhamento de quaisquer situações, dificultará a implementação de ações que podem, em alguns casos, impedir que outras práticas delituosas sejam perpetradas, garantindo o bem-estar social.

PREENCHIMENTO DE BOLETIM DE OCORRÊNCIA (voltado para a Inteligência Policial)

FINALIDADE (Na visão da Inteligência):

É a busca da produção do conhecimento, a fim de esclarecer pontos obscuros que impedem e/ou dificultam a elucidação dos fatos, na identificação do indivíduo criminoso, bem como de subsidiar na prevenção da criminalidade.

IMPOTÊNCIA (do Policial Militar/Polícia Militar):

Primeiro Órgão Governamental a chegar ao local do fato;

A população tende a procurar a Polícia Militar para pedir proteção e passar informações; No "calor da ocorrência" as pessoas costumam falar com mais liberdade acerca de fatos presenciados ou dos quais tenham conhecimento, sendo comum que, posteriormente, por conta própria ou orientadas por outros, passem a evitar qualquer tipo de envolvimento com situações delitivas, tornando-se mais comedidas no repasse de informações e acabando por omitir dados que "possam comprometer" de alguma forma a sua "tranquilidade".

OBJETIVOS:

- a. Capacitar os policiais militares a coletar e registrar o máximo de informações possíveis, durante as ocorrências que venham a atender;
- b. Utilizar as informações prestadas para subsidiar no lançamentos do policiamento ostensivo;
- c. Utilização do Boletim de Ocorrência como peça do procedimento investigativo pela

Polícia Judiciária;

- d. Utilização dos dados, por parte do setor de estatísticas, para aplicação em seus diversos ramos (campos);
- e. Avaliação (análise) do dado por um especialista na área de Inteligência;
- f. Credibilidade da (na) informação, pelos usuários dos Órgãos da Secretaria de Defesa Social e pelo Poder Judiciário.

FORMA:

- a. COERÊNCIA: o texto deve ser escrito de forma racional, obedecendo a uma sequência lógica;
- b. CLAREZA: evidenciar de forma objetiva, quem são os envolvidos e quais são os fatos constatados;
- c. DETALHES: narrar os fatos de forma minuciosa.
- d. TEORIA: evitar "fantasiar" os fatos, que devem ser descritos de forma imparcial, refletindo com precisão a situação desencadeada e não a opinião pessoal do policial. Caso seja necessário que o Policial Militar exponha o seu ponto de vista, deve fazê-lo de forma pessoal, dirigindo-se diretamente aos encarregados do caso;
- e. REPETÊNCIA: os crimes tendem a ser cometidos de forma semelhante, no que se refere aos dias, horários, locais; muitas vezes mantendo, inclusive, correlação quanto ao perfil das vítimas, uma vez que existem inúmeros fatores que contribuem, direta ou indiretamente, para a facilitação da prática criminosa (exemplo: locais ermos, com pouca luminosidade, horários de pouca circulação de pessoas, distração da vítima, fragilidade, outros);
- f. TERRITORIALIDADE: - Os crimes, em geral, têm relações com características das áreas onde ocorrem;

BOLETIM DE OCORRÊNCIA:

Dados Complementares	

AVALIAÇÃO (ANÁLISE) DO FATO:

É o segmento através do qual, o Agente de Inteligência aplicará o seu conhecimento técnico e sua experiência, na busca do dado negado. Nesta etapa, deverá ser estabelecido relacionamento dos fatos, na construção de um conhecimento ainda não observado. Visa trazer ótica diferenciada do caso que está sendo estudado, a fim de auxiliar na elucidação do evento ocorrido.

Análise de Inteligência

Segundo a Doutrina Nacional de Inteligência de Segurança Pública, a **Análise** é a etapa da fase do Processamento do Ciclo de Produção de Conhecimento, CPC, na qual o **Analista** decompõe os dados e/ou conhecimentos reunidos e pertinentes, em suas partes constitutivas, já devidamente avaliadas, relacionadas aos Aspectos Essenciais levantados e examina cada uma delas, a fim de estabelecer sua importância em relação ao assunto que está sendo estudado (Brasília, julho de 2009).

Considerando o conceito de **Análise**, conforme parágrafo anterior, devemos destacar sua importância como etapa do CPC, estando presente nos Ramos da Atividade de Inteligência de Segurança Pública (ISP): Inteligência e

Contraineligência, os quais são interdependentes e se destinam a produzir conhecimentos e protegê-los, respectivamente, visando tomada de Decisão na esfera da Segurança Pública.

A **Análise** de Inteligência de Segurança Pública ainda é considerada um dos Requisitos Básicos de um Órgão de Inteligência, não sendo menos importantes que outros setores, como: Arquivo, Comunicações, Informática, Apoio Administrativo, Inteligência Eletrônica, Operações de Inteligência e Contraineligência.

Não podemos esquecer que a **Análise** também está presente em todas as fases do Ciclo de Produção de Conhecimento: Planejamento, Reunião de Dados, Processamento, Avaliação, Integração, Interpretação, além da própria **Análise**; tornando o trabalho de produção de conhecimentos o mais científico possível. Esta metodologia (CPC) é conduzida pelo profissional de ISP, comumente denominado de **Analista**.

A metodologia do CPC é aplicável, no todo ou em parte, aos quatro tipos de conhecimento: Informe, Informação, Apreciação e Estimativa, de acordo com as peculiaridades de cada um.

O CPC não despreza a importância de outros fatores que concorrem para o êxito do **Analista** na produção do conhecimento, dentre eles, particularmente: seus atributos pessoais, sua experiência profissional e seu embasamento cultural, além de um acurado espírito analítico, devendo se destacar pela objetividade e pela capacidade intelectual superior (curiosidade intelectual, capacidade de apreensão, imaginação criadora e disciplina intelectual), pautando sua conduta nos mais elevados padrões éticos e morais, com destaque para a lealdade, a integridade, a discrição e o profissionalismo (capacidade de trabalho, dedicação, responsabilidade e cooperação).

a. Análise Criminal

Não podemos esquecer a Análise Criminal, a qual é utilizada em grande escala pelas Organizações Policiais em todo o mundo, sendo, inclusive uma ferramenta essencial para a Análise de Inteligência.

Segundo Gottlieb (2003), conhecido internacionalmente por suas atividades de treinamento técnico-profissional em Segurança Pública, mais especificamente em Análise Criminal, e membro do “Alpha Group Center” da Califórnia` (EUA) “A Análise Criminal é um conjunto de processos sistemáticos direcionados para o provimento de informação oportuna e pertinente sobre os padrões do crime e suas correlações de tendências, de modo a apoiar as áreas operacionais e administrativas no planejamento e distribuição de recursos para prevenção e supressão das atividades criminais”.

A Análise Criminal surgiu nos Estados Unidos no ano de 1920, quando através de catalogação de registros de ocorrências começaram a perceber incidências de crimes em determinadas localidades e através de análise detectaram que poderiam direcionar de forma mais oportuna o policiamento, para a prevenção e diminuição da criminalidade.

b. Tipos de Análise Criminal

Tática: processo analítico de produção de conhecimento em suporte às atividades policiais operacionais (policiamento ostensivo), visando subsidiar pronta resposta às ocorrências criminais surgidas num determinado momento e lugar;

Estratégica: é voltada para a resolução de problemas de longo alcance na gestão da segurança pública, partindo de projeções de cenários em que as premissas básicas indicam diferenciação qualitativa e/ou aumento ou diminuição da criminalidade futura (padrões e tendências);

Administrativa: focada nas atividades de produção de vários tipos de conhecimento, incluindo o econômico, geográfico, social e organizacional (policial), com a finalidade de instrumentar a gestão policial, a do Executivo local e da Comunidade, além de grupos da Sociedade Organizada.

c. Etapas da Análise Criminal

Registro dos fatos: registro do BO no Sistema de Informação;

Integração dos dados: agrupar o maior número possível de dados e informações, que são complementares e permitem a visão sistêmica do problema;

Categorização: distinguir os crimes de diferente natureza;

Desdobramento em tabelas: visa transformar os dados brutos em informações, mapeando o crime de forma a visualizar quais os locais e horários de maior incidência;

Análise dos dados: processo de produção do conhecimento através do confronto entre as informações e a realidade vivenciada por cada analista, permitindo formular problemas, definir hipóteses, traçar objetivos;

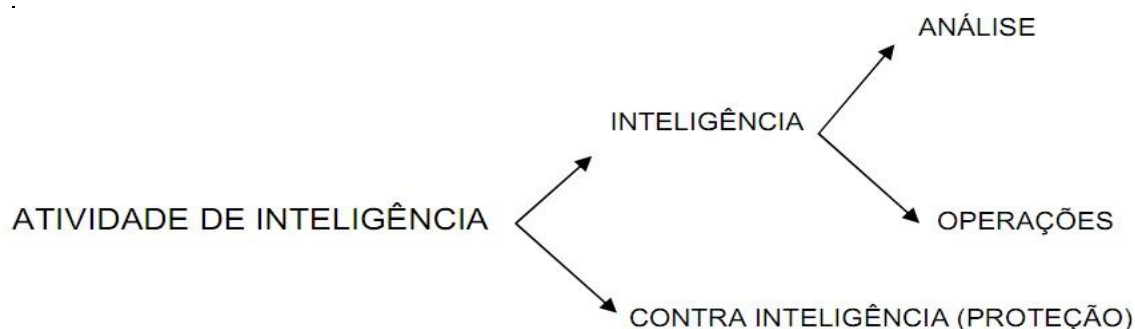
Definição e implantação de estratégias: depois da análise do problema, surgem diferentes formas de intervenção, visando reduzir e controlar os índices de crimes e delitos praticados;

Acompanhamento: deve haver um acompanhamento da dinâmica criminal, visto que o hábito do criminoso pode ser barrado através do policiamento ostensivo preventivo, ensejando que o mesmo procure novos locais.

d. Análise Criminal e Inteligência

A Análise Criminal é uma metodologia aplicada na atividade de inteligência, que desempenha um papel muito importante para a produção de conhecimento e aplicação de estratégia para resolução e redução da criminalidade.

Ramos da Atividade de Inteligência



e. Produção de Conhecimento - Análise Criminal e Inteligência

- Planejamento;
- Reunião de dados e/ou conhecimentos;
- Processamento;
- Avaliação;
- Análise;
- Integração; □ Interpretação;
- Difusão.

f. Ciclo da Análise Criminal em Inteligência

Quando a informação chega até o analista, divide-se em integração e análise.

- **Integração** é a junção coerente dos documentos que serão avaliados pelo analista.

- **Análise** é quando começa o processo analítico propriamente dito. O estudo minucioso de todos os dados obtidos através de coleta ou busca, estabelecendo a relevância, comparações, relacionando fatos, eventos (acontecimentos), pessoas e organizações.

Depois de realizada a busca e coleta serão extraídas as premissas para formulação das hipóteses e identificação dos vazios e indícios:

- **Premissa:** informação verdadeira;
- **Hipótese:** teoria não confirmada resultante de processo analítico, podendo ser modificada, pois é provisória;
- **Vazios:** falta de informações relevantes ou complementares;
- **Indícios:** caminhos que podem preencher os vazios.

g. Ferramentas da Análise Criminal

- Aplicativo Excel da MS; □ Aplicativo CAL do BROFFICE;
- Sistema INFOPOL da SDS/PE.

Contra inteligência

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

a. Conceitos Básicos

- **Responsabilidade:** é a obrigação legal, individual e coletiva, em relação a preservação da segurança;
- **Acesso:** é a possibilidade e/ou a oportunidade de uma pessoa obter dados ou conhecimentos sigilosos que devem ser protegidos. O acesso deriva de autorização oficial emanada de autoridade competente – o credenciamento – ou da superação das medidas de salvaguarda aplicadas aos documentos sigilosos;
- **Comprometimento:** é a perda da segurança de dados ou conhecimentos, provocada por fatores humanos, naturais e acidentais;
- **Vazamento:** é a divulgação não autorizada de dados ou conhecimentos sigilosos.

b. Segmentos da Contra-Inteligência

A Contra-Inteligência atua por meio de três segmentos: a Segurança Orgânica, a Segurança de Assuntos Internos e a Segurança Ativa, no entanto, para efeito didático pedagógico, abordaremos nesta apostila apenas a o Segmento da Segurança Orgânica.

Segurança Orgânica

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

A SEGOR caracteriza-se pelo conjunto de medidas integradas e meticulosamente planejadas, destinadas a proteger o pessoal, a documentação, as

instalações, o material, as operações de ISP, as comunicações e telemática, e a informática.

a. Segurança de Pessoal

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

A Segurança de Pessoal é o conjunto de medidas, voltado para assegurar comportamentos adequados à salvaguarda de conhecimentos e dados sigilosos. Tem por finalidade PREVENIR e OBSTRUIR ações adversas de INFILTRAÇÃO, RECRUTAMENTO e ENTREVISTA e os procedimentos inadequados que possam comprometer os conhecimentos e dados sigilosos que devam ser protegidos.

AÇÕES ADVERSAS:

- Infiltração;
- Recrutamento;
- Entrevista.

MEDIDAS:

- Segurança de pessoal no processo seletivo;
- Segurança de pessoal no desempenho da função;
- Segurança de pessoal no desligamento.

SEGURANÇA DE PESSOAL NO PROCESSO SELETIVO

Visa dificultar ações de infiltração e a admissão de indivíduos com características e antecedentes pessoais, que apontem para a possibilidade de atuação daquele, no sentido de causar o comprometimento.

PROCEDIMENTOS	AÇÕES
---------------	-------

Sensibilidade das funções.	Listar as rotinas de cada função Determinar a sensibilidade de cada função
Levantamento de dados pessoais (LDP)	Aplicar questionário
Entrevista Inicial	Confirmar dados obtidos no LDP Levantar as motivações Identificar as expectativas do candidato em relação à organização
Investigação de segurança	Pesquisar os antecedentes de cada candidato (hábitos, ligações, ambiente familiar, residencial e profissional)
Controle na consulta ao candidato	Tomar medidas cautelares que evitem o comprometimento, caso haja insucesso no convite. Tratar apenas de assuntos administrativos e confirmar dados.
Aplicação de testes seletivos	Confirmar as potencialidades do candidato Ratificar/ Retificar o diagnóstico obtido, emitindo parecer, favorável ou não a admissão.

SEGURANÇA DE PESSOAL NO DESLIGAMENTO

Visa levantar vulnerabilidades e verificar se o comportamento do indivíduo desligado, está dentro dos padrões de responsabilidade e comprometimento quanto à manutenção de sigilo, assumidos no momento da admissão na AI.

PROCEDIMENTOS	AÇÕES
Entrevista Final	Conscientizar o servidor de sua responsabilidade na manutenção de sigilo de conhecimentos e dados sigilosos, aos quais tenha tido acesso durante sua permanência no Órgão. Orientar o servidor para manter um comportamento adequado;

	Identificar o grau de satisfação com o órgão, atividade futura, possibilidade de ser colaborador.
Controle após o Desligamento	Verificar se o servidor é vulnerável; Verificar se está causando problemas.

b. Segurança da Documentação e de Materiais

É o conjunto de normas, medidas e procedimentos voltados para a proteção dos documentos de Inteligência, no sentido de evitar o comprometimento e/ou o vazamento. A Segurança da Documentação é garantida através do exato cumprimento dos regulamentos, instruções ou normas que regem a produção, a classificação, a expedição, o recebimento, o registro, o manuseio, a guarda, o arquivamento e a destruição de documentos sigilosos.

A segurança de materiais é o conjunto de normas, medidas e procedimentos voltados para a guarda e a preservação do material.

QUESTÕES FUNDAMENTAIS:

- O que proteger?
- Contra quem proteger?
- Como proteger?

MEDIDAS:

- Segurança na produção;
- Segurança na difusão e na recepção;
- Segurança no manuseio;
- Segurança no arquivamento e na recuperação; ☐ Segurança na eliminação.

SEGURANÇA NA PRODUÇÃO DE DOCUMENTOS / MATERIAIS.

Visa atribuir um grau de sigilo, controlar recursos e marcar os documentos sigilosos com sinais de segurança.

PROCEDIMENTOS	AÇÕES
Atribuição preliminar de um grau de sigilo	Atribuir, na fase de planejamento, um grau de sigilo, considerando o assunto, a finalidade e o usuário. Muitas vezes o grau de sigilo já vem determinado pela autoridade que solicitou a missão.
Controle de recursos utilizados	Controlar e/ou destruir os recursos utilizados na elaboração de documentos sigilosos, tais como: rascunhos, notas, desenhos, carbonos, fitas, mídias, etc. Utilizar depósitos específicos para “Lixo Classificado”
Numeração de Páginas.	Numerar as páginas que compõem o documento, representando um sinal de segurança contra extravio e subtração das mesmas.
Classificação e Marcação do Grau de Sigilo	Definir e marcar o grau de sigilo de acordo com a legislação.
Autenticação	Estabelecer e utilizar sinais convencionais para confirmar a autenticidade da documentação (Ex: Tipo e tamanho de fonte, forma e a localização da assinatura da autoridade competente)

SEGURANÇA DE DOC. / MAT. NA DIFUSÃO E NA RECEPÇÃO

Visa estabelecer controles e segurança nas rotinas de tramitação de documentos entre emissor e o usuário. Definir responsabilidades.

PROCEDIMENTOS	AÇÕES
---------------	-------

Acondicionamento do Documento	Adotar providências cautelares que permitam a identificação de indícios de violação de seu acondicionamento. Ex: duplo envelopamento, lacre, etc.
-------------------------------	---

SEGURANÇA DE DOC. / MAT. NO MANUSEIO

Visa estabelecer medidas de segurança para reprodução, custódia e revisão de classificação sigilosa dos documentos, durante a utilização.

PROCEDIMENTOS	AÇÕES
Controle e Reprodução	e Solicitar autorização para reprodução de documentos sigilosos. Capacitar o servidor responsável pela reprodução nos aspectos técnicos e de segurança; Criar formulários para controle de cópias ostensivas e de cópias de documentos sigilosos; Numerar as cópias de DSC e registrar o seu destinatário; Marcar o grau de sigilo das cópias.
Controle e Custódia	Registrar e controlar a retirada de documentos do arquivo. Controlar a tramitação de documentos: identificação, data/ hora/ setor/ usuário.
Reclassificação e Desclassificação	Verificar a autorização para reclassificação e desclassificação de documento sigiloso.
Seleção dos Doc. para Arquivamento e Destruição	Estabelecer critérios para selecionar a documentação a ser arquivada ou destruída, com base no conteúdo e oportunidade de seu possível aproveitamento.

SEG. DE DOC. / MAT. NO ARQUIVAMENTO/ RECUPERAÇÃO

Consiste na definição de locais de processos de arquivamento e à recuperação de documentos sigilosos e estabelecimento de rotinas para emergências.

PROCEDIMENTOS	AÇÕES
Escolha do Local	Selecionar o local para a instalação de arquivos e documentos sigilosos, atentando para a circulação de pessoas e para a evacuação em situação de emergência. Sinalizar a área com a marcação de classificação devida.
Escolha do Tipo de Arquivo ou Cofre	Escolher o tipo de arquivo ou cofre, considerando os diferentes graus de sigilo da documentação que vai abrigar.
Controle no Arquivamento e na Recuperação	Estabelecer rotinas para o arquivamento e para recuperação dos documentos. Definir responsabilidades para o manuseio e o controle dos documentos sigilosos arquivados.
Rotinas para Evacuação em Emergência	Criar Prioridades; Definir responsabilidades; Determinar locais alternativos para abrigar os documentos a serem salvos.

SEG DE DOC. / MAT. NA ELIMINAÇÃO / DESTRUICÃO

Visa definir meios e locais de destruição, determinar formas de controle e rotinas para situações de emergências.

PROCEDIMENTOS	AÇÕES
Escolha dos Meios	Selecionar os documentos; Definir responsabilidades; Escolher os meios a serem utilizados: incineração, trituração, etc.
Escolha do Local	Determinar os locais a serem utilizados.

Controle da Destruição	Estabelecer rotinas para destruição; Centralizar e controlar os procedimentos, a fim de evitar falhas e desvios de documentos; Observar a legislação pertinente.
Rotinas para situações de emergências	Prever procedimentos de destruição em situações de emergência; Definir Responsabilidades; Definir formas.

c. Segurança das Instalações

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

MEDIDAS:

- Demarcação de áreas;
- Implantação de barreiras;
- Contramedidas eletrônicas;
- Prevenção de acidentes;
- Prevenção e combate a incêndios.

DEMARCAÇÃO DE ÁREAS

Visa sinalizar as áreas sigilosas e restritas por meio de convenções - restrição do acesso.

PROCEDIMENTOS	AÇÕES
Identificação	Definição das áreas: LIVRES, RESTRITAS, SIGILOSAS. Classificação das áreas: RESERVADA, CONFIDENCIAL, SECRETA, ULTRASECRETA.
Delimitação	Estabelecer os limites de cada área a ser protegida. Ex: cercas, paredes, muros, etc.
Marcação e Sinalização	Utilizar sinalização (linguagem clara ou códigos) para informar às pessoas, os diferentes graus de sensibilidade de cada área.

IMPLANTAÇÃO DE BARREIRAS

Visam impedir / dificultar o ingresso não autorizado de pessoas e permitir o controle da circulação.

PROCEDIMENTOS	AÇÕES
Instalação de cercas, muros, fossos, grades, etc.	Criar obstáculos para impedir ou dificultar o acesso de pessoas não autorizadas.
Sistema de Guarda e Vigilância	Utilizar barreiras humanas para controlar o acesso e a circulação, bem como controlar intrusão – postos fixos e móveis e comunicação entre postos.
Identificação e Controle de Pessoas Identificação e Controle de Veículos Controle de Entrada e Saída de Material	Utilizar sistemas de identificação para pessoas e veículos: Passes, Crachás, Cartões / Adesivos para veículos em serviço e para veículos particulares, etc. Utilizar sistema de revistas (pessoas e veículos) – simples, rápida, circunstanciada ou completa para controlar entrada e saída de documentos e materiais.

Sistema de Barreiras	Utilizar dispositivos para controlar o acesso e a circulação de pessoas.
Sistema de Iluminação de Segurança	Instalar pontos de luz nas áreas mais sensíveis, para facilitar a vigilância e dificultar o acesso não autorizado.
Sistema de Alarmes	Selecionar o tipo de alarme adequado a área da qual se quer restringir o acesso; Instalar alarmes nas áreas mais sensíveis.
Mecanismos de Fechamento	Manter os claviculários sob o controle da Segurança Orgânica.

e. Segurança das Comunicações e Telemática

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

MEDIDAS:

- Segurança da transmissão;
- Segurança do conteúdo.

SEGURANÇA DA TRANSMISSÃO

Visa proteger fisicamente os meios de comunicação e a análise do fluxo de mensagens.

PROCEDIMENTOS	AÇÕES
Escolha dos locais para instalação dos equipamentos	Criar obstáculos às ações de interceptação;

	Levar em conta a circulação de pessoas e a implementação de ações de espionagem e de sabotagem (o acesso ao local deve ser controlado).
Escolha dos Meios de Comunicação (equipamentos)	Escolher de acordo com a classificação sigilosa do conhecimento ou dado a ser transmitido. Atender ao princípio da oportunidade. Atender aos princípios da segurança. Alternar os meios, horários e operadores (para dificultar a monitoração e a interceptação).
Exploração dos Meios de comunicação	Estabelecer regras para o uso correto de cada meio. Disciplinar: quem pode transmitir o quê, através de quais meios e em que momento.
Utilização do Código de Chamada	Utilizar nomes-código para as organizações (identificar a real origem da chamada).
Exploração do tráfego Falso	Utilizar falsas mensagens para embair ou confundir o interceptador quanto ao volume, à intensidade do fluxo e ao conteúdo dos conhecimentos e dados.

SEGURANÇA DO CONTEÚDO

Visa dificultar o entendimento, por elementos adversos, do texto transmitido ou recebido.

PROCEDIMENTOS	AÇÕES
Preparação da Mensagem	Eliminar os estereótipos e tornar os textos claros, precisos e concisos, para receber o tratamento

	criptográfico (se for o caso) adequado ao seu grau de sigilo.
Escolha dos Recursos Criptológicos	Adequar a complexidade do recurso às características do conteúdo e ao seu grau de sigilo. A segurança está diretamente relacionada ao tempo que resistirá à ação de criptoanálise adversa. Garantir o equilíbrio entre OPORTUNIDADE e SEGURANÇA.
Exploração dos Recursos Criptológicos	Escolher e usar adequadamente o recurso criptológico (conhecimento técnico). Quanto mais mensagens transmitidas, mais fácil a criptoanálise adversa.
Utilização do Código de Assinantes	Utilizar nomes-código para os assinantes (devem ser trocados com frequência para dificultar a identificação dos interlocutores).
Utilização do Código de Autenticação	Utilizar sinais convencionados, inseridos no corpo da mensagem, para confirmar ao correspondente a real origem da mensagem. Confirmar também a autenticidade do conteúdo.

f. 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.

PRINCIPAIS RISCOS:

- Erros de operação (intencional ou não);
- Erros em entrada de dados (implantação);
- Falhas nos equipamentos;
- Falhas na transmissão; □ Fraudes e sabotagens;

- Sinistros.

AMEAÇAS INTENCIONAIS:

- Furto de equipamentos e de dados;
- Cópia de arquivos (em cds, pendrives etc);
- Interceptação dos canais de comunicação;
- Uso indevido dos recursos computacionais (misturar rede interna e internet no mesmo equipamento);
- Tentativas de acesso não autorizado;
- Uso indevido de senhas (divulgação para outros, roubo, empréstimo); ☐ Sabotagem (adulteração, apagamento de arquivos, inserção de vírus, etc.).

AMEAÇAS NÃO-INTENCIONAIS:

- Linhas cruzadas;
- Irradiações eletromagnéticas;
- Ligações impróprias;
- Listagens, discos, cds, não autorizados (piratas);
- Uso de mídias particulares.

OUTRAS AMEAÇAS:

- Terceirização (Serviço e Manutenção).

MEDIDAS:

Segurança de Hardware e Software - Controle de Usuários

SEGURANÇA DE HARDWARE E SOFTWARE

PROCEDIMENTOS	AÇÕES
Proteção de Dados e de Software	Desenvolver padrões e procedimentos de segurança para a proteção dos dados criados ou mantidos na jurisdição das funções de processamento de dados.
Controle de mudança	Controlar as transferências de programas de aplicação entre os ambientes de testes e de produção-garantir integridade dos sistemas de aplicação.
Implantação de Backup de Sistemas e Arquivos	Elaborar plano de recuperação para arquivos críticos. Garantir a recuperação dos sistemas de computação e dos arquivos num período razoável de tempo.
Registro de Ocorrências e Auditoria	Utilizar os registros de ocorrência (logs para garantir o registro dos eventos ocorridos no sistema). Manter atualizados os registros para auditoria, para rastrear o acesso a dados sigilosos.
Emprego da Criptologia	Utilizar processo de Criptologia, adequados ao conteúdo dos bancos de dados e a transmissão das mensagens.
Implantação de Redes	Implantar redes remotas em locais seguros, garantindo a integridade dos dados que irão trafegar.
Controle de Acesso aos Ambientes	Implementar restrições físicas de acesso aos equipamentos.

CONTROLE DE USUÁRIOS

PROCEDIMENTOS	AÇÕES
Controle de Ambientes	A Segurança Orgânica deve avaliar os riscos e a sensibilidade dos dados, que possam ser acessados, nos locais mobiliados com terminais e microcomputadores.

g. Plano de Segurança Orgânica (PLASEGOR)

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

O PLASEGOR será resultado de um processo harmônico e integrado, após percorridas as seguintes fases: Estudo de Situação, Decisão, Elaboração do Plano, Implantação do Plano e Supervisão das Ações Planejadas.

Segue abaixo, os itens que fazem parte da estrutura do Plano de Segurança Orgânica:

- Situação Geral;
- Finalidade;
- Objetivo;
- Competências;
- Legislação de Referências;
- Conceituações;
- Execução;
- Segurança do Pessoal;
- Segurança da Documentação e do Material;
- Segurança dos Sistemas de Telemática;
- Segurança das Comunicações;
- Segurança da Informática;
- Segurança das Áreas e das Instalações;
- Disposições Finais; □ Data;
- Assinatura.

Ameaças a Atividade de Inteligência

- a. Espionagem;

- b. Terrorismo;
- c. Sabotagem;
- d. Fenômenos da natureza;
- e. Acidentes;
- f. Conduta inadequada de servidores;
- g. Boatos;
- h. Vazamento.

- **Espionagem:** São ações desenvolvidas na busca de conhecimentos.

Tipos de Espionagem

- Furto;
- Cópias;
- Lixo;
- OMD (Observação, Memorização e Descrição);
- Fotografia.

Podemos ter ainda como ações de espionagem: Hackers, Crackers, Engenharia Social, etc.

Engenharia Social: é a ferramenta mais moderna da espionagem. “Processo de obtenção de informações do interesse do agressor, com finalidade(s) específica(s), e com o uso de métodos e de técnicas especiais (influência e persuasão)”. (Kevin Mitnik, “A Arte de Enganar”).

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

- **Sabotagem:** São ações voltadas a prejudicar ou interromper a atividade de inteligência.

Tipos de sabotagem:

- Destruição;
- Adulteração; e
- Interrupção.

- **Fenômenos da natureza**

São eventos da natureza que também podem prejudicar ou interromper a Atividade de Inteligência. □ Vazamento;

- Intempéries.

- **Acidentes**

São ações praticadas por integrantes de Agências de Inteligência que podem vir a causar algum tipo de problema para a atividade.

Nesse contexto, podemos destacar:

- Imperícia; □ Negligência;
- Imprudência.

- **Conduta inadequada de servidores**

São ações praticadas por servidores e ex-servidores que podem significar sérias ameaças para a Atividade de Inteligência.

- **Boatos**

São informações não confirmadas que, transmitidas de forma deliberada, podem causar grandes problemas para a Atividade de Inteligência.

- **Vazamento**

É a divulgação, de forma não autorizada, de dados e ou conhecimentos sigilosos produzidos.

Podemos ainda citar a FALTA DE ESTRUTURA FÍSICA como ameaça à Atividade de Inteligência.

Referências

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. Brasília, 2009.

CEPIK, Marco A. C.. Serviços de Inteligência: Agilidade e transparência como dilemas de institucionalização. Instituto Universitário de Pesquisas. Tese de Doutorado. Rio de Janeiro. IUPERJ, 2001.

SUN TZU. A arte da guerra: os treze capítulos originais. Trad. e adapt. Nikko Bushidô. São Paulo: Jardim dos Livros, 2007.

DZIEKANIAK, Gisele; ROVER, Aires. Sociedade do Conhecimento: características, demandas e requisitos. Revista de Informação. v. 12 n. 5, out. 2011. Disponível em: <http://www.dgz.org.br/out11/Art_01.htm>. Acesso em 03 nov. 2012.

MEDEIROS, Francisco José de. A Atividade de Inteligência no Mundo Atual. Disponível

em: <http://www.abraic.org.br/index.php?option=com_content&view=article&id=115:a-atividade-de-inteligencia-do-mundo-atual&catid=3:destaque&Itemid=50>. Acesso em: 4 nov. 2012.

VERONEZZI, Felipe. Os 7 Tipos de Inteligência: de que Tipo é o seu Cérebro?. Disponível em: <<http://www.guiadacarreira.com.br/artigos/auto-conhecimento/7-tipos-de-inteligencia/>> . Acesso em 2 nov. 2012.

As melhores Agências de Inteligência do Mundo. Disponível em: <<http://facebooktrends.com.br/osmelhores/as-melhores-agencias-de-inteligencia-domundo/>> Acesso em 5 nov. 2012.

Bíblia Sagrada. Disponível em:

<http://www.bibliacatolica.com.br/01/4/13.php#ixzz2Bjq9d3PU>>. Acesso em 7 nov. 2012.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=Lei_9883_de_07%2F12%2F1_999>. Acesso em: 03 nov. 2012.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 03 nov. 2012.

Evolução Organizacional da ABIN. Disponível em:<http://www.abin.gov.br/modules/mastop_publish/?tac=Evolu%EAo_organizacao>. Acesso em: 02 nov. 2012.

Wikipédia. A Cifra de Cesar. Disponível em:http://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar>. Acesso em: 02 nov. 2012.
https://pt.scribd.com/search?content_type=tops&page=1&query=Intelig%C3%Aancia%20de%20Seguran%C3%A7a&language=13



famart
GRUPO EDUCACIONAL