

**Disciplina:** Inteligência: Estratégia de Defesa Civil

**Autores:** Esp. Jackson Cilio Leoni dos Santos

**Revisão Conteúdos:** M.e Romário Keiti Pizzatto Fugita

**Revisão Ortográfica:** Jacqueline Morissugui Cardoso

**Ano:** 2017



F A C U L D A D E  
SÃO BRAZ

**Copyright © - É expressamente proibida a reprodução do conteúdo deste material integral ou de suas páginas em qualquer meio de comunicação sem autorização escrita da equipe da Assessoria de Marketing da Faculdade São Braz (FSB). O não cumprimento destas solicitações poderá acarretar em cobrança de direitos autorais.**

**Jackson Cilio Leoni dos Santos**



**Inteligência: Estratégia de Defesa  
Civil**

**1ª Edição**

**SÃO BRAZ**

**2017**

**Curitiba, PR**

**Editora São Braz**



# FACULDADE SÃO BRAZ

## FICHA CATALOGRÁFICA

SANTOS, Jackson Cilio Leoni dos.

Inteligência: Estratégia de Defesa Civil / Jackson Cilio Leoni dos Santos.  
– Curitiba, 2017.

48 p.

Revisão de Conteúdos: Romário Keiti Pizzatto Fugita.

Revisão Ortográfica: Jacqueline Morissugui Cardoso.

Material didático da disciplina de Inteligência: Estratégia de Defesa Civil  
– Faculdade São Braz (FSB), 2017.

ISBN: 978-85-5475-056-5

## **PALAVRA DA INSTITUIÇÃO**

Caro(a) aluno(a),

Seja bem-vindo(a) à Faculdade São Braz!

Nossa faculdade está localizada em Curitiba, na Rua Cláudio Chatagnier, nº 112, no Bairro Bacacheri, criada e credenciada pela Portaria nº 299 de 27 de dezembro 2012, oferece cursos de Graduação, Pós-Graduação e Extensão Universitária.

A Faculdade assume o compromisso com seus alunos, professores e comunidade de estar sempre sintonizada no objetivo de participar do desenvolvimento do País e de formar não somente bons profissionais, mas também brasileiros conscientes de sua cidadania.

Nossos cursos são desenvolvidos por uma equipe multidisciplinar comprometida com a qualidade do conteúdo oferecido, assim como com as ferramentas de aprendizagem: interatividades pedagógicas, avaliações, plantão de dúvidas via telefone, atendimento via internet, emprego de redes sociais, e grupos de estudos com alunos e tutores, o que proporciona excelente integração entre professores e estudantes.

Bons estudos e conte sempre conosco!

Faculdade São Braz

## **Apresentação da Disciplina**

Nesta disciplina será trabalhado com a contextualização da Lei nº 9.883/1999 e da atividade de Inteligência no Brasil ao longo de 4 fases principais. Durante as aulas diversos conceitos serão esclarecidos com a utilização de exemplos de operações realizadas em que será possível visualizar a aplicabilidade das técnicas e definições.

Estar prevenido para o maior número de situações possíveis é a chave para o sucesso de suas ações, por isso é importante associar o conteúdo a situações já vividas, ampliando sua visão.

Por fim o objetivo é a capacidade de adaptar e até mesmo criar ações de inteligência em suas atividades, como uma estratégia eficaz em Defesa Civil.

F A C U L D A D E  
SÃO BRAZ

**Copyright © - É expressamente proibida a reprodução do conteúdo deste material integral ou de suas páginas em qualquer meio de comunicação sem autorização escrita da equipe da Assessoria de Marketing da Faculdade São Braz (FSB). O não cumprimento destas solicitações poderá acarretar em cobrança de direitos autorais.**

## **Apresentação da Aula 1 – Contexto Histórico e Principais Conceitos em Inteligência**

Nesta aula serão apresentados alguns conceitos da inteligência e como ela se desenvolveu no contexto nacional, com leis que estruturam a função da inteligência no âmbito da Defesa Civil.

### **1. CONTEXTO HISTÓRICO E PRINCIPAIS CONCEITOS EM INTELIGÊNCIA**

## **Para Refletir**



Imagine que você está prestes a adquirir um carro, será que saber sobre as condições legais, de procedência e mecânica do automóvel, são importantes para você? Ou ainda, na compra de um imóvel, seria prudente coletar e analisar informações sobre a vizinhança, proximidade de mercado ou posto de gasolina próximo, e sobre as condições de estrutura? Existem informações sobre você, que toma cuidado para manter em sigilo (senhas, por exemplo)? Se você respondeu sim para alguma dessas perguntas, percebe a importância da informação na tomada de decisão? E ainda, na importância e segurança em manter algumas dessas informações protegidas, em sigilo? Agora imagine uma nação, um líder de estado, o Presidente. Existem muitas informações extremamente importantes para o processo de tomada de decisões. Assim como existem muitas informações que devem permanecer em sigilo. A atividade de Inteligência está diretamente relacionada a essa reflexão.

Inicialmente, é de grande importância abordar os estudos direcionados à Lei nº 9.883 de 1999, um importante marco para a área de Inteligência no País com a criação da SISBIN e da sua agência central, a ABIN.

#### **1.1. Sistema Brasileiro de Inteligência (Lei nº 9.883/99 e decreto 4.376/2002)**

O SISBIN – Sistema Brasileiro de Inteligência foi instituído pelo então Presidente Fernando Henrique Cardoso na Lei nº 9.883/99

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. (BRASIL, 1999, s/p.)

Essa mesma lei também cria em seu artigo 3º o órgão da Presidência da República que ocupa a posição central no SISBIN (Sistema brasileiro de Inteligência), que terá a seu cargo a responsabilidade de planejar, executar, coordenar, supervisionar e controlar as atividades de Inteligência de todo o País.

## 1.2. A ABIN – Agência Brasileira de Inteligência

Após 3 anos, a Lei recebe o Decreto 4.376/2002 que vai dispor sobre a organização e o funcionamento do SISBIN. Esse decreto é importante, pois é justamente no seu 4º artigo, onde define-se os órgãos que o compõem, mais especificamente no inciso XIII que a Defesa Civil será enquadrada. O decreto acompanha o inciso foi dado posteriormente, no Decreto nº4.872/2003: “XIII - Ministério da Integração Nacional, por meio da Secretaria Nacional de Defesa Civil” (BRASIL, 2003, s/p.).

## Importante



A nomeação, assim como as atividades e prioridades da Inteligência no Brasil acompanham o contexto sócio-histórico e suas transformações.

Na tabela a seguir, formulada a partir de informações históricas disponíveis no site da ABIN, é possível acompanhar todas essas mudanças e em qual das 4 fases (embrionária, bipolaridade, transição, contemporânea) está inserida.

**Tabela 1.1 Fases da Inteligência no Brasil** (Fonte ABIN, s/d.)

| Fase                                | Sigla        | Órgão de Inteligência                               | Descrição                                                               |
|-------------------------------------|--------------|-----------------------------------------------------|-------------------------------------------------------------------------|
| Fase Embrionária<br>1927 -1964      | 1927 – CDN   | Conselho de Defesa Nacional                         | Início formal da atividade no Brasil                                    |
|                                     | 1934 - CSSN  | Conselho Superior de Segurança Nacional             |                                                                         |
|                                     | 1946 - SFICI | Serviço Federal de Informações e Contra Informações | Considerado o primeiro órgão de inteligência do Estado brasileiro       |
| Fase da Bipolaridade<br>1964 – 1990 | 1964 - SNI   | Serviço Nacional de Informação                      | Tecnologia, sigilo, reestruturação                                      |
| Fase de Transição<br>1990 – 1999    | 1990 - SAE   | Secretaria de Assuntos Estratégicos                 | Reavaliação e autocritica para adequação ao novo contexto governamental |
|                                     | 1995 – SGPR  | Secretaria Geral da Presidência da República        |                                                                         |
|                                     | 1996 – CMPR  | Casa Militar da Presidência da República            |                                                                         |
| Fase Contemporânea<br>1999 – hoje   | 1999 - ABIN  | Agência Brasileira de Inteligência                  | Consolidação de Atuação                                                 |

Em sua fase embrionária também chamada de fase dos conselhos, inicia formalmente as atividades em 1927 com o Conselho de Defesa Nacional, criado para fornecer suporte às ações estratégicas do Poder Executivo e tinha como uma de suas missões acompanhar e avaliar as evoluções conjecturais do país (movimentos revolucionários como o tenentismo) avaliando sua consequência para o Estado. A criação em 6 de setembro de 1946 (que viria a ser oficializado com o dia do profissional de Inteligência no Brasil) da SFICI, considerada como a primeira agência de Inteligência do Estado brasileiro marca a consolidação da atividade, pertencente a 2ª seção do Conselho Nacional de Segurança tem como responsabilidade organizar e dirigir o serviço federal de informação e contra informação.

A fase da bipolaridade está inserida no controverso contexto da Guerra Fria, a criação do órgão SNI ligado diretamente ao presidente e ao Conselho de Segurança Nacional é marcado pela incorporação da antiga SFICI (incluindo os funcionários civis e militares), instalação de uma Agência Central e criação de 12 agências regionais por todo o território nacional. O contexto geopolítico externo é marcado pela Bipolaridade Rússia x EUA, já internamente o país vive o chamado Regime de Exceção, após a intervenção militar de 1964. O SNI tem como missão coordenar, integrar e informar e para isso coordena o SISNI (Sistema Nacional de Informações), implementado através do PNI (Plano Nacional de Informações), a preocupação com tecnologia e com o sigilo também é um marco significativo dessa fase.

A fase de transição, que ocorre no momento de redemocratização do país em 88 na Nova República, é marcada por uma reavaliação e reestruturação do serviço de inteligência no Estado brasileiro. Vinculado à SAE – Secretaria de Assuntos Estratégicos, criada em 1990 pelo então Presidente Fernando Collor de Melo como parte da promessa de campanha de extinguir o SNI, tem inicialmente como órgão de inteligência o DI (Departamento de Inteligência) e posteriormente a SSI/ SI (Subsecretaria e Secretaria de Inteligência). Os quais tem como missão salvaguardar os interesses do estado contraespionagem, sabotagem e terrorismo. Teve sua vinculação alterada de SAE para SGPR (Secretaria Geral da Presidência da República), e por fim a CMPR (Casa Militar da Presidência da República).

A fase contemporânea é marcada pela criação em 1999 da ABIN e do SISBIN (Sistema Brasileiro de Inteligência). A Agência Brasileira de Inteligência é o órgão central desse sistema, mas outros também o compõem.

Em 2004, o SISBIN era formado pelo GSI, ABIN, Ministério da Defesa, Ministério das Relações Exteriores, Casa Civil da Presidência da República (órgão responsável pela gestão do Sistema de Proteção da Amazônia), Ministério da Justiça, Ministério da Fazenda, Ministério da Integração Regional, Ministério da Ciência e Tecnologia, Ministério do Meio Ambiente, Ministério da Saúde, Ministério da Previdência Social e, ainda, pelo Ministério do Trabalho. Entretanto, o peso relativo de cada um desses treze componentes principais é bastante distinto. (CEPIK. 2005. p. 88)

Durante a fase atual a agência esteve vinculada em sua maior parte ao GSI/PR (Gabinete de Segurança Institucional da Presidência da República), órgão esse que possui status de ministério, em 2015 a então Presidente Dilma Rousseff vinculou a ABIN para a SG (Secretaria de Governo), sendo reincorporado GSI em 2016 pelo então Presidente Michel Temer que recriou o Gabinete. A missão corresponde ao cenário nacional, tendo como preocupação o combate ao crime organizado, terrorismo, narcotráfico, biopirataria, espionagem industrial e econômica e os ilícitos transnacionais. Para isso o órgão assessora diretamente a Presidência da República. Segundo Cepik (2005. p.83)

Em relação às mudanças organizacionais mais importantes ocorridas depois da criação da ABIN em 1999, é importante destacar pelo menos cinco transformações recentes: a) subordinação da agência ao Gabinete de Segurança Institucional – GSI da Presidência da República; b) criação da Comissão Mista de Controle das Atividades de Inteligência – CCAI no Congresso; c) regulamentação da participação dos ministérios no âmbito do SISBIN; d) criação do

Sistema de Inteligência de Defesa – SINDE; e) criação do Subsistema de Inteligência de Segurança Pública – SISP (...) O GSI transformou-se no principal instrumento agregador dos fluxos informacionais vindos de vários órgãos federais e no locus de gestão de crises nas áreas de segurança interna e externa. Embora a ABIN seja definida legalmente como o órgão central do sistema e exerça um papel de primus inter pares, na prática sua subordinação ao GSI aumentou o poder de agenda da Presidência da República sobre as prioridades do trabalho de obtenção e análise de informações, ao mesmo tempo que reduziu a autoridade da ABIN sobre os demais órgãos participantes.

Além do SISBIN existem duas outras redes de inteligência no Brasil, o SISP e o SINDE. O SISP, Subsistema de Inteligência e Segurança pública foi criado no Decreto nº 3.695, de 21 de dezembro de 2000; tendo como órgão central a SENASP (Secretaria Nacional de Segurança Pública do Ministério da Justiça) e traz em seu artigo 1º e no parágrafo 3 respectivamente:

Subsistema de Inteligência de Segurança Pública, com a finalidade de coordenar e integrar as atividades de inteligência de segurança pública em todo o País, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo.

(...)

Cabe aos integrantes do Subsistema, no âmbito de suas competências, identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza. (BRASIL, 2000, s/p.)

Por sua vez, o SINDE (Sistema de Inteligência de Defesa), foi criado em 2002 em uma medida administrativa do Ministério da Defesa por meio da Portaria Normativa nº 295/MD, o qual segundo Cepik (2005. p.89):

Este sistema foi criado para articular os centros de inteligência da Marinha (CIM), Exército (CIE), Aeronáutica (CIAer) e Estado-Maior de Defesa (EMD-2) com o Ministério da Defesa”. Essas 3 redes/ sistemas de inteligência ficam subordinados ao GSI.

### **1.3. Conceito de Inteligência e Contraineligência**

As atividades de Inteligência exercidas pelo Estado brasileiro variam conforme o contexto geopolítico, concordando com Paula (2012. p.123) quando diz que “A concepção da atividade de inteligência, ao longo das transformações históricas de suas estruturas, também sofreu um processo de evolução”, atualmente a ABIN (2005. p. 85-85) traz em uma de suas publicações um conceito interessante sobre sua atual visão de ações de inteligência:

A Inteligência não tem poder de polícia, usa-se o cérebro para avaliar a informação. Esta pode ser classificada de diversas maneiras, tais como: informação militar, tática, geral, diplomática, política, econômica, social, biográfica, científica, tecnológica e informação sobre comunicações e transportes. O seu processo envolve as seguintes fases: necessidade de conhecimento; coleta de dados na imprensa ou outros similares, incluindo coleta de dados não disponíveis; processamento dos dados; disseminação do conhecimento ao usuário, para a tomada de decisão.

O conceito de inteligência utilizado no SISBIN é abrangente e de certa forma vago, a Lei 9.883/1999 define:

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. (BRASIL, 1999, s/p.)

Sendo a contrainteligência a atividade que busca neutralizar a inteligência adversa. Segundo Paula (2012. p. 126)

Percebe-se que “inteligência” vai muito além das atividades de Estado e de Governo, envolvendo um conjunto de ações interligadas que tem como propósito a busca da certeza e verdade sobre fatos que possam, direta ou indiretamente, afetar a vida das pessoas, da sociedade e do próprio governo, principalmente no sentido de se evitarem situações de crise ou de riscos reais ou potenciais. Assim, analisando o histórico do serviço de inteligência no Brasil, e a constância nessas atividades, percebe-se que o conceito de inteligência está diretamente associado à obtenção, utilização e gestão de informação. E o conceito de contrainteligência com o sigilo da informação que se possui, isto é, de impedir que outros possam obter e utilizar essas mesmas informações.

#### **1.4. Atividade de Inteligência**

O setor de inteligência avançou consideravelmente na contemporaneidade, desenvolvendo soluções (os chamados produtos) de inteligência. Ainda que o contexto geopolítico brasileiro influencie e controle e autonomia do sistema, suas atividades podem ser entendidas em linhas gerais como obtenção e análise de informação para produção de conhecimento e proteção de informação.

Atualmente, a ABIN utiliza a definição contextualizada na Lei 9.883/99 que diz que:

# Importante



Atividade de Inteligência é o exercício de ações especializadas para obtenção e análise de dados, produção de conhecimento e proteção de conhecimentos para o país.

Essas atividades ocorrem em 3 níveis - estratégico, tático e operacional. Na prática, as atividades desenvolvidas nessas 3 esferas se articulam, ocorrendo, inclusive, simultaneamente em alguns momentos (produção e proteção do conhecimento), essa separação é didática para se compreender melhor o conceito de atividade de inteligência.

As atividades voltadas a estratégia, estão diretamente ligadas à formulação de políticas públicas, importante para delimitar e legalizar as ações de inteligência, e ainda na forma de diretrizes nacionais ou elaboração/formulação de instrumentos legais para serem utilizados nas operações de inteligência.

As atividades táticas estão voltadas ao planejamento/ assessoria de ações policiais, militares ou ainda de fiscalização. E as atividades de nível operacional são aquelas voltadas para o apoio a ações de combate militar (como perseguição e busca de criminosos), enfrentamentos e também prevenção de ilícitos.



Fonte: Elaborado pelo DI (2017)

<https://i0.wp.com/www.jornalopcao.com.br/wp-content/uploads/2015/10/gt31.jpg>

<http://supremapropaganda.com.br/wp-content/uploads/2016/04/reuniao-de-briefing.jpg>

<https://www.estudarfora.org.br/wp-content/uploads/2013/11/Carreiras-privadas-620x270.jpg>

#### 1.4.1. CCAI – Comissão Mista de Controle das atividades de Inteligência

## Curiosidade



A fase contemporânea da Inteligência tem início em 1999 com a Lei que cria o SISBIN, no entanto seu projeto de Lei é de 1997, essa articulação parte de uma proposta de campanha presidencial que trouxe como uma de suas preocupações um maior controle das atividades de Inteligência, devido aos resquícios do ocorrido na época da intervenção militar. A CCAI é reflexo dessa preocupação.

A CCAI (Comissão Mista de Controle das Atividades de Inteligência) iniciou suas atividades em 21 de novembro de 2000, e tem como uma de suas resoluções mais importantes a Resolução nº2 de 2013 do Congresso Nacional (CN), assinada pelo então Presidente do Senado Federal, Renan Calheiros. Ela é composta por 6 parlamentares, pelos líderes da Maioria e Minoria na Câmara dos Deputados e no Senado Federal, pelos presidentes da Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal. A Condução dessa comissão é rotativa, o que traz como benefício a ampliação de visão e como ponto negativo uma certa lentidão na resposta de algumas demandas.

## Amplie Seus Estudos



### SUGESTÃO DE LEITURA



Conforme consta na resolução 2ª de 2013 - CN, em seu artigo 10º, a CCAI é responsável por consolidar relatórios a respeito de suas atividades. E apesar de conter informações de caráter sigiloso, o que leva a omissão da integridade das informações, os relatórios contêm dados obrigatórios das atividades desempenhadas pelo CCAI, como descrito no art. 11º da mesma lei. O relatório consta no portal do senado federal,

disponível em:

<https://legis.senado.leg.br/comissoes/comissao?1&codcol=449>

Em 2015, na gestão da Deputada Jô Moraes, a Comissão realizou 9 reuniões oficiais, 4 de audiência pública e 5 reuniões deliberativas. Foram tratados diversos temas como a preparação para os jogos olímpicos e paraolímpicos de 2016; a PEC 67 de 2012 (reforma da legislação da Inteligência). PNI (Política Nacional de Inteligência); relatório das visitas aos órgãos do SISBIN.

#### **1.4.2. MD30-M-01**

As atividades de inteligência seguem normativas específicas em suas operações de inteligência, um importante documento no contexto do SINDE é o MD30-M-01, o 3º volume do manual de Doutrina de Operações Conjuntas publicado em 2011 pelo Ministério da Defesa.

Nesse manual são tratados assuntos como: o plano de inteligência, elaborado pelo órgão central do sistema que orienta o exercício das atividades; plano de obtenção de conhecimento; ciclo de inteligência; dentre outros assuntos voltados a nível tático e operacional.

## **Amplie Seus Estudos**



### **SUGESTÃO DE LEITURA**

O Ciclo de Inteligência utilizado na Doutrina envolve conceitos importantes de coleta, análise e produção de conhecimento. As etapas são: Direção, Reunião, Produção e Disseminação. O Manual é disponível para consulta pública, conheça também mais sobre o ciclo, sobre a hierarquia da informação e tomada de decisões, e o CIOP (Centro de Inteligência Operacional). Disponível em:  
<http://www.esg.br/images/manuais/Manual%20de%20Doutrina%20de%20Operacoes%20Conjuntas%20-%203%C2%BA%20Volume.pdf>

As atividades de inteligência percorridas no manual (BRASIL, 2011) são voltadas à defesa, conheça em linhas gerais das atividades descritas:

I. Previsões - A análise das informações permite previsões, e estas a preparação e elaboração de planos de contingência.

II. Monitoramento – efetuar o monitoramento abrangente (étnico, sociológico, econômico), avaliando possíveis alterações políticas e monitorando personalidades de liderança.

III. Indicadores de alarme – esses indicadores são indícios de modificações (situações) que podem apresentar risco (imediato ou futuro) a estabilidade.

IV. Manutenção e atualização de bancos de dados – fontes de informação obtidas de várias formas, mídia comum, publicações oficiais, bancos de dados de acesso restrito.

V. Informações correntes – essa atividade envolve a atualização e caminho da informação no momento da operação.

VI. Atualização de Ordem de Batalha – tais como: dados militares, dados referentes ao terrorismo, meio ambiente, dentre outros.

VII. Estudo de alvos – avaliando dados do alvo e analisando possíveis danos ou previsões em cenários distintos.

VIII. Apoio a outras atividades – atualmente voltado principalmente a guerra eletrônica.

### **1.5. Análise de Informações**

Uma importante atividade de inteligência é a análise de informações, didaticamente dividida em 3 momentos: coleta, seleção/triagem e processamento. As técnicas utilizadas dependem da delimitação do objetivo, ou seja, do conhecimento que se deseja produzir.

## **Para Refletir**



A análise é extremamente importante, vamos refletir por um momento, no atual contexto, a facilidade de se conseguir um grande volume de informação a respeito de um acontecimento é elevada. Essa facilidade pode causar uma impressão ingênua de que o processo de produção de conhecimento é simples. No entanto, informação distorcida vem junto com a informação necessária. Essa distorção é causada pois existe disponível muita informação falsa, produzida e disseminada com objetivos escusos. Além dessa

variável, erros ou induções na coleta de informação podem contaminar o resultado final.

Um importante produto da Inteligência brasileira é a Metodologia ARENA (Avaliação de Risco com Ênfase na Ameaça), desenvolvida pela ABIN. Para compreender melhor é possível acompanhar o relatório sobre os Jogos Olímpicos ocorridos no Brasil em 2016, em que a metodologia foi utilizada.



Fonte:  
[http://www.abin.gov.br/conteudo/uploads/2015/05/AVALIA%C3%87%C3%83O\\_DE\\_RISCO\\_RIO\\_2016.jpg](http://www.abin.gov.br/conteudo/uploads/2015/05/AVALIA%C3%87%C3%83O_DE_RISCO_RIO_2016.jpg)

A Inteligência é uma importante estratégia em Defesa Civil, pois tanto a previsão como a rápida resposta nas situações de risco e crise dependem de importantes decisões. Algumas dessas decisões foram tomadas muito antes, na elaboração de planos e análises minuciosas. Para tomar essas decisões é preciso conhecer, estar informado de uma série de variáveis.

## Resumo da Aula

Nesta aula foi discutido sobre a importância da tomada de decisões e como ela é um momento crucial e complexo. A atividade de inteligência visa coletar e analisar dados para produzir conhecimento que dará suporte a essas decisões. A proteção (Contraineligência) também é parte das atividades de

inteligência. O atual sistema brasileiro de inteligência encontra-se na sua 4ª fase (Contemporânea), iniciado com a Lei 9.883 de 1999. A defesa Civil foi inserida nesse contexto pelo Decreto 4.376 de 2002.

## Atividade de Aprendizagem



Elabore um modelo de análise de dados para ser aplicado em um bairro do município onde exerce sua atividade profissional ou reside. O modelo deve possuir as etapas:

- 1 coleta da informação, em que você descreve de que maneira a informação vai ser alcançada;
  - 2 seleção e triagem dos dados, em que serão validadas as informações coletadas, com uma distinção entre confiável ou não, relevante ou não;
  - 3 processamentos da informação, em que se desenvolve uma interpretação das informações selecionadas para produção do conhecimento (riscos);
- Para a atividade tenha como foco os possíveis riscos que o bairro possa ter.

### **Apresentação da Aula 2 – Metodologia Analítica**

Esta aula será dedicada a dois casos práticos visando a melhor fixação de conteúdo, além da apresentação da metodologia analítica, que tem por finalidade a seleção e o processamento da informação, que servem como delineadores da confiabilidade tanto da fonte dos dados como da informação.

## **2. METODOLOGIA ANALÍTICA**

A análise de informações é uma poderosa ferramenta de inteligência, em tal processo pode-se utilizar diversos métodos analíticos. A metodologia ARENA foi desenvolvida pela ABIN para ser utilizada em grandes eventos, constitui-se de um dos produtos de contrainteligência mais importantes utilizados na atualidade. Na área da Defesa Civil o Projeto Mapeamento do CPRM possui métodos analíticos voltados à coleta, análise e processamento das informações coletadas para produção de conhecimento de extrema importância que podem ser utilizados na elaboração de Planejamento em Defesa Civil, serão discutidos

métodos analíticos utilizados em no planejamento de Defesa Civil tendo como foco a Análise de Risco de Desastres Tecnológicos.

Na atualidade, a facilidade em se obter um volume de dados/informações, pode representar uma falsa sensação de conhecimento. No entanto, muitas informações contém ruído de informação, não são fidedignas, isto é, são informações falsas produzidas com intenção maliciosa ou sem compromisso com a exatidão dos dados. Outra variável é o erro ou induções na própria coleta dos dados, que pode desconstruir toda a produção do conhecimento, visto que seus alicerces podem ser incertos.

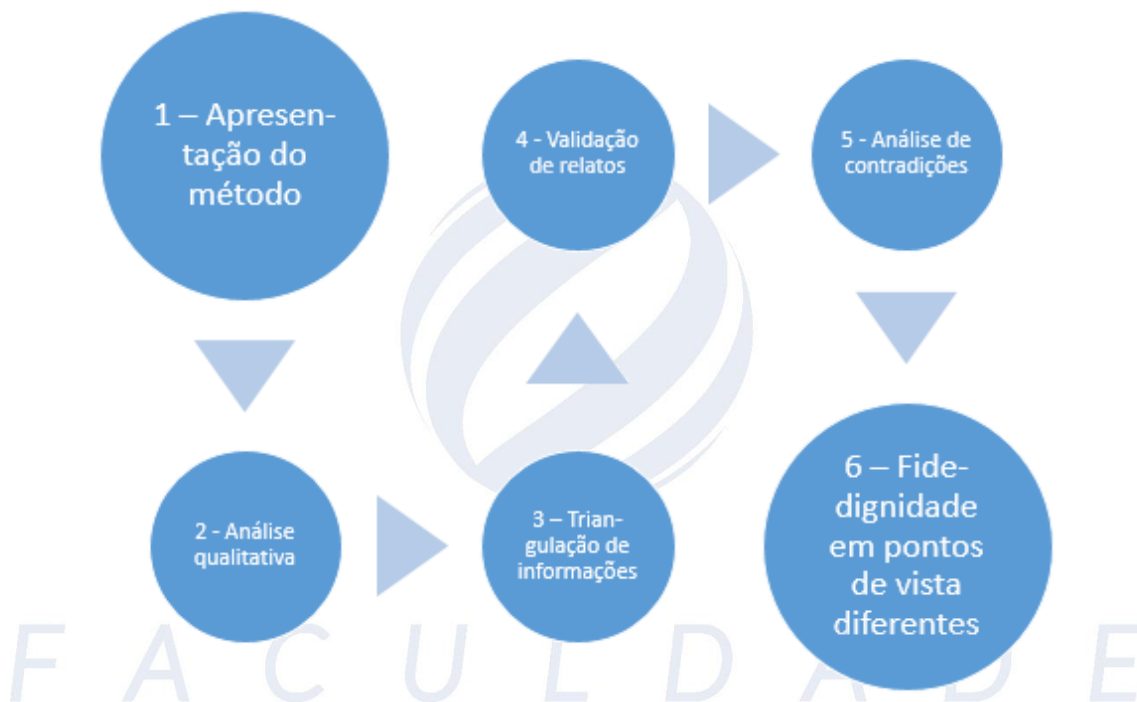
## Curiosidade



A noção de ruído vem da teoria das comunicações de Shannon, que aguçadamente utiliza deste conceito para construir a teoria da complexidade pelo ruído. Na comunicação, ruídos são erros na transmissão de mensagens e indesejáveis em uma comunicação, motivo pelo qual, na teoria da comunicação, não existe positividade na presença de ruídos. (LEFEVRE, 2009, p.1.195).

A fidedignidade é um dos elementos que validam uma pesquisa, para se assegurar que isso ocorra algumas orientações devem ser seguidas, a pesquisadora Minayo (2012, p.625) apresenta 6 passos para salvaguardar a fidedignidade das informações. Iniciando na apresentação do método de forma que seja avaliável por qualquer outro avaliador, apresentando a teoria utilizada, o método e técnicas adequadas. Em segundo lugar, efetuar uma análise qualitativa explicando as ações no campo, evidenciando as possíveis dificuldades na construção do objeto, pois a interação do próprio pesquisador na obtenção de dados pode ser uma das variáveis. No terceiro passo a autora reforça a triangulação de informações para garantir a validade, ou seja, buscar diferentes ângulos através da comparação dos dados obtidos utilizando técnicas diferentes para coleta dos mesmos e fontes de informações diferentes. O quarto passo se refere à validação de relatos comparando esses com observação de campo dos seguintes parâmetros: Especificidade, exatidão e intervalo de trabalho. Em quinto lugar a autora salienta que os relatos e fatos que contradigam a hipótese inicial do investigador não deve ser ocultada ou descartada, mas sim, analisada com cuidado e critério problematizando-o. Por

fim utilizar a fidedignidade em diversos pontos de vista que possam surgir na pesquisa, isso se deve a diversidade de sentidos, no relato a verdade pode não se manifestar de forma única.



Fonte: Elaborado pelo DI (2017).

Na análise de informações, é importante utilizar um método para o processamento de informação, sendo que o método mais utilizado é a metodologia analítica.

## Curiosidade



Existem outros métodos famosos, a escolha do método depende em grande parte da pergunta/problema, ou seja dos objetivos que se deseja alcançar. Curioso sobre esses outros métodos?

Aqui vão alguns: Método experimental, observação, hermenêutico, dialético, fenomenológico e método histórico. Cada um deles é importante em seu contexto de aplicação.

O método analítico guia-se através da lógica empírica e procura conhecer um todo através de suas partes, isto é, analisando suas variáveis e para isso utiliza-se de diversas técnicas, como observação de campo, coleta de dados em pesquisa (fontes públicas e/ ou específicas de acesso restrito), cruzamento de informações, histórico do objeto, etc.

No desenvolvimento, implementação ou adaptação de um método analítico é importante preocupar-se com sua validação, que indicará que o método é adequado para o objetivo a que se propõe analisar. Juntamente com outros pesquisadores, Brito (2003, p.130) elencou 10 critérios que servem de parâmetro para a validação de um método analítico, confira a seguir:

|   |                             |    |                              |
|---|-----------------------------|----|------------------------------|
| 1 | Especificidade/Seletividade | 6  | Exatidão                     |
| 2 | Função da Resposta          | 7  | Precisão                     |
| 3 | Intervalo de Trabalho       | 8  | Limite de Detecção (LD)      |
| 4 | Linearidade                 | 9  | Limite de Quantificação (LQ) |
| 5 | Sensibilidade               | 10 | Robustez                     |

Fonte: Elaborado pelo autor adaptado pelo DI (2017).

A seguir serão apresentados em maiores detalhes cada um dos critérios, acrescentando as reflexões de Barros (2002, p.176). A especificidade é a capacidade de o método analisar/selecionar um dado mesmo quando outros são apresentados junto a esse e pode ser testada com outro método comprobatório. A função da resposta é obtida no gráfico analítico, onde a correlação dos elementos deve estar clara e pode ser apresentada de forma qualitativa (intensidade da correlação). O intervalo de trabalho é a faixa de dados que se pretende analisar, deve ser definido com maior precisão possível. A linearidade, que pode ser apresentada no gráfico analítico, refere-se à habilidade do método de apresentar resultados definidos, seja por lógica matemática ou na correlação dos objetos.

A sensibilidade é o critério que define o nível de confiança entre concentrações próximas, o que variações de valor nos resultados. A exatidão é a comparação com o valor obtido dos dados coletados com a amostra, pode ser utilizado como técnica a comparação com MRC (Material de Referência Certificado), ou com o mesmo dado obtido utilizando uma técnica diferente (por exemplo em estudos colaborativos, combinando os dados analisados por diferentes grupos/laboratórios e comparando seus resultados); este critério determina o nível de confiança dos dados. A precisão refere-se ao desvio padrão

ou coeficiente de variação (CV), obtido na comparação da proximidade dos dados obtidos.

## Vocabulário



### **Desvio Padrão – Nas palavras de Gonçalves (2013, s/p.):**

O desvio-padrão, assim como a variância, é uma medida de dispersão. A função dele é mostrar como ocorre a dispersão dos elementos da população ou da amostra com relação à média dessa mesmas populações e amostras. [...] Quando avaliamos o desvio padrão podemos afirmar que quanto maior for o desvio-padrão, maior será a dispersão em relação à média, quanto menor o desvio-padrão, menor o desvio haverá em relação à média.

Retornando aos critérios de Brito (2003), o Limite de detecção se trata de um valor que é determinado como o limiar inferior das amostras ou informações, para que essa informação seja considerada válida para o método utilizado. Já o limite de quantificação está relacionado ao limite da precisão e exatidão da técnica/ instrumento utilizado. Por fim, a Robustez do método, que deve ser investigada já na sua elaboração, determina quais as variáveis do método analítico podem sofrer alterações sem que isso afete seus resultados.

### **2.1. Metodologia ARENA - Avaliação de Risco com Ênfase na Ameaça**

A metodologia ARENA é o produto de inteligência desenvolvido pela ABIN, considerada um dos pilares das atividades de contrainteligência realizadas pela agência para assegurar a segurança em grandes eventos, além disso também é utilizada na proteção de infraestruturas críticas. A título de exemplo dos grandes eventos, essa técnica foi utilizada, em 2011, no FEMAL (Fórum Econômico Mundial – América Latina), na Jornada Mundial da Juventude em 2013, na Copa do Mundo FIFA Brasil em 2014, e nos Jogos Olímpicos e Paraolímpicos em 2016. No contexto da utilização da técnica em infraestruturas críticas a metodologia foi utilizada em 2009 na Eletronorte, Usina Hidrelétrica de Tucuruí/PA; em 2010 no Complexo Uranífero Mineiro-Industrial de Lagoa Real em Caetité/BA / Indústrias Nucleares Brasileiras (INB); e em 2015 Usina Hidrelétrica de Xingó/AL/SE / Companhia Hidro Elétrica do São Francisco.

## Curiosidade



A ABIN tem como uma de suas publicações mais importantes a Revista Brasileira de Inteligência (RBI)? A revista é disponível ao acesso público no endereço eletrônico: <http://www.abin.gov.br/central-de-conteudos/publicacoes/>

A metodologia ARENA – Análise de Risco com Ênfase na Ameaça, não só analisa ameaças e vulnerabilidades como também estabelece medidas corretivas visando o aperfeiçoamento dos sistemas de proteção, considerando instalações físicas, os sistemas de comunicação e a gestão de pessoal.

Conforme definido pela ABIN:

## Importante

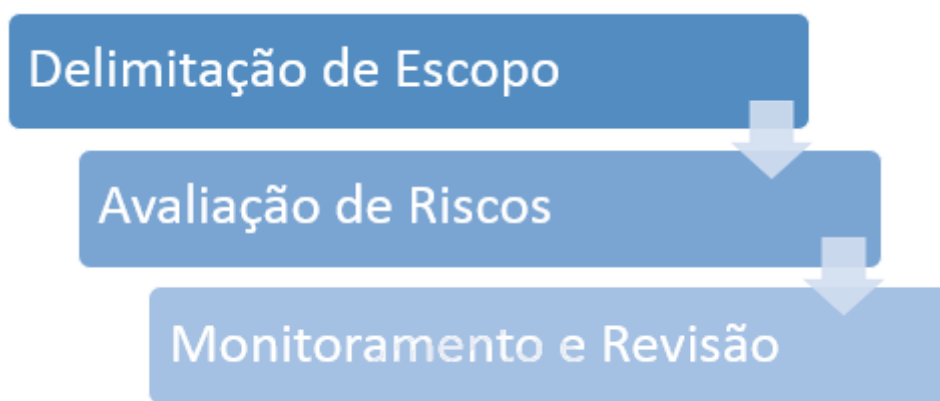


No âmbito da metodologia, o “risco” corresponde à uma potencial consequência negativa – denominada “impacto” – ocasionado pela exploração de uma vulnerabilidade por determinado agente ou fenômeno identificado como “fonte de ameaça”.

As fontes de ameaça são variáveis que apresentam potencial de provocar situações de ameaça ao objeto que se está analisando. Tais variáveis podem ser entidades, fenômenos da natureza, grupos de pessoas ou ainda agentes biológicos. Com isto delimita-se o grau de risco, fruto da correlação de 3 aspectos: 1) a fonte de ameaça; 2) vulnerabilidades dos sistemas de proteção; e 3) impactos negativos oriundos da exploração dessas vulnerabilidades.

Ao fim da análise o ARENA processa essas informações em um documento com indicação e orientações para o aperfeiçoamento dos níveis de segurança (instalações e processos), para que as autoridades responsáveis pela segurança desses grandes eventos possam tomar as devidas medidas e/ou efetuar monitoramento das variáveis que permanecerem inseguras.

São três fases: Delimitação do Escopo, Avaliação de Riscos, Monitoramento e Revisão.



Fonte: Elaborado pelo DI (2017).

Na fase preliminar efetua-se a delimitação do escopo, isto é, a ABIN juntamente com a entidade que receberá a avaliação definem qual vai ser a abrangência do projeto.

Na avaliação de riscos, segunda etapa, ocorre a coleta de dados e a caracterização das ameaças. A determinação dos riscos considerados primários é dividida em 6 etapas:

Etapa 1 – Identificação do contexto e das “fontes de ameaças”: realização de entrevistas, visitas técnicas de campo, análise de processos e confecção de matriz para identificação das principais ameaças.

Etapa 2 – Caracterização das “Fontes de Ameaça”: determinação dos atributos e potencialidades de cada ameaça identificada.

Etapa 3 – Avaliação dos Sistemas de Proteção: identificação, avaliação e classificação dos controles existentes.

Etapa 4 – Estimação da efetividade da ameaça: mensuração da capacidade de a ameaça explorar determinada vulnerabilidade.

Etapa 5 – Estimação do Impacto: determinação do potencial de dano das ameaças.

Etapa 6 – Determinação do Risco:

1. Definição do nível de risco associado à exploração de uma determinada vulnerabilidade, correlacionando efetividade da ameaça e impacto associado

2. Recomendação de medidas de proteção voltadas à diminuição dos níveis de riscos e à mitigação dos prejuízos correlatos

3. Determinação de matriz dos riscos residuais, remanescentes após aplicação das medidas de proteção recomendadas. (ABIN, s/d. s/p.)

Na terceira e última etapa, é feita a revisão dos dados e monitoramento contínuo das ameaças que foram identificadas nas etapas anteriores.

Faz parte da metodologia, como uma ferramenta transversal de revisão dos resultados a reavaliação constante dos dados obtidos em todas as etapas, essa metodologia pressupõe ciclos de verificação dos dados, assim a fase de reavaliação permite que se ajuste os níveis de risco calculados.

## 2.2. Métodos analíticos utilizados em Defesa Civil

Para aplicação em Defesa Civil também são utilizados métodos analíticos, sendo um deles o modelo de Avaliação de Riscos de Desastres conforme orientação da Secretaria Nacional de Defesa Civil (2007), o modelo utilizado é específico para Desastres Tecnológicos, mas essa mesma sistemática de avaliação pode ser aplicada aos desastres naturais, humanos e mistos, com as devidas adaptações.

### Converse Com Seus Colegas



Você conhece o Projeto Mapeamento? Esse projeto é desenvolvido pela SEDESC em 275 municípios dentre os mapeados pelo Serviço Geológico do Brasil – CPRM e ele está disponível para consulto no portal do Ministério da Integração.

Produzindo dados e análise da vulnerabilidade a desastres naturais para elaboração de Mapas de Risco e apresentação de proposta de intervenções para prevenção de desastres. Com seus colegas, discuta sobre a importância de ter esse conhecimento e principalmente da publicação dessas informações para a população.

Conforme o manual, a avaliação de risco ocorre em 3 etapas em todos os desastres:

1. Análise das ameaças de eventos adversos;
2. Análise do grau de vulnerabilidade;
3. Caracterização dos riscos de desastre.

Os riscos tecnológicos têm ainda 2 etapas importantes, que consistem no estudo da evolução dos eventos adversos e acidentes, na definição de alternativas de gestão referentes ao processo de redução dos desastres assim como da limitação dos danos. As hipóteses de planejamento, serão estudadas na próxima aula.

#### 2.2.1. Análise das Ameaças de Eventos Adversos

A análise das ameaças de eventos adversos utiliza diversos métodos de estudo analítico com objetivo de contemplar o maior número de variáveis, como os métodos apresentados na sequência.

Método de Análise Preliminar de Risco: a equipe técnica em conjunto com a comunidade deve identificar os desastres potenciais mais importantes e de maior probabilidade da região alvo assim como suas características.

Método de Análise de Falhas e de Efeitos: pode ter como alvo equipamentos mecânicos, para identificar falhas. No contexto dos desastres tecnológicos essa análise compreende, a título de exemplo, tabulação dos sistemas e equipamentos de uma planta industrial; identificação de modalidades de falhas possíveis em cada um desses sistemas e equipamentos; e por fim, a especificação desses efeitos considerados desfavoráveis, falhas que afetam o sistema e o conjunto das instalações.

O Método de Análise de Falha Humana é um método empírico analítico utilizado para identificar potenciais (ou já observados) causas e efeitos de erro humano. Tendo em consideração questões de equipamento que contribuem para provocar o erro.

Outro método, o de Análise de Falhas dos Equipamentos, estuda falhas relacionadas a condições dos equipamentos (aberto, fechado, ligado ou desligado), e parâmetros para detecção dessas falhas.

Há também a técnica da Árvore de Eventos, que se trata de uma técnica dedutiva utilizada para prever possíveis consequências desfavoráveis a partir de um evento inicial, seja esse evento um fenômeno natural, erro humano ou falha de equipamento. A Árvore de Eventos difere da Árvore de Falhas que se baseia na construção de uma cadeia de eventos sobre uma possível falha.

A técnica DOW (Proposto pela empresa americana DOW Chemical), é um método utilizado para estudar plantas industriais, avaliando seus danos prováveis caso ocorra o desastre. O objetivo é não só especificar os riscos, mas também para indicar medidas de prevenção. O método MOND (Proposto pela empresa inglesa ICI – Divisão MOND) foi desenvolvido a partir do DOW, com o objetivo mais específico de: analisar a toxicidade, reatividade e inflamabilidade dos resíduos, produtos e insumos da planta industrial alvo. (BROWN, 1998, p.5)

| Análise de Ameaças de Eventos Adversos                      |                                                                   |                                                 |                                                                      |
|-------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------|----------------------------------------------------------------------|
| <b>Análise Preliminar do Risco</b><br>• Comunidade e região | <b>Análise de Falhas e de Efeitos</b><br>• Equipamentos mecânicos | <b>Análise de Falha Humana</b><br>• Erro humano | <b>Análise Falha dos Equipamentos</b><br>• Condição dos equipamentos |
| <b>Árvore de Eventos</b><br>• Consequências de um evento    | <b>Árvore de Falhas</b><br>• Consequências de uma falha           | <b>Técnica DOW</b><br>• Danos prováveis         | <b>Técnica MOND</b><br>• Resíduos perigosos                          |

Fonte: Elaborado pelo DI (2017).

## Importante



A análise de Risco das Ameaças ocorre em 3 etapas:

1. Identificação e caracterização das ameaças;
2. Caracterização dos Efeitos Desfavoráveis;
3. Avaliação da Magnitude dos Eventos Adversos e dos Níveis de Exposição;

### 2.2.2. Análise do Grau de Vulnerabilidade

Uma vez definidas as ameaças, o próximo passo é analisar as consequências do desastre. Essa análise tem como foco a vulnerabilidade dos sistemas e da segurança. Num contexto de desastre tecnológico é importante lembrar duas correlações importantes, cidades com alto desenvolvimento social, econômico e tecnológico tem maior incidência de desastres por questões quantitativas.

A metodologia de análise do grau de vulnerabilidade é composta de 5 procedimentos importantes. Iniciando com a Vigilância Ambiental que se dá nas ações de observação, medição e descrição dos condicionantes macroambientais do sistema como concentração de agentes poluentes disponíveis (ar, água, solo, alimentos, ambiente de trabalho, etc.). A Análise Ambiental é utilizada para detectar compostos químicos no sistema analisado. O limite de Controle, é o indicativo de nível aceitável da exploração ambiental do sistema, quando

ultrapassado deve-se rapidamente desenvolver medidas de reestabelecimento para que a situação volte à sua normalidade.

O Limite de Exposição refere-se ao nível máximo de exposição humana à determinada variável, esse limite não deve ser ultrapassado. Por fim, a Avaliação Ambiental é utilizada para se produzir conhecimento sobre o estado do ambiente, seja intacto ou submetido a níveis de degradação, considerando sua recuperação e tendências evolutivas; é realizado com técnicas de monitorização, vigilância ambiental, coleta e comparação de informações e revisão permanente dos dados obtidos.



Fonte: Elaborado pelo DI (2017).

## Para Refletir



Imagine que uma empresa procura uma área para instalação de uma unidade que lida com **produtos perigosos**, aplicando os itens acima ela deve considerar os seguintes fatores:

- Distanciar-se de áreas de vulnerabilidade natural;
- Deve considerar as dimensões da planta, prevendo ampliações que respeitem o distanciamento dos focos de risco evitando a generalização do desastre;
- Verificar relevo; geologia; profundidade do lençol freático;
- Estudar proximidade de áreas que atuem facilitando o armazenamento ou tratamento dos rejeitos sólidos e dos afluentes líquidos; direção e o regime dos ventos afluentes;

Buscando assim manter-se distante ao máximo de áreas de risco. Reflita sobre as consequências e riscos que a falta de uma análise de vulnerabilidade traz para a população.

### 2.2.3. Caracterização dos Riscos de Desastres

Por fim, desenvolve-se um estudo de situação frente a um evento adverso observando as variáveis vulneráveis, considerando o efeito e danos possíveis. Em sua probabilidade e intensidade dos danos prováveis.

O estudo do Risco Geral do Processo (Fator RGP), tem como objetivo elementos que refletem na magnitude do evento. Como operações químicas (explosivos, corrosivos) desenvolvidas na unidade, o grau de isolamento das unidades de processamento, as condições gerais das vidas de acesso e evacuação.

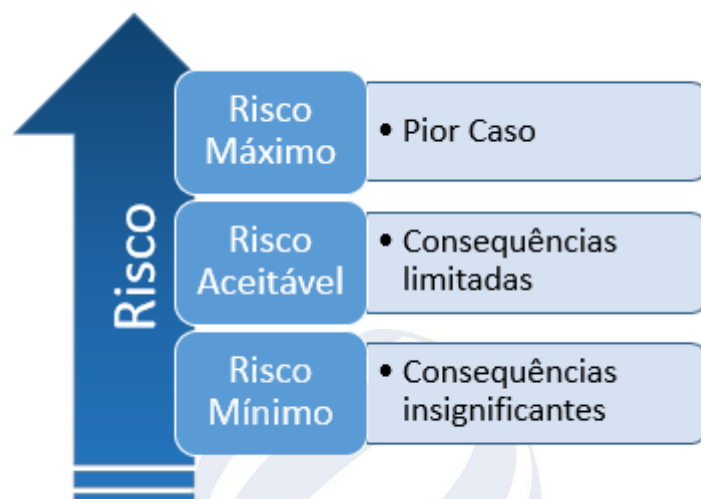
O Fator RGP, estuda o risco específico do processo, da probabilidade de ocorrência, que está diretamente relacionado a fatores como níveis de temperatura e substâncias perigosas e as possibilidades de vazamento.

## Converse Com Seus Colegas



A consequência do pior caso é um estudo de risco máximo, a título de exemplo, imagine um grande complexo tecnológico que tem vazamento de todo o seu material tóxico direto em uma área de maior vulnerabilidade, mas não só isso, imagine que o evento ocorreu a noite atingindo diretamente um grupo populacional que estava exposto ao risco e não recebeu o devido alerta a tempo.

O risco mínimo leva à análise em um cenário de fácil ação, com consequências que chegam a ser insignificantes. Próximo ao risco aceitável, onde o risco de desastre tem consequências limitadas. Por fim, o Estudo de Avarias analisa modificações das condições do funcionamento de determinado equipamento ou planta industrial que tenha como resultado a redução na eficiência de determinada operação ou processo. Sendo considerada leve quando é uma avaria que não impede seu funcionamento ou utilização e grave quando impede, ou ainda quando compromete as operações da unidade.



Fonte: Elaborado pelo DI (2017).

### Resumo da Aula

Nesta aula foi discutido mais sobre os métodos de análise de informações tendo como base exemplos práticos. No contexto da Inteligência na Segurança foi apresentado o ARENA, utilizado na avaliação e risco de grandes eventos realizados no Brasil.

Aprofundou-se o conhecimento de inteligência analisando um exemplo em que situação essa atividade é desenvolvida na Defesa Civil, conhecendo as etapas e critérios importantes na elaboração da avaliação de risco de desastre tecnológico.

## Atividade de Aprendizagem



Na atividade anterior você desenvolveu um modelo de análise de dados. Complemente o modelo construído com algumas das técnicas vistas nesta aula sobre as análises de risco.

### Apresentação da Aula 3 – Análise de Hipóteses e Premissas; Técnicas de Gráfico de Ligação

Nesta aula será mostrada a aplicação da análise de informações, mais especificamente da metodologia analítica. Serão analisados casos práticos da aplicação dessas metodologias, como a metodologia ARENA, constituída de uma Análise de Risco com Ênfase na Ameaça.

Será avaliada a elaboração de um plano de análise de risco e de ameaças tendo como base um exemplo de desastre tecnológico.

### 3. ANÁLISE DE HIPÓTESES E PREMISSAS

A partir do processamento dos dados coletados é possível formular ou analisar hipóteses e premissas relacionadas ao objeto. Para isso algumas técnicas podem ser de extrema valia, como técnicas de Gráfico de Ligação, que permitem uma melhor visualização dos dados.

A hipótese é uma ideia que se admite, independentemente de estar certa ou errada, mas a partir da qual se pode deduzir uma série de conjecturas, de possibilidades, de consequências, tendo como base experiências ou apenas imaginação. Já a premissa é justamente a própria proposição na qual se baseia uma conclusão, é o ponto de partida do raciocínio. Perceba que uma hipótese, pode conter uma série de premissas. A confusão com esses dois termos é comum analisar um caso prático tendo como base o Decreto nº 6.703 de 18 de dezembro de 2008.



#### DECRETO Nº 6.703, DE 18 DE DEZEMBRO DE 2008

Aprova a Estratégia Nacional de Defesa, e dá outras providências.

**O PRESIDENTE DA REPÚBLICA:** no uso da atribuição que lhe confere o art. 84, inciso VI, alínea “a”, da Constituição, e tendo em vista o disposto no Decreto de 6 de setembro de 2007, que institui o Comitê Ministerial de Formulação da Estratégia Nacional de Defesa,

**Decreta:**

**Art. 1º** Fica aprovada a Estratégia Nacional de Defesa anexa a este Decreto

[...]

**Introdução do anexo**

A análise das hipóteses de emprego das Forças Armadas - para resguardar o espaço aéreo, o território e as águas jurisdicionais brasileiras - permite dar foco mais preciso às diretrizes estratégicas. Nenhuma análise de hipóteses de emprego pode, porém, desconsiderar as ameaças do futuro. Por isso mesmo, as diretrizes estratégicas e as capacidades operacionais precisam transcender o horizonte imediato que a experiência e o entendimento de hoje permitem descortinar.

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/Decreto/D6703.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm)

Partindo da premissa de que o Brasil é um país pacífico, que não tem um forte histórico ou tradição de envolvimento em guerras; essa informação pode levar a conclusão de que o exercício militar de defesa não tem tanta importância. Mas, como cita o referido decreto, é necessário “transcender o horizonte imediato que a experiência e o entendimento de hoje permitem descortinar” (BRASIL, 2008).

## Para Refletir



Por um momento, considere a hipótese de que uma determinada liderança política hostil ao Brasil tome poder em um país vizinho e arme não somente um ataque às fronteiras, como uma série de atentados no nosso território. Encontraria um país com fracas defesas e poderia instaurar o caos. Vamos analisar essa hipótese, neste cenário quais contra-medidas seriam mais eficazes para garantir a segurança? Como prever essa situação? Como monitorar as variáveis certas?

Pensando nisso a Estratégia Nacional de Defesa elaborou um plano de hipótese de emprego das forças armadas, que tem como uma de suas premissas, estar preparado mesmo em tempos de paz, sendo parte da estratégia a análise e preparação das hipóteses de emprego das forças armadas.

Nessa reflexão foi utilizada a hipótese como partida de um estudo, definido por Porto (2014) como “análises orientadas a hipóteses”, por coletar dados baseado em uma suposição, uma ideia para comprová-la, refutá-la ou estar preparado caso ocorra. No entanto existe outro viés da análise de hipóteses: após a coleta, análise e processamento dos dados o conhecimento produzido pode ser a hipótese, manifestada na forma de previsões e de medidas a serem tomadas para se evitar ou atenuar determinada situação alvo como um risco eminente por exemplo.

Uma situação dessas requer um estudo mais aprofundado do conceito de análise de hipóteses e premissas aplicadas diretamente no contexto de defesa civil, para isso é possível utilizar as orientações do manual de planejamento em Defesa Civil (BRASIL, 2007).

Relembrando a metodologia de estudo de um plano de avaliação de riscos de desastres, mais especificamente sua 6ª etapa.

# Importante



Relembrando as etapas da avaliação de riscos de desastres:

1. Identificação e caracterização das ameaças;
2. Caracterização dos efeitos desfavoráveis;
3. Avaliação da magnitude dos fenômenos adversos e dos níveis de exposição;
4. Caracterização do grau de vulnerabilidade;
5. Caracterização dos riscos;
6. Caracterização das hipóteses de planejamento;

Na 6ª etapa os riscos já foram avaliados, e agora é possível definir alternativas de gestão. O planejamento estratégico, conforme a Doutrina Brasileira de Defesa Civil tem dois objetivos gerais: minimizar os desastres e restabelecer a situação de normalidade. A minimização dos desastres ocorre com o fortalecimento da segurança intrínseca, o que envolve ações de prevenção e preparação para emergências e desastres. O restabelecimento da situação de normalidade compreende a resposta ao desastre e a reconstrução. Por fim a prevenção envolve avaliação e redução dos riscos de desastres.

Na definição de alternativas de gestão, após o estudo de situação é possível estabelecer diretrizes relacionadas com os planos de prevenção aos desastres, segurança industrial (na hipótese de um desastre tecnológico) e contingência ou resposta aos desastres.

Outro exemplo interessante da aplicação da análise de hipóteses e premissas é o **plano de contingência**, elaborado para orientar, determinar ações de preparação e de resposta em um determinado cenário onde o evento adverso ocorra. Um exemplo disso é o plano elaborado pela defesa civil do estado de Santa Catarina, o qual tem como objetivos facilitar as atividades de preparação e otimizar as atividades de resposta. O plano pode ser genérico, mas neste material será exemplificado o modelo específico para inundações e deslizamentos.

### 3.1. Plano de Contingência para Inundações e Deslizamentos

## Para Refletir



Vamos analisar a hipótese, imagine um cenário de inundações e deslizamentos, como responderemos a esse evento? Como iremos socorrer e auxiliar as pessoas? Como reabilitar o cenário e reduzir os danos e prejuízos?

Nessa breve análise é preciso delimitar uma hipótese, na qual se define: qual o problema; como, quando e onde ocorre; na sequência se planeja o que fazer e também quem irá fazer. Nesse plano serão apresentados os 7 passos para elaboração, conforme orientação da Defesa Civil de Santa Catarina.

1 – Montagem do grupo de planejamento – deve ser abrangente, reunindo autoridade formal, conhecimento técnico (especialistas), e representantes de comunidades afetadas.

2 – Pesquisa

2.1 Revisão de planos existentes – legislação federal, estadual e municipal, normas administrativas, planos aplicáveis à áreas de risco e áreas vizinhas, convênios, acordos de cooperação, entre outros.

2.2 Análise e mapeamento de risco – fundamental para a identificação de medidas de prevenção e preparação. Possibilita definir quais riscos devem ser priorizados, quais ações devem ser planejadas e recursos necessários.

2.3 Identificação dos Recursos Existentes - listar e quantificar recursos comparando os existentes com os necessários.

2.4 Identificação dos aspectos especiais de planejamento – identificar aspectos específicos como características geomorfológicas, via de transporte, grupos com necessidades especiais, área de interesse especial (reservas), entre outras.

3 – Desenvolvimento – elaboração do Plano de Contingência propriamente dito.

4 – Validação – verificar conformidade com a legislação pertinente, procedimentos operacionais padronizados pelas agências com responsabilidade pela sua implementação. Verificar utilidade na prática – simulados.

5 – Aprovações – deve receber aprovação das agências e órgãos envolvidos. Enviar para organizações darem sugestões: Defesa Civil, órgãos ambientais, de saúde, educação, etc.

6 - Teste do Plano – simulação total ou parcial, envolvendo os principais órgãos responsáveis pela implementação do plano e as principais funcionalidades previstas.

7 – Manutenção – documento dinâmico, deve sofrer manutenção sistemática para garantir sua aplicabilidade ao longo do tempo. (SANTA CATARINA, 2013, s/p.)

Seguidos os 7 passos, e desenvolvendo também o processo de melhoria, que nada mais é do que um ciclo de revisão periódica e sistemática anual.

### **3.1.1. Estrutura do Plano de Contingência**

Na introdução do plano é onde se discorre sobre os dados do município, alvo do cenário da hipótese, será descrita a competência legal referente à elaboração do plano relacionando os participantes. Nesta parte é imprescindível itens como documento de aprovação, página de assinaturas, registro de alterações no plano, registro das cópias distribuídas do mesmo e sumário.

Na finalidade é onde se descreve a serventia do plano, ou seja, quais os resultados se pretende obter. Por exemplo: procedimentos a serem adotados na resposta a emergência e desastres provocados pela enxurrada, incluindo monitoramento, alerta, alarme e resposta contemplando ações de socorro, de ajuda humanitária e ações de reabilitação do cenário, na intenção de reduzir os danos e prejuízos decorrentes do evento.

Na sequência desses levantamentos está a etapa de descrição das premissas, ou mais especificamente as situações e pressupostos com o máximo de detalhes possíveis. Delimitando a situação (enxurradas e deslizamento por exemplo); descrevendo o cenário com identificação do local, descrição das características, fatores contribuintes ao evento, evolução e possibilidade de monitoramento e alerta, resultados estimados dos danos produzidos, e por fim, componentes críticos relacionados a geografia (ou hidrografia, geomorfologia do solo, etc). É preciso delimitar também os pressupostos do planejamento, ou seja, variáveis favoráveis à resposta do evento para que o plano se concretize.

Na descrição de operações descreveremos cada etapa do gerenciamento da situação no cenário imaginado. Essa descrição geral da operação explica a dinâmica do monitoramento, como serão realizados o alerta e o alarme, quais serão exatamente as respostas e como se dará o retorno à normalidade. É importante delimitar uma cadeia de comando para facilitar o gerenciamento das operações de resposta.

O plano pode trazer orientações e ações divididas por etapas. No pré-impacto há atuações de monitoramento, alerta, acionamento e mobilização de recursos. Na etapa das ações iniciais pós-desastre a ideia é definir nesse plano um sistema de comando, identificando riscos ainda existentes, dimensionar o evento e as necessidades de recursos e consolidar as primeiras informações, organizando a área afetada. É muito importante especificar quem fará o que,

quando, como e com quais recursos. Na etapa de resposta ao desastre estão descritas as ações de socorro e a assistência às vítimas. A etapa de reabilitação do cenário é voltada para a avaliação dos danos, decretação de situação de emergência ou estado de calamidade pública, recuperação de infraestrutura, restabelecimento dos serviços essenciais, ações de segurança pública e informação sobre os danos e desaparecidos. Por fim, a desmobilização é a etapa do plano em que se encontram os parâmetros para a conclusão das atividades, quais os responsáveis por essa etapa definindo a necessidade de ações de médio a longo prazo.

No plano deve estar clara a atribuição de responsabilidades, detalhando a atribuição dos órgãos envolvidos, com definição dos organizadores de cada ação e as linhas de comunicação e autoridade, tanto na ativação quanto na fase de desmobilização.

Na administração e logística é a parte do plano em que são descritos os recursos necessários, tanto financeiros quanto ajuda voluntária e parceria entre órgãos e entidades governamentais e não governamentais.

A etapa de relacionamento com outros planos, destina-se um espaço para articulação com outros planos existentes que possam contribuir nas ações de resposta para o cenário imaginado.

Enfim, a última parte da estrutura do plano é destinada para instruções de uso do plano (instalações, fluxo, percurso) e instruções para a manutenção do plano. A manutenção compreende não só a monitoria, como também exercícios e treinamentos para uma melhor resposta no cenário imaginado.



Fonte: Elaborado pelo DI (2017).

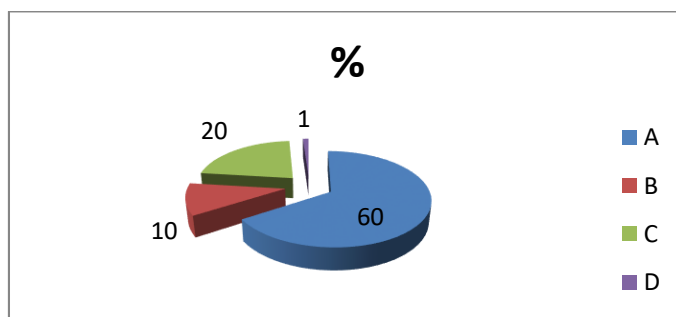
Seguindo essa estrutura de forma detalhada, o plano elaborado certamente seria capaz de permitir uma resposta mais ágil e eficaz no evento imaginado na hipótese.

### 3.2. Técnica de Gráfico de Ligação

Seja na análise de hipóteses e premissas ou na avaliação de riscos e ameaças. Há situações em que o volume de informações é grande, e são de simples entendimento, mas que ficam com uma interpretação incerta ou descorrelacionada. Ou ainda, há momentos em que a análise de um fragmento do cenário oculta a visualização do cenário como um todo.

Uma das ferramentas de auxílio na representação dos dados, na percepção das informações são as representações gráficas, as quais segundo Flores (2005) “servem de suporte para a comunicação de dados, por exemplo, de estatística, de probabilidade (...) possuem regras, códigos instituídos para a sua composição e requerem um tratamento específico”. Utilizando gráficos e fluxogramas para criar uma melhor visualização da informação.

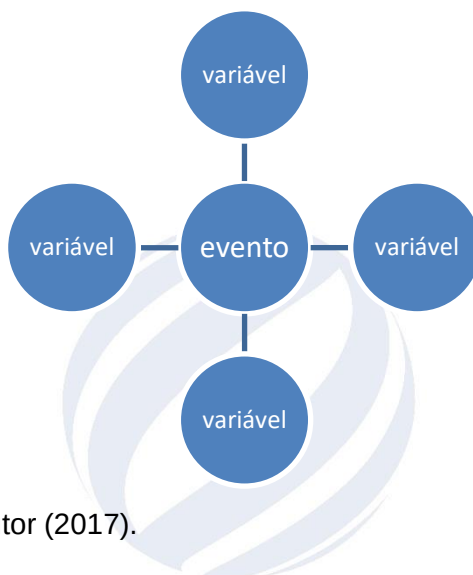
Uma possibilidade é o gráfico de pizza, que no exemplo abaixo é representado por 4 variáveis, A, B, C e D. Essa representação quando utilizada para representar porcentagem permite uma rápida percepção de qual elemento tem maior ou menor representatividade no sistema.



Fonte: Elaborado pelo autor (2017).

Outra representação gráfica que pode ser utilizada é o gráfico de ligação. Essa é uma representação que pode ser apresentada de forma simples ou complexa que permite uma melhor visualização da relação das variáveis com um objeto, ou ainda, entre si e o objeto. Na forma simples as variáveis interagem

com o evento principal. Já na representação complexa as variáveis podem interagir entre si.



Fonte: Elaborado pelo autor (2017).

No exemplo de plano de contingência das últimas aulas é possível aplicar o gráfico de ligação para melhor visualizar as ações na etapa de resposta ao desastre. É importante observar que foram especificados alguns dos responsáveis pelas atividades, e como frisado anteriormente atividades (variáveis) que têm o mesmo responsável também foram relacionadas entre si.



Fonte: Elaborado pelo autor (2017).

É possível reparar que a visualização do todo é facilitada nessa representação.

## Resumo da Aula

Nesta aula foi possível conhecer mais sobre a análise de hipótese e premissas, utilizando essa análise em casos práticos.

Foram apresentadas reflexões sobre a utilização de representações gráficas para melhor visualização das informações, aplicando ao exemplo anterior o gráfico de relação.

## Atividade de Aprendizagem



Você já desenvolveu um modelo de análise de dados com avaliação de risco. Vamos aprofundar ainda mais sua visão. Na sua análise de risco você criou uma hipótese, um cenário onde pode ocorrer um evento, um desastre. Crie um gráfico de relação das variáveis que podem causar esse evento. Seu gráfico terá como item central um evento hipotético da análise de risco, e no entorno variáveis relacionadas à causa ou ao agravamento da magnitude do cenário.

### Apresentação da Aula 4 – Análise Telefônica, Cruzamento de Informações

Nesta aula serão apresentadas duas ferramentas de análise de informações para complementar o modelo já construído nesta disciplina. Será dado maior enfoque na utilização das tecnologias, como a análise telefônica, e questões de defesa contra-ataques digitais.

## 4. ANÁLISE TELEFÔNICA

A análise de informações obtidas via interceptação telefônica consiste em uma ferramenta muito utilizada nos processos de decisão de âmbito jurídico, motivo pelo qual é importante conhecer essa técnica.

A constituição de 1988, prevê direitos e garantias fundamentais, tanto individuais quanto coletivos. O assunto da aula de hoje é delicado, pois foca justamente na quebra de um desses direitos.



## CONSTITUIÇÃO FEDERAL DE 1988

### Título II

[...]

**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

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

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)

Como é possível observar, a quebra do sigilo é prevista na constituição, nos casos estabelecidos. Além desse dispositivo, o inciso é regulamentado na Lei nº 9.296 de 24 de julho de 1996, a qual melhor especifica as situações de quebra, quem pode solicitar, dentre outras informações pertinentes.

Essa quebra, devidamente autorizada, permite que se conheça o conteúdo das transmissões e a utilize como dados. Mas existem situações previstas na lei nas quais essa interceptação não será admitida, que são os casos onde não há indícios razoáveis de participação em infração penal; casos onde a prova pode ser obtida de outros meios disponíveis que não envolvam quebra de sigilo e por fim, se a infração penal tiver como punição máxima apenas a pena de detenção, não se justifica a quebra, como bem ressalta Grinover (1997), ao analisar o artigo 2º da referida Lei.

A técnica de análise telefônica também pode ser utilizada nas mais diversas pesquisas. Pazo (2012), por exemplo, utilizou a análise em um serviço telefônico anônimo para analisar questões voltadas para a violência conjugal.

No entanto, o inciso XII do artigo 5º, conforme salienta Burrowes (2007, p.9) é mais abrangente, não considerando apenas a questão de análise telefônica, mas sim de toda a forma de comunicação de dados. Isso inclui também comunicação via internet e celulares (ou smartphones).

Contextualizando essa técnica como atividade de inteligência, sob o viés de Cepik (2002): na inteligência, a interceptação, decodificação e análise das comunicações, é uma das técnicas utilizadas em operações de inteligência. A análise visa transformar dados em informação sobre intenção e significados, para isso é necessário identificar seus emissores e possíveis receptores, contextualizar a simbologia não só da gíria, mas de possíveis códigos utilizados na mensagem. O que para um leigo pode parecer um mero emaranhado de palavras sem sentido, ou uma simples conversa. Pode esconder na realidade informações sobre sequestro, tráfico, terrorismo, etc.

Cabe ressaltar que a ABIN não se enquadra na determinação legal sobre interceptação telefônica e, portanto, não pode executar escuta telefônica.

#### **4.1. Cruzamento de Informações**

Como foi visto sobre a metodologia analítica de informações a triangulação é uma ferramenta para relacionar informações em âmbitos diferentes, mas com pontos em comum.



Triangulação de informações, comparação de dados de diferentes fontes ou com diferentes técnicas de coleta.

Ou seja, comparação de informações obtidas de fontes diferentes ou com técnicas de coletas diferentes para identificar a fidedignidade dessas informações.

A triangulação é justamente uma técnica de cruzamento de informações. Esse método pode ser utilizado não só para se verificar a fidedignidade ou validação de um método, mas também pode ser utilizado na análise de hipóteses e premissas e na própria formulação de uma hipótese utilizando o gráfico de relações.

A seguir consta um relato exemplificando a funcionalidade do cruzamento de informações.

Em audiência da Comissão Parlamentar de Inquérito (CPI) dos Crimes Cibernéticos realizada em 29 de março de 2016, o oficial de inteligência Eduardo Izycki apresentou um relatório com mapeamento contendo as principais ameaças identificadas com relação à segurança digital das Olimpíadas.

O oficial expôs com relação ao ativismo digital, considerando este como o tipo de ataque com maior probabilidade de incidência, conforme afirmou sobre o relatório explicou: “Aqui se encontram mensagens ideológicas com cunho político, fomentando manifestações ou algum tipo de ação concreta”.

Esse ativismo digital já havia sido registrado anteriormente, em 2013 na Copa das Confederações e em 2014 na Copa do Mundo, onde as ações de hackers envolviam a desconfiguração de páginas oficiais de instituições organizadoras da competição e inclusão de mensagens de cunho ideológico.

Essas ações também foram realizadas por agentes externos, que nas palavras do oficial “Não se limita o ativismo digital a uma mensagem nacional, brasileira. Diversos atores estrangeiros têm promovido ataques nesse mesmo sentido em páginas do governo brasileiro”, explicando ainda que na proximidade da data do evento em questão haveria uma tendência crescente de incidência deste tipo de ataque.

Essas observações foram feitas através do mapeamento, que utilizou como técnica, justamente, o cruzamento de informações, tendo como base registros de cerca de dois milhões de ataques na forma de desconfiguração de páginas, dos quais o agente explicou que “O que se observou é que, desses dois milhões de ataques, 100 mil foram dirigidos contra governos de 200 países. Dentro dos ataques contra governos, nós temos precisamente 12.405 ataques contra serviços do governo brasileiro”.

## Saiba Mais



Em 2016, ocorreram ataques terroristas na França e na Bélgica. O que fundamenta a importância de se discutir sobre esse tema em grandes eventos. Saiba mais, pesquise sobre o massacre de Munique ocorrido durante os jogos Olímpicos que resultou em muitos mortos.

No contexto da Defesa Civil a técnica pode ser utilizada em diversas situações. A título de exemplo, a Coordenação de Gerenciamento de Desastres da Defesa Civil do Município de Angra dos Reis, elaborou um mapa de ameaças múltiplas (contemplando prevenção, mitigação, preparação, resposta e recuperação), onde percebeu a necessidade do cruzamento de informações. Ao estabelecer como objetivo a criação de um sistema que crie um banco de dados e gere relatórios e cruzamento de informações.

Para isso é importante a preocupação com um banco de dados, concordando com Morgan (2009)

Um banco de dados permite armazenar informações de diferentes formatos, sua capacidade de recuperação dos dados através de consultas torna-o uma ferramenta adequada que agiliza muitas tarefas. Sua função de armazenamento, consultas, cruzamento de informações garantem a geração de relatórios e o gerenciamento de grande massa de dados.

## Amplie Seus Estudos



### SUGESTÃO DE LEITURA

S2ID – Sistema Integrado de Informações Sobre Desastres. Esse sistema integra diversos recursos da SEDEC e tem como um dos seus objetivos a disponibilização de informações sistematizadas na gestão.

Além do acesso restrito, o portal possui um banco de informações de consulta pública abrangendo: banco de dados, arquivo digital de documentos sobre desastres, biblioteca virtual de títulos referentes à gestão de riscos e desastres e um atlas brasileiro.

Disponível em: <https://s2id.mi.gov.br/#>

Por fim, é possível concluir que o cruzamento de informações está diretamente inserido na atividade de Defesa Civil, e que a manutenção do banco de dados fornecerá as informações para serem analisadas enriquecendo as premissas e hipóteses geradas no processo.

### Resumo da Aula

Nesta aula foi possível observar a importância e complexidade que análises de escutas telefônicas têm principalmente na atividade de inteligência, além do cruzamento de informações para validação de dados.

# Atividade de Aprendizagem

---



Incrementa o modelo de análise de riscos que foi construído com os conhecimentos desenvolvidos a cada aula com o que foi trabalhado nesta aula, o método de cruzamento de informações.



FACULDADE  
SÃO BRAZ

## **Resumo da Disciplina**

Nesta disciplina foi possível constatar que a atividade de inteligência visa coletar e analisar dados para produzir conhecimento que dará suporte a decisões, tanto no aspecto pessoal como institucional (Governos e empresas). A proteção (Contraineligência) também faz parte das atividades de inteligência.

Foi apresentado um histórico da organização de inteligência nacional com as mudanças que sofreu a cada governante que assumia o poder. Além disso mostrou-se as esferas de atuação das atividades de inteligência, e as etapas para o processo de produção do conhecimento.

Foi desenvolvido um aprofundamento no conhecimento de inteligência analisando um exemplo de aplicação em que essa atividade é desenvolvida na Defesa Civil, conhecendo as etapas e critérios importantes na elaboração da avaliação de risco de desastre tecnológico.

Discutiu-se sobre a análise telefônica e cruzamento de informações, percebendo a importância do monitoramento e manutenção de um banco de dados com esta finalidade. Também foi estudada a análise de hipótese e premissas, utilizando essa análise em casos práticos para aprofundar o entendimento do assunto.

E para apresentar esses dados foi apresentada uma reflexão sobre a utilização de representações gráficas para melhor visualização das informações, aplicando o gráfico de relação.

## REFERÊNCIAS

ABIN. Agência Brasileira de Inteligência. **Avaliação de riscos.** Metodologia ARENA. S/d. Disponível no acesso:

<http://www.abin.gov.br/atuacao/produtos/avaliacoes-de-riscos/> Acesso em 30/01/17.

ABIN. Agência Brasileira de Inteligência. **Histórico.** S/d. Disponível no acesso:

<http://www.abin.gov.br/institucional/historico/> Acesso em 30/01/17.

ABIN. **Agência expõe ameaças cibernéticas contra os Jogos Olímpicos em CPI da Câmara.** Gabinete de segurança Institucional. 2016. Acesso disponível em: <http://www.abin.gov.br/agencia-expoe-ameacas-ciberneticas-contr-os-jogos-olimpicos-em-cpi-da-camara/>

ABIN. **REVISTA BRASILEIRA DE INTELIGÊNCIA.** Brasília: Abin, v. 1, n. 1, dez. 2005.

BARROS, C.B. **Validação de Métodos Analíticos.** São Paulo: Biológico. V.64, nº 2. p. 175-177. Jul/dez. 2002.

BRASIL. CASA CIVIL. **Decreto nº 6.703, de 18 de dezembro de 2008.** Aprova a Estratégia Nacional de Defesa, e dá outras providências. 2008. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/Decreto/D6703.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm) Acesso em 30/01/17

BRASIL. CCAI. **Relatório de atividades 2015.** Comissão Mista de Controle das Atividades de Inteligência. Brasília. 2015.

BRASIL. **Constituição Da República Federativa de 1988.** Brasília. 1988.

Acesso disponível em:

[https://www.planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm#art5xii](https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm#art5xii)

BRASIL. **Decreto nº 4.872, de 6 de novembro de 2003.** Dá nova redação aos arts. 4º, 8º e 9º do Decreto no 4.376, de 13 de setembro de 2002, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999. Brasília. 2003.

Disponível em

[http://www.planalto.gov.br/ccivil\\_03/decreto/2003/d4872.htm](http://www.planalto.gov.br/ccivil_03/decreto/2003/d4872.htm) Acesso em 30/01/17.

BRASIL. **Decreto nº 4.376, de 13 de setembro de 2002.** Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei no 9.883, de 7 de dezembro de 1999, e dá outras providências.

Brasília. 2002. Disponível em

[https://www.planalto.gov.br/ccivil\\_03/decreto/2002/d4376.htm](https://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm) Acesso em 30/01/17.

BRASIL. **Decreto nº 3.695, de 21 de dezembro de 2000.** Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de

Inteligência, e dá outras providências. Brasília. 2000. Disponível em [https://www.planalto.gov.br/ccivil\\_03/decreto/d3695.htm](https://www.planalto.gov.br/ccivil_03/decreto/d3695.htm) Acesso em 30/01/17

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília. 1996. Acesso disponível em: [https://www.planalto.gov.br/ccivil\\_03/LEIS/L9296.htm](https://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm)

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Brasília. 1999. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9883.htm](https://www.planalto.gov.br/ccivil_03/leis/l9883.htm) Acesso em 30/01/17.

BRASIL. Ministério da Defesa. **MD30-M-01. Manual de Doutrina de Operações Conjuntas**. 3º Volume. 1ed. 2011

BRASIL. Ministério da Defesa. **PORTARIA NORMATIVA Nº 295/MD, DE 3 DE JUNHO DE 2002**. Institui o Sistema de Inteligência de Defesa, e dá outras providências. Brasília. 2002. Disponível em [http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/295\\_2002.pdf](http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/295_2002.pdf) Acesso em 30/01/17.

BRASIL. Ministério da Integração Nacional. **Manual de Planejamento em Defesa Civil**. Brasília: Secretaria de Defesa Civil. Volume 1. 2007.

BRASIL. Ministério da Integração Nacional. **Manual de Planejamento em Defesa Civil**. Brasília: Secretaria de Defesa Civil. Volume 4. 2007.

BRASIL. Ministério da Integração. **Manual de Planejamento em Defesa Civil**. Brasília: Secretaria nacional de Defesa Civil. V.4. 2007.

BRASIL. Ministério da Integração. **Projeto Mapeamento**. 2015. Disponível em: <http://www.mi.gov.br/web/guest/projeto-mapeamento> Acesso em 30/01/17

BRASIL. Senado Federal. **Resolução nº2 de 2013**. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso. Brasília. 2013.

BRITO, Natilene Mesquita, et al. **Validação de métodos analíticos: estratégia e discussão**. Curitiba: rev. Pest. r. ecotoxicol. e meio ambiente. V.3 p.129-146. 2003.

BROWN, A. E. P. **Análise de Risco**. Boletim Técnico. Janeiro-fevereiro/98. 1998

BURROWES, Frederick B. A **proteção constitucional das comunicações de dados**: internet, celulares e outras tecnologias. Revista Jurídica da Presidência, v. 9, n. 87, p. 09-24, 2007

CEPIK, Marco. **Inteligência e Políticas Públicas**: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*, v. 2, n. 2, p. 246-267, 2002.

CEPIK, Marco. **Regime Político e Sistema de Inteligência no Brasil**: Legitimidade e Efetividade como Desafios Institucionais. *DADOS – Revista de Ciências Sociais*, Rio de Janeiro, Vol. 48, no 1, pp. 67 a 113. 2005.

DEFESA CIVIL, Secretaria Municipal. **Mapa de Ameaças Múltiplas na Plataforma Google Earth**. Coordenação de Gerenciamento de desastres. Acesso disponível em: [http://www.mi.gov.br/c/document\\_library/get\\_file?uuid=208facd0-bb89-4433-bfb4-53a5685c96fb&groupId=185960](http://www.mi.gov.br/c/document_library/get_file?uuid=208facd0-bb89-4433-bfb4-53a5685c96fb&groupId=185960) Acesso em 30/01/17

FLORES, Cláudia R.; MORETTI, Mércles T. **O funcionamento cognitivo e semiótico das representações gráficas**: ponto de análise para a aprendizagem matemática. *GT: Educação Matemática*, São Paulo, n. 19, 2005.

GOLÇALVES, Felipe. **O Que é Desvio Padrão e as Diferenças entre Desvio Padrão da População e da Amostra**. 2013. Disponível em: <http://linkconcursos.com.br/o-que-e-desvio-padrao-diferencas-amostra-populacao/> Acesso em 09/01/2017

GRINOVER, Ada Pellegrini. **O regime brasileiro das interceptações telefônicas**. *Revista CEJ*, v. 1, n. 3, p. 131-141, 1997  
<http://www.scielo.org/pdf/csc/v17n3/v17n3a07> Acesso em 30/01/17.

JÚNIOR, Maj Eng VANDIR P. S. **O sistema de inteligência no nível operacional**: o apoio à decisão na era do conhecimento. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército. EMCB. 2013.

LEFEVRE, Fernando; LEFEVRE, A. M. C; MARQUES, M. C. C. **Discurso do sujeito coletivo, complexidade e auto-organização**. São Paulo: USP. *rev. Ciência e Saúde Coletiva*, v. 14, n.14, p.1193- 1204, 2009.

MINAYO, Maria Cecília de Souza. **Análise qualitativa**: teoria, passos e fidedignidade. *Ciência Saúde Coletiva*. 17(3), 2012.

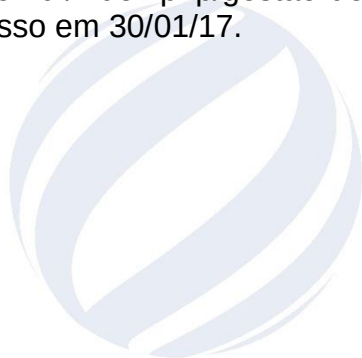
MORGAN, Jolvani; SAUSEN, Tânia Maria. **Banco de dados para o Núcleo de Pesquisa e Aplicação de Geotecnologias em Desastres Naturais e Eventos Extremos do Centro Regional Sul de Pesquisas Espaciais do INPE**. Instituto Nacional de Pesquisas Espaciais–INPE Centro Regional Sul de Pesquisas Espaciais–CRS, 2009.

PAULA. Geovani de. Et col. **Tecnologia Da Informação E Comunicação E As Atividades De Inteligência**. *Revista Ordem Pública*. Vol.5 nº1. 2012.

PAZO, Concepcion Gandara; CAVALCANTI DE AGUIAR, Adriana. **Sentidos da violência conjugal**: análise do banco de dados de um serviço telefônico anônimo. *Physis: Revista de Saúde Coletiva*, v. 22, n. 1, 2012.

PORTO, Fábio; Ziviani, Artur. **Ciência de Dados**. Petrópolis: LNCC-Laboratório Nacional de Computação Científica. 2014. Disponível em: <http://www.lncc.br/~ziviani/papers/III-Desafios-SBC2014-CiD.pdf> Acesso em 30/01/17.

SANTA CATARINA. Defesa Civil. **Plano de Contingência**: orientações e anexo. 2013. Disponível no acesso <http://www.defesacivil.sc.gov.br/index.php/gestao-de-risco-2013/plano-de-contigencia-2013.html> Acesso em 30/01/17.



F A C U L D A D E  
SÃO BRAZ