MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

SEGURANÇA

PCA 7-19

PLANO PARA CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO DO DECEA

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

SEGURANÇA

PCA 7-19

PLANO PARA CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO DO DECEA

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 20/DGCEA, DE 3 DE FEVEREIRO DE 2012.

Aprova a edição do Plano para capacitação em Segurança da Informação do Departamento de Controle de Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1.049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art.1º Aprovar a edição da PCA 7-19 "Plano para Capacitação em Segurança da Informação do DECEA", que com esta baixa.

Art. 2º Esta Instrução entra em vigor na data de sua publicação.

(a) Ten Brig Ar RAMON BORGES CARDOSO
Diretor-Geral do DECEA

(Publicado no BCA nº 42, de 01 de março de 2012).

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES 7
1.1 FINALIDADE 7
1.2 ABREVIATURAS E SIGLAS 7
1.3 ÂMBITO 8

2 PLANEJAMENTO DA CAPACITAÇÃO 9
2.1 OBJETIVO 9
2.2 DESENVOLVIMENTO 9
2.3 NÍVEL ESTRATÉGICO 9
2.4 NÍVEL TÁTICO 9
2.5 NÍVEL OPERACIONAL 9

3 CURSOS 10
3.1 PERFIL ESTRATÉGICO 10
3.2 PERFIL TÁTICO 11
3.3 PERFIL OPERACIONAL 15

4 VAGAS E CUSTOS ESTIMADOS 23

5 COMPETÊNCIA 24
5.1 SDAD 24
5.2 SDTE 24

6 DISPOSIÇÕES FINAIS 25

REFERÊNCIAS 26

1 DISPOSIÇÕES PRELIMINARES

O amplo uso de sistemas de informação com grande integração através das redes de comunicação no Controle do Espaço Aéreo expõe um novo risco associado à manutenção da integridade, da confidencialidade e da disponibilidade das informações de interesse do DECEA.

Considerado o elo mais fraco do sistema de Segurança da Informação, conforme abordado por publicações científicas e seminários, os recursos humanos devem ser capacitados para controlar os riscos associados à quebra da Segurança da Informação.

1.1 FINALIDADE

O DECEA e as suas organizações subordinadas devem assegurar a confidencialidade, integridade e disponibilidade dos sistemas de informação, sejam os de uso operacional, sejam os de uso administrativo. Assim, torna-se indispensável que as pessoas envolvidas no uso e gerenciamento da tecnologia da informação possam:

a) entender os papeis e responsabilidades relacionadas à missão da Organização;

b) entender a política, procedimentos e boas práticas da Segurança da Informação; e

c) ter o conhecimento mínimo adequado dos controles gerenciais, operacionais e técnicos disponíveis para proteção do parque tecnológico de que são responsáveis.

1.2 ABREVIATURAS E SIGLAS

5W1H – Ferramenta de gestão (*What, When, Where, Why, Who e How*)

ASSICEA – Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo

BSA – *Basic Service Area*

BSS – *Basic Service Set*

BSSID – *Basic Service Set Identifier*

CERT – Centro de Estudos, Resposta e Tratamento de Incidentes

CSIRT – *Computer Security Incidents Response Team* (Equipe de Resposta a Incidentes de Segurança da Informação)

COBIT – *Control Objectives for Information and related Technology*

DNS – *Domain Name Serve*

DSSS – *Direct Sequence Spread Spectrum*

EAP – *Extensible Authentication Protocol*

ESA – *Extended Service Area*

FCA – Ferramenta de gestão (Fato-Causa-Ação)

FHSS – *Frequency Hopping Spread Spectrum*

GID – *Group ID*

IBNS – *Identity Based Networking Services*

IAPP – *Inter-Access-Point Protocol*
IDS – *Intrusion Detection System*
NAT – *Network Address Translation*
OFDM – *Orthogonal Frequency-Division Multiplexing*
OM – Organização Militar
PAT – *Port Address Translation*
PEAP – *Protected Extensible Authentication Protocol*
PGP – *Pretty Good Privacy*
PKI – *Public Key Infrastructure*
SQL – *Structured Query Language*
SSSI – Seção de Segurança de Sistemas de Informação
SSID – *Service Set Identifier*
SSL – *Secure Sockets Layer* (predecessor do TLS)
SUID – *Set User Identifier*
TCP/IP – *Transmission Control Protocol/Internet Protocol*
TI – Tecnologia da Informação
TLS – *Transport Layer Security* (sucessor do SSL)
VPN – *Virtual Private Network*

1.3 ÂMBITO

O presente Plano aplica-se a todas as organizações subordinadas ao DECEA.

2 PLANEJAMENTO DA CAPACITAÇÃO

2.1 OBJETIVO

Desenvolver capacitação em Segurança da Informação nos recursos humanos do DECEA e das Organizações subordinadas alocados para as atividades de TI que reflitam as necessidades de negócio, considerando os riscos conhecidos.

2.2 DESENVOLVIMENTO

2.2.1 O Plano de Capacitação em Segurança da Informação deve ser focado em perfis comuns a toda organização. O programa deve atingir todos os níveis das atividades de TI elencadas na DCA 21-1 – Diretriz de Reestruturação das Atividades e Infraestrutura de TI no Âmbito do DECEA -, definidas em três níveis: estratégico, tático e operacional.

2.2.2 Os requisitos de treinamento foram delineados com base nas competências mínimas de desempenho nas atividades relacionadas à área de Segurança da Informação, com base nos cursos de treinamento disponíveis em mercado.

2.2.3 Deve ser reconhecido que os indivíduos têm conhecimento anterior e que portanto tem diferentes níveis de entendimento.

2.2.4 De maneira geral, todos necessitam de treinamento em conceitos e procedimentos de Segurança da Informação, contudo, haverá necessidade de capacitação diferenciada conforme o tipo de atividade exercida.

2.3 NÍVEL ESTRATÉGICO

No nível estratégico, a capacitação deve compreender uma formação ampla que permita traçar objetivos globais, sistematizar e criar normas aplicáveis à Segurança da Informação.

2.4 NÍVEL TÁTICO

No nível tático, a capacitação deve permitir a tradução dos objetivos gerais em objetivos e atividades mais específicos a cada organização, aplicáveis à Segurança da Informação.

2.5 NÍVEL OPERACIONAL

No nível operacional, os planos específicos do nível tático são transformados em instruções práticas a serem aplicadas aos ativos de informação.

Tabela 1 – Tipos de cursos

Nível	Tipo de Curso
Estratégico	Cursos com enfoque no planejamento estratégico e normativo
Tático	Cursos com enfoque no planejamento tático
Operacional	Cursos com enfoque prático

3 CURSOS

Foram levantados alguns cursos que preenchem necessidades de capacitação em Segurança da Informação dos diferentes perfis de atividades de TI inerentes aos sistemas da área operacional do SISCEAB e da área administrativa do DECEA.

3.1 PERFIL ESTRATÉGICO

Público Alvo: SDTE e ASSISCEA.

3.1.1 Curso de especialização em Segurança da Informação, com pelo menos 360 horas de duração e o seguinte conteúdo mínimo:

a) Gestão Básica de Segurança da Informação:
   - Conceitos Gerais de Redes de Computadores e TCP/IP;
   - Conceitos Básicos Sistemas Operacionais;
   - Conceitos Gerais de Segurança da Informação; e
   - Gestão Corporativa nas Organizações.

b) Gestão de Sistemas Seguros:
   - Criptografia e Certificação Digital;
   - Segurança em Ambiente Linux;
   - Segurança em Ambiente Microsoft; e
   - Análise e Investigação de Redes - *Forensics*.

c) Gestão de Segurança Corporativa:
   - Normas e Padrões: ISO 27001, COBIT e outras;
   - Inteligência Competitiva e Contra-Inteligência;
   - Aspectos Jurídicos de TI;
   - Segurança Física e Controle de Acesso; e
   - Metodologia de Pesquisa.

d) Gestão Avançada de Segurança da Informação:
   - Gestão de Risco;
   - Plano de Continuidade de Negócios;
   - Política de Segurança da Informação;
   - Equipe de Respostas a Incidentes;
   - Auditoria de Segurança; e
   - Planejamento e Gerência do *Security Office*.

e) Gestão de Redes Seguras:
   - Defesa de Perímetro - *Firewall, Proxy, Router*, IDS/IPS;
   - Segurança em Redes sem Fio;
   - *Ethical Hacking*; e
   - Segurança em VoIP.

3.1.1.1 Total de vagas: Discriminada na Tabela 2 deste Plano e visa dotar o SDTE e a ASSI, com no mínimo dois representantes de cada setor, com as competências necessárias para a condução da gestão corporativa da Segurança da Informação no DECEA e nas Organizações subordinadas.

3.2 PERFIL TÁTICO

Público Alvo: Chefes das SSSI e um integrante das SSSI do CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, PAME, CISCEA, ICEA, CGNA, GEIV, ICA e 1° GCC.

3.2.1 Curso de Formação em *Security Officer*, módulo 1, com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) conceitos gerais de Segurança da Informação;

b) gestão de riscos;

c) legislação, regulamentação, normas, investigação e ética;

d) política de Segurança da Informação;

e) classificação de informações;

f) gestão de continuidade de negócios;

g) gestão de pessoas em Segurança da Informação;

h) segurança física e operacional; e

i) organização da Segurança da Informação**.**

3.2.1.1 Total de vagas: A quantidade de vagas para o treinamento se encontra detalhada na Tabela 2 deste Plano e visa capacitar as Seções de Segurança da Informação, no mínimo com dois representantes de cada SSSI, com as competências necessárias para condução da gestão interna da Segurança da Informação no âmbito das Organizações Militares do DECEA.

3.2.2 Curso de Formação em *Security Officer*, módulo 2, com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) criptografia;

b) controle de acesso;

c) segurança em redes e telecomunicações;

d) segurança em *Hosts; e*

e) arquitetura e modelos de segurança.

3.2.2.1 Total de vagas: A quantidade de vagas para o treinamento se encontra detalhada na Tabela 2 deste Plano e visa capacitar as Seções de Segurança da Informação, com no mínimo dois representantes, nas competências necessárias para condução da gestão interna da Segurança da Informação no âmbito das Organizações Militares do DECEA.

3.2.3 Curso de Auditor Líder em Sistemas de Gestão da Segurança da Informação NBR ISO/IEC 27001 com pelo menos 40 horas de duração e seguinte conteúdo mínimo:

a) benefícios da certificação e da auditoria de Segurança da Informação;

b) apresentação dos requisitos da norma ISO 27001;

c) princípios de auditoria de Segurança da Informação;

d) como fazer auditoria;

e) como elaborar checklists;

f) perfil do auditor líder;

g) principais atividades dos auditores;

h) etapas da auditoria;

i) logística para organização da auditoria;

j) avaliação dos resultados e comentários; e

k) estudo de caso: Certificação ISO 27001:2005.

3.2.3.1 Total de vagas: A quantidade de vagas para o treinamento se encontra detalhada na Tabela 2 deste Plano e visa capacitar as Seções de Segurança da Informação, no mínimo com dois representantes de cada SSSI, com as competências necessárias para realização de Auditoria Interna de Segurança da Informação no âmbito das Organizações Militares subordinadas ao DECEA.

3.2.4 Curso em Gestão de Continuidade de Negócios com ênfase na Norma BS 25999 com pelo menos 24 horas de duração e o seguinte conteúdo mínimo:

a) Sistema de Gestão de Continuidade de Negócios:
   - descrição do gerenciamento de continuidade de negócios;
   - política de continuidade de negócios; e
   - administração da continuidade.

b) Análise de Impacto no Negócio:
   - importância e criticidade;
   - inventário de ativos;
   - análise de impacto nos negócios (*Business Impact Analisys*); e
   - avaliação de riscos.

c) Estratégia de Continuidade:
   - tratamento dos riscos;
   - estratégias;
   - emergências civis;
   - exercícios e simulações; e
   - seleção de estratégias de continuidade.

d) Desenvolvimento e Implementação de Planos:
   - plano de administração de crises;
   - plano de recuperação de desastres;
   - plano de continuidade operacional;
   - plano de gestão da continuidade; e
   - plano de testes e validação.

e) Plano de Gerenciamento de Incidentes:
   - teste e manutenção; e
   - campanhas de sensibilização, divulgação e treinamento.

3.2.4.1 Total de vagas: A quantidade de vagas para o treinamento se encontra detalhada na Tabela 2 deste Plano e visa capacitar as Seções de Segurança da Informação, no mínimo com dois representantes, com as competências necessárias para a elaboração e condução dos Planos de Continuidade dos Sistemas Críticos no âmbito das Organizações Militares do DECEA.

3.2.4.2 Curso em Indicadores de Desempenho do Sistema de Gestão de Segurança da Informação com base na NBR ISO/IEC 27004 com pelo menos 8 horas de duração e o seguinte conteúdo mínimo:

a) Módulo I: Termos e definições relacionados com os indicadores do SGSI;

b) Módulo II: A relação dos indicadores do SGSI com o ciclo PDCA;

c) Módulo III: A Gestão dos Indicadores:
   - criação de uma cultura e clima para efetuar as medições;
   - interpretação dos resultados em relação às metas estabelecidas e sua comparação com os referenciais de excelência;
   - conceitos básicos de estatística aplicados à gestão dos indicadores de desempenho do SGSI; e
   - principais cuidados a serem tomados na gestão dos indicadores.

d) Módulo IV: O Programa de Medição da Segurança da Informação:
   - objetivos da medição da Segurança da Informação;
   - fatores que contribuem para o sucesso de um Programa de Medição da Segurança da Informação;
   - o Modelo de Medição da Segurança da Informação;
   - responsabilidades da Direção;
   - desenvolvimento de métricas e medições;
   - operação da Sistemática de Medição da Segurança da Informação; e
   - análise dos dados e comunicação dos resultados às partes interessadas pertinentes (RPI), incluindo fatos relevantes.

e) Módulo V: Avaliação e melhoria do Programa de Medição da Segurança da Informação:
   - análise dos resultados das medições para identificar necessidades de melhoria do SGSI;
   - emprego das ferramentas da gestão (FCA, Diagrama de Ishikawa, Pareto, 5W1H);
   - uso das informações comparativas pertinentes como referenciais de excelência, baseadas nos critérios da FNQ-Fundação Nacional da Qualidade; e
   - implantação, monitoramento e avaliação da eficácia das ações corretivas e preventivas adotadas.

f) Módulo VI: Exemplos de Modelos de Medição da Segurança da Informação:
   - exercícios de fixação de conceitos.

3.2.4.3 Total de vagas: A quantidade de vagas para o treinamento se encontra detalhada na Tabela 2 deste Plano e visa capacitar as Seções de Segurança da Informação, com no mínimo dois representantes, nas competências necessárias para estabelecimento e manutenção das métricas relativas à Segurança da Informação no âmbito das Organizações Militares do DECEA.

3.2.5 Curso *Certified Ethical Hacker* com pelo menos 46 horas de duração e o seguinte conteúdo mínimo:

a) *Introduction to Ethical Hacking;*

b) *Footprinting and Reconnaissance;*

c) *Scanning Networks;*

d) *Enumeration;*

e) *System Hacking;*

f) *Trojans and Backdoors;*

g) *Viruses and Worms;*

h) *Sniffers;*

i) *Social Engineering;*

j) *Denial of Service;*

k) *Session Hijacking;*

l) *Hacking Webservers;*

m) *Hacking Web Applications;*

n) *SQL Injection;*

o) *Hacking Wireless Networks;*

p) *Evading IDS, Firewalls and Honeypots;*

q) *Buffer Overflows;*

r) *Cryptography; e*

s) *Penetration Testing.*

3.2.5.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos em sistemas Unix e Windows;

b) comandos, ferramentas administrativas e funcionamento interno;

c) conhecimentos básicos de rede TCP/IP;

d) protocolos;

e) conhecimentos sobre o funcionamento de sistemas de arquivos;

f) particionamento e abstrações; e

g) leitura básica em inglês técnico.

3.2.5.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes da ASSI, do SDTE e do PAME, no mínimo com dois representantes de cada setor, com as competências necessárias para realização dos Testes de Invasão na infraestrutura tecnológica do DECEA e OM subordinadas. A critério do SDTE, poderão ser capacitados representantes das SSSI a fim de apoiar o DECEA na condução das realizações dos Testes de Invasão.

3.2.6 Curso de Teste de Invasão em Redes e Sistemas com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) elaboração planejamento e preparação:
   - definição de escopo;
   - perfil do atacante;

- limitações de tempo;
- permissão;
- detalhes da infraestrutura;
- acordo de confidencialidade;
- equipamento e recursos necessários;
- relatório de linha de tempo;
- acesso a testes anteriores; e
- inspeção física.

b) obtenção de informações:
- whois;
- sondagem e mapeamento;
- identificação de vulnerabilidades; e
- classificação de vulnerabilidades.

c) Invasão:
- quebrando senhas;
- ataques a aplicações Web;
- ataques de negação de serviço;
- *sniffing*;
- injeção de código;
- *buffer overflow*;
- *cross-site scripting* (XSS);
- sequestro de sessão;
- *exploits*;
- escalada de privilégios; e
- canais secretos, *backdoors* e *rootkits*.

d) controles de acesso e segurança física; e

e) finalização dos testes.

3.2.6.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos básicos de TCP/IP; e

b) conhecimentos básicos de sistemas GNU/Linux.

3.2.6.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes da ASSI, do SDTE e do PAME, no mínimo com dois representantes de cada setor, com as competências necessárias para realização dos Testes de Invasão na infraestrutura tecnológica do DECEA e OM subordinadas. A critério do SDTE, poderão ser capacitados representantes das SSSI a fim de apoiar o DECEA na condução das realizações dos Testes de Invasão.

3.3 PERFIL OPERACIONAL

Público Alvo: integrantes das SSSI do CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, PAME, CISCEA, ICEA, CGNA, GEIV, ICA e 1° GCC.

NOTA: Poderão ser indicados dois participantes por OM.

3.3.1 Curso em Auditoria de Segurança em aplicações WEB com pelo menos 24 horas de

duração e o seguinte conteúdo mínimo:

a) Introdução:
   - Utilização;
   - Benefícios;
   - Arquitetura;
   - Aspectos básicos de segurança; e
   - Protocolos e tecnologias.

b) Principais Ameaças:
   - Injeções;
   - *Cross-Site Scripting* (XSS);
   - Quebra de Autenticação / Roubo de Sessão;
   - Referência direta à objetos;
   - *Cross-Site Request Forgery* (CSRF);
   - Falhas de Configuração;
   - Armazenamento Inseguro;
   - Falha na Restrição de Acesso à URLs;
   - Canal Inseguro; e
   - Redirecionamentos Não-Validados.

c) Testes de Segurança:
   - Exposição de Informação;
   - Configurações e Manutenção;
   - Autenticação;
   - Gerenciamento de Sessões;
   - Autorização;
   - Funcionalidades e Lógica;
   - Validação de Dados;
   - Disponibilidade;
   - Web Services; e
   - AJAX.

d) Ferramentas:
   - Reconhecimento: HTTRACK, Httprint, Maltego CE;
   - Varreduras e Análises: Nikto, W3AF, Samurai WTF, Metasploit, Nmap, SQLmap, SQLbrute, SQLninja;
   - Proxies: WebScarab, Paros Proxy, Burp Suite, Rat Proxy;
   - Firefox add-ons: Greasemonkey, Firebug, FoxyProxy, User Agent Switcher, Tamper Data, DOM Inspector, Add N Edit Cookies, Firesheep; e
   - Sniffers: TCPdump, Wireshark.

e) Estudos de Casos.

3.3.1.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos básicos de TCP/IP; e

b) conhecimentos básicos de sistemas GNU/Linux.

3.3.1.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das equipes de TI e das SSSI, no mínimo

com um representante de cada setor, com as competências necessárias para realização de auditoria de segurança com foco nos serviços e páginas WWW disponibilizadas na INTERNET.

3.3.2 Curso Fortalecimento (*Hardenning*) de servidores Windows e Linux com pelo menos 24 horas de duração e conteúdo mínimo:

a) Problemas de Segurança:
   - *Exploits* remotos, sequestro de sessão e como se proteger;
   - Cavalos de tróia, *backdoors* e *rootkits*;
   - SQL *Injection*, *Cross-Site Scripting* (XSS) e outros problemas em aplicações Web;
   - *Scripts* e programas SUID/GID;
   - Configuração de sistemas de arquivos;
   - Diretórios com escrita global;
   - Permissões e privilégios;
   - Confiando no ambiente e no usuário; e
   - Ataques contra senhas e como se proteger.

b) *Hardening* de Servidor Unix/Linux - Parte 1:
   - Procedimentos pós-instalação;
   - Controle de acesso em Sistemas de Arquivos;
   - Controle de Acesso de usuários; e
   - Registros (Logs) do sistema.

c) *Hardening* de Servidor Unix/Linux - Parte 2:
   - Configuração de Firewall;
   - Abrindo a porta secreta do sistema; e
   - Sistemas de monitoramento.

3.3.2.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos básicos de TCP/IP; e

b) conhecimentos básicos de sistemas GNU/Linux.

3.3.2.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das equipes de TI e da SSSI, no mínimo com um representante de cada setor, com as competências necessárias para identificação de vulnerabilidades em servidores Linux e/ou Windows e a aplicação dos controles necessários para mitigá-las.

3.3.3 Curso de Segurança de Redes com roteadores e switches Cisco (SNRS Securing Networks with Router and Switches 1.0) com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) Module 1: Plataforma de Segurança com Switches:
   - Configuração Avançada *Layer 2 Security*;
   - Introdução ao CISCO IBNS;
   - Implementando Autenticação Básica 802.1x;
   - Configuração Autenticação Básica 802.1x; e
   - Configuração Avançada de Autenticação e Autorização Básica 802.1x.

b) Module 2: Plataforma de Segurança com Roteadores:
   - Introdução ao Cisco *Network Foundation Protection Strategy*;
   - Segurança do *Control Plane*;
   - Segurança do *Management Plane*; e
   - Segurança do *Data Plane*.

c) Module 3: Segurança de Comunicações site a site:
   - Introdução aos Fundamentos de VPN e IPsec;
   - Implementação de IPsec VPNs com PKI;
   - Implementação de GRE com IPsec;
   - Configuração de Alta Disponibilidade em VPNs e VTI;
   - Implementação de DMVPN; e
   - Implementação de GET VPN.

d) Module 4: Segurança de Comunicações em Acessos Remotos:
   - Implementação de Cisco IOS *Remote Access usando Cisco Easy* VPN;
   - Introdução ao Cisco IOS SSL VPN; e
   - Configuração do Cisco IOS SSL VPN.

e) Module 5: Contenção e Controle de Ameaças:
   - Configuração do NAT e PAT;
   - Configuração do Cisco IOS *Classic Firewall*;
   - Configuração do Cisco IOS *Classic Firewall on a Cisco Router*;
   - Configuração do Cisco IOS *Zone-Based Policy Firewall*; e
   - Configuração do Cisco IOS IPS.

3.3.3.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos básicos de TCP/IP;

b) conhecimentos básicos de sistemas GNU/Linux; e

c) familiaridade com equipamentos de rede CISCO.

3.3.3.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das equipes de TI e da SSSI, no mínimo com um representante de cada setor, com as competências necessárias para identificação de vulnerabilidades em switches de rede e a aplicação dos controles necessários para mitigá-las.

3.3.4 Curso Visão Geral da Criação e Gerenciamento de Equipes de Respostas a Incidentes de Segurança da Informação (*Overview of Creating and Managing Computer Security Incident Response Teams*) com pelo menos 8 horas de duração e o seguinte conteúdo mínimo:

a) Fundamentos:
   - CERT *Resiliency Engineering Framework*;
   - *Incident Management Process Framework*; e
   - Relacionamento entre os processos de Gerenciamento de Incidentes e os CSIRTs.

b) Criando um CSIRT Efetivo:
   - O que é um CSIRT;
   - O que faz um CSIRT; e
   - Categorias gerais de CSIRTs.

c) Componentes de um CSIRT:
   - público alvo;
   - missão;
   - questões organizacionais;
   - financiamento;
   - serviços; e
   - políticas e procedimentos.

d) Questões de Gerenciamento Operacional:
   - questões relacionadas com o pessoal do CSIRT;
   - gerenciando a infra-estrutura do CSIRT; e
   - avaliando a efetividade do CSIRT.

e) O Processo de Gerenciamento de Incidentes:
   - preparar;
   - proteger;
   - detectar;
   - triar; e
   - responder.

3.3.4.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) Não há.

3.3.4.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa apresentar aos integrantes das SSSI, no mínimo com dois representantes, os conceitos básicos associadas à Equipe de Tratamento e Respostas aos Incidentes de Segurança da Informação.

3.3.4.3 Curso em Fundamentos de Tratamento de Incidentes de Segurança da Informação (*Fundamentals of Incidents Handling*) com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) compreensão do ambiente do CSIRT;

b) código de ética de um CSIRT;

c) ferramentas de segurança usadas por um CSIRT;

d) revisão sobre *probes*, *scans* e tipos comuns de ataques;

e) identificação de informações críticas;

f) tratamento do *hotline* de um CSIRT;

g) triagem;

h) visão geral do sistema DNS;

i) análise de notificações de incidentes;

j) busca de informações de contato;

k) coordenação da resposta a incidentes;

l) PGP (*Pretty Good Privacy*) para CSIRTs;

m) tratamento de ataques comuns: *e-mail spoofing*, *e-mail bombing*, *spamming*, *denial of service*, código malicioso; e

n) cooperação com as polícias e os operadores da justiça.

3.3.4.4 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) conhecimentos básicos de TCP/IP;

b) conhecimentos básicos de administração de servidores Linux ou Windows; e

c) Ter o curso de Fundamentos em Tratamento de Incidentes de Segurança da Informação.

3.3.4.5 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das SSSI, no mínimo com dois representantes, na execução dos processos básicos associados à Equipe de Tratamento e Respostas aos Incidentes de Segurança da Informação, no âmbito de cada Organização Militar subordinada ao DECEA.

3.3.5 Curso Avançado em Tratamento de Incidentes de Segurança da Informação (*Advanced Incident Handling for Technical Staff*) com pelo menos 40 horas de duração e o seguinte conteúdo mínimo:

a) revisão sobre informações críticas e probes e scans típicos;

b) conseqüências de incidentes envolvendo acesso privilegiado;

c) resposta e recuperação de incidentes envolvendo acesso privilegiado;

d) visão geral de ferramentas típicas dos invasores;

e) compreensão de ataques de negação de serviço;

f) tratamento de eventos maiores (*major events*);

g) o papel da análise de artefatos no processo de tratamento de incidentes;

h) causas fundamentais das vulnerabilidades;

i) tratamento de vulnerabilidades;

j) publicação de informações produzidas pelo CSIRT; e

k) estudo de caso.

3.3.5.1 Para a realização do curso, são necessários os seguintes conhecimentos prévios:

a) completar o curso *Fundamentals of Incident Handling* ou o curso *Overview of Creating and Managing Computer Security Incident Response Teams*;

b) conhecimentos básicos de TCP/IP; e

c) conhecimentos básicos de sistemas GNU/Linux.

3.3.5.2 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das SSSI, no mínimo com dois representantes, na execução dos processos avançados associados à Equipe de Tratamento e Respostas aos Incidentes de Segurança da Informação, no âmbito de cada Organização Militar subordinada ao DECEA.

3.3.5.3 Curso Segurança em Redes *Wireless* com pelo menos 24 horas de duração e o seguinte conteúdo mínimo:

a) Visão Geral:
   - histórico das transmissões sem fio;
   - tipos de sistemas de transmissão sem fio; e
   - vantagens e desvantagens da *wireless* LAN.

b) Princípios de Radiofreqüência:
   - definição de onda;
   - Spread Spectrum;
   - freqüência e modulação; e
   - técnicas de modulação FHSS, DSSS e OFDM.

c) Terminologia:
   - cliente;
   - *access point*;
   - BSS e BSA;
   - ESS e ESA;
   - SSID e BSSID;
   - IAPP;
   - serviços oferecidos; e
   - mobilidade.

d) Métodos de Acesso:
   - operações atômicas;
   - cliente escondido;
   - detecção do uso do barramento;
   - formato do frame;
   - fragmentação de pacotes; e
   - transmissão unicast e broadcast/multicast.

e) Projeto de Redes *Wireless* LAN:
   - medição de sinal;
   - perda por espaço livre (Free Space Loss) e Fresnel Zone;
   - tipos e características das antenas;
   - topologias lógicas e distribuição de canais;
   - site survey;
   - roaming; e
   - ajuste fino.

f) Segurança em *Wireless* LAN:
   - conceitos de criptografia;
   - autenticação;
   - WEP;
   - 802.1X/EAP;
   - EAP/TLS; e
   - PEAP.

g) *Wireless* Móbile:
   - introdução às redes celulares;
   - características dos sistemas 1G, 2G, 2,5G e 3G;

- sistemas 1G;
- sistemas 2G;
- sistemas 2,5G;
- sistemas 3G; e
- *mobile* IP.

3.3.5.4 Para a realização do curso, é necessário o seguinte conhecimento prévio:

a) conhecimentos básicos de redes.

3.3.5.5 Total de vagas: A quantidade de vagas para o treinamento se encontra discriminada na Tabela 2 deste Plano e visa capacitar integrantes das equipes de TI e da SSSI, no mínimo com um representante de cada setor, com as competências necessárias para identificação de vulnerabilidades em redes Wireless e a aplicação dos controles necessários para mitigá-las

4 VAGAS E CUSTOS ESTIMADOS

4.1 O número de vagas para os cursos seguirão a seguinte distribuição para 2012 e 2013:

Tabela 2 - Número de vagas

	Vagas			Custo Estimado (R$) Referência: 2011	
Curso	Estratégico	Tático	Operacional	Unitário	Subtotal
Especialização em Segurança da Informação	4			13.760,00	55.040,00
Formação em *Security Officer* módulo 1		24		2.750,00	66.000,00
Formação em *Security Officer* módulo 2		24		2.750,00	66.000,00
Auditor Líder em Sistema de Gestão de Segurança da Informação ISO 27001		24		4.300,00	103.200,00
Gestão de Continuidade de Negócios com ênfase na Norma BS 25999		24		2.178,00	65.232,00
Indicadores de Desempenho do Sistema de Gestão de Segurança da Informação com base na NBR ISO/IEC 27004		24		880,00	21.120,00
Certified Ethical Hacker		6		3.500,00	21.000,00
Teste de Invasão em Redes e Sistemas		6		2.500,00	15.000,00
Auditoria de Segurança em aplicações WEB			24	1500,00	36.000,00
Fortalecimento (*Hardenning*) servidores Windows e Linux			24	1500,00	36.000,00
Segurança de Redes com roteadores e switches Cisco (SNRS - Securing Networks with Cisco Routers and Switches 1.0)			24	4.800,00	115.200,00
Visão Geral da Criação e Gerenciamento de Equipes de Respostas a Incidentes de Segurança da Informação (*Overview of Creating and Managing Computer Security Incident Response Teams*)			24	1.000,00	24.000,00
Fundamentos de Tratamento de Incidentes de Segurança da Informação (*Fundamentals of Incidents Handling*)			24	2.300,00	55.200,00
Avançado em Tratamento de Incidentes de Segurança da Informação (*Advanced Incident Handling for Technical Staff*)			24	2.300,00	55.200,00
Segurança em Redes *Wireless*			24	1.100,00	26.400,00
					760.592,00

4.2 A distribuição de vagas dos perfis tático e operacional será realizada entre as organizações militares subordinadas (CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, PAME, CISCEA, ICEA, CGNA, GEIV, ICA e 1° GCC).

5 COMPETÊNCIA

5.1 SDAD

Compete ao SDAD:

a) propor FIP (Ficha de Planejamento de Projeto) para o PLANSET; e

b) elaborar processo para aquisição dos cursos previstos neste Planejamento.

5.2 SDTE

Compete ao SDTE:

a) elaborar os projetos básicos ou termos de referência com especificações para os cursos previstos neste Planejamento; e

b) coordenar a execução contratual.

6 DISPOSIÇÕES FINAIS

6.1 As instruções estabelecidas neste Plano são de caráter geral e devem ser periodicamente revisadas.

6.2 Casos não previstos deverão ser levados à apreciação do Exmo Sr Diretor Geral do DECEA.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Diretriz de Reestruturação das Atividades e Infraestrutura de TI no Âmbito do DECEA*: **DCA 21-1**. [Rio de Janeiro], 2009.