

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-2

MENTALIDADE DE SEGURANÇA

2008

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA**



INTELIGÊNCIA

FCA 200-2

MENTALIDADE DE SEGURANÇA

2008



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

PORTARIA Nº 3/CIAER, DE 19 DE DEZEMBRO DE 2008.

Aprova a edição do Folheto que dispõe sobre Mentalidade de Segurança.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA, tendo em vista o disposto no Inciso II, do art. 4º do Regulamento do Centro de Inteligência da Aeronáutica, aprovado pela Portaria nº C-7/GC3, de 27 de setembro de 2005, resolve:

Art. 1º Aprovar a edição do FCA 200-2 “Mentalidade de Segurança”, que com esta baixa.

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

Art. 3º Revoga-se a Portaria Reservada CISA nº R-001, de 23 de maio de 1985, publicada no Boletim Externo Reservado do Estado-Maior da Aeronáutica nº 017, de 29 de maio de 1985.

Brig Ar PAULO AFONSO PINHEIRO LARI
Chefe do CIAER

(Publicado no BCA nº 005, de 9 de janeiro de 2009)

SUMÁRIO

PREFÁCIO	7
1 DISPOSIÇÕES PRELIMINARES	9
1.1 <u>FINALIDADE</u>	9
1.2 <u>ÂMBITO</u>	9
2 A SEGURANÇA DA INFORMAÇÃO	10
2.1 <u>INDSCRIÇÃO</u>	10
2.2 <u>ENGENHARIA SOCIAL</u>	11
2.3 <u>O PORQUÊ DAS FALHAS DE SEGURANÇA</u>	13
2.4 <u>A SEGURANÇA E O USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO</u>	15
3 MEDIDAS PREVENTIVAS	18
3.1 <u>GENERALIDADES</u>	18
3.2 <u>MEDIDAS DE OBSTRUÇÃO</u>	18
3.3 <u>MEDIDAS DE CONSCIENTIZAÇÃO</u>	19
4 DISPOSIÇÕES FINAIS	20
ÍNDICE	21

PREFÁCIO

A palavra segurança descrita neste documento significa a ação de proteger os conhecimentos sensíveis, instalações e materiais pertencentes ao Comando da Aeronáutica contra ameaças de qualquer natureza.

Segurança envolve pessoas, processos e tecnologias, sendo que geralmente as pessoas são o ponto mais susceptível em um esquema de proteção. Uma pessoa maliciosa, descuidada ou alheia às medidas de salvaguarda de conhecimentos sigilosos compromete o melhor dos planos de segurança.

A segurança da informação desempenha um papel estratégico dentro das Organizações, tornando-se uma necessidade crescente e indispensável para qualquer setor da atividade humana. Sendo assim, seja qual for a forma em que a informação é apresentada (impressa, escrita, falada, entre outras) faz-se necessário que ela seja sempre protegida adequadamente.

O uso dos recursos de tecnologia da informação atuais é indispensável em todo setor de trabalho, fornecendo o suporte às diversas atividades desempenhadas. Porém, os ataques para obtenção de informações empregando tais recursos são cada vez mais sofisticados, valendo-se, principalmente, da ingenuidade e do despreparo dos usuários. Dessa forma, estratégias voltadas para o aumento da mentalidade de segurança devem ser adotadas também no mundo virtual, para minimizar os riscos de comprometimento e de vazamento de informações.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Este documento tem por finalidade alertar o efetivo quanto aos cuidados e aos procedimentos referentes ao trato de assuntos sigilosos, ao uso de instalações e materiais pertinentes ao COMAER, elevando a mentalidade de segurança no âmbito das Organizações Militares.

1.2 ÂMBITO

O presente Folheto aplica-se a todas as OM do COMAER.

2 A SEGURANÇA DA INFORMAÇÃO

A segurança da informação é caracterizada pela preservação da:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Integridade:** salvaguarda da exatidão e da completeza da informação e dos métodos de processamento.

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

No entanto, ameaças como a indiscrição, a engenharia social e a não observância de Normas e Regulamentos para a salvaguarda de assuntos sigilosos acabam prejudicando uma ou mais dessas características de segurança.

2.1 INDISCRICÃO

Muitas tentativas têm sido realizadas para convencer as pessoas desse perigo, com pouco êxito. Em festas, em solenidades, na rua e em qualquer lugar em que as pessoas se reúnem, a indiscrição é muito freqüente. É difícil convencer que existem, trabalhando e convivendo em tais ambientes, pessoas que podem gerar prejuízos. Seus olhos e ouvidos podem estar em qualquer lugar, captando conhecimentos aparentemente inofensivos que, unidos a outros, podem produzir um conhecimento importante e sensível.

2.1.1 QUEM SÃO OS INIMIGOS

Realmente, são de difícil identificação. Eles não andam caracterizados pela vestimenta nem disfarçados. Não se expressam de maneira diferente nem usam uma gíria especial que os identifique. Na realidade eles são, ou procuram ser, pessoas comuns. Normalmente, o que os diferencia é a habilidade em obter conhecimentos, em fazer-nos falar, contar coisas.

Essas pessoas servem, sempre, a interesses contrários aos nossos. Podem ser estrangeiras, naturais ou naturalizadas; podem trabalhar em proveito de outro país ou para um grupo com interesses antagônicos aos nossos; podem ser conhecidos ou desconhecidos, ou seja, qualquer um.

Consciente ou inconscientemente, estarão sempre a serviço de grupos ou países com interesse em comprometer ou prejudicar nossos valores de democracia, integração nacional, integridade de patrimônio, tecnologia, soberania e paz.

No mundo globalizado atual, tudo o que uma nação faz interessa, de alguma forma, a outros. Um país adquire poder sobre outro quando conhece seus segredos. Por esse motivo, é vital que seja garantida a segurança da informação por meio do conhecimento do problema e de muita disciplina.

2.1.2 DESCUIDO

O vazamento de informações sensíveis raramente é proposital. Na maioria dos casos, o responsável é alguém que, sem perceber e sem intencionar, fornece esses

conhecimentos. Por meio de comentários descuidados, telefonemas, salas de bate-papo na internet, e-mail, não observância dos procedimentos de salvaguarda de documentos sigilosos e de outras formas de conduta inconseqüente, uma pessoa pode passar informações vitais.

Para evitar uma conduta desse tipo é necessária muita atenção e discrição.

2.1.3 PRINCIPAIS INTERESSES

O desenvolvimento do senso crítico é fundamental para evitar o vazamento de informações como:

- a) o grau e o tipo de treinamento;
- b) o equipamento utilizado, suas características e desempenho (performance);
- c) o montante e a localização dos recursos financeiros, materiais e humanos;
- d) o estágio em que se encontram os novos conhecimentos e tecnologias; e
- e) demais informações sobre o Preparo e o Emprego da Força Aérea Brasileira.

2.2 ENGENHARIA SOCIAL

A arte de trapacear, de construir métodos e estratégias de enganar, fruto de informações cedidas por pessoas, ou de ganhar a confiança para obter informações, são ações antigas, oriundas dos tempos mais remotos e ganharam um novo termo: Engenharia Social.

Engenharia porque constrói, com base em informações, em táticas de acesso a sistemas e informações sigilosas, de forma indevida. Social porque utiliza pessoas que trabalham e vivem em grupos organizados.

Podemos dizer que a engenharia social é um tipo de ataque, onde a principal “arma” utilizada é a habilidade de lidar com pessoas, induzindo-as a fornecer informações, executar programas e, muitas vezes, fornecer senhas de acesso.

A Engenharia Social visa explorar as pessoas no intuito de ocasionar a perda, a indisponibilidade ou a violação da informação. Ela vai diretamente ao elo mais fraco de qualquer sistema de segurança: o ser humano. O chamado Engenheiro Social utiliza a sua criatividade, poder de persuasão e habilidade, para envolver a vítima em uma situação, onde, muitas vezes, ela nem percebe que abriu as “portas” para um invasor.

2.2.1 FORMA DE ATAQUE

O “ataque” do Engenheiro Social pode ocorrer por intermédio de um bom papo, numa mesa de bar, ao telefone ou, em casos mais sofisticados, por meio da sedução.

O sucesso desse “ataque” está no fato de o usuário abordado nem sequer dar-se conta do que acabou de acontecer. Ou seja, o Engenheiro Social, além de obter a informação que deseja, ainda mantém as “portas” abertas com o seu “informante”.

A falta de consciência das técnicas de Engenharia Social utilizadas e o excesso de autoconfiança das pessoas (por não se considerarem ingênuas e acharem que não podem ser manipuladas) são os principais fatores que favorecem o sucesso da Engenharia Social. A ingenuidade ou a confiança de um usuário é utilizada pelos Engenheiros Sociais para se conseguir informações, que muitas vezes parecem sem importância, mas nas mãos erradas podem causar muito estrago.

Muitos acreditam que os Engenheiros Sociais utilizam ataques com mentiras elaboradas bastante complexas, porém, muitos ataques são diretos, rápidos e muito simples, onde eles simplesmente pedem a informação desejada.

2.2.2 PRINCIPAIS ALVOS

Os alvos principais são os usuários detentores de privilégios equivalentes aos dos Chefes como, por exemplo, auxiliares e secretários, que muitas vezes têm acesso ao correio eletrônico e aos sistemas gerenciais, conhecendo, inclusive, a senha utilizada pelo seu superior hierárquico.

Como a motivação, a habilidade e a oportunidade são essenciais a um atacante que deseja ter acesso à informação, pessoas de dentro da OM formam os mais perigosos grupos de atacantes. Por serem conhecidos, transmitem confiança a outros servidores e possuem a oportunidade necessária para um ataque.

As técnicas mais costumeiras, que podem ser usadas de maneira individual ou combinadas, são:

- a) contatos telefônicos, simulando atendimento de suporte ou uma ação de emergência;
- b) contato por meio de e-mail, atuando como estudante com interesse em pesquisa sobre determinado assunto ou como pessoa com interesse específico em assunto de conhecimento da vítima;
- c) contato por intermédio de ferramentas de *Instant Messaging* (Yahoo, Messenger, MS Messenger, Mirabilis ICQ, etc), simulando pessoa com afinidades com a vítima;
- d) uso de telefone público, para dificultar detecção;
- e) varredura do lixo físico ou eletrônico, para obtenção de informações adicionais para tentativas posteriores de contato;
- f) disfarce de equipe de manutenção; e
- g) visita pessoal, como estudante, estagiário, representante de empresa ou pessoa com disfarce de ingenuidade.

2.3 O PORQUÊ DAS FALHAS DE SEGURANÇA

A necessidade de comunicação do ser humano gera falhas de segurança da informação por características de comportamento como:

- a) vaidade;
- b) confiança nos outros;
- c) entusiasmo;
- d) ignorância; e
- e) outros motivos importantes, como a perda do senso crítico causada pela ingestão de bebidas alcoólicas.

2.3.1 VAIDADE

A vaidade é uma das fraquezas humanas. As pessoas vaidosas geralmente estão insatisfeitas consigo e utilizam-se da vaidade para acalmar o ego. Todavia, este propósito nem sempre é atingido, uma vez que o exibicionista, no lugar de impressionar, pode ser rotulado como uma pessoa inconveniente.

A vaidade é responsável pela maioria das indiscrições: cerca do 90% (noventa) por cento. O vaidoso tem necessidade de mostrar o que sabe, de ser o “bem informado”.

Frases como: “Trabalho nisto há muito tempo” ou “Você sabia que...” - muitas vezes, são o prenúncio de uma indiscrição por vaidade.

A vaidade está presente, em maior ou menor grau, em todos nós. É preciso desenvolver a autocrítica e o autocontrole para dominá-la e não sermos dominados por ela.

Uma boa maneira de lidarmos com a vaidade é desenvolver a autoconfiança. As pessoas seguras, confiantes, não sentem necessidade de mostrar o que sabem.

Também, não devemos aceitar provocações. Deixemos o oponente vencer-nos no debate sempre que, para vencer, for necessário ser indiscreto. Aliás, situações desse tipo são ótimas para desenvolver o nosso autocontrole e para melhorar a nossa argumentação.

Não devemos, ainda, justificar uma missão expondo conhecimentos sensíveis. Não digamos a ninguém mais do que o necessário, só para provar que não estamos fazendo menos do que devíamos.

2.3.2 CONFIANÇA NAS PESSOAS

Essa é uma qualidade que deve ser desenvolvida e incentivada, mas de uma maneira disciplinada.

A confiança é primordial nas relações humanas, mas isto não significa que devamos dizer às pessoas, por mais que confiemos nelas, coisas que não devam saber.

Não confundamos a confiança com a necessidade de conhecer. Nossa companheira (ou companheiro) é digna de toda confiança, mas não precisa tomar

conhecimento de assuntos sigilosos de interesse do COMAER. Podemos ser duplamente irresponsáveis ao passar conhecimentos para aquelas pessoas em quem confiamos, pois elas também serão suspeitas no caso de haver comprometimento.

Desconfiemos das pessoas que buscam nossa confiança e conhecimentos sensíveis dos quais somos detentores.

A maioria de nós acredita ser um bom juiz para julgar as pessoas e, assim sendo, não sermos enganados. Muitas vezes, esquecemos que “alguém” pode ser hábil o suficiente para nos iludir, pois, do contrário, não haveria esse tipo de ataque.

Desconfiemos, também, dos meios normais de telecomunicações: eles não são seguros e são uma fonte importante de conhecimentos para quem se propõe a obter nossos segredos. Não devemos tratar assuntos sigilosos por telefone ou por outros meios de telecomunicações, sem o uso de criptografia adequada.

Todo conhecimento sensível que possuímos, num determinado momento, não é nossa propriedade. Esse conhecimento está conosco por empréstimo, para o exercício de nossas tarefas profissionais. Não podemos trair a confiança que nos foi depositada.

É importante termos em mente que a parcela de segredos dos quais somos detentores pode significar, num futuro bem próximo, a diferença entre a vitória e a derrota, entre a vida e a morte, entre o sucesso e o fracasso.

2.3.3 ENTUSIASMO

Essa é outra causa muito importante na revelação de conhecimentos sigilosos. Alguém treinado pode extrair segredos de uma pessoa entusiasmada, com facilidade.

À semelhança do ódio, o entusiasmo tira nosso senso crítico.

Muitas vezes alguém não acredita, ou finge não acreditar, naquilo que estamos expondo. A conversa, nesse caso, pode se desenvolver do seguinte modo:

Alvo: “Em breve estaremos produzindo uma aeronave de combate com estas características”.

Interlocutor: “Será? Ouvi dizer que...”.

Alvo: “Negativo. Você sabia que, atualmente...”.

Controlemos o entusiasmo.

Desenvolvamos, internamente, a “satisfação do dever cumprido”.

Não deixemos que a emoção seja nosso juiz, que fale pela razão.

2.3.4 IGNORÂNCIA

A Ignorância a que nos referimos é o desconhecimento, por parte de qualquer pessoa, do valor e da sensibilidade dos assuntos de que é detentora.

Nem sempre fica claro qual o conhecimento a ser protegido. Como regra geral, podemos dizer que quase todos os assuntos militares são sensíveis.

Lembremo-nos de que se consegue um conhecimento total pela reunião de seus fragmentos.

Muitas vezes, uma pessoa já possui o conhecimento, mas precisa de nossa versão para confirmá-lo.

Sejamos discretos e evitemos comentários sobre:

- a) efetivos, equipamentos e instalações;
- b) projetos e estudos;
- c) “pontos fortes” e vulnerabilidades;
- d) produção;
- e) rumores; e
- f) sobre qualquer coisa que contenha dados militares não divulgados pelos setores encarregados no COMAER.

Caso persista alguma dúvida, procuremos a orientação do Comandante; ou falemos de outros assuntos, mudando o foco da conversa.

2.4 A SEGURANÇA E O USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO

É comum acreditar-se que a Segurança da Informação pode ser obtida com tecnologia correta e processos bem implementados. Essa crença de que somente tecnologia e processos seriam suficientes para tornar, determinados ambientes e recursos, seguros é sistematicamente derrubada quando pessoas desligam controles, ignoram avisos e deixam de executar procedimentos e protocolos previamente estabelecidos.

Todos os usuários desejam segurança, porém, quando eles têm que interagir com ela e tomar decisões baseando-se em procedimentos de segurança, a maioria acha que ela atrapalha. É costumeiro que usuários nem pensem duas vezes para contornar os procedimentos de segurança em determinadas situações, como por exemplo, quando se aproxima um prazo para entrega de um trabalho importante. Eles podem desativar dispositivos de proteção e de segurança ou até mesmo fornecer uma senha, pois o trabalho precisa ser feito e tem prazo de conclusão.

Os atacantes conhecem esta maneira de agir dos usuários e exploram este comportamento até mesmo criando este tipo de situação para que a segurança seja quebrada.

Algumas vezes, nossas noções de segurança no mundo real não são levadas para este mundo digital simplesmente porque sentimos não ser “nossa responsabilidade”. Se um estranho nos perguntar na rua pelos nossos dados pessoais (nome, endereço, telefone, conta bancária, senha do cartão de crédito, etc) certamente será repellido. Se, no entanto, um estranho nos liga no trabalho demonstrando urgência, apresentando-se como um funcionário

do helpdesk e solicitando nossa senha para realizar um procedimento qualquer em nosso computador, é bem provável que seja atendido. Afinal, o pior que pode acontecer é que alguns recursos d OM serão usados indevidamente (“não é a minha conta bancária em jogo ...”).

Temos a tendência de:

- a) não usar firewalls ou antivírus, porque deixam a máquina mais lenta;
- b) fornecer senhas pessoais a colegas, porque, afinal de contas, eles têm de dar continuidade ao trabalho mesmo na nossa ausência; e
- c) abrir anexos de e-mails não solicitados, mas recebidos de amigos, porque “se meu amigo me enviou, então não tem risco, porque ele provavelmente já deve ter aberto também”.

2.4.1 JOGO DA SEGURANÇA

Vejamos a figura abaixo que compõe um “Jogo da Segurança” ou “Jogo dos Erros” com algumas ameaças e vulnerabilidades.



Figura 1 – Jogo da Segurança

Vamos levantar algumas das ameaças e vulnerabilidades desse ambiente que nada tem a ver com tecnologia:

- a) visitas tendo acesso à área de trabalho onde funcionários lidam com informações sigilosas;
- b) acesso indevido a sites de entretenimento;
- c) uso de jogos;

- d) uso de *post-its* com senha e nome de usuário anotados e visíveis;
- e) documentos em papel, de caráter oficial, jogados no lixo, sem o devido descarte ou eliminação;
- f) funcionário revelando sua senha ao telefone;
- g) xícara de café sobre arquivos de backups.
- h) equipamento de alarme desligado;
- i) fornecimento de arquivos a pessoa não devidamente identificada, cujo crachá está oculto; e
- j) informações de acesso como nome e senha de usuário visíveis na tela de um computadores.

Como se vê, em todas as situações acima, o fator humano teve uma participação fundamental. Não há o que se possa fazer, nesse caso, para aumentar a segurança do ambiente corporativo, que não seja a educação e o treinamento de seus funcionários.

3 MEDIDAS PREVENTIVAS

3.1 GENERALIDADES

O acesso a assuntos sigilosos deve restringir-se às pessoas credenciadas no grau de sigilo adequado, os quais tenham a NECESSIDADE DE CONHECER.

Todo indício de procedimento inadequado deve ser investigado para esclarecimento da suspeita. As medidas corretivas variam com o tipo de falha constatada, desde de um simples esclarecimento sobre a medida de segurança não cumprida ou alteração de normas, até a aplicação de pena mais rigorosa.

3.2 MEDIDAS DE OBSTRUÇÃO

São aquelas destinadas a impedir, eliminar ou minimizar o risco de falhas na segurança da informação. Por assim dizer, citam-se:

3.2.1 SEGURANÇA QUANTO À INDISCRICÃO

Conforme dito anteriormente, a principal preocupação quanto à indiscrição é com a “insegurança falada”. Deve-se ficar alerta para não ser alvo de engenheiros sociais principalmente pelo descuido, ignorância, entusiasmo, excesso de confiança nas pessoas ou vaidade para demonstrar conhecimento. A melhor prevenção é evitar falar demais e desenvolver a capacidade de ouvir e escutar.

3.2.2 SEGURANÇA ESCRITA

Tudo o que foi dito até agora, com algumas modificações, também é válido para os conhecimentos escritos, porém alguns cuidados podem ajudar a proteger os documentos sensíveis:

- a) manter limpa a mesa de trabalho, não deixando expostos os documentos sigilosos;
- b) não manusear documentos sigilosos próximos de pessoas não autorizadas;
- c) confeccionar os documentos sigilosos, de preferência, em uma só máquina, controlando seu acesso;
- d) usar proteção entre as folhas do bloco de rascunho, para evitar a marcação nas folhas inferiores;
- e) na correspondência pessoal tratar somente de assuntos ostensivos;
- f) manter os documentos sigilosos virados nas caixas de entrada e saída, evitando expor seu conteúdo; e
- g) consultar sempre o RCA 205-1 “Regulamento para a Salvaguarda dos Assuntos Sigilosos da Aeronáutica” que regula e padroniza, no âmbito do Comando da Aeronáutica (COMAER), procedimentos necessários à salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam.

3.2.3 SEGURANÇA DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Os recursos de tecnologia da informação pertencentes às OM e que estão disponíveis para o usuário devem ser utilizados em atividades estritamente relacionadas às funções institucionais desempenhadas pelo usuário.

O usuário responsável pelo uso do recurso de tecnologia da informação deve zelar pelo seu estado e funcionamento, comunicando qualquer defeito ou comportamento anormal à área de informática da OM.

O usuário deve abster-se de prestar informações sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, exceto quando o desempenho das suas atividades assim exigir.

A configuração do ambiente operacional da estação de trabalho somente pode ser alterada automaticamente pela rede ou por técnico qualificado e credenciado da área de informática da OM.

O usuário deve realizar cópia de segurança dos dados armazenados no disco rígido da estação de trabalho e tomar as devidas medidas de segurança quanto ao armazenamento dessas cópias. A preferência deve ser sempre pela utilização das unidades de armazenamento da rede.

As senhas de acesso são pessoais e intransferíveis. Devem ser de difícil adivinhação (não usar nomes, números conhecidos como telefone, datas, dados biográficos, placas de carro) e alteradas periodicamente. É importante ter em mente que qualquer utilização da identificação do usuário e da senha de acesso é de responsabilidade do usuário a ele vinculado.

O acesso à Internet, Intraer ou redes externas provido pela OM visa, exclusivamente, auxiliar o trabalho e a aumentar a produtividade do usuário, devendo restringir-se às páginas com conteúdo estritamente relacionado com as funções institucionais desempenhadas pelo mesmo. O acesso a sites com conteúdo malicioso é uma das principais armas utilizadas pelos atacantes para invadir estações de trabalho e redes corporativas.

É possível fazer uso de e-mail para enviar informações sensíveis, observando o que preceitua o RCA 205-1, desde que se utilizem os devidos recursos de criptografia.

3.3 MEDIDAS DE CONSCIENTIZAÇÃO

O primeiro passo em direção a se obter ambientes mais seguros é conscientizar ou sensibilizar as pessoas acerca deste problema. “O problema existe, logo, ou sou parte dele ou parte da sua solução” deve ser o resultado obtido ao fim deste processo.

As pessoas também devem ser orientadas a respeito da verificação das credenciais de todos os que ingressem na organização e alertadas no sentido de que assuntos de serviço, classificados ou sensíveis, devam ser discutidos apenas nas áreas destinadas a esse fim, enfatizando-se o perigo de falar sobre assuntos sigilosos em locais públicos, até mesmo em seu carro ou residência.

4 DISPOSIÇÕES FINAIS

O Centro de Inteligência da Aeronáutica (CIAER), Órgão Central do Sistema de Inteligência da Aeronáutica (SINTAER), e/ou os Elos de Inteligência das OM atuarão, quando solicitados, no processo de assessoria aos respectivos Comandantes, Chefes ou Diretores, objetivando implementar, por meio de procedimentos específicos, melhorias nas medidas de segurança orgânica visando salvaguardar conhecimentos sigilosos.

Este Folheto substitui o FMA 205-2 “Mentalidade de Segurança”, aprovado pela Portaria Reservada CISA nº R-001, de 23 de maio de 1985, publicada no Boletim Externo Reservado do Estado-Maior da Aeronáutica nº 017, de 29 de maio de 1985.

ÍNDICE

A Segurança da Informação, 2

- a segurança e o usuário de tecnologia da informação, 2.4
- confiança nas pessoas, 2.3.2
- descuido, 2.1.2
- engenharia social, 2.2
- entusiasmo, 2.3.3
- forma de ataque, 2.2.1
- ignorância, 2.3.4
- indiscrição, 2.1
- jogo da segurança, 2.4.1
- o porquê das falhas de segurança, 2.3
- principais alvos, 2.2.2
- principais interesses, 2.1.3
- quem são os inimigos, 2.1.1
- vaidade, 2.3.1

Disposições finais, 4

Disposições preliminares, 1

- âmbito, 1.2
- finalidade, 1.1

Medidas preventivas, 3

- generalidades, 3.1
- medidas de conscientização, 3.3
- medidas de obstrução, 3.2
- segurança dos recursos de tecnologia da informação, 3.2.3
- segurança escrita, 3.2.2
- segurança quanto à indiscrição, 3.2.1