MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

PCA 7-18

PLANO DE DIVULGAÇÃO DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

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

TECNOLOGIA DA INFORMAÇÃO

PCA 7-18

PLANO DE DIVULGAÇÃO DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

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

PORTARIA DECEA Nº 66/DGCEA, DE 25 DE MAIO DE 2012.

Aprova a edição do Plano de Divulgação de 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 1049/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 7-18 "Plano de Divulgação de Segurança da Informação do Departamento de Controle do Espaço Aéreo", que com esta baixa.

Art. 2º Este Plano entra em vigor na data de sua publicação.

(a) Ten Brig Ar MARCO AURÉLIO GONÇALVES MENDES
Diretor-Geral do DECEA

(Publicado no BCA nº 115, de 18 de junho de 2012.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Este documento tem por finalidade apresentar o Plano de Divulgação de Segurança da Informação do Departamento de Controle do Espaço Aéreo.

1.2 OBJETIVO

O Plano de Divulgação de Segurança da Informação é um documento que estabelece, em conformidade com os objetivos estratégicos do PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, ações de segurança da informação, visando divulgar o assunto no âmbito do DECEA e em suas Organizações Militares subordinadas.

1.3 JUSTIFICATIVA

1.3.1 No ano de 2010, foi aprovado o PCA 7-11 Plano Diretor de Segurança da Informação no DECEA, que orienta como a segurança da informação deve contribuir para os objetivos estratégicos do DECEA. Nesse plano estão descritas as ações de segurança da informação que serão executadas para atingir esses objetivos. A ação de nº 26 descreve: Estabelecer programa de conscientização e aculturamento sobre segurança da informação, onde servidores militares e civis do DECEA e demais prestadores de serviço contratados recebam, quando pertinente, treinamento apropriado e regular de acordo com a Política da Aeronáutica para o Controle do Espaço Aéreo e com a Política do DECEA para Segurança da Informação. Esta ação deverá ser concluída em curto prazo, mediante coordenação da ASSICEA – Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo – e apoio do Subdepartamento Técnico e da Assessoria de Comunicação Social do DECEA.

1.3.2 A incorporação de diversas ações estratégicas de comunicação para divulgação da segurança da informação é essencial. A criação de cartazes, logomarca e toda uma campanha publicitária de propaganda e comunicação interna acompanham o Plano de Divulgação de Segurança da Informação, com o intuito de transmitir a ideia e conseguir o apoio e a participação de todo o efetivo do DECEA e de suas Organizações Militares subordinadas.

1.3.3 Com o apoio e o comprometimento das pessoas que estão em contato direto com as informações ficará bem mais fácil desenvolver o processo de segurança da informação e aprimorá-lo por meio da adoção de controles de segurança mais rígidos.

1.3.4 É responsabilidade da Direção do DECEA assegurar que todos os usuários dos sistemas de informação saibam como proteger os ativos da Organização e estejam de acordo com os documentos normativos de segurança da informação. Contudo, a responsabilidade pela preservação da Segurança da Informação é de toda a Organização.

1.3.5 Nesse contexto, a elaboração de um Plano de Divulgação de Segurança da Informação se faz necessária para direcionar quais são as campanhas de divulgação e que ferramentas serão utilizadas para educar e conscientizar as pessoas sobre o tema segurança da informação.

1.3.6 Um dos objetivos do Plano de Divulgação de Segurança da Informação é prover meios para que as pessoas adquiram mais conhecimento em segurança da informação, tornando, assim, os níveis desses riscos aceitáveis.

1.4 METODOLOGIA

O processo de preparação do Plano de Divulgação de Segurança da Informação do Departamento de Controle do Espaço Aéreo englobou as seguintes etapas:

1.4.1 ANÁLISE DE RISCOS

1.4.2 A segurança da informação está presente nas cinco categorias de ativos de informação alocados no DECEA e em suas Organizações Militares subordinadas. São elas:

a) informação conceitual: mensagens, textos, dados de um sistema, informações de pessoas etc.

b) a tecnologia que suporta a informação: correio eletrônico, editor de texto, sistemas de informação, computador etc.

c) pessoas: todos os servidores militares e civis, prestadores de serviço, fornecedores etc.

d) processos: sequência de tarefas (ou atividades) que ao serem executadas transformam insumos em um resultado com valor agregado, está focada nos processos de segurança da informação. Por exemplo: processo de gerenciamento de acesso, gerenciamento de incidentes, processo de cópias de segurança da informação etc.

e) ambiente: ambientes que armazenam informações a serem protegidas, como, por exemplo, sala técnica, datacenter, escritório etc.

1.4.3 Neste contexto, foi realizado no ano de 2009, nas principais Unidades Subordinadas do DECEA, o processo de análise de riscos, que consiste em identificar, estimar e tratar os riscos presentes no DECEA. Mediante esse processo foram identificados e estimados os riscos presentes no ativo de informação na categoria Pessoas.

1.4.4 Para termos uma análise quantitativa dos riscos do tipo de ativo de informação, Pessoas no âmbito do DECEA e suas Unidades subordinadas, foi realizada a análise sempre com três tipos de pessoas: um gestor da Organização Militar, um técnico de Tecnologia da Informação e um usuário final. Assim, podemos ter uma visão de pessoas que desempenham atividades em diferentes funções dentro da Organização Militar.

1.4.5 Segue abaixo a tabela com o número total de riscos identificados no ativo de informação Pessoas:

Tabela 1 – Número Total de Riscos Identificados no Ativo de Informação Pessoas

OM	GESTOR	TÉCNICO TI	USUÁRIO
CINDACTA I	5	3	7
CINDACTA II	2	4	7
CINTACTA III	5	5	9
CINDACTA IV	3	4	8
ICEA	3	5	7
SRPV-SP	3	5	7
1ºGCC	5	5	9
CGNA	3	5	7
CISCEA	3	3	8
DECEA-SRL	3	4	8
DTCEA-BE	2	5	9
DTCEA-CT	3	4	7
DTCEA-GL	3	5	7
DTCEA-SV	4	4	9
DTCEATM-RJ	3	5	8
GEIV	2	5	7
ICA	5	3	9
PAME	2	5	7
DTCEA-EG	3	4	8
Total	62	83	148

NOTA: Total geral de **293** riscos identificados nos ativos de informação Pessoas.

1.4.6 ELABORAÇÃO DO PLANO DE DIVULGAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Com base na consolidação de resultados da análise de riscos, foi elaborado o presente Plano de Divulgação de Segurança da Informação, que visa definir o nível desejado de aprendizado e conhecimento sobre o tema da segurança da informação que todas as pessoas devem ter, além de determinar as ações de divulgação de segurança da informação.

1.5 CONCEITUAÇÃO

Os conceitos dos termos e expressões utilizados neste Plano constam do Glossário da Aeronáutica (MCA 10-4, de 30 de janeiro de 2001) e do Manual de Abreviaturas, Siglas e Símbolos da Aeronáutica (MCA 10-3, de 22 de abril de 2003) e no Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo (MCA 7-1, de 30 de março de 2012).

1.6 FUNDAMENTOS LEGAIS

a) DCA 14-8 Política de Segurança da Informação do Comando da Aeronáutica, de 2006;

b) DCA 7-2 Política de Segurança da Informação do Departamento de Controle do Espaço Aéreo, de 2010;

c) PCA 7-11 Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo, de 2010;

d) PCA 7-14 Plano Diretor de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo, de 2010;

e) Instrução Normativa GSI/PR nº 1, de 2008;

f) ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, de 2006; e

g) ABNT NBR ISO/IEC 27004 Gestão da Segurança da Informação – Medição.

1.7 ÂMBITO E GRAU DE SIGILO

Este documento aplica-se ao DECEA e às suas Organizações Militares subordinadas, sendo classificado como OSTENSIVO.

2 CONSCIENTIZAÇÃO E EDUCAÇÃO EM SEGURANÇA DA INFORMAÇÃO

2.1 IDENTIFICAÇÃO DAS NECESSIDADES DE CONSCIENTIZAÇÃO E EDUCAÇÃO EM SEGURANÇA DA INFORMAÇÃO

2.1.1 Neste item estão descritos os riscos identificados no processo de análise de riscos e as recomendações para sua mitigação. É importante ressaltar que as necessidades de educação e conscientização serão extraídas das recomendações de tratamento dos riscos.

2.1.2 Seguem abaixo os riscos identificados para Gestor:

Tabela 2 – Riscos Identificados em Gestor

Riscos	Recomendações
Roubo de Informações devido aos fiscais de contrato não receberem treinamentos suficientes sobre fiscalização de contratos.	Convém que sejam realizados treinamentos periódicos para a comissão de fiscalização dos contratos de Segurança e Tecnologia da Informação existente no DECEA segundo os procedimentos descritos na Instrução Normativa nº 04, que trata sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
Roubo de informações devido à existência de falhas no processo de classificação das informações.	Convém que todas as informações sejam classificadas de acordo com o RCA 205-1 Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica.
Erro ou uso indevido devido à falta de fiscalização do cumprimento dos procedimentos descritos nas Normas Padrão de Ação (NPA).	Convém que seja criado um processo periódico para fiscalização dos procedimentos descritos nas Normas Padrão de Ação (NPA).
Roubo de informações devido à acumulação de funções.	Convém que seja designado mais de um indivíduo para efetuar atividades críticas.
Erros devido aos fiscais de contrato não receberem treinamento suficiente sobre fiscalização de contratos.	Convém que sejam realizados treinamentos periódicos para a comissão de fiscalização dos contratos de Segurança e Tecnologia da Informação existente no DECEA segundo os procedimentos descritos na Instrução Normativa nº 04, que trata sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

2.1.3 Seguem abaixo os riscos identificados para Técnico de Tecnologia da Informação:

Tabela 3 – Riscos Identificados para Técnico de Tecnologia da Informação

Riscos	Necessidades de Educação e Conscientização
Falhas de software devido à não execução de um procedimento periódico para verificação de novas vulnerabilidades publicadas.	Convém que os técnicos de Tecnologia da Informação sejam orientados a assinar fóruns de segurança da informação de listas de vulnerabilidades que são publicadas pelos fabricantes de softwares na internet.
Furto ou roubo devido ao armazenamento inseguro das mídias de armazenamento de dados (cópias de segurança).	Convém orientar os técnicos a armazenar as mídias em locais seguros, como, por exemplo, um cofre ou sala cofre.
Indisponibilidade de serviços ou informações devido à proteção inadequada das documentações de instalação e configurações dos equipamentos e sistemas tecnológicos.	Convém orientar os responsáveis pela administração de recursos de Tecnologia da Informação para guardarem documentos importantes em gavetas, armários ou cofres, mantendo-os trancados após sua utilização.
Indisponibilidade de serviços ou informações devido ao não conhecimento para responder aos incidentes de segurança da informação.	Convém que os técnicos responsáveis pelos recursos de Tecnologia da Informação sejam orientados sobre os procedimentos de resposta a incidentes de segurança.
Indisponibilidade de serviços ou informações devido ao transporte inadequado das mídias de armazenamento de dados (cópia de segurança).	Convém que os técnicos de Tecnologia da Informação sejam orientados quanto aos riscos associados ao transporte das mídias de armazenamento de dados (cópia de segurança).

2.1.4 Seguem abaixo os riscos identificados para Usuário Final:

Tabela 4 – Riscos Identificados para Usuário Final

Riscos	Necessidades de Educação e Conscientização
Ação de código malicioso devido à não verificação da atualização do programa de antivírus na estação de trabalho.	Convém que os usuários sejam orientados a verificar se o programa de antivírus está sendo atualizado.
Acesso lógico não autorizado mediante o fornecimento de informações pelo usuário final a pessoas não autorizadas.	Convém que os usuários sejam orientados quanto ao fornecimento de informações, observando os seguintes aspectos: consulta aos responsáveis pela informação antes de repassá-la a terceiros, encaminhamento da solicitação de informações sensíveis ao responsável ou registro da sua permissão e preservação das informações produzidas dentro da organização sob sua propriedade.
Repúdio devido à não utilização de aviso legal no envio de mensagens de correio eletrônico.	Convém que seja utilizado um aviso legal padrão que informe aos destinatários da mensagem que o conteúdo da mesma é restrito, proibindo a divulgação ou cópias não

	autorizadas pela organização, além de alertar possíveis punições no caso do uso impróprio. Convém que uma assinatura padrão com o aviso legal seja estabelecida pela organização militar e que o usuário a utilize sem alterações não autorizadas.
Acesso lógico não autorizado devido à escolha de senhas fracas	Convém orientar os usuários a escolher senhas fortes.
Acesso lógico não autorizado devido à falta de cuidados ao digitar informações sigilosas nas estações de trabalho próximo a pessoas desconhecidas	Convém que os usuários sejam orientados a não digitar informações sigilosas quando existirem pessoas desconhecidas ao redor.
Roubo de informações devido a documentos deixados na mesa.	Convém que os usuários sejam orientados a não deixar informações sigilosas expostas nas mesas.
Acesso físico não autorizado devido ao não acompanhamento de visitantes na organização.	Convém acompanhar visitantes na organização quando estiverem em circulação nas áreas internas. Deve ser dada atenção especial às áreas sensíveis ou equipadas com ativos críticos, onde a vigilância deve ser mais rígida.
Uso não autorizado de informações e ativos de Tecnologia da Informação devido ao computador do usuário ficar em local desprotegido.	Convém evitar posicionar sua estação de trabalho, especialmente os computadores móveis, adjacentes a janelas do prédio ou de divisórias, ou em áreas de circulação, de forma a atrair a atenção de usuários curiosos ou mal-intencionados.
Queda de performance devido à utilização inadequada do serviço de mensagens de correio eletrônico.	Convém que os usuários sejam orientados quanto ao uso dos recursos de Tecnologia da Informação.

3 TEMAS DE DIVULGAÇÃO

3.1 De acordo com o demonstrativo de riscos do item 2.1, se faz-se necessária uma campanha de educação e conscientização em segurança da informação abordando os seguintes aspectos:

a) divulgação da DCA 7-2 Política de Segurança da Informação do Controle do Espaço Aéreo;

b) classificação das informações em conformidade com o RCA 205-1 Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica;

c) divulgação e treinamento sobre a Instrução Normativa nº 04;

d) treinamento em elaboração de documentos normativos de segurança da informação;

e) informações sobre o controle de segregação de funções;

f) divulgação de como elaborar uma senha forte;

g) aspecto de vazamento de informações;

h) política de cópias de segurança da informação;

i) conhecimento sobre incidentes de segurança da informação;

j) política de mesa e tela limpa;

k) conhecimento sobre códigos maliciosos;

l) utilização de internet e correio eletrônico;

m) visitantes e fornecedores que trabalham nas instalações das Organizações Militares; e

n) utilização dos recursos de ativos de informação.

4 IMPLANTAÇÃO DO PLANO DE DIVULGAÇÃO DE SEGURANÇA DA INFORMAÇÃO

4.1 PLANO DE AÇÃO

4.1.1 Este Plano de Divulgação está fundamentado nas melhores práticas de segurança da informação e nas legislações aplicáveis ao DECEA.

4.1.2 O Plano tem por finalidade aglutinar projetos estratégicos ou atividades que contribuam para o alcance dos objetivos estabelecidos para a segurança da informação, bem como apresentar indicadores para acompanhar a implantação das ações de divulgação de segurança da informação no âmbito do DECEA e das suas Organizações Militares subordinadas.

4.1.3 As ações propostas poderão sofrer alterações em decorrência de evoluções tecnológicas, de mudanças no ambiente do DECEA e de novas necessidades, tanto de manutenção quanto de desenvolvimento do SISCEAB.

4.1.4 As ações enumeradas em seguida estão em conformidade com o PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, publicado em 2010, no que se refere ao seu Nono Objetivo, cuja íntegra segue abaixo.

a) Ações para "NONO OBJETIVO"

Objetivo:	Capacitar e Conscientizar o Capital Humano
Indicadores:	• Quantidade de Campanhas de Conscientização Realizadas • Quantidade de Oficiais e Graduados Capacitados em Segurança da Informação
Ações:	Estabelecer programa de conscientização e aculturamento sobre segurança da informação, onde servidores militares e civis do DECEA e demais prestadores de serviço contratados recebam, quando pertinente, treinamento apropriado e regular de acordo com a Política da Aeronáutica para o Controle do Espaço Aéreo e com a Política do DECEA para Segurança da Informação. Esta ação deverá ser concluída em curto prazo, mediante coordenação da Assessoria de Segurança de Sistemas de Informação e apoio do Subdepartamento Técnico. Justificar ao COMAER a necessidade de capacitar Oficiais e funcionários civis de nível superior a conhecer os conceitos básicos de segurança da informação e de gestão de segurança da informação e propor conteúdo didático para tais cursos de capacitação. Esta ação deverá ser concluída em longo prazo, mediante coordenação da Assessoria de Segurança de Sistemas de Informação e apoio dos Subdepartamentos Técnico e Administrativo. Justificar ao COMAER a necessidade de capacitar Oficiais, Civis e Graduados, a conhecer os conceitos básicos de segurança da informação e de técnicas avançadas de defesa contra ataques cibernéticos e propor conteúdo didático para tais cursos de capacitação. Esta ação deverá ser concluída em longo prazo, mediante coordenação da Assessoria de Segurança de Sistemas de Informação e apoio dos Subdepartamentos Técnico e Administrativo.

4.2 DETALHAMENTO DAS AÇÕES

Nos próximos itens serão apresentadas as ações de divulgação de segurança da informação propostas para a execução do Plano de Divulgação de Segurança da Informação. Para cada ação descrita deverá ser aberto um projeto pela ASSICEA, sendo gerenciado de acordo com as boas práticas de gestão de projetos.

4.2.1 PESQUISA INICIAL

4.2.1.1 Deverá ser realizada uma pesquisa com todo o efetivo do DECEA e de suas Organizações Militares subordinadas sobre o tema "Segurança da Informação", objetivando avaliar o nível de conhecimento sobre o assunto, além de disseminar seus principais conceitos.

4.2.1.2 A pesquisa será a primeira abordagem de conscientização para implementação da cultura de segurança da informação no DECEA.

4.2.1.3 A metodologia utilizada deverá ser a aplicação de questionário eletrônico, disponibilizado na página da intraer. A primeira pesquisa abordará perguntas simples sobre o tema, contendo aproximadamente 20 perguntas e quatro opções de respostas. O sistema da pesquisa deverá disponibilizar um comentário com a resposta correta, caso o usuário marque alguma resposta incorreta.

4.2.1.4 Essa será a primeira integração do efetivo com o assunto, servindo para a obtenção de dados estatísticos a respeito do nível de cultura dos usuários finais.

4.2.1.5 Os Presidentes, Chefes, Comandantes ou Diretores de cada Organização Militar deverão auxiliar neste processo, por meio do apoio da Assessoria de Comunicação Social da Unidade.

4.2.1.6 Seguem os principais temas da pesquisa "Segurança da Informação":

Temas
Prática da Segurança da Informação
Classificação da Informação
Mesa e Tela Limpa
Protetor de Tela
Descarte de Informações Sensíveis
Compartilhamento da Senha de Acesso
Senhas
Utilização de Antivírus
Reporte de Incidentes de Segurança
Política de Segurança da Informação do DECEA
Armazenamento de Informações
Controle de Acesso
Engenharia Social
Informações Sigilosas
Segurança Física
Continuidade das Operações
Segurança em Recursos Humanos
Utilização dos Recursos de Tecnologia da Informação
Utilização de Softwares não Homologados
Utilização do Correio Eletrônico

4.2.1.7 Em um segundo momento, a avaliação poderá ser disponibilizada alternativamente na página intraer do DECEA.

4.2.2 PÁGINA ELETRÔNICA DA ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO – ASSICEA

4.2.2.1 A página eletrônica da ASSICEA será desenvolvida em consonância com o padrão estabelecido pela Assessoria de Comunicação Social (ASCOM) para os sites dos setores internos do DECEA, alocados no Portal do DECEA na Rede Intraer.

4.2.2.2 A página eletrônica da ASSICEA terá como propósito estabelecer-se como uma plataforma de informação no meio digital para as questões relativas à segurança da informação do DECEA, bem como a interface digital de contato entre o efetivo do DECEA e a ASSICEA.

4.2.3 SIMPÓSIO INTERNO SOBRE SEGURANÇA DA INFORMAÇÃO

4.2.3.1 A Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo, por intermédio do SDTE – Subdepartamento Técnico do DECEA – e com o apoio da ASCOM – Assessoria de Comunicação Social – fará a coordenação do primeiro Simpósio Interno de Segurança da Informação, a ser realizado em duas partes, no Auditório do DECEA, localizado no quinto andar do prédio do DECEA.

4.2.3.2 Este evento tem como objetivo divulgar as ações de segurança da informação no âmbito do DECEA e em suas unidades subordinadas, bem como educar e conscientizar sobre a importância da segurança da informação na rotina pessoal e de trabalho, a fim de promover comportamento favorável à implantação de políticas de segurança da informação.

4.2.3.3 O Simpósio Interno de Segurança da Informação é direcionado, preferencialmente, para todo o efetivo militar e civil, prestadores de serviço e fornecedores que de alguma forma manipulam informações do DECEA. O calendário deve levar em consideração as atividades e prioridades de cada departamento, além de ser programado de modo a facilitar e adequar horário e participação de todos os militares e civis do DECEA. (OBS: Pode ser fixada uma agenda variável para participação do efetivo no simpósio).

4.2.3.4 A programação do Simpósio Interno de Segurança da Informação está dividida em duas partes, a primeira será realizada de modo obrigatório para todo o efetivo do DECEA no período da manhã, das 9h às 12h. O efetivo será dividido em até 70 pessoas por dia, que é a capacidade do auditório.

4.2.3.5 A sugestão proposta é a seguinte:

a) primeiro dia: efetivo do Subdepartamento de Administração;

b) segundo dia: efetivo do Subdepartamento Técnico;

c) terceiro dia: efetivo do Subdepartamento de Operações;

d) quarto dia: efetivo do Gabinete; e

e) quinto dia: efetivo da VICEA e demais assessorias do Diretor-Geral.

4.2.3.6 Segue abaixo a sugestão de programação do evento:

TODOS OS DIAS	
AUDITÓRIO	
ATIVIDADES	**PALESTRANTE**
Primeira palestra – Fundamentos de Segurança da Informação	**SDTE**
Segunda palestra – Segurança da Informação no DECEA	**Empresa GA Security and Audit**
Peça de Teatro sobre o tema Segurança da Informação	
Intervalo – Coffe-break	
Terceira palestra – PCA 7-11 Plano Diretor de Segurança da Informação	**SDTE**
DCA 7-2 Política de Segurança da Informação do DECEA	**Empresa GA Security and Audit**

4.2.3.7 Segue abaixo a descrição das palestras:

Palestra	Descrição
1ª - Fundamentos de Segurança da Informação	A fim de nivelar o conhecimento de todo o efetivo em segurança da informação, essa palestra apresenta os principais conceitos sobre o tema.
2ª - Segurança da Informação no DECEA	Apresentar o modelo organizacional da segurança da informação no DECEA e em suas Unidades subordinadas (Assessoria de Segurança de Sistemas da Informação do Controle do Espaço Aéreo e a Seção de Segurança de Sistemas da Informação).
3ª - PCA 7-11 Plano Diretor de Segurança da Informação	Descreve qual é o plano do DECEA para a segurança da informação nos próximos anos, informando como a segurança da informação irá contribuir com os objetivos estratégicos do DECEA.
4ª - DCA 7-2 Política de Segurança da Informação do DECEA	Apresenta as responsabilidades, princípios e diretrizes que todos devem seguir ao manusear as informações pertencentes ao DECEA.

4.2.3.8 Após a divulgação para todo o efetivo dos princípios básicos de segurança da informação e dos documentos normativos em vigor no DECEA e em suas Unidades subordinadas, deverá ser realizada a segunda parte do Simpósio Interno de Segurança da Informação.

4.2.3.9 A segunda parte tem como objetivo divulgar outros aspectos mais técnicos sobre o tema segurança da informação e terá como público-alvo as seções de tecnologia da informação e as seções de segurança de sistemas da informação das Unidades subordinadas ao DECEA.

4.2.3.10 Segue abaixo a proposta de programação para o evento organizado em dois dias.

PRIMEIRO DIA	
AUDITÓRIO	
ATIVIDADES	PALESTRANTE
Abertura do Auditório	
Abertura inicial – A importância do Simpósio Interno de Segurança da Informação	Chefe do SDTE
Primeira palestra – Peça de Teatro sobre o tema segurança da Informação	Empresa Contratada
Segunda palestra – Estrutura organizacional e relacionamentos da ASSICEA	SDTE
Intervalo – Coffe-break	
Terceira palestra – Área de atuação das Seções de Segurança de Sistemas da Informação nas Unidades Subordinadas ao DECEA	Empresa GA Security and Audit
Horário de Almoço	
Quarta palestra – Classificação das informações em conformidade com o RCA 205-1 Regulamento para salvaguarda de assuntos sigilosos da Aeronáutica	Seção de Inteligência
Quinta palestra – Gestão de Riscos em Tecnologia e Segurança da Informação	Empresa GA Security and Audit
Término das atividades	

SEGUNDO DIA	
AUDITÓRIO	
ATIVIDADES	PALESTRANTE
Abertura do Auditório	
Primeira palestra – Fundamentos básicos em Gestão de Continuidade de Negócios	Empresa GA Security and Audit
Segunda palestra – Como elaborar uma senha forte	Empresa GA Security And Audit
Intervalo – Coffe-break	
Terceira palestra – SGSI - Sistema de Gestão de Segurança da Informação no âmbito do DECEA e suas unidades subordinadas	Empresa GA Security and Audit
Horário de Almoço	
Quarta palestra – Monitoramento de Rede e Gestão de Incidentes de Segurança da Informação	Empresa GA Security and Audit
Quinta palestra – Resultados sobre o Simpósio Interno de Segurança da Informação	Diretor-Geral do DECEA
Confraternização – Coquetel de Encerramento	

4.2.3.11 Segue abaixo a descrição de cada palestra que será apresentada no evento.

Palestra	Descrição
1ª - A importância do Simpósio Interno de Segurança da Informação	Descreve a importância do Simpósio Interno de Segurança da Informação e apresenta um resumo sobre todas as palestras do evento.
2ª - Estrutura organizacional e relacionamentos da ASSICEA	Apresenta a estrutura organizacional e os relacionamentos da Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo para gerir a Segurança da Informação do Departamento de Controle do Espaço Aéreo.
3ª - Área de atuação das Seções de Segurança de Sistemas da Informação nas Unidades subordinadas ao DECEA	Apresenta a missão e a área de atuação das Seções de Segurança de Sistemas da Informação nas Unidades subordinadas ao DECEA.
4ª - RCA 205-1 – Classificação da informação	Em conformidade com o RCA 205-1, essa palestra apresenta os cuidados que o efetivo deve ter para classificar as informações sobre seu domínio.
5ª - Gestão de Riscos em Tecnologia e Segurança da Informação	Apresenta a metodologia de gestão de riscos em segurança da informação, com exemplos práticos por meio do software PrismaTechonologies.
6ª - Fundamentos básicos em Gestão de Continuidade de Negócios	Apresenta os fundamentos básicos em gestão de continuidade de negócios.
7ª - Como elaborar uma senha forte	Dicas de como elaborar uma senha forte para proteger as informações que estão armazenadas em sistemas de informação ou em redes de computadores.
8ª - Sistema de Gestão de Segurança da Informação	Apresenta como a segurança da informação será gerenciada no DECEA.
9ª - Monitoramento de Rede e Gestão de Incidentes de Segurança da Informação	Apresenta a gestão de incidentes de segurança da informação em redes de telecomunicações que está sendo realizada no DECEA.
10ª - Resultados do Simpósio Interno de Segurança da Informação	Apresenta os principais resultados do Simpósio Interno de Segurança da Informação.

4.2.3.12 Em todas as palestras, com exceção da 1ª e 10ª, deverá ser entregue aos convidados um formulário contendo o questionário de avaliação da palestra, com o objetivo de medir o resultado do assunto a ser apresentado e com o propósito de melhoria contínua do evento para o próximo ano.

4.2.3.13 Esse questionário deve ser elaborado pela Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo.

4.2.3.14 Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: da ASSICEA – coordenar o simpósio interno de segurança da informação; e da ASCOM – realizar a divulgação do simpósio interno de segurança da informação.

4.2.4 DIA "D" DE SEGURANÇA DA INFORMAÇÃO

4.2.4.1 Deverá ser agendado com o Comandante, Chefe ou Diretor de cada Organização Militar subordinada ao DECEA um dia de eventos de segurança da informação, contento

palestras, mesa-redonda, fórum e jogos, para incentivar todo o efetivo da Organização Militar às boas práticas de segurança da informação.

4.2.4.2 As palestras do Simpósio Interno de Segurança da Informação poderão ser aproveitadas para o Dia "D" de segurança da informação.

4.2.4.3 Os temas de divulgação estão descritos no capítulo 3 deste Plano de Divulgação de Segurança da Informação.

4.2.4.4 Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: do Comandante, Chefe ou Diretor da Organização Militar – prover a infraestrutura necessária para a realização do dia "D" de segurança da informação; da ASSICEA – coordenar o dia "D" de segurança da informação em conjunto com a SSSI; da ASCOM – realizar a divulgação do dia "D" de segurança da informação.

4.2.5 TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

4.2.5.1 Deverá ser elaborado durante o período vigente deste Plano de Divulgação de Segurança da Informação um ciclo de palestras e cursos sobre o tema segurança da informação.

4.2.5.2 As palestras deverão ter uma ficha de presença dos participantes, e após a realização da palestra, o instrutor deverá encaminhar essa ficha para a ASSICEA arquivar e atualizar um banco de dados dos participantes.

4.2.5.3 Os cursos deverão ser ministrados por instrutores capacitados e após o seu término deverá ser emitido certificado de participação descrevendo o nome do curso, o objetivo do curso, o número de horas de aprendizado e a assinatura do instrutor responsável. Após a realização do curso o instrutor deverá encaminhar a lista de pessoas treinadas para a ASSICEA arquivar e atualizar um banco de dados dos participantes.

4.2.5.4 Os temas deverão ser escolhidos de acordo com o item 4.2.2 deste PCA, ou seja, de acordo com o resultado das pesquisas deverão ser elaborados os conteúdos para mitigar os óbices identificados sobre o conhecimento de segurança da informação do efetivo do DECEA e de suas Organizações Militares subordinadas.

4.2.5.5 Deve-se criar um processo de ambientação nas políticas de segurança da informação para os novos servidores militares e civis durante a sua contratação.

4.2.5.6 De acordo com a última análise de risco realizada no âmbito do DECEA e em suas Organizações Militares subordinadas, é recomendado executar, nestes primeiros 12 meses de vigência do PCA, os seguintes cursos descritos na tabela abaixo:

Curso	**Objetivo**
Fundamentos Básicos em Segurança da Informação	Nivelar o conhecimento dos participantes nos conceitos de segurança da informação presentes na ABNT NBR ISO/IEC 27002:2005.
Gestão de Riscos em segurança da informação	Explicar a metodologia de gestão de riscos presente na ABNT NBR ISO/IEC 27005:2008.
Auditoria em Segurança da Informação	Prover aos participantes a metodologia de auditoria do sistema de gestão de segurança da informação presente na ABNT NBR ISO/IEC 27001:2006.
Gestão de Documentos	Prover o entendimento sobre os documentos normativos

Normativos de Segurança da Informação	de segurança da informação: política, normas, procedimentos e instrução.
Gerenciamento de Mudanças	Prover conhecimento aos participantes para gerenciar, controlar e testar as mudanças programadas na Infraestrutura de TI, analisando o impacto dessas mudanças.
Gestão de Incidentes de Segurança da Informação	Prover conhecimento sobre a correta gestão de incidentes de segurança da informação.

4.2.5.7 É importante ressaltar que o público-alvo de cada palestra ou curso deverá ser correspondente ao desempenho da função exercida pelo servidor militar ou civil.

Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: da ASSICEA – realizar as palestras e cursos; da ASCOM – divulgar, para o público-alvo escolhido, as palestras e cursos.

4.2.6 ELABORAÇÃO DE UMA CARTILHA DE SEGURANÇA DA INFORMAÇÃO

Deverá ser elaborada uma cartilha com as boas práticas de segurança da informação. Essa cartilha deverá ser distribuída para todo o efetivo militar e civil, prestadores de serviços e fornecedores que manipulam informações do DECEA e em suas Organizações Militares subordinadas.

4.2.7 PROTEÇÃO DE TELA PARA OS DESKTOPS SOBRE O TEMA SEGURANÇA DA INFORMAÇÃO

4.2.7.1 Deverá ser elaborada proteção de tela com as boas práticas de segurança da informação para ser instalada na estação de trabalho de todo o efetivo do DECEA e em suas Organizações Militares subordinadas.

4.2.7.2 Recomenda-se implementar, em conjunto, o controle de segurança da informação chamado de tela limpa. Esse controle determina que se a máquina ficar mais de 5 minutos sem interação com o usuário, deve-se bloquear automaticamente a estação de trabalho e começar a passar as imagens de proteção de tela com o tema sobre segurança da informação.
O principal objetivo da proteção de tela é proporcionar um recurso de proteção para as estações de trabalho na ausência dos usuários, implementando o controle de tela limpa nas máquinas dos usuários. Esta ferramenta representa também importante auxílio na fixação de conceitos sobre o tema segurança da informação.

4.2.7.3 Seguem abaixo os requisitos para a confecção da proteção de tela:

a) a utilização da proteção de tela de segurança da informação deverá ser recomendada para todas as estações de trabalho pertencentes ao DECEA e de suas Organizações Militares subordinadas;

b) a elaboração da proteção de tela de segurança da informação deverá ser feita pela ASCOM com o auxílio da ASSICEA; e

c) a proteção de tela de segurança da informação deverá ser instalada na rede pelo suporte local de tecnologia da informação da Organização Militar.

4.2.7.4 O conteúdo da proteção de tela de segurança da informação deverá conter as boas práticas de segurança da informação especificadas pela ASSICEA, além dos temas que estão descritos no capítulo 3 deste Plano de Divulgação de Segurança da Informação.

4.2.7.5 Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: da ASSICEA – prover o conteúdo para elaboração da proteção de tela; da ASCOM – elaborar a proteção de tela de segurança da informação; da STI – Seção de Tecnologia da Informação de cada organização Militar subordinada ao DECEA a instalação da proteção de tela de segurança da informação nas máquinas de todo o efetivo da Organização Militar.

4.2.8 PAPEL DE PAREDE DE SEGURANÇA DA INFORMAÇÃO

4.2.8.1 Assim como a proteção de tela de segurança da informação, esta ferramenta tem como objetivo principal fixar os conceitos de segurança da informação.

4.2.8.2 Seguem abaixo os requisitos para a confecção do papel de parede:

a) o papel de parede de segurança da informação deve mostrar perguntas referentes aos conceitos já divulgados neste Plano de Divulgação de Segurança da Informação;

b) o uso do papel de parede de segurança da informação deverá ser facultativo;

c) a elaboração do papel de parede de segurança da informação deverá ser feita pela ASCOM, com o auxílio da ASSICEA;

d) deverá ser disponibilizado na página eletrônica da ASSICEA um link que permita aos usuários realizar um download do papel de parede;

e) sempre que possível, devem ser produzidas novas versões do papel de parede;

f) poderão ser disponibilizadas simultaneamente versões distintas do papel de parede. Desta forma, o usuário poderá escolher aquela que mais o agradar e trocá-la com maior frequência; e

g) periodicamente devem ser disponibilizadas novas versões do papel de parede, de modo a evitar que os usuários percam o interesse.

4.2.8.3 O conteúdo do papel de parede de segurança da informação deverá conter as boas práticas de segurança da informação especificadas pela ASSICEA, além dos temas que estão descritos no capítulo 3 deste Plano de Divulgação de Segurança da Informação.

4.2.8.4 Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: da ASSICEA – prover o conteúdo para elaboração do papel de parede de segurança da informação; da ASCOM – elaborar o papel de parede de segurança da informação; da STI – Seção de Tecnologia da Informação de cada Organização Militar subordinada ao DECEA – a instalação do papel de parede de segurança da informação nas máquinas de todo o efetivo da Organização Militar.

4.2.9 ENVIO DE E-MAIL MARKETING SOBRE AS PRINCIPAIS NOTÍCIAS DE SEGURANÇA DA INFORMAÇÃO

4.2.9.1 Deverá ser encaminhado e-mail informativo a todo o efetivo do DECEA e em suas Organização Militares subordinadas sobre o tema segurança da informação e quando houver alguma atualização no site da ASSICEA.

4.2.9.2 Esta é uma forma de divulgação eficiente e ampla, pois a mensagem será enviada a todo o efetivo, mantendo o usuário pensando em Segurança da Informação, ainda que

indiretamente. Esta ferramenta apresenta a vantagem da utilização frequente do e-mail, transmitindo a informação por meio de mensagens curtas e diretas. Além disso, também poderá ser utilizada para mensagens que deverão ser enviadas a públicos específicos.
Especificação desta ação de divulgação de segurança da informação:

a) será responsabilidade da ASSICEA gerenciar as mensagens do e-mail *marketing* de divulgação de segurança da informação; e

b) o e-mail *marketing* de divulgação de segurança da informação deverá ser utilizado para divulgar a DCA 7-2 Política de Segurança da Informação do DECEA e as Normas de Segurança da Informação inicialmente.

4.2.9.3 Segue na tabela abaixo uma proposta de conteúdo para o envio de e-mail marketing:

Assunto	Mensagens	Público-Alvo
Usuários	A informação é um ativo valioso para o sucesso da missão da sua Organização Militar. Contribua, proteja este ativo.	Usuário
Internet	A Internet é uma porta de entrada que pode ocasionar acesso indevido e vazamento de informações. Utilize-a de forma segura!!!	Usuário
Correio Eletrônico	Atenção às mensagens de Correio Eletrônico com assuntos importantes para o seu trabalho. Correntes, piadas, cartões... Delete esta ideia!!!	Usuário
Continuidade de Operações	Conhecer os riscos é o primeiro passo para planejar a continuidade operacional dos processos de sua área.	Chefe ou Comandante
Equipamentos de Tecnologia da Informação	Não deixe que toda a proteção oferecida por sua Organização Militar seja colocada em risco. Proteja o seu computador portátil ou estação de trabalho.	Usuário
Acesso à Informação	Otimize o seu tempo, utilize somente as informações necessárias para o desempenho de suas funções.	Usuário
Cópias de Segurança	Prevenir é muito melhor do que remediar. Armazene as informações referentes ao seu trabalho na rede.	Usuário
Segurança Física	Valorize os recursos da sua Organização Militar, ajude a protegê-los.	Usuário
Senha	Quantas pessoas possuem a chave da sua casa? E quantas têm a sua senha de acesso? Proteja-se.	Usuário
Reporte de Incidentes	Risco, falhas e incidentes de segurança da informação podem ser evitados com a sua ajuda. Como? Reportando no site da ASSICEA.	Usuário
Gestor	Zelar pela segurança dos ativos de informação e conscientizar a sua área é um de seus desafios.	Chefe ou Comandante

4.2.10 CARTAZES EM LUGARES ESTRATÉGICOS SOBRE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES MILITARES

4.2.10.1 Deverão ser elaborados pela ASCOM, em conjunto com a ASSICEA, cartazes informativos sobre as boas práticas de segurança da informação.

4.2.10.2 Estes cartazes deverão ser afixados em locais estratégicos em cada Organização Militar, de modo a despertar a atenção de todo efetivo sobre o tema Segurança da Informação. Essa é uma forma de divulgação visual na qual os cartazes serão utilizados, basicamente, para conscientização.

4.2.10.3 Abaixo estão descritos os requisitos para confecção dos cartazes.

a) os cartazes deverão ser colocados no ambiente interno da Organização Militar, como, por exemplo: corredores dos elevadores, quadros de avisos e próximos às máquinas de café;

b) sempre que possível, deverão ser incluídas nos cartazes ilustrações que se relacionem ao assunto;

c) a ASSICEA e a ASCOM serão os responsáveis pela elaboração, conteúdo e especificação dos cartazes; e

d) algumas sugestões de conteúdo para os cartazes:

Assunto	Bandeiras da Segurança (Pratique Segurança da Informação)
Senha	A senha é sua chave de acesso e identificação única. Não deixe que alguém se faça passar por você.
Vírus	Não deixe que um vírus de computador acabe com o trabalho de uma semana inteira. Utilize o antivírus antes de abrir arquivo em mídias removíveis.
Correio Eletrônico	Evite que o e-mail jogue contra você. Fique atento a arquivos grandes, suspeitos, e adote boas práticas de uso.
Pirataria	Não seja surpreendido pela presença de programa de computadores irregulares. Só instale programas legais autorizados.
Informação	Compartilhe as informações de forma segura. Até mesmo o que se fala no elevador pode comprometer seu trabalho.
Tratamento da Informação	Adote as melhores práticas de segurança no manuseio, armazenamento, transporte e descarte de informações.
Reporte de Incidentes	Faça a sua parte. Reporte situações de risco, falhas de segurança e incidentes para que todos fiquem mais seguros.
Classificação da Informação	Classifique suas informações de acordo com o grau de sigilo. Assim todos saberão o que fazer com ela.
Política de Segurança da Informação	Não seja o elo fraco da corrente de segurança. Informe-se sobre a DCA 7-2 Política de Segurança da Informação do DECEA.
Internet	Seja um usuário consciente. Não exponha a segurança da Organização Militar com acessos indevidos e improdutivos.
Segurança Física	A quebra de segurança não ocorre somente através dos computadores. Guarde com segurança mídias que contenham informações sensíveis.
Protetor de tela	Não deixe seu computador desassistido, bloqueie o seu computador sempre que se ausentar.

4.2.10.4 Esta ação de divulgação de segurança da informação deverá ter como responsabilidade: da ASSICEA – prover o conteúdo para elaboração dos cartazes de segurança da informação; da ASCOM – elaborar os cartazes de segurança da informação.

4.3 PLANO DE COMUNICAÇÃO

4.3.1 O Plano de Comunicação visa garantir o processo de geração, distribuição e armazenagem de todas as informações relativas aos projetos especificados no item 4.2, de forma acurada e consistente, por meio apropriado e no momento certo, para as partes interessadas envolvidas ou afetadas pelo projeto.

4.3.2 As informações produzidas pelos projetos seguirão a matriz presente neste Plano.

4.3.3 As reuniões de acompanhamento deverão produzir uma ata de reunião, conforme o modelo disponibilizado pela ICA 10-1 CORRESPONDÊNCIA E ATOS OFICIAIS DO COMANDO DA AERONÁUTICA. A ata deverá ser revisada e assinada por todos os participantes e ser arquivada na pasta do projeto.

4.3.4 O líder do projeto deverá designar ou acumular a função de coordenador de comunicações, que ficará responsável por:

a) manter repositório em meio eletrônico dos documentos produzidos pelo projeto;

b) manter repositório dos e-mails enviados entre as partes interessadas pelo projeto; e

c) manter uma pasta ou arquivo com os documentos em papel produzidos pelo projeto, devendo disponibilizar estas informações de acordo com a sua criticidade e destinação às partes interessadas.

4.3.5 Segue abaixo a matriz de comunicação:

MATRIZ DE COMUNICAÇÃO						
AÇÃO	**OBJETIVO**	**PÚBLICO - ALVO**	**CANAL / EVENTO**	**PERIODICIDADE**	**RESPONSABILIDADE**	**MATERIAIS**
	Divulgar a aprovação do projeto	Equipe do projeto	Reunião de abertura	Uma vez	Líder do projeto	Ata da reunião, Termo de abertura de projeto e Declaração de escopo do projeto.
	Acompanhar as atividades em progressos e próximos passos	Equipe do projeto	Reunião de status de projeto	Quinzenal	Líder do projeto	Ata de reunião
	Comunicar situação do projeto	Chefe da ASSICEA e Alto Comando do DECEA	E-mail ou Documento enviado pelo SIGADAER	Mensal	Líder do projeto	Relatório de acompanha-mento do projeto

Legenda da matriz:

Ação – Número da ação correspondente no Plano de Divulgação de Segurança da Informação.

Objetivo – Contém o objetivo da ação que se deseja comunicar.

Público-Alvo – Parcela do público que deverá receber as informações.

Canal / Evento – Define qual meio de comunicação deverá ser utilizado.

Periodicidade – Número de eventos que deverá ser comunicado para a ação.

Responsabilidade – Define de quem é a responsabilidade de comunicar a ação.

Materiais – Definem quais tipos de documentos deverão ser enviados.

4.3.6 Essa matriz poderá conter outros itens, dependendo do contexto interno do projeto que deverá ser comunicado.

4.4 RESPONSABILIDADES GERAIS

4.4.1 DECEA: prover infraestrutura necessária para a execução das ações de divulgação de segurança da informação.

4.4.2 SDTE: acompanhar o processo de implantação das ações de segurança da informação e facilitar acesso às pessoas para a execução do Plano de Divulgação de Segurança da Informação.

4.4.3 ASSICEA: coordenar as ações de segurança da informação, elaborar conteúdo para a divulgação de segurança da informação, executar e administrar as ações de segurança da informação.

4.4.4 ASCOM: prover a correta divulgação das ações de divulgação de segurança da informação.

4.5 PERÍODOS DE PLANEJAMENTO

4.5.1 A implantação da segurança da informação no âmbito do DECEA será estabelecida por meio de um planejamento modular, composto por dois períodos distintos. Considerando o nível de maturidade que se deseja atingir, cada período compreenderá uma determinada fase, sendo elas:

a) primeira fase (curto prazo) – até 12 meses; e

b) segunda fase (médio prazo) – até 24 meses.

5 CONTROLE E AVALIAÇÃO DE DESEMPENHO

5.1 INDICADORES PARA MONITORAMENTO DO PLANO DE DIVULGAÇÃO DE SEGURANÇA DA INFORMAÇÃO

5.1.1 Os principais objetivos na mediação de indicadores para as ações de divulgação de segurança da informação são os seguintes:

a) avaliar a eficácia das ações e seus grupos de controle de segurança da informação implementados;

b) verificar a extensão na qual os requisitos de segurança da informação identificados foram atendidos;

c) facilitar a melhoria no desempenho da segurança da informação em termos dos riscos identificados no item 2 deste Plano de Divulgação de Segurança da Informação; e

d) fornecer entradas para a análise crítica pelo Alto-Comando do DECEA para facilitar as tomadas de decisões relacionadas à divulgação da segurança da informação e justificar as melhorias necessárias para a conscientização e educação do efetivo do DECEA e das suas Organizações Militares subordinadas.

5.1.2 Conforme a ABNT NBR ISO/IEC 27004:2010, os indicadores, que devem ser objetivamente verificáveis, representam uma forma de aferição do que se quer alcançar por meio das ações de divulgação de segurança da informação e determinam como medir a proporção de consecução de cada uma das ações ao longo de sua implantação.

5.1.3 Para cada um dos indicadores é necessário determinar as fontes de dados, bem como onde serão coletadas as informações.

5.1.4 Estes indicadores deverão ser acompanhados por meio de um sistema que permita a tomada de decisões gerenciais, em tempo hábil, voltadas para as soluções de problemas de segurança, servindo de base para a revisão de metas estabelecidas. Deverão ser utilizados para o efetivo gerenciamento da segurança da informação no DECEA e das Organizações subordinadas.

5.1.5 Todas as ações de divulgação de segurança da informação descritas neste Plano de Divulgação de Segurança da Informação antes do início da sua implementação deverão ter uma tabela de medição de indicadores conforme exemplo abaixo:

TABELA DE MEDIÇÃO DE INDICADORES	
Nome da ação de segurança da informação	Treinamento em Segurança da Informação
Identificador numérico	001 – PCA Plano de Divulgação de Segurança da Informação item 4.2.7.
Propósito do modelo de medição	Avaliar a conformidade com o requisito de treinamento de conscientização e educação de todo o efetivo do DECEA e das suas Organizações Militares subordinadas em segurança da informação.
Descrição da ação de segurança da informação	Verificar item 4.2.7 do PCA Plano de Divulgação de Segurança da Informação.
Objeto de medição	Banco de dados de todo o efetivo do DECEA e das suas Organizações Militares subordinadas em segurança da informação.
Atributo	Registro das palestras e cursos realizados.
Medição básica	Número de pessoas que receberam o treinamento de conscientização e educação em segurança da informação. Número de pessoas que precisam receber o treinamento de conscientização e educação em segurança da informação.
Método de medição	Lista de registro de treinamento de conscientização e educação em segurança da informação preenchida e assinada pelos participantes.
Cliente da medição	Alto-Comando do DECEA e Chefes, Comandantes e Diretores das Organizações Militares subordinadas ao DECEA.
Responsável pela análise crítica da medição	Alto-Comando do DECEA e Chefes, Comandantes e Diretores das Organizações Militares subordinadas ao DECEA.
Proprietário da Informação	ASSICEA
Responsável por coletar o indicador	ASSICEA e SSSI
Comunicador do indicador	ASSICEA
Frequência de coleta dos dados	Semestralmente
Frequência de comunicação dos resultados de medição	Anual
Revisão de Medição	Realizar a análise crítica anual
Período de medição	Anual

Legenda da tabela de Medição de Indicadores

Nome da ação de segurança da informação – Nome do projeto de segurança da informação em conformidade com o PCA 7-11.

Identificador numérico - Identificador numérico únicio específico da Organização Militar

Propósito do modelo de medição - Descreve as razões para introduzir a medição

Objeto de medição - Objeto que é caracterizado atrvés da medição de seus atributos. Um objeto pode incluir processos, planos, projetos, recursos, e sistemas, ou componentes de sistemas.

Atributo - Propriedade ou caracterisiticas de um objeto de medição que pode ser distinguida quantitativamente ou qualitativamente por meios manuais ou automatizados.

Medição básica - Uma medição básica é definida em termos de um atributo e o método de medição especificado para quantificá-lo por exemplo, número de pessoas treinadas, número de localidades, custo acumulado até a data. Assim que um dado é coletado, um valor é atribuído a uma medida básica.

Método de medição - Sequência lógica de operações usada na quantificação de um atributo em relação a uma escala especificada.

Cliente da medição - Direção ou parte interessada que solicita ou exige informações sobre a eficácia da ação de segurança da informação, dos controles ou grupod e controles.

Responsável pela análise crítica da medição - Pessoa ou entidade da Organização Militar que valida se os modelos de medição desenvolvidos são apropriados para avaliar a eficácia da ação de segurança da informação, de controles ou grupo de controles.

Proprietário da Informação - Pessoa ou entidade da Organização Militar que possui a informação de um objeto de medição e atributos e é responsável pela medição.

Responsável por coletar o indicador - Pessoa ou entidade da Organização Militar responsável pela coleta, registro e armazenamento dos dados.

Comunicador do indicador - Pessoa ou entidade da Organização Militar responsável pela análise dos dados e comunicação dos esultados da mediação.

Frequência de coleta dos dados - Com que frequencia os dados são coletados.

Frequência de análise de dados - Com que frequencia os dados são analisados.

Frequência de relatos dos resultados de medição - Data de revisão da medição (expiração ou renovação da validade da medição).

Período de medição - Define o período sendo medido.

6 DISPOSIÇÕES FINAIS

6.1 O presente Plano aplica-se ao período de 24 meses e deverá ser revisado sempre que mudanças significativas, estruturais ou conjunturais justificarem essa necessidade, a critério do Diretor-Geral do DECEA.

6.2 Os projetos e atividades de segurança da informação deverão ser especificados por meio da tradução das ações de divulgação de segurança da informação contidas neste relatório em projetos de segurança da informação.

6.3 Este Plano de Divulgação de Segurança da Informação deverá estar em conformidade com as Diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Aeronáutica -, e será revisado e atualizado sempre que forem atualizadas ou aprovadas Normas relativas ao assunto pela Diretoria de Tecnologia da Informação do Comando da Aeronáutica.