Curso Curso de Contrainteligência com ênfase em Segurança Orgânica

Contextualização da Contrainteligência como um ramo da Inteligência.

Interpretação dos aspectos constitutivos do Ramo Contrainteligência, com foco em planejamento de segurança orgânica aplicada ao domínio organizacional.

Objetivos

Objetivo Geral

- Praticar as competências essenciais à elaboração de um Programa para o Desenvolvimento de Contrainteligência (PDCI), com ênfase na segurança orgânica, para a proteção do conhecimento e dos demais ativos que a uma dada organização interesse salvaguardar.

Objetivos Particulares

- Debater a Inteligência como macroprocesso e como produto, bem como sua aplicação em diversos níveis e contextos;
- Discutir a modelagem da Contrainteligência e sua interface com a Inteligència;
- Realizar o diagnóstico de um sistema e dos riscos sobre ele incidentes ;
- Aplicar o método cartesiano ao processo decisório, formulando, analisando e comparando opções diferentes para o tratamento de riscos em contexto de CI;
- Analisar um Programa de Desenvolvimento de Contrainteligência.

Público alvo

O curso está orientado a atender os gestores que participam ou irão participar de projetos de Segurança e para aqueles que buscam um melhor entendimento desta abordagem para utilização no dia-a-dia da gestão estratégica. Tais como:

- Profissionais de empresas em processo de implantação de Gestão de Riscos e continuidade nos negócios;
- Diretores que queiram divulgar a atividades de contra inteligência para toda organização;
- Gerentes e/ou Coordenadores que queiram padronizar e acompanhar todos os processos ligados a segurança em geral;
- Gestores que desejem implementar a filosofia de Gestão Estratégica da Segurança baseada em procedimentos mensuráveis e efetivos;
- Integrantes de Agências de Inteligência de Órgãos de Segurança Pública;
- Agentes de Segurança ligados ao Poder Judiciário Federal (TRE, TRT, TRF, STF dentre outros);
- Profissionais que desejam se especializar em Segurança;
- Profissionais responsáveis pela contratação de pessoas cujas empresas optam pela segurança orgânica e precisam estar totalmente cientes de uma série de responsabilidades legais, bem como das competências exigidas para o exercício de funções relacionadas com o tema.

Metodologia de ensino

Aula expositiva dialogada, Brainstorming, Estudo de Caso, Estudo Dirigido, Painel Integrado, Uso de Vídeos.

Níveis de Avaliação

Reação: nível de satisfação dos participantes em relação à ação educacional aplicada logo após o seu término.

Formas de Avaliação da Aprendizagem

Avaliação do tipo Formativa com função de orientar, corrigir, informar sobre a aprendizagem do participante da ação através de feedbacks.

Competências a desenvolver:

- Ter a capacidade de apoiar no desenvolvimento do modelo de processos de segurança para a Organização;
- Ter a capacidade de interagir com o desenvolvimento da ações táticas voltadas para o aprimoramento das atividades de inteligência da Organização;

Benefícios

Participando deste treinamento o aluno terá uma visão geral de Planejamento e Gestão Estratégica de Riscos em seus aspectos de Contra Inteligência com ênfase na Segurança Orgânica, bem como conhecer a metodologia mais adotada atualmente para implementá-la, tendo assim um conhecimento mais evoluido sobre esta metodologia ou abordagem de Gestão.

Após o treinamento o participante será capaz de:

- Contextualizar dentro de seu ambiente de atuação os preceitos de Contra Inteligência e sua aplicação na gestão estratégica;
- Debater a Inteligência como macroprocesso e como produto, bem como sua aplicação em diversos níveis e contextos;

- Discutir a modelagem da Contrainteligência e sua interface com a Inteligência;
- Ir ao detalhe e praticar as tecnicas sugeridas neste treinamento;
- Realizar o diagnóstico de um sistema e dos riscos sobre ele incidentes;
- Aplicar o método cartesiano ao processo decisório, formulando, analisando e comparando opções diferentes para o tratamento de riscos em contexto de CI;
- Analisar um Programa de Desenvolvimento de Contrainteligência.
- Conhecer as atuais práticas de mercado ligadas a Inteligência e Contra Inteligência e sua relação aos chamados ativos tangíveis e intangíveis (base da maioria dos negócios focados em serviços), dando um passo para a implementação da Gestão de Riscos de forma ampla.

Para este Curso iremos manter turmas reduzidas e daremos certificados de participação, além de serviços de apoio e “coffee-break” nos intervalos.

Pré requisitos

Não há pré-requisitos para este curso.

É recomendado conhecimento básico sobre a abordagens de Gestão Estratégica de Riscos em seus aspectos de inteligência de maneira geral e segurança de forma específica.

Algumas leituras básicas poderão ser sugeridas pelo Facilitator antes do início do curso (sem custo adicional).

Material Didático

- Apostila contendo os slides;
- Quadro branco, Datashow, filmetes selecionados pelo Facilitador;
- Textos selecionados para estudo dirigido;
- Casos para análise.
- Cartilhas com referencial para planejamento.

Conteúdo Programático

UNIDADE I - FUNDAMENTOS DA INTELIGÊNCIA

1.1. Conceitos.
1.2. Inteligência e Tomada de Decisão.
1.3. Princípios, fontes de dados, a coleta e a busca
1.4. O Ciclo da Inteligência - Orientação, Obtenção, Produção e Utilização.

UNIDADE II- FUNDAMENTOS DA CONTRAINTELIGÊNCIA

2.1. Concepção Sistêmica.
2.2. A Segurança Orgânica.
2.3. A Segurança Ativa.
2.4.Concepção de Planejamento e Implantação de Programa de Contrainteligência em Organizações.

UNIDADE III - PLANEJAMENTO DE CONTRAINTELIGÊNCIA

3.1. Análise da Missão.
3.2. Levantamento da Situação Corrente do Sistema - Estrutura, Funções, Atores.
3.3. Vulnerabilidades.
3.4. O Gerenciamento dos Riscos.
3.5. Montagem de Linhas de Ação.
3.6. Análise das Linhas de Ação Opostas.
3.7. Comparação das Linhas de Ação.
3.8. Decisão.

UNIDADE IV - GESTÃO - PROGRAMA DE DESENVOLVIMENTO DE CONTRAINTELIGÊNCIA

4.1. Caracterização.
4.2. Documentação Normativa.
4.3. Programa de Conscientização.
4.4. Programa de Treinamento Continuado.
4.5. Gerência, Auditoria e Validação.
4.6. Mecanismos de Segurança.
4.7. Contingência e de Controle de Danos.

Atividades Específicas

Em grupo

- Levantamento de Atores, Variáveis e Vulnerabilidades

- Análise de Riscos

- Execução de Processo Decisório Estruturado (Montar; Lançar, Analisar, Comparar)

UNIDADES		ASSUNTOS		OBJETIVOS		CH
Nr	TÍTULO	Nr	TÍTULO	PARTICULARES	ESPECÍFICOS	(*)
1	FUNDAMENTOS DA INTELIGÊNCIA	**1.1**	Conceitos	- Debater a Inteligência como macroprocesso e como produto, bem como sua aplicação em diversos níveis e contextos;	- Reconhecer as origens e a evolução histórica da Inteligência. - Identificar os principais conceitos afetos ao domínio da Inteligência e sus níveis de	4
		1,2	Inteligência e tomada de decisão.		- Correlacionar a Inteligência ao processo decisório.	
		1,3	Princípios, fontes de dados, a coleta e a busca		- Descrever as formas de obtenção de dados	
		1,4	O Ciclo da Inteligência - orientação, obtenção,		- Interpretar a Inteligência como um processo cíclico.	
2	FUNDAMENTOS DA CONTRAINTELIGÊNCIA	**2.1**	Concepção sistêmica.	- Discutir a modelagem da Contrainteligência e sua interface com a Inteligência.	- Discutir uma modelagem de CI aplicável a diferentes setores.	12
		2.2	Segurança orgânica.		- Interpretar o emprego de controles de CI aplicáveis ao pessoal, material, documentos, áreas e instalações. - Interpretar o emprego de controles de CI aplicáveis ao aos meios de tecnologia de	
		2.3	Segurança ativa.		- Interpretar o emprego de controles de CI em contexto de contraespionagem, contraterrorismo, contrassabotagem, contrapropaganda e contrainteligência interna.	
		2.4	Uma concepção de planejamento e implantação de programa de contrainteligência em		- Analisar uma	
3.	PLANEJAMENTO DA CONTRAINTELIGÊNCIA	**3.1**	Análise da missão	- Realizar o diagnóstico de um sistema e dos riscos sobre ele incidentes ; - Aplicar o método cartesiano ao processo decisório, formulando, analisando e comparando opções diferentes para o tratamento de riscos em contexto de CI;	- Interpretar as intenções da liderança da organização e suas condicionantes para o planejamento de CI.	12
		3.2	Levantamento da Situação Corrente do Sistema -		- Identificar o contexto organizacional alvo de um planejamento de CI.	
		3.3	Vulnerabilidades e ameças		- Identificar as vulnerabilidades de uma organização, ã luz do planejamento de CI. - Mapear as ameaças a uma organização, ã luz do planejamento de CI	
		3.4	O Gerenciamento dos Riscos		- Realizar a análise qualitativa dos riscos identificados ‘a segurança.	
		3.5	Montagem de Linhas de Ação		- Formular alternativas diferentes para o tratamento de riscos em contexto de CI.	
		3.6	Análise das Linhas de Ação Opostas		- Aperfeiçoar alternativas em face das possibilidades das ameaças identificadas.	
		3.7	Comparação das Linhas de Ação		- Formular critérios de comparação entre alternativas de tratamento de riscos.	
		3.8	Decisão		- Aplicar a análise multicritério para a seleção de melhor opção para gerenciar riscos.	
4	GESTÃO - PROGRAMA DE DESENVOLVIMENTO DE CONTRAINTELIGÊNCIA (PDCI)	**4.1**	Estrutura.	- Analisar um Programa de Desenvolvimento de Contrainteligência.	- Analisar a estrutura de um Plano de Desenvolvimento de Contrainteligência.	4
		4.2	Documentação normativa.		- Descrever maneiras de obter o engajamento organizacional para a CI.	
		4.3	Conscientização		- Identificar a necessidade de qualificação de pessoal no campo de CI.	
		4.4	Treinamento continuado.		- Descrever formas de validar o PDCI.	
		4.5	Gerência, auditoria e validação.		- Associar os controles resultantes do gerenciamento de riscos ao PDCI.	
		4.6	Mecanismos de controle.		- Caracterizar a necessidade de planos de contingência e de controle de danos.	
		4.7	Contingência e controle de danos.			

Bibliografia Básica
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. Proteção de Conhecimentos Sensíveis e Sigilosos. Coletânea de Legislação Nr 4. 1. Ed. Brasília:Gráfica ABIN, 2009, 107 p. Disponível em:< http://www.abin.gov.br/modules/mastop_publish/files/files_4a5e263a016d2.pdf> Acesso em : 15 fev. 2016. EXÉRCITO BRASILEIRO. Estado-Maior do Exército. C 30-3 (reservada): Contrainteligência. 1. Ed. Brasília:EGGCF, 2009.
Bibliografia Complementar
COMITÊ GESTOR DA INTERNET NO BRASIL. Cartilha de Segurança para Internet. Versão 4.0. São Paulo:2012. Disponível em:< http://cartilha.cert.br/ > Acesso em : 15 fev. 2016. OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE. Protecting Key Assets: A Corporate Counterintelligence Guide. Disponível em:< http://www.ncsc.gov/publications/reports/fecie_all/ProtectingKeyAssets_CorporateCIGuide.pdf > Acesso em : 15 fev. 2016. US ARMY. FM 34-60: Counterintelligence. Washington DC: 1995, 302 p. Disponível em:< http://fas.org/irp/doddir/army/fm34-60/> Acesso em : 15 fev. 2016.