SEGURANÇA DA INFORMAÇÃO DIGITAL (SID)

A SID engloba as ações de proteção aos sistemas de informação digital, para garantir a utilização dos serviços pelos usuários autorizados e evitar intrusões e modificações não autorizadas das informações digitais armazenadas, em processamento ou em trânsito, em meio eletrônico.

A SID abrange, inclusive, a segurança dos recursos humanos, da documentação, do material, das áreas e das instalações. Também deve prevenir, detectar, deter e documentar eventuais ameaças ou ataques.

REQUISITOS BÁSICOS DE SID

A SID está fundamentada na garantia e na manutenção dos seguintes requisitos básicos sobre as informações digitais:

a) sigilo: a informação digital somente ser acessada por alguém autorizado;

b) autenticidade: a origem da informação digital deve ser realmente aquela apresentada;

REQUISITOS BÁSICOS DE SID

c) integridade: a informação digital somente ser modificada por alguém autorizado; e

d) disponibilidade: a informação digital estar disponível para alguém autorizado a acessá-la no momento próprio.

AÇÕES DE PROTEÇÃO DOS SISTEMAS DE INFORMAÇÃO DIGITAL

São as ações que, baseadas num conjunto de procedimentos, recursos (programas e equipamentos de segurança e de criptografia) e normas aplicáveis, visam a proteger os sistemas de informação digital. Todas as ações de segurança de informações devem estar plenamente documentadas, haja vista que seus registros e análises possibilitarão um contínuo aperfeiçoamento analítico, visando à plena manutenção dos requisitos básicos de SID.

Essas ações de proteção englobam as seguintes atividades:

a) **planejamento**: visam à preparação para prevenção de possíveis ameaças ou riscos às informações digitais;

b) histórico: registro de ocorrências que possam vir a ocorrer no ambiente onde se processam ou trafegam informações digitais;

c) análise: auditorias e avaliações de vulnerabilidades, de riscos ou de incidentes que possam ocorrer no ambiente onde se processam ou trafegam informações digitais;

d) correção: correções e reparos no ambiente onde se processam ou trafegam informações digitais, para pronto restabelecimento de suas condições operacionais e dos requisitos básicos de SID; e

e) adestramento: visam adestrar o pessoal quanto aos documentos, aos procedimentos e às demais instruções de SID.

SEGURANÇA EM DESENVOLVIMENTO DE SISTEMAS

É o conjunto de procedimentos, de recursos de SID e de normas aplicáveis, que visam proteger o desenvolvimento dos sistemas de informação digital.

Esta segurança visa à garantia de que o sistema, quando pronto e implantado, atende às especificações de segurança estabelecidas para o seu respectivo funcionamento, compreendendo o conjunto de procedimentos, de recursos de SID e de normas aplicáveis para obter:

a) **segurança do ambiente de desenvolvimento:** conjunto de ações visando à proteção dos códigos-fonte, da equipe de desenvolvimento e do ambiente em que as atividades são realizadas;

b) segurança do processo de desenvolvimento: conjunto de ações visando garantir que o processo de desenvolvimento do sistema siga padrões técnicos de segurança conhecidos e auditáveis, que impeçam a existência de códigos maliciosos agregados ou falhas que comprometam a segurança; e

c) segurança dos Recursos Humanos de desenvolvimento: conjunto de ações visando à proteção do pessoal envolvido, direta ou indiretamente, com atividades de desenvolvimento. Devem ser observados os aspectos de segurança no processo seletivo, no desempenho da função e no desligamento.

POLÍTICAS DA DOUTRINA DE SID

Desenvolvimento Interno de Recursos de SID.

Nacionalização de Recursos de SID.

Conscientização do Pessoal.

Desenvolvimento Interno de Recursos de SID

O COTIM (Concelho de TI da Marinha) promulgará normas e diretrizes para o desenvolvimento de sistemas de informações digitais, bem como a DCTIM (Diretoria de Comunicações e TI da Marinha) adotará as medidas necessárias para promover a eliminação da dependência externa da MB em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à criptologia e à segurança dos sistemas de informações digitais.

Nacionalização de Recursos de SID

Na impossibilidade de desenvolvimento pela MB, a DGMM (Diretoria Geral de Material da Marinha) deve estabelecer normas e diretrizes para o desenvolvimento de sistemas de informações digitais, promovendo a capacitação industrial do País, visando à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como deve empreender ações para estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados à SID.

Conscientização do Pessoal

As OM devem envidar esforços para desenvolver e manter um alto nível de conscientização do pessoal quanto à SID, programando palestras, adestramentos, exercícios internos e outras atividades cabíveis, englobando publicações, normas e procedimentos afetos ao assunto.

Pouco adiantará o estabelecimento de rigorosas medidas de segurança, se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência; e

a) Mentalidade de Segurança

O esforço para as atividades de SID deve ser de todos e não somente do pessoal diretamente envolvido com o setor de informática da OM. O fator mais importante para a SID é a existência de uma mentalidade de segurança em todo o pessoal.

b) Adestramentos de SID

As OM devem prever, em seu Programa de Adestramento, o contínuo adestramento de SID para todo o seu pessoal, de modo a possibilitar a manutenção e a garantia de uma elevada mentalidade de segurança.