CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

DIGITAL

DIRETORIA DE COMUNICAÇÕES E
TECNOLOGIA DA INFORMAÇÃO DA MARINHA
Rio de Janeiro, Brasil
2016

ÍNDICE

INTRODUÇÃO

Toda informação que trafega no Sistema de Comunicações da Marinha (SISCOM) é classificada como um ativo valioso para a MB, não importando a forma em que é apresentada, armazenada ou compartilhada. Sua disponibilidade e precisão é essencial para o cumprimento das nossas missões, obrigando-nos a protegê-la adequadamente.

Especificamente, nosso ambiente computacional interliga toda a MB, inclusive no exterior, por meio da Rede de Comunicações Integrada da Marinha (RECIM), da Internet ou de recursos próprios da MB, como radioenlaces, fibras ópticas ou outros canais. A sua proteção é fundamental para evitar a exposição da informação a uma imensa variedade de ameaças e ataques.

Assim, a Segurança da Informação Digital (SID) na MB busca o constante aperfeiçoamento da mentalidade de segurança, a execução dos procedimentos normativos e o correto emprego da tecnologia para proteger a informação. A SID representa as medidas que visam garantir os requisitos de SIGILO, AUTENCIDADE, INTEGRIDADE e DISPONIBILIDADE da informação, em face do seu valor, dos ambientes envolvidos e dos riscos identificados.

Ressalta-se que é fundamental uma permanente construção e estímulo da MENTALIDADE DE SEGURANÇA em todos os integrantes da MB, desde os altos escalões até as escolas de formação.

Com este fim, publicamos a Cartilha de Segurança da Informação Digital que apresenta conceitos básicos e recomendações importantes, consolidando um breve resumo dos principais tópicos das normas de SID adotadas pela MB.

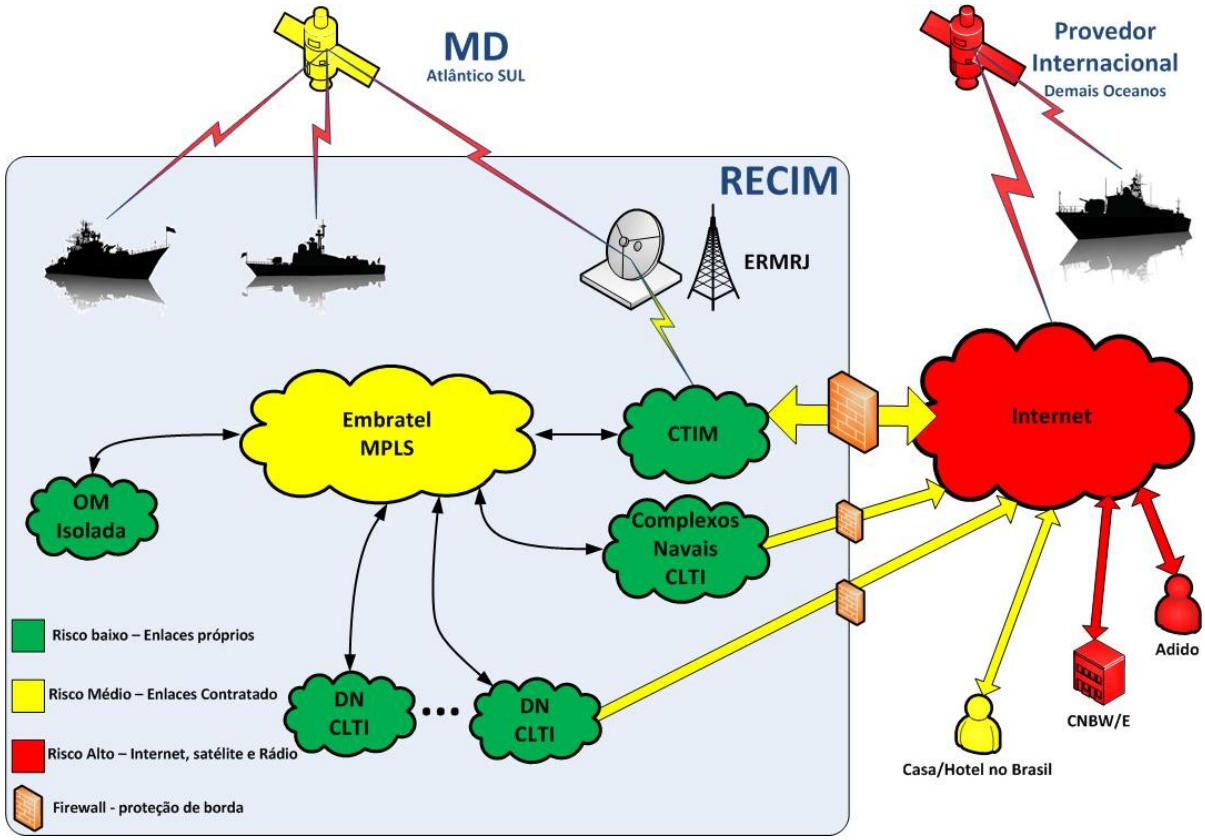
A leitura da Cartilha não isenta o conhecimento do conteúdo das demais Publicações e Instruções Normativas relacionadas ao assunto, especialmente àqueles que operam ou mantém equipamentos conectados à RECIM ou empregados pelo SISCOM.

A INTERNET

A Internet e uma grande rede de computadores em escala mundial que permite o acesso a informacoes e a variadas formas de transferencia de dados. Alguns dos servicos disponiveis na Internet sao os acessos a paginas web, o acesso remoto a outras maquinas, transferencia de arquivos, correio e boletins eletronicos.

(DGMM-0540, Art 5.2)

A RECIM



A Rede de Comunicações Integrada da Marinha (RECIM) é o conjunto de elementos computacionais, organizados em rede, que compõem a infraestrutura responsável pelo tráfego de informações na MB. Abrange a Rede de Telefonia da Marinha (RETELMA) e utiliza o conceito de INTRANET para prover aos seus usuários o acesso a recursos e serviços de TI no âmbito da MB.

(DGMM-0540, inciso 3.2.1)

OFICIAL DE SEGURANÇA DAS INFORMAÇÕES DIGITAIS (OSID)

Tarefas que desempenha na OM:

- Estabelecer e divulgar a Instrução de Segurança das Informações Digitais (ISID) da OM, bem como verificar sua implementação;

- Assessorar o Titular da OM nos assuntos de SID;

- Identificar os recursos de TI que necessitam de proteção, de acordo com o respectivo grau de sigilo da informação por eles processada ou armazenada, devendo estar explícito na ISID da OM;

- Reportar prontamente os incidentes de SID, após uma avaliação preliminar, ao Titular da OM;

- Supervisionar o monitoramento da rede local no intuito de coibir tráfegos anômalos, acessos à Internet por modem, conexões 3G, 4G, WiMAX, WiFi e outras redes sem fio não autorizadas pela DCTIM; e

- Realizar anualmente uma Auditoria Interna de SID na OM, emitindo Relatório de Auditoria (RAD) a ser arquivado no Histórico de Rede Local (HRL), utilizando-se das listas de verificações disponibilizadas pela DCTIM.

(DGMM-0540, artigo 7.6)

ADMINISTRADOR DA REDE LOCAL (ADMIN)

Tarefas que desempenha na OM:

- É o ponto de contato com o Centro Local de Tecnologia da Informação (CLTI), sendo responsável por gerenciar e manter a rede local operando, observando as determinações do Titular da OM e do OSID;

- Auxiliar o OSID na divulgação da ISID da OM e normas em vigor;

- Criar, apagar ou alterar perfis ou privilégios de usuários ou grupos de usuários, documentando estas atividades;

- Controlar e gerenciar os acessos aos sistemas;

- Somente atribuir privilégios de administrador nas estações de usuários àqueles devidamente autorizados pelo titular da OM, com as respectivas justificativas de exceção registradas no Histórico da Rede Local (HRL), lançadas no Termo de Responsabilidade Individual (TRI) e comunicadas à DCTIM por mensagem.

(DGMM-0540, artigo 7.8)

AMEAÇAS

Conjunto de fatores <u>externos</u> ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

(DGMM-0540, inciso 6.2.6 / DCTIMARINST 31-03)

SPAM é uma mensagem não-solicitada mas que foi enviada a um usuário da Internet. Originalmente, a técnica era utilizada para propaganda. Porém, atualmente, é a técnica mais empregada para disseminação de código malicioso na Internet, constituindo-se em elevada ameaça à RECIM quando ocorre interação do usuário.

(DGMM-0540, inciso 5.9.1)

Os usuários devem comunicar imediatamente ao seu superior hierárquico e ao Oficial de Segurança da Informação Digital (OSID) da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de Segurança da Informação Digital (SID) estabelecidos.

(DGMM-0540, art 7.9, alínea l)

ATAQUES NA INTERNET

Em geral, os ataques provenientes de *hackers*, por meio da Internet, são:
- intencionais: associados à intenção premeditada;
- ativos: envolvem interrupção, modificação ou fabricação de informações ou do sistema; e
- externos: praticados por usuário externo à RECIM que conseguiu vencer as barreiras de proteção existentes.

(DGMM-0540, inciso 8.5.14)

Para mitigar esse risco, o uso de Redes Sem Fio é vedado para interligar equipamentos na rede local da OM, visto que um atacante poderá acessar a rede local por meio de um acesso não autorizado à rede sem fio.

(DGMM-0540, inciso 8.5.14)

CÓDIGO MALICIOSO

Código malicioso ou *Malware* é um termo que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Exemplos: Vírus, Vermes (*worms)* e Cavalos de Tróia (*trojan*).

(DGMM-0540, inciso 6.2.7)

Os usuários devem utilizar os programas de proteção de estação de trabalho, com gerenciamento centralizado pelo Centro de Tecnologia da Informação da Marinha (CTIM), contra atividades e programas maliciosos e homologados pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), tais como antivírus e anti-spyware.

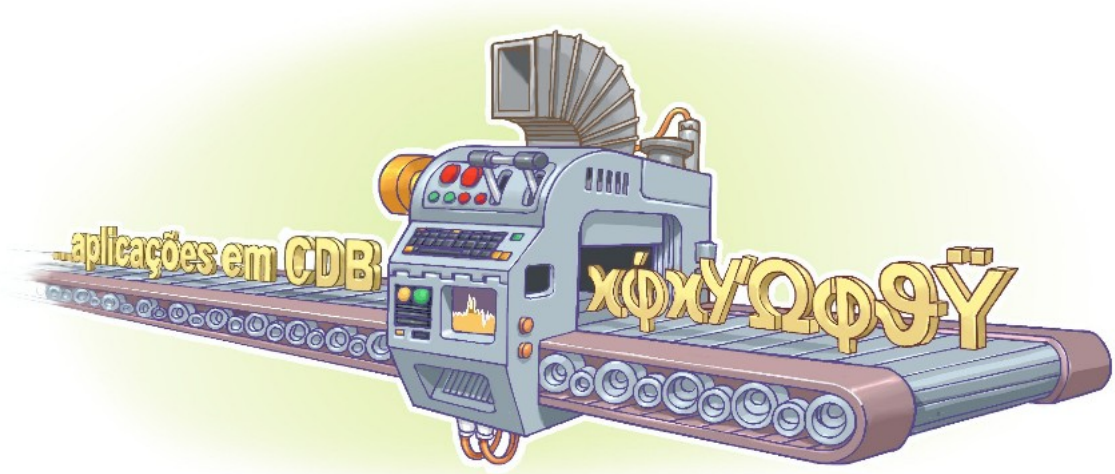
(DGMM-0540, inciso 8.5.4, alínea a)

CORREIO ELETRÔNICO

Os usuários devem atentar que:
- o uso do correio eletrônico da MB é restrito para o interesse do serviço;
- não é permitida a transferência de arquivo que pertença a MB por "e-mail" para caixa postal externa, exceto no interesse de serviço;
- É vedado o uso de correio eletrônico por meio de páginas específicas da Internet (*webmail*); e
- toda informação processada, armazenada ou em trâmite no ambiente computacional da OM pode ser auditada, incluindo o correio eletrônico.

(DGMM-0540, inciso 8.5.14)

CRIPTOGRAFIA



A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

A segurança criptológica consiste no emprego de processos de codificação ou cifração para alterar-se o comteúdo original da informação, de modo a torná-lo incompreensível quando examinado sem o uso dos mesmos códigos ou cifras.
É vedada a utilização de quaisquer dispositivos criptológicos que não os previamente autorizados e homologados pela DCTIM para uso na MB.

(DGMM-0540, Art. 8.7)

ENGENHARIA SOCIAL

Conjunto de técnicas utilizadas por *hackers* para se obter informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta as habilidades e fragilidades sociais do ser humano.

(DGMM-0540, inciso 8.8.2)

O OSID deve divulgar recomendações referentes as técnicas de Engenharia Social para todo o pessoal da OM, a fim de minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicações disponíveis.

(DGMM-0540, artigo 7.6)

Usuários não devem passar a estranhos nenhuma informação sobre os sistemas utilizados em sua rede local de comunicações digitais, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança e equipamentos de comunicações.

(DGMM-0540, inciso 8.8.2, alínea d)

GOLPES NA INTERNET

Todos os acessos na Internet são registrados, sendo periodicamente examinados pela DCTIM/CTIM, ficando disponíveis para eventuais auditorias, durante um período de tempo limitado, conforme previsto em lei.

(DGMM-0540, artigo 5.5)

Usuários não devem passar informações de nomes, telefones e outras informações pessoais de qualquer servidor civil ou militar da OM, nem confirmar a estranhos a existência de determinada pessoa na OM.

(DGMM-0540, inciso 8.8.2, alíneas a e b)

PRIVACIDADE

Os cuidados quanto à privacidade protegem tanto o indivíduo quanto aqueles que o rodeiam (família, amigos e trabalho).

Cuidados básicos em redes sociais:
- Limitar a quantidade de informação pessoal postada;
- Lembrar-se que a internet é pública;
- Cuidado ao falar com estranhos em chats, blogs, comunidades, pois as pessoas podem não ser o que aparentam; e
- Não acreditar em tudo que se lê online.

(DCTIMARINST 31-01, subitem 2.3)

A Segurança Orgânica compreende medidas voltadas para a prevenção e a obstrução das ações adversas de qualquer natureza que possam comprometer a salvaguarda de conhecimentos de interesse da MB ou do País.
Uma vez que o conhecimento está vinculado aos recursos humanos, é importante ressaltar a necessidade de proteção e acompanhamento.

(DGMM-0540, artigo 5.5)

REGRAS PARA SENHAS

- Toda senha é sempre individual e intransferível;
- Nunca compartilhá-la;
- Não usar sequências fáceis ou óbvias de caracteres;
- Não utilizar palavras existentes em dicionários;
- Alternar caracteres minúsculos, maiúsculos, númericos e especiais, no tamanho mínimo exigido;
- Não escrevê-la em lugares visíveis, nem deixar em local de fácil acesso; e
- Trocá-la regularmente.

(DGMM-0540, inciso 8.5.5)

SEGURANÇA COMPUTACIONAL

O uso de mecanismos de proteção pode contribuir para que seu computador não seja infectado/invadido e utilizado para atividades maliciosas.

O ADMIN deve efetuar e garantir as atualizações dos sistemas existentes no ambiente computacional e rede local.

(DGMM-0540, artigo 7.8, alínea j)

Os usuários devem utilizar os programas de proteção de estação de trabalho, com gerenciamento centralizado pelo CTIM, contra atividades e programas maliciosos e homologados pela DCTIM, tais como antivírus e anti-spyware.

(DGMM-0540, inciso 8.5.4, alínea a)

SEGURANÇA EM DISPOSITIVOS MÓVEIS

Ameaças e vulnerabilidades causadas pelo uso de dispositivos móveis (ex: *tablet*, celular etc):
- operação inadequada (uso inapropriado de aplicativo ou quebra de mecanismos de segurança. ex: *jailbreak ou rooting*);
- perda, roubo ou furto;
- interceptação de voz e dados; ou
- execução de códigos maliciosos.

(MATERIALMARINST-22-04, item 3)

Tais ameaças e vulnerabilidades podem ocasionar o vazamento de informações sigilosas, pois, uma vez que a informação seja compartilhada na Internet, ou acessada por terceiros, não haverá mais o controle sobre suas cópias, divulgação e conteúdo.

(MATERIALMARINST-22-04, item 3)

SEGURANÇA DE REDES

Não é permitida a instalação de modem 3G em estação de trabalho que se conecta à RECIM. No caso da eventual necessidade de se utilizar modem 3G como solução de acesso, o projeto deverá ser apreciado pela DCTIM que irá analisar as reais necessidades.

(DGMM-0540, inciso 8.5.7)

É vedada a instalação de qualquer programa para uso em rede, sem análise e autorização prévias da DCTIM, pois podem impactar negativamente o desempenho e a segurança da rede.

(DGMM-0540, inciso 8.5.13)

É vedado o uso de redes sem fio para a interligação de equipamentos na rede local da OM. Nenhum dispositivo de rede sem fio deve ser implementado sem análise e autorização prévias da DCTIM.

(DGMM-0540, inciso 8.6.2)

USO SEGURO DE INTERNET

A Política de Controle de Acesso tem o propósito de permitir ao pessoal da MB a utilização segura das informações disponíveis naquela rede, minimizar possíveis vulnerabilidades na RECIM e restringir o acesso a sítios não autorizados por conterem conteúdo impróprio ou não relacionado às atividades das OM.

(DCTIMARINST 30-06B, item 3)

A MB implementou mecanismos de segurança para proteção da RECIM, como proxy, firewall e analisadores de conteúdo, a fim de controlar os acessos aos diversos nós de conexão com a Internet. O acesso à Internet via RECIM está condicionado a um elenco de serviços, protocolos, aplicações e usuários autorizados. Para acessos utilizando protocolos específicos, necessários à aplicações especiais das OM, faz-se necessária a prévia solicitação à DCTIM. Todos os acessos são registrados em logs, ficando disponíveis para atender auditorias.

(DGMM-0540, artigo 5.5)

VULNERABILIDADES

Ativo é qualquer coisa que tenha valor para a organização, podendo ser: ativo físico; de informação; de serviço; ou intangível (reputação e a imagem da organização).

(DGMM-0540, inciso 6.2.1)

Vulnerabilidade é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

(DGMM-0540, inciso 6.2.7)

Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação digital ou de comunicações.

(DCTIMARINST 31-03, subitem 3.28)

A falta de uma MENTALIDADE DE SEGURANÇA por parte do nosso pessoal é a maior vulnerabilidade da RECIM.

RESPONSABILIDADES E ATRIBUIÇÕES DOS USUÁRIOS

- Tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado;
- Utilizar em sua Estação de Trabalho (ET) somente programas homologados para uso na MB;
- Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- Não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente; e
- Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da OM pode ser auditada.

(DGMM-0540, artigo 7.8)

Recomenda-se a leitura da Nota Técnica nº 14/2016, que trata sobre o enquadramento legal de vazamento de informações.

CONCLUSÃO
MENTALIDADE DE SEGURANÇA

“Uma corrente é tão segura quanto o seu elo mais fraco.”

O fator mais importante para a SID é a existência de uma MENTALIDADE DE SEGURANÇA incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência.

(DGMM-0540, artigo 8.8)

Diretoria de Comunicações e Tecnologia da Informação da Marinha
Departamento de Segurança da Informação Digital

Rua Primeiro de Março, 118 – Ed. Barão de Ladário - 4º andar
Centro - Rio de Janeiro/RJ – 20.010-000 - Tel: (21) 2104-6060

CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

DIGITAL

DIRETORIA DE COMUNICAÇÕES E
TECNOLOGIA DA INFORMAÇÃO DA MARINHA
Rio de Janeiro, Brasil
2016

ÍNDICE

INTRODUÇÃO

Toda informação que trafega no Sistema de Comunicações da Marinha (SISCOM) é classificada como um ativo valioso para a MB, não importando a forma em que é apresentada, armazenada ou compartilhada. Sua disponibilidade e precisão é essencial para o cumprimento das nossas missões, obrigando-nos a protegê-la adequadamente.

Especificamente, nosso ambiente computacional interliga toda a MB, inclusive no exterior, por meio da Rede de Comunicações Integrada da Marinha (RECIM), da Internet ou de recursos próprios da MB, como radioenlaces, fibras ópticas ou outros canais. A sua proteção é fundamental para evitar a exposição da informação a uma imensa variedade de ameaças e ataques.

Assim, a Segurança da Informação Digital (SID) na MB busca o constante aperfeiçoamento da mentalidade de segurança, a execução dos procedimentos normativos e o correto emprego da tecnologia para proteger a informação. A SID representa as medidas que visam garantir os requisitos de SIGILO, AUTENCIDADE, INTEGRIDADE e DISPONIBILIDADE da informação, em face do seu valor, dos ambientes envolvidos e dos riscos identificados.

Ressalta-se que é fundamental uma permanente construção e estímulo da MENTALIDADE DE SEGURANÇA em todos os integrantes da MB, desde os altos escalões até as escolas de formação.

Com este fim, publicamos a Cartilha de Segurança da Informação Digital que apresenta conceitos básicos e recomendações importantes, consolidando um breve resumo dos principais tópicos das normas de SID adotadas pela MB.

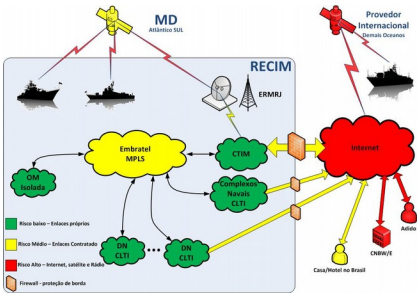
A leitura da Cartilha não isenta o conhecimento do conteúdo das demais Publicações e Instruções Normativas relacionadas ao assunto, especialmente àqueles que operam ou mantém equipamentos conectados à RECIM ou empregados pelo SISCOM.

A INTERNET

A Internet e uma grande rede de computadores em escala mundial que permite o acesso a informacoes e a variadas formas de transferencia de dados. Alguns dos servicos disponiveis na Internet sao os acessos a paginas web, o acesso remoto a outras maquinas, transferencia de arquivos, correio e boletins eletronicos.

(DGMM-0540, Art 5.2)

A RECIM



A Rede de Comunicações Integrada da Marinha (RECIM) é o conjunto de elementos computacionais, organizados em rede, que compõem a infraestrutura responsável pelo tráfego de informações na MB. Abrange a Rede de Telefonia da Marinha (RETELMA) e utiliza o conceito de INTRANET para prover aos seus usuários o acesso a recursos e serviços de TI no âmbito da MB.

(DGMM-0540, inciso 3.2.1)

OFICIAL DE SEGURANÇA DAS INFORMAÇÕES DIGITAIS (OSID)

Tarefas que desempenha na OM:
- Estabelecer e divulgar a Instrução de Segurança das Informações Digitais (ISID) da OM, bem como verificar sua implementação;
- Assessorar o Titular da OM nos assuntos de SID;
- Identificar os recursos de TI que necessitam de proteção, de acordo com o respectivo grau de sigilo da informação por eles processada ou armazenada, devendo estar explícito na ISID da OM;
- Reportar prontamente os incidentes de SID, após uma avaliação preliminar, ao Titular da OM;
- Supervisionar o monitoramento da rede local no intuito de coibir tráfegos anômalos, acessos à Internet por modem, conexões 3G, 4G, WiMAX, WiFi e outras redes sem fio não autorizadas pela DCTIM; e
- Realizar anualmente uma Auditoria Interna de SID na OM, emitindo Relatório de Auditoria (RAD) a ser arquivado no Histórico de Rede Local (HRL), utilizando-se das listas de verificações disponibilizadas pela DCTIM.

(DGMM-0540, artigo 7.6)

ADMINISTRADOR DA REDE LOCAL (ADMIN)

Tarefas que desempenha na OM:
- É o ponto de contato com o Centro Local de Tecnologia da Informação (CLTI), sendo responsável por gerenciar e manter a rede local operando, observando as determinações do Titular da OM e do OSID;
- Auxiliar o OSID na divulgação da ISID da OM e normas em vigor;
- Criar, apagar ou alterar perfis ou privilégios de usuários ou grupos de usuários, documentando estas atividades;
- Controlar e gerenciar os acessos aos sistemas;
- Somente atribuir privilégios de administrador nas estações de usuários àqueles devidamente autorizados pelo titular da OM, com as respectivas justificativas de exceção registradas no Histórico da Rede Local (HRL), lançadas no Termo de Responsabilidade Individual (TRI) e comunicadas à DCTIM por mensagem.

(DGMM-0540, artigo 7.8)

AMEAÇAS

Conjunto de fatores <u>externos</u> ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

(DGMM-0540, inciso 6.2.6 / DCTIMARINST 31-03)

SPAM é uma mensagem não-solicitada mas que foi enviada a um usuário da Internet. Originalmente, a técnica era utilizada para propaganda. Porém, atualmente, é a técnica mais empregada para disseminação de código malicioso na Internet, constituindo-se em elevada ameaça à RECIM quando ocorre interação do usuário.

(DGMM-0540, inciso 5.9.1)

Os usuários devem comunicar imediatamente ao seu superior hierárquico e ao Oficial de Segurança da Informação Digital (OSID) da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de Segurança da Informação Digital (SID) estabelecidos.

(DGMM-0540, art 7.9, alínea l)

ATAQUES NA INTERNET

Em geral, os ataques provenientes de *hackers*, por meio da Internet, são:
- intencionais: associados à intenção premeditada;
- ativos: envolvem interrupção, modificação ou fabricação de informações ou do sistema; e
- externos: praticados por usuário externo à RECIM que conseguiu vencer as barreiras de proteção existentes.

(DGMM-0540, inciso 8.5.14)

Para mitigar esse risco, o uso de Redes Sem Fio é vedado para interligar equipamentos na rede local da OM, visto que um atacante poderá acessar a rede local por meio de um acesso não autorizado à rede sem fio.

(DGMM-0540, inciso 8.5.14)

CÓDIGO MALICIOSO

Código malicioso ou *Malware* é um termo que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Exemplos: Vírus, Vermes (*worms)* e Cavalos de Tróia (*trojan*).

(DGMM-0540, inciso 6.2.7)

Os usuários devem utilizar os programas de proteção de estação de trabalho, com gerenciamento centralizado pelo Centro de Tecnologia da Informação da Marinha (CTIM), contra atividades e programas maliciosos e homologados pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), tais como antivírus e anti-spyware.

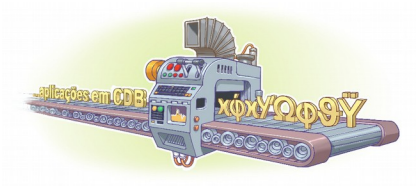
(DGMM-0540, inciso 8.5.4, alínea a)

CORREIO ELETRÔNICO

Os usuários devem atentar que:
- o uso do correio eletrônico da MB é restrito para o interesse do serviço;
- não é permitida a transferência de arquivo que pertença a MB por "e-mail" para caixa postal externa, exceto no interesse de serviço;
- É vedado o uso de correio eletrônico por meio de páginas específicas da Internet (*webmail*); e
- toda informação processada, armazenada ou em trâmite no ambiente computacional da OM pode ser auditada, incluindo o correio eletrônico.

(DGMM-0540, inciso 8.5.14)

CRIPTOGRAFIA



A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

A segurança criptológica consiste no emprego de processos de codificação ou cifração para alterar-se o comteúdo original da informação, de modo a torná-lo incompreensível quando examinado sem o uso dos mesmos códigos ou cifras.
É vedada a utilização de quaisquer dispositivos criptológicos que não os previamente autorizados e homologados pela DCTIM para uso na MB.

(DGMM-0540, Art. 8.7)

ENGENHARIA SOCIAL

Conjunto de técnicas utilizadas por *hackers* para se obter informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta as habilidades e fragilidades sociais do ser humano.

(DGMM-0540, inciso 8.8.2)

O OSID deve divulgar recomendações referentes as técnicas de Engenharia Social para todo o pessoal da OM, a fim de minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicações disponíveis.

(DGMM-0540, artigo 7.6)

Usuários não devem passar a estranhos nenhuma informação sobre os sistemas utilizados em sua rede local de comunicações digitais, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança e equipamentos de comunicações.

(DGMM-0540, inciso 8.8.2, alínea d)

GOLPES NA INTERNET

Todos os acessos na Internet são registrados, sendo periodicamente examinados pela DCTIM/CTIM, ficando disponíveis para eventuais auditorias, durante um período de tempo limitado, conforme previsto em lei.

(DGMM-0540, artigo 5.5)

Usuários não devem passar informações de nomes, telefones e outras informações pessoais de qualquer servidor civil ou militar da OM, nem confirmar a estranhos a existência de determinada pessoa na OM.

(DGMM-0540, inciso 8.8.2, alíneas a e b)

PRIVACIDADE

Os cuidados quanto à privacidade protegem tanto o indivíduo quanto aqueles que o rodeiam (família, amigos e trabalho).

Cuidados básicos em redes sociais:
- Limitar a quantidade de informação pessoal postada;
- Lembrar-se que a internet é pública;
- Cuidado ao falar com estranhos em chats, blogs, comunidades, pois as pessoas podem não ser o que aparentam; e
- Não acreditar em tudo que se lê online.

(DCTIMARINST 31-01, subitem 2.3)

A Segurança Orgânica compreende medidas voltadas para a prevenção e a obstrução das ações adversas de qualquer natureza que possam comprometer a salvaguarda de conhecimentos de interesse da MB ou do País.
Uma vez que o conhecimento está vinculado aos recursos humanos, é importante ressaltar a necessidade de proteção e acompanhamento.

(DGMM-0540, artigo 5.5)

REGRAS PARA SENHAS

- Toda senha é sempre individual e intransferível;
- Nunca compartilhá-la;
- Não usar sequências fáceis ou óbvias de caracteres;
- Não utilizar palavras existentes em dicionários;
- Alternar caracteres minúsculos, maiúsculos, númericos e especiais, no tamanho mínimo exigido;
- Não escrevê-la em lugares visíveis, nem deixar em local de fácil acesso; e
- Trocá-la regularmente.

(DGMM-0540, inciso 8.5.5)

SEGURANÇA COMPUTACIONAL

O uso de mecanismos de proteção pode contribuir para que seu computador não seja infectado/invadido e utilizado para atividades maliciosas.

O ADMIN deve efetuar e garantir as atualizações dos sistemas existentes no ambiente computacional e rede local.

(DGMM-0540, artigo 7.8, alínea j)

Os usuários devem utilizar os programas de proteção de estação de trabalho, com gerenciamento centralizado pelo CTIM, contra atividades e programas maliciosos e homologados pela DCTIM, tais como antivírus e anti-spyware.

(DGMM-0540, inciso 8.5.4, alínea a)

SEGURANÇA EM DISPOSITIVOS MÓVEIS

Ameaças e vulnerabilidades causadas pelo uso de dispositivos móveis (ex: *tablet*, celular etc):
- operação inadequada (uso inapropriado de aplicativo ou quebra de mecanismos de segurança. ex: *jailbreak ou rooting*);
- perda, roubo ou furto;
- interceptação de voz e dados; ou
- execução de códigos maliciosos.

(MATERIALMARINST-22-04, item 3)

Tais ameaças e vulnerabilidades podem ocasionar o vazamento de informações sigilosas, pois, uma vez que a informação seja compartilhada na Internet, ou acessada por terceiros, não haverá mais o controle sobre suas cópias, divulgação e conteúdo.

(MATERIALMARINST-22-04, item 3)

SEGURANÇA DE REDES

Não é permitida a instalação de modem 3G em estação de trabalho que se conecta à RECIM. No caso da eventual necessidade de se utilizar modem 3G como solução de acesso, o projeto deverá ser apreciado pela DCTIM que irá analisar as reais necessidades.

(DGMM-0540, inciso 8.5.7)

É vedada a instalação de qualquer programa para uso em rede, sem análise e autorização prévias da DCTIM, pois podem impactar negativamente o desempenho e a segurança da rede.

(DGMM-0540, inciso 8.5.13)

É vedado o uso de redes sem fio para a interligação de equipamentos na rede local da OM. Nenhum dispositivo de rede sem fio deve ser implementado sem análise e autorização prévias da DCTIM.

(DGMM-0540, inciso 8.6.2)

USO SEGURO DE INTERNET

A Política de Controle de Acesso tem o propósito de permitir ao pessoal da MB a utilização segura das informações disponíveis naquela rede, minimizar possíveis vulnerabilidades na RECIM e restringir o acesso a sítios não autorizados por conterem conteúdo impróprio ou não relacionado às atividades das OM.

(DCTIMARINST 30-06B, item 3)

A MB implementou mecanismos de segurança para proteção da RECIM, como proxy, firewall e analisadores de conteúdo, a fim de controlar os acessos aos diversos nós de conexão com a Internet. O acesso à Internet via RECIM está condicionado a um elenco de serviços, protocolos, aplicações e usuários autorizados. Para acessos utilizando protocolos específicos, necessários à aplicações especiais das OM, faz-se necessária a prévia solicitação à DCTIM. Todos os acessos são registrados em logs, ficando disponíveis para atender auditorias.

(DGMM-0540, artigo 5.5)

VULNERABILIDADES

Ativo é qualquer coisa que tenha valor para a organização, podendo ser: ativo físico; de informação; de serviço; ou intangível (reputação e a imagem da organização).

(DGMM-0540, inciso 6.2.1)

Vulnerabilidade é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

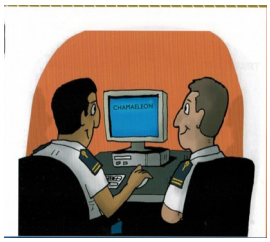
(DGMM-0540, inciso 6.2.7)

Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação digital ou de comunicações.

(DCTIMARINST 31-03, subitem 3.28)

A falta de uma MENTALIDADE DE SEGURANÇA por parte do nosso pessoal é a maior vulnerabilidade da RECIM.

RESPONSABILIDADES E ATRIBUIÇÕES DOS USUÁRIOS



- Tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado;
- Utilizar em sua Estação de Trabalho (ET) somente programas homologados para uso na MB;
- Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- Não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente; e
- Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da OM pode ser auditada.

(DGMM-0540, artigo 7.8)

Recomenda-se a leitura da Nota Técnica nº 14/2016, que trata sobre o enquadramento legal de vazamento de informações.

CONCLUSÃO
MENTALIDADE DE SEGURANÇA

"Uma corrente é tão segura quanto o seu elo mais fraco."

O fator mais importante para a SID é a existência de uma MENTALIDADE DE SEGURANÇA incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência.

(DGMM-0540, artigo 8.8)

Diretoria de Comunicações e Tecnologia da Informação da Marinha
Departamento de Segurança da Informação Digital

Rua Primeiro de Março, 118 – Ed. Barão de Ladário - 4º andar
Centro - Rio de Janeiro/RJ – 20.010-000 - Tel: (21) 2104-6060