

EMENTA	
Área temática	III - Inteligência
Disciplina	3 - Contraineligência
Módulo	a - Segmentos de contraineligência
Código	III.3.a
<p>Mapa de competências</p> <p>A partir dos conhecimentos aplicados, embasados na relação ensino-aprendizagem, são competências decorrentes desse processo o desenvolvimento de habilidades operativas e cognitivas para a compreensão dos conceitos, finalidades, segmentos e fluxos da contraineligência e ameaças à instituição e seus agentes; domínio e operacionalização das técnicas, medidas de segurança e ferramentas disponíveis para salvaguarda dos recursos corporativos (humanos, materiais, informações, documentos, instalações, operações e a própria instituição); bem como o reconhecimento da relevância da atividade de contraineligência para a polícia judiciária no exercício de suas atribuições.</p>	
Carga horária recomendada: 60 horas	
<p>Descrição</p> <p>A contraineligência é atividade imprescindível ao trabalho da Polícia Judiciária e, por isso, delimitar os conceitos, fundamentos, valores e princípios que a regem é crucial. A Doutrina Nacional de Inteligência de Segurança Pública (2015), concebe a contraineligência como:</p> <p style="text-align: center;">“ramo da atividade de ISP que se destina proteger a atividade de Inteligência e a instituição a que pertence, mediante a produção de conhecimento e implementação de ações voltadas à salvaguarda de dados e conhecimentos sigilosos, além da identificação e neutralização das ações adversas de qualquer natureza.” (página 45)</p> <p>Valem-se das boas práticas dos fundamentos de contraineligência a proteção dos ativos institucionais contra ameaças como a espionagem, a sabotagem, o vazamento de informações e o terrorismo. Observadas as normas estabelecidas para prevenir, detectar e neutralizar todos os tipos de ações adversas, viabiliza-se que a organização opere com alto nível de confidencialidade, integridade, disponibilidade, autenticidade, controles de acesso e conformidade.</p> <p>Genericamente, a contraineligência é composta por três segmentos intrinsecamente relacionados e interdependentes: o primeiro, de caráter defensivo, denominado segurança orgânica, visa à prevenção de ameaças e incidentes aos ativos institucionais; o segundo, cujas medidas são de caráter eminentemente ofensivas e reativas, conhecido como segurança ativa, preconiza a detecção, obstrução e neutralização de ações adversas aos interesses institucionais; e por fim, a segurança de assuntos internos, destinada à produção de conhecimento para assessoria das ações correicionais da instituição.</p> <p>Partindo do pressuposto de que as medidas de salvaguarda dos recursos e da própria atividade e imagem institucional é dever e responsabilidade de todos os integrantes da Polícia Civil, o conhecimento sobre os segmentos da contraineligência aplicado às atividades e rotinas de Polícia Judiciária como ação formativa é essencial, através de um processo de ensino-aprendizagem no ambiente corporativo.</p>	
<p>Objetivo</p> <p>Criar condições para que o policial civil possa:</p> <ul style="list-style-type: none"> ➤ ampliar conhecimentos para entender a definição, os segmentos e métodos de proteção e salvaguarda dos recursos institucionais; 	

- desenvolver e exercitar habilidades para aplicar as ferramentas e técnicas de contrainteligência na prevenção, identificação e neutralização de ameaças para proteção da Polícia Civil enquanto instituição e de sua atividade;
- fortalecer atitudes para reconhecer a importância das atividades de contrainteligência e tornar eficaz o hábito de proteção dos ativos institucionais da Polícia Civil.

Conteúdo Programático

1. Preceitos fundamentais da contrainteligência
 - 1.1. Principais ameaças
 - 1.1.1. Comprometimento
 - 1.1.2. Vazamento
 - 1.1.3. Sabotagem
 - 1.1.4. Terrorismo
 2. Segurança orgânica
 - 2.1. Segurança de pessoal
 - 2.1.1. Determinação de sensibilidade das funções
 - 2.1.2. Processo seletivo de recursos humanos
 - 2.1.3. Investigação de perfil
 - 2.1.4. Credenciamento para função
 - 2.1.5. Acompanhamento e controle do desempenho das funções
 - 2.1.6. Segurança no desligamento
 - 2.1.7. Entrevista final
 - 2.1.8. Cancelamento de acessos
 - 2.1.9. Controle após desligamento
 - 2.2. Segurança de documentação e material
 - 2.2.1. Atribuição preliminar, classificação e marcação de grau de sigilo
 - 2.2.1.1. Legislação e atos normativos na classificação de documentos
 - 2.2.1.2. Normativas estaduais da Secretaria de Segurança Pública e da Polícia Civil do Estado de Goiás
 - 2.2.2. Controle do fluxo de documentos e patrimônio
 - 2.2.3. Segurança no manuseio de documentação e material
 - 2.2.3.1. Capacitação / verificação de habilitação
 - 2.2.3.2. Controle de reprodução
 - 2.2.3.3. Controle de custódia
 - 2.2.4. Segurança no arquivamento / destruição e recuperação de documentação e material
 - 2.2.4.1. Seleção dos documentos/materiais a serem arquivados/destruídos
 - 2.2.4.2. Escolha de meios, locais e controle de arquivamento e destruição
 - 2.2.4.3. Rotinas de treinamento de backup, destruição e evacuação em situações de emergência
 - 2.2.5. Identificação de indícios de violação
 - 2.3. Segurança da informação
 - 2.3.1. Conceitos e princípios sobre segurança da informação
 - 2.3.2. Políticas de segurança da informação
 - 2.3.3. Lei 12.527/2011 sobre sigilo e classificação das informações
 - 2.3.4. Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018)
 - 2.3.5. Aspectos humanos da segurança da informação
 - 2.3.6. Pilares da segurança em redes de computadores: confidencialidade, integridade e disponibilidade
 - 2.3.7. Conceitos de segurança nas redes de computadores com e sem fio

- 2.3.8. Segurança em Cloud Computing
- 2.3.9. Segurança em IoT
- 2.3.10. Segurança em ambientes móveis
- 2.3.11. Segurança das comunicações sem fio: bluetooth, wi-fi
- 2.3.12. Principais vulnerabilidades e medidas de segurança
- 2.3.13. Vazamento de dados
- 2.3.14. Tipos de ataques e possíveis contramedidas
- 2.3.15. Análise de vulnerabilidade e teste de invasão (pentest)
- 2.3.16. Análise de riscos
- 2.3.17. Histórico e formas de ataques
- 2.3.18. Modos de mitigação de ataques
- 2.3.19. Criptografia como solução de proteção de dados
- 2.3.20. Infraestrutura, ciclo de vida e de uso das chaves públicas
- 2.3.21. Assinatura digital
- 2.3.22. Sistemas de autenticação
- 2.3.23. Esteganografia
- 2.4. Segurança das áreas e instalações
 - 2.4.1. Logística na demarcação das áreas
 - 2.4.2. Implementação de barreiras
 - 2.4.3. Estabelecimento de linhas de proteção
 - 2.4.4. Adoção de controle de acesso e circulação de pessoas
 - 2.4.5. Emprego de normas e procedimentos adicionais de segurança
 - 2.4.6. Treinamento em caso de incidentes / emergências
 - 2.4.7. Detecção de intrusão e monitoramento de alarme
 - 2.4.8. Estabelecimento de segurança em ambientes fechados
 - 2.4.9. Isolamento das áreas de expedição e de carga
 - 2.4.10. Emprego de equipamentos de segurança
 - 2.4.11. Estabelecimento de proteção elétrica
 - 2.4.12. Proteção do cabeamento
- 2.5. Segurança das operações
 - 2.5.1. Planejamento
 - 2.5.2. Compartimentação das informações da operação
 - 2.5.3. Reconhecimento (RECON)
 - 2.5.4. Briefing
 - 2.5.5. Cadeia de custódia
 - 2.5.6. Sigilo das técnicas e elementos operacionais x exposição na mídia dos resultados da operação
- 3. Segurança ativa
 - 3.1. Características
 - 3.1.1. Diuturna
 - 3.1.2. Extenuante
 - 3.1.3. Ampla e Complexa
 - 3.1.4. Exigência de controle e acompanhamentos contínuos
 - 3.2. Modalidades
 - 3.2.1. Contrapropaganda
 - 3.2.2. Contraespionagem
 - 3.2.3. Contrassabotagem
 - 3.2.4. Contraterrorismo
- 4. Segurança de assuntos internos
 - 4.1. Conceito

<p>4.2. Finalidades</p> <p>4.3. Produção de conhecimento para a corregedoria</p> <p>4.4. Suporte às demandas correicionais</p>
<p>Bibliografia indicada</p> <p>ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.</p> <p>BEAL, Adriana. Segurança da informação: princípios e melhores práticas para proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.</p> <p>BRASIL. Doutrina Nacional da Atividade de Inteligência: fundamentos doutrinários. Brasília: Abin, 2016.</p> <p>BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. 4ª ed. Brasília: 2015.</p> <p>FERRO JUNIOR, Celso Moreira. OLIVEIRA FILHO, Edemundo Dias de. PRETO, Hugo Cesar Fraga; colaboração de George Felipe de Lima Dantas. Segurança Pública Inteligente (Sistematização da Doutrina e das Técnicas da Atividade). Goiânia: Kelps, 2008.</p> <p>STALLINGS Willian. Criptografia e segurança de redes: princípios e práticas. 6ª. edição. Pearson, 2015.</p>
<p>Estratégias de ensino e aprendizagem</p> <p>As estratégias de ensino e aprendizagem estão dispostas na MACPC/GO e devem ser escolhidas pelo facilitador, restringindo-se a métodos e técnicas adequados aos objetivos.</p>
<p>Avaliação de Aprendizagem</p> <p>A avaliação do aluno seguirá as disposições do Regimento Interno da ESPC. Serão ainda utilizadas avaliações de aprendizagem diagnóstica, formativa e somativa, como forma de aperfeiçoamento do ensino.</p>
<p>Referências Bibliográficas</p> <p>BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Doutrina Nacional de Inteligência de Segurança Pública. 4ª ed. Brasília: 2015.</p> <p>SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA. MATRIZ CURRICULAR NACIONAL para ações formativas dos profissionais da área de segurança pública/ coordenação: Andréa da Silveira Passos..(et AL). Brasília: Secretaria Nacional de Segurança Pública, 2014.</p>