

INTRODUÇÃO À ATIVIDADE DE INTELIGÊNCIA

APRESENTAÇÃO

Bem-vindo à disciplina de **Introdução à Atividade de Inteligência!**

Este material foi desenvolvido especialmente para você, Sargento do Corpo de Bombeiros Militar, com o objetivo de apresentar conceitos fundamentais da Atividade de Inteligência aplicados ao seu contexto operacional diário.

Durante sua carreira, você frequentemente se depara com situações que geram **informações valiosas**: edificações com armazenamento irregular de produtos perigosos, áreas de risco, padrões de ocorrências, vulnerabilidades estruturais e outros dados que, se bem coletados e transmitidos, podem **prevenir desastres, salvar vidas e apoiar decisões estratégicas do comando**.

Este curso não pretende transformá-lo em um analista de inteligência, mas capacitá-lo a reconhecer seu papel essencial como **sensor qualificado** no sistema de inteligência institucional, diferenciando a atividade de inteligência da investigação, compreendendo como registrar e proteger informações sensíveis, e aplicando medidas básicas de segurança orgânica.

Bons estudos!

SUMÁRIO

UNIDADE I – FUNDAMENTOS E LEGALIDADE

- O que é Inteligência?
- Inteligência x Investigação x Vistoria Técnica
- Dado, Informação e Conhecimento
- Princípios e Limites Éticos
- Base Legal da Atividade de Inteligência

UNIDADE II – O SARGENTO COMO SENSOR DO SISTEMA

- Observação Qualificada no Serviço Operacional
- Identificação de Indicadores Relevantes
- A Fidedignidade do Dado

UNIDADE III – PROTEÇÃO DO CONHECIMENTO

- Contraineligência e Segurança Orgânica
- Segurança nas Comunicações
- Uso Responsável de Redes Sociais
- Compartimentação da Informação
- Práticas de Proteção no Ambiente de Trabalho

UNIDADE I – FUNDAMENTOS E LEGALIDADE

1.1 O QUE É INTELIGÊNCIA?

Quando ouvimos a palavra "inteligência", geralmente pensamos em capacidade intelectual. Mas no contexto institucional e de segurança pública, **Inteligência** tem um significado específico:

INTELIGÊNCIA é a atividade de obtenção, análise e disseminação de conhecimentos sobre fatos e situações que possam influenciar o processo decisório e a ação governamental, visando à salvaguarda da sociedade e do Estado.

No âmbito da Segurança Pública, a **Inteligência de Segurança Pública (ISP)** é definida como:

"O exercício permanente e sistemático de ações especializadas para identificar, avaliar e acompanhar ameaças reais ou potenciais, orientadas para produção e salvaguarda de conhecimentos necessários para subsidiar os tomadores de decisão."

Para o Bombeiro Militar, isso significa:

- **Observar** situações de risco durante atendimentos
- **Identificar** padrões e indicadores relevantes
- **Registrar** dados de forma precisa
- **Transmitir** informações ao comando de forma organizada
- **Proteger** dados sensíveis

A inteligência **NÃO** é espionagem ilegal ou violação de privacidade – é uma atividade legítima, regulamentada e essencial para a gestão de riscos e tomada de decisões estratégicas.

1.2 INTELIGÊNCIA X INVESTIGAÇÃO X VISTORIA TÉCNICA

É fundamental compreender as diferenças entre essas três atividades:

ASPECTO	INTELIGÊNCIA	INVESTIGAÇÃO	VISTORIA TÉCNICA
Objetivo	Assessorar decisões / Prevenir	Produzir provas / Punir	Verificar conformidade técnica
Natureza	Consultiva	Executiva	Técnica
Foco	Futuro (prospecção)	Passado (autoria/materialidade)	Presente (conformidade)
Produto	Relatórios de Inteligência	Inquérito Policial	Laudo Técnico
Metodologia	Análise de dados	Coleta de provas	Inspeção técnica

EXEMPLO PRÁTICO:

Situação: Durante vistoria em uma festa, você observa armazenamento irregular de GLP próximo a instalações elétricas improvisadas.

- **VISTORIA TÉCNICA:** Você identifica a irregularidade, notifica o responsável, lavra auto de infração.
- **INTELIGÊNCIA:** Você observa que o responsável tem conexões com outros estabelecimentos da região, que o padrão se repete em eventos similares e que há indícios de rede de fornecimento clandestino. Você registra essas observações adicionais e transmite ao setor competente.
- **INVESTIGAÇÃO:** Se houver crime (ex: falsificação de documentos de segurança), a Polícia Civil ou Federal investigará autoria e materialidade para processo judicial.

O Sargento atua prioritariamente na vistoria técnica, mas pode exercer papel importante na coleta de dados para inteligência, sem jamais realizar investigação criminal (que não é competência do CBMAC).

1.3 DADO, INFORMAÇÃO E CONHECIMENTO

Compreender essa diferença é essencial para atuar na atividade de inteligência:

DADO

- É a **matéria-prima bruta**

- Ainda não foi processado ou avaliado
- Exemplo: "Havia 20 botijões de GLP no local"

INFORMAÇÃO

- É o **dado contextualizado e organizado**
- Já possui algum significado
- Exemplo: "Havia 20 botijões de GLP armazenados irregularmente próximo à rede elétrica, em ambiente sem ventilação adequada"

CONHECIMENTO

- É a **informação analisada e avaliada**
- Possui credibilidade atestada
- Gera subsídio para decisão
- Exemplo: "Há risco elevado de explosão no estabelecimento X devido ao armazenamento inadequado de 20 botijões de GLP próximos à instalação elétrica precária. Recomenda-se interdição imediata e fiscalização de outros estabelecimentos do mesmo proprietário"

O PAPEL DO SARGENTO:

Você é responsável por **coletar dados fidedignos** e, quando possível, **organizá-los como informação** para que analistas especializados produzam **conhecimento** que subsidiará decisões do comando.

1.4 PRINCÍPIOS DA ATIVIDADE DE INTELIGÊNCIA

A atividade de inteligência é regida por princípios fundamentais:

LEGALIDADE

Todas as ações devem estar dentro da lei. Não há espaço para métodos ilegais.

IMPESSOALIDADE

A análise deve ser isenta, livre de opiniões pessoais ou preconceitos.

SIGILO

Informações sensíveis devem ser protegidas e compartilhadas apenas com quem precisa saber.

PRECISÃO

Dados devem ser exatos, verificáveis e confiáveis.

OPORTUNIDADE

A informação deve chegar a tempo de ser útil para a decisão.

PERMANÊNCIA

A atividade é contínua, não pontual.

SIMPLICIDADE

Clareza na comunicação e nos procedimentos.

COMPARTIMENTAÇÃO

Informações são compartilhadas estritamente com quem tem necessidade e autorização para conhecê-las.

1.5 BASE LEGAL DA ATIVIDADE DE INTELIGÊNCIA

A atividade de inteligência no Brasil é regulamentada por legislação específica:

PRINCIPAIS NORMAS:

Lei nº 9.883/1999

- Institui o Sistema Brasileiro de Inteligência (SISBIN)
- Cria a Agência Brasileira de Inteligência (ABIN)

Decreto nº 4.376/2002

- Organiza e regulamenta o funcionamento do SISBIN

Decreto nº 3.695/2000

- Cria o Subsistema de Inteligência de Segurança Pública (SISP)

Lei nº 12.527/2011 (Lei de Acesso à Informação)

- Regulamenta o acesso e sigilo de informações públicas
- Define graus de classificação de documentos sigilosos

Constituição Federal/1988

- Artigo 144: Segurança Pública como dever do Estado
- Garante direitos fundamentais e limites de atuação

LIMITES ÉTICOS E LEGAIS:

O QUE É PERMITIDO:

- Coletar dados em fontes abertas (redes sociais públicas, notícias, informações públicas)
- Observar e registrar fatos durante atendimentos legítimos
- Organizar e analisar informações disponíveis
- Proteger dados sensíveis da instituição

O QUE É VEDADO:

- Violar correspondência ou comunicações privadas
- Realizar infiltração, interceptação telefônica ou entrada sem autorização judicial
- Perseguir cidadãos ou violar direitos fundamentais
- Usar informações para fins pessoais ou políticos
- Divulgar dados sigilosos indevidamente

UNIDADE II – O SARGENTO COMO SENSOR DO SISTEMA

2.1 OBSERVAÇÃO QUALIFICADA NO SERVIÇO OPERACIONAL

No dia a dia do Bombeiro Militar, você já pratica naturalmente a **observação técnica**: avalia riscos, identifica perigos, dimensiona recursos necessários. A **observação qualificada para inteligência** adiciona uma camada de atenção a **indicadores estratégicos** que vão além da ocorrência imediata.

O QUE OBSERVAR?

Durante atendimentos, vistorias e operações, fique atento a:

1. INDICADORES DE RISCO ESTRUTURAL

- Edificações em situação precária em áreas densamente povoadas
- Ocupações irregulares em áreas de risco (encostas, margens de rios)
- Construções sem projeto de segurança em locais de grande circulação



2. PRODUTOS PERIGOSOS E ARMAZENAMENTO IRREGULAR

- Grandes quantidades de inflamáveis sem medidas de segurança
- Armazenamento clandestino de fogos de artifício ou explosivos
- Produtos químicos incompatíveis armazenados juntos
- Transporte irregular de cargas perigosas



3. PADRÕES E REINCIDÊNCIAS

- Estabelecimentos do mesmo proprietário com irregularidades similares
- Concentração de ocorrências em determinada região/horário
- Eventos que se repetem com características semelhantes

4. VULNERABILIDADES EM GRANDES EVENTOS

- Deficiências em planos de contingência
- Rotas de fuga inadequadas ou bloqueadas
- Superlotação sistemática
- Equipamentos de segurança desatualizados ou insuficientes



5. AÇÕES SUSPEITAS OU INCOMUNS

- Resistência desproporcional a ações de fiscalização
- Tentativas de ocultação de informações relevantes
- Situações que fogem ao padrão normal de ocorrências



IMPORTANTE:

Observar não significa **suspeitar de todos** ou **vigiar** pessoas. Significa estar atento a **fatos objetivos e relevantes** que possam gerar riscos ou subsidiar planejamentos.

2.2 A FIDEDIGNIDADE DO DADO

Um dado só tem valor se for **confiável**. Por isso, ao coletar informações, você deve atentar para:

CARACTERÍSTICAS DO DADO FIDEDIGNO:

1. PRECISÃO

✗ "Havia muitos botijões"

✓ "Havia aproximadamente 20 botijões de GLP de 13kg"

2. OBJETIVIDADE

✗ "O local era perigoso"

✓ "O local apresentava fiação elétrica exposta, ausência de extintores e saídas de emergência obstruídas"

3. VERIFICABILIDADE

- Sempre que possível, registre com fotos, vídeos, documentos
- Anote data, hora, endereço exato
- Identifique testemunhas ou responsáveis pelo local

4. ATUALIDADE

- Dados perdem valor com o tempo
- Sempre registre a data e hora da observação

5. CONTEXTUALIZAÇÃO

- Informe as circunstâncias da observação
- Não tire conclusões precipitadas

TÉCNICA: OMD (Observação, Memorização e Descrição)

OBSERVAÇÃO: Use todos os sentidos, não apenas a visão **MEMORIZAÇÃO:** Fixe mentalmente os detalhes relevantes imediatamente **DESCRIÇÃO:** Registre de forma clara e objetiva assim que possível

2.3 IDENTIFICAÇÃO DE INDICADORES RELEVANTES

Nem toda informação é relevante para inteligência. Você deve desenvolver a capacidade de **filtrar** o que realmente importa:

CRITÉRIOS DE RELEVÂNCIA:

Pergunte-se:

- Esta informação pode prevenir um desastre futuro?
- Pode subsidiar um planejamento estratégico do comando?
- Revela um padrão ou tendência importante?
- Indica vulnerabilidade que precisa ser corrigida?
- Pode proteger vidas ou patrimônio?

Se a resposta for **SIM** para qualquer dessas perguntas, o **dado é relevante**.

EXEMPLOS PRÁTICOS:

SITUAÇÃO	RELEVÂNCIA	POR QUÊ?
Botijão de GLP sem lacre em residência	Baixa	Irregularidade comum, risco localizado
50 botijões sem lacre em depósito clandestino	ALTA	Risco coletivo, possível rede de distribuição irregular
Incêndio em veículo na via pública	Baixa	Ocorrência pontual sem indicadores adicionais
3º incêndio em veículos na mesma região em 15 dias	ALTA	Padrão que pode indicar ação criminosa organizada
Festa com alvará vencido	Baixa	Problema administrativo local
Casa noturna com reincidência de superlotação e saídas bloqueadas	ALTA	Risco iminente, negligência sistemática

UNIDADE III – PROTEÇÃO DO CONHECIMENTO (SEGURANÇA ORGÂNICA)

3.1 CONTRAINTELIGÊNCIA E SEGURANÇA ORGÂNICA

Se **Inteligência** é produzir conhecimento para proteger, **Contrainteligência** é **proteger o conhecimento** e a própria atividade de inteligência.

SEGURANÇA ORGÂNICA (SEGOR) é o conjunto de medidas preventivas destinadas a proteger pessoal, documentação, instalações, material, comunicações e operações da instituição.

OBJETIVOS DA SEGURANÇA ORGÂNICA:

- Prevenir **vazamento** de informações sensíveis

- Evitar **comprometimento** de operações
- Proteger **pessoal, dados e instalações**
- Garantir a **credibilidade institucional**

AMEAÇAS MAIS COMUNS:

1. **Vazamento de informações** por descuido (conversa em local inadequado, documentos perdidos)
2. **Exposição indevida** em redes sociais
3. **Engenharia social** (pessoas mal-intencionadas obtendo informações fingindo ser quem não são)
4. **Acesso não autorizado** a sistemas ou documentos
5. **Manipulação ou desinformação**

3.2 SEGURANÇA NAS COMUNICAÇÕES

COMUNICAÇÕES INSTITUCIONAIS:

REGRAS BÁSICAS:

- ✓ Use **canais oficiais** para assuntos do serviço
- ✓ Nunca discuta operações sigilosas por **WhatsApp pessoal**
- ✓ Evite detalhes sensíveis em **rádio aberto** (frequências não criptografadas)
- ✓ Prefira **ofícios ou sistemas institucionais** para dados classificados
- ✗ Jamais fotografe ou filme **documentos sigilosos** com celular pessoal

E-MAIL:

- Use apenas e-mail **institucional** para assuntos oficiais
- Verifique o destinatário antes de enviar
- Classifique adequadamente o assunto
- Não encaminhe correntes ou mensagens não oficiais

RÁDIO:

- Use linguagem **codificada** conforme protocolo da unidade
- Evite expor **nomes completos, endereços exatos, detalhes táticos** desnecessários
- Lembre-se: rádio pode ser **interceptado**

3.3 USO RESPONSÁVEL DE REDES SOCIAIS

As redes sociais são uma das **maiores vulnerabilidades** para a segurança orgânica atualmente.

CUIDADOS ESSENCIAIS:

- ✗ **NUNCA:**

- Publicar fotos de **vítimas ou ocorrências sensíveis**
- Divulgar **detalhes de operações em andamento**
- Expor **locais de risco ou vulnerabilidades** antes de correção
- Fazer **comentários pejorativos** sobre instituições ou operações
- Revelar **informações classificadas**

✓ **SEMPRE:**

- Pensar: "Esta publicação pode comprometer uma operação, expor uma vítima ou prejudicar a imagem da corporação?"
- Lembrar que você representa a instituição mesmo fora de serviço
- Usar bom senso e ética

FOTOS E VÍDEOS DE OCORRÊNCIAS:

QUANDO PODE:

- Registros institucionais para documentação interna
- Divulgação **autorizada pelo comando** para fins educativos/institucionais

QUANDO NÃO PODE:

- Vítimas identificáveis sem consentimento
- Cenas chocantes ou vexatórias
- Detalhes de investigações em andamento
- Informações que possam gerar pânico

3.4 COMPARTIMENTAÇÃO DA INFORMAÇÃO

Compartimentação é o princípio de que **nem todos precisam saber de tudo.**

NECESSIDADE DE CONHECER X NECESSIDADE DE SABER:

NECESSIDADE DE SABER:

- Tenho interesse pessoal ou curiosidade sobre algo

NECESSIDADE DE CONHECER:

- Preciso desta informação **para exercer minha função**

Compartilhe informações sensíveis apenas com quem tem NECESSIDADE DE CONHECER.

CLASSIFICAÇÃO DE INFORMAÇÕES (Lei 12.527/2011):

GRAU	PRAZO MÁXIMO	CARACTERÍSTICAS
ULTRASSECRETO	25 anos (renovável 1x)	Risco à soberania, integridade territorial, relações internacionais
SECRETO	15 anos	Risco à segurança da sociedade ou do Estado
RESERVADO	5 anos	Prejudicial a operações, investigações, direitos individuais
OSTENSIVO	Sem sigilo	Pode ser publicamente divulgado

COMO APLICAR NO DIA A DIA:

- Planos de contingência de grandes eventos: **RESERVADO** (no mínimo)
- Dados sobre vulnerabilidades estruturais de edificações críticas: **RESERVADO**
- Informações operacionais de rotina: **OSTENSIVO**
- Boletins internos sobre gestão administrativa: **OSTENSIVO**

3.5 PRÁTICAS DE PROTEÇÃO NO AMBIENTE DE TRABALHO

SEGURANÇA FÍSICA:

DOCUMENTOS:

- ✓ Guarde documentos sigilosos em **locais trancados**
- ✓ Jamais deixe pastas com dados sensíveis sobre a mesa ao sair
- ✓ Destrua rascunhos e documentos descartados (**fragmentação**)
- ✗ Não leve documentos sigilosos para casa sem autorização

COMPUTADORES E SISTEMAS:

- ✓ **Bloqueie a tela** ao se ausentar
- ✓ Mantenha **senhas fortes e atualizadas** (nunca compartilhe)
- ✓ Use **antivírus** e mantenha sistemas atualizados

✗ Não conecte **pendrives desconhecidos**

✗ Não acesse sites suspeitos ou pessoais em computadores institucionais

CONVERSAS:

✓ Discuta assuntos sensíveis em **ambientes reservados**

✗ Evite falar de operações em **locais públicos** (bares, ônibus, fila de banco)

✓ Lembre-se: **paredes têm ouvidos**

ENGENHARIA SOCIAL: COMO SE PROTEGER

Engenharia Social é a técnica de manipular pessoas para obter informações confidenciais.

• EXEMPLO:

Alguém liga para o quartel se passando por autoridade e pede informações sobre efetivo, escalas ou operações.

COMO SE PROTEGER:

- **Confirme a identidade** de quem solicita informações
- **Não forneça dados** por telefone/e-mail sem validação
- **Retorne a ligação** para o número oficial da pessoa/instituição
- **Desconfie** de urgências exageradas ou pressão psicológica
- **Comunique ao superior** qualquer abordagem suspeita

SEU PAPEL COMO SARGENTO:

Você é um **elo essencial** entre a ponta operacional e o comando estratégico.

Observando com atenção qualificada, registrando com precisão e protegendo dados sensíveis, você contribui para:

- **Prevenção de desastres**
- **Planejamento estratégico do comando**
- **Tomada de decisões baseadas em evidências**
- **Segurança da instituição e dos profissionais**

"O homem de inteligência jamais será contemplado com honrarias de heróis. Pesa sobre si, o ônus de ser, em essência, o guardião do silêncio. Sua derrota é a frustração pessoal pelo conhecimento inatingido e sua vitória repousa na trincheira do anonimato."

Parabéns por concluir esta disciplina! Continue estudando, observando e protegendo.

REFERÊNCIAS BIBLIOGRÁFICAS

- BRASIL. **Lei nº 9.883/1999**. Institui o Sistema Brasileiro de Inteligência (SISBIN). Brasília, 1999.
- BRASIL. **Decreto nº 4.376/2002**. Dispõe sobre a organização e o funcionamento do SISBIN. Brasília, 2002.
- BRASIL. **Lei nº 12.527/2011**. Regula o acesso a informações (LAI). Brasília, 2011.
- **Doutrina Nacional de Inteligência de Segurança Pública (DNISP)**, 4ª edição. Ministério da Justiça e Segurança Pública, 2015.
- GONÇALVES, Joanisval Brito. **Atividade de Inteligência e Legislação Correlata**. 3ª ed. Niterói: Impetus, 2013.
- **Apostila CIAI - Curso de Introdução à Atividade de Inteligência**. Coordenação de Doutrina e Capacitação em Inteligência – CDCI/DEP/SEGEN/MJSP, 2020.