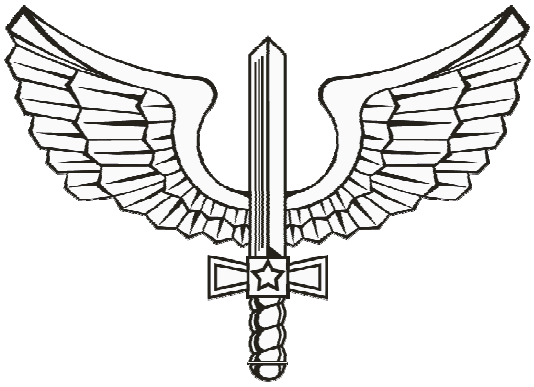
MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA



TECNOLOGIA DA INFORMAÇÃO

MCA 7-1

GLOSSÁRIO 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

MCA 7-1

GLOSSÁRIO 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 4/SDTE, DE 16 DE MARÇO DE 2012.

Aprova a edição do Manual do Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo.

O CHEFE DO SUBDEPARTAMENTO TÉCNICO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 1º, inciso II, alínea "h", da Portaria DECEA nº 1-T/DGCEA, de 2 de janeiro de 2012, resolve:

Art. 1º Aprovar a edição do MCA 7-1 "Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo", que com esta baixa.

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

(a) Brig Eng LUIZ ANTÔNIO FREITAS DE CASTRO
Chefe do SDTE

(Publicado no BCA nº 63, de 30 de março de 2012)

SUMÁRIO

PREFÁCIO

Esta publicação tem o propósito de prover o Departamento de Controle do Espaço Aéreo de ferramenta que proporcione o entendimento dos conceitos e termos utilizados na área de Segurança da Informação. Visa ainda a economia de tempo na pesquisa de terminologia empregada nos documentos normativos da Política de Segurança da Informação do DECEA.

Os termos, palavras, vocábulos e expressões aqui contidos foram dispostos em ordem alfabética, para facilitar o manuseio deste manual.

Cabe lembrar que o Glossário de Segurança da Informação do Departamento do Controle do Espaço Aéreo nunca estará atualizado. Ele deverá ser periodicamente revisado, na medida em que novas definições e conceitos forem surgindo, ou caindo em desuso, no âmbito do DECEA e suas Organizações Militares subordinadas.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O Glossário de Segurança da Informação tem por finalidade padronizar a utilização de termos, palavras, vocábulos e expressões de uso corrente sobre o tema segurança da informação.

1.2 ÂMBITO

O presente Manual aplica-se ao Departamento de Controle do Espaço Aéreo e Organizações Militares subordinadas.

2 O GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO

2.1 LETRA A

2.1.1 ACESSO FÍSICO

Possibilidade de estar fisicamente próximo a um ativo, podendo causar danos a sua disponibilidade, confidencialidade e integridade.

2.1.2 ACESSO LÓGICO

Possibilidade de interagir com o ativo remotamente podendo manipular sua informação sem, no entanto, estar fisicamente próximo ao mesmo.

2.1.3 *ADWARE*

Do Inglês *Advertising Software*. *Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

2.1.4 AMEAÇAS

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas na confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização.

2.1.5 AMBIENTE EXTERNO

Ambiente que circunda o local da organização o qual não pode ser controlado pela mesma.

2.1.6 ANÁLISE DE RISCO

Constitui-se no uso sistemático de informações para identificar fontes de risco e estimar seu valor.

2.1.7 AP

Do Inglês *Access Point*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

2.1.8 ÁREA

Organização Militar subordinada ao DECEA, conforme estrutura organizacional formalmente definida.

2.1.9 ÁREA SIGILOSA

É aquela onde documentos, materiais, comunicações e sistemas de informações sigilosos são tratados, manuseados, transmitidos ou guardados e que, portanto, requer medidas especiais de segurança e controle de acesso.

2.1.10 ARQUIVOS ELETRÔNICOS

Formato de armazenamento de informações em discos magnéticos. Arquivos eletrônicos podem conter tanto informações de usuários quanto dados do sistema operacional e códigos de execução de programas.

2.1.11 ASSINATURA DIGITAL

Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

2.1.12 ASSINATURA ELETRÔNICA

Sistema onde cada usuário possui um código e, através de uma função matemática (*hash*), pode-se garantir que o documento/mensagem não teve sua origem ou conteúdo forjado.

2.1.13 ASSUNTO SIGILOSO

É aquele que, por sua natureza, deva ser de conhecimento restrito e, portanto, requeira a adoção de medidas especiais para sua segurança.

2.1.14 ATACANTE

Pessoa responsável pela realização de um ataque.

2.1.15 ATAQUE

Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques às tentativas de negação de serviço.

2.1.16 ATIVO

Constitui-se em qualquer coisa que tenha valor para o DECEA.

2.1.17 ATIVO DE INFORMAÇÃO

Todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada e os equipamentos em que ela é manuseada, transportada e descartada. O termo ativo possui esta denominação por ser considerado um elemento de valor para um indivíduo ou organização e que, por esse motivo, necessita de proteção adequada.

2.1.18 AUDITORIA BASEADA EM RISCO

Auditoria planejada com base em uma avaliação de análise de riscos.

2.1.19 AUDITORIA DE CONFORMIDADE

Tipo de auditoria específica para avaliar a extensão em que a auditoria atingiu em conformidade com os requisitos estabelecidos.

2.1.20 AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

Processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente para determinar a extensão na qual os critérios da auditoria são atendidos.

2.1.21 AUDITORIA DO SGSI

Auditoria centrada sobre a organização do Sistema de Gestão da Segurança da Informação (SGSI).

2.1.22 AUTENTICIDADE

Garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e de que a mensagem ou informação não foi alterada após o seu envio ou validação.

2.1.23 AVALIAÇÃO DE IMPACTO DE MUDANÇA

Documento que indique os possíveis impactos gerados por uma determinada mudança.

2.2 LETRA B

2.2.1 *BACKDOOR*

Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

2.2.2 *BACKUP*

Cópia que se faz de cada arquivo do computador, como garantia para o caso em que se perca os dados originais gravados no computador.

2.2.3 *BLUETOOTH*

Termo que se refere a uma tecnologia de rádio-freqüência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

2.2.4 BOATO

E-mail que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou

órgão governamental. Através de uma leitura minuciosa deste tipo de e-mail, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

2.2.5 *BOT*

Um *bot*, diminutivo de *robot*, é um utilitário concebido para simular ações humanas, em geral numa taxa muito mais elevada do que seria possível para um editor humano sozinho. No contexto de sistemas pode ser um utilitário que desempenha tarefas rotineiras.

2.2.6 *BOTNET*

Rede formada por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc.

2.2.7 *BUFFER OVERRUN/OVERFLOW*

Erros conhecidos como estouro de pilha, ocorrem quando se excede o espaço em que são armazenados os dados.

2.3 LETRA C

2.3.1 CAIXA POSTAL

Local onde ficam armazenados os *e-mails* de um usuário. Tanto localmente quanto remotamente.

2.3.2 CAVALO DE TRÓIA

Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

2.3.3 CERTIFICADO DIGITAL

Mecanismo que permite a troca de mensagens com garantia de autenticidade do remetente e criptografia dos dados.

2.3.4 CLASSIFICAÇÃO

Atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação.

2.3.5 CÓDIGOS MALICIOSOS

Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, worms, bots, cavalos de tróia, rootkits, etc.

2.3.6 CONEXÃO SEGURA

Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

2.3.7 CONFIDENCIALIDADE

Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

2.3.8 CONTA DE USUÁRIO

Identificação individual de usuário, constituída por um código de usuário acompanhado de uma senha, a qual define os direitos de acesso do usuário aos recursos de Tecnologia da Informação do DECEA e das suas unidades subordinadas.

2.3.9 CONTROLE

São as práticas, os procedimentos e os mecanismos utilizados para a proteção da informação e dos ativos a ela correlacionados, que podem ser de natureza administrativa, técnica, legal, ou de gestão.

2.3.10 CORREIO ELETRÔNICO

Sistema de envio e recebimento de mensagens eletrônicas, mais conhecidas como "*E-mail*". Também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da Internet.

2.3.11 *COVERT CHANNELS*

Os *covert channels* são caminhos não previstos para conduzir fluxo de informações, mas que, no entanto podem existir num sistema ou rede. Por exemplo, a manipulação de bits no protocolo de pacotes de comunicação poderia ser utilizada como um método oculto de sinalização. Devido à sua natureza, seria difícil, se não impossível, precaver-se contra a existência de todos os possíveis *covert channels*. No entanto, a exploração destes canais freqüentemente é realizada por código troiano. A adoção de medidas de proteção contra código malicioso reduz, conseqüentemente, o risco de exploração de *covert channels*.

2.3.12 *CRACKER*

Indivíduo comumente dedicado a quebrar chaves de proteção de programas de computador e invadir sistemas, violando a integridade das informações com intenção maliciosa.

2.3.13 CREDENCIAMENTO

É o ato de concessão de Credencial de Segurança.

2.3.14 CREDENCIAL DE SEGURANÇA

Certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo.

2.3.15 CRIPTOGRAFIA

Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifração, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifração. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

2.3.16 CRITICIDADE

Intensidade do impacto causado pela ausência de um ativo no negócio, pela redução de suas funcionalidades para o processo de negócio ou pelo seu uso não autorizado.

2.3.17 CSI – COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do DECEA e suas Organizações Militares Subordinadas.

2.3.18 CUSTÓDIA

Lugar onde se guarda algo com segurança. Guarda, proteção.

2.3.19 CUSTODIANTE

Usuário responsável pela guarda adequada da informação, que cuida do ativo onde está armazenado a informação no dia-a-dia.

2.4 LETRA D

2.4.1 DDOS

Do Inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet. Ver Negação de serviço.

2.4.2 DESASTRE

Caracteriza-se por qualquer evento que afete os processos críticos do negócio de uma organização. Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada organização, mas não para outras.

2.4.3 DIRETRIZ

Descrição que orienta o que deve ser feito e como se fazer, para se alcançarem os objetivos estabelecidos nas políticas.

2.4.4 DISPONIBILIDADE

Qualidade de tornar disponível para usuários, sempre que necessário e para qualquer finalidade, toda informação gerada ou adquirida por um indivíduo ou instituição.

2.4.5 DISCO RÍGIDO

Meio magnético o qual armazena os arquivos de um computador mesmo que o mesmo seja desligado.

2.4.6 *DMZ* (*DEMILITARIZED ZONE*)

É a área de rede que permanece entre a rede interna de uma organização e uma rede externa, em geral a rede Internet. Comumente, uma *DMZ* contém equipamentos apropriados para o acesso à rede Internet, como servidores para web (HTTP), servidores *FTP*, servidores para *e-mail* (*SMTP*) e servidores *DNS*.

2.4.7 DNS

Do Inglês *Domain Name System*. Serviço que traduz nomes de domínios para endereços IP e vice-versa.

2.4.8 DOCUMENTOS NORMATIVOS

São os documentos que compõe a Política de Segurança da Informação do DECEA. Podemos citar os seguintes documentos: Normais gerais de Segurança da Informação, Procedimentos de Segurança da Informação e Instrução de Trabalho de Segurança da Informação.

2.4.9 *DOWNLOADS*

É a transferência de arquivos de um computador para outro.

2.5 LETRA E

2.5.1 ENDEREÇO ELETRÔNICO

É uma cadeia de caracteres, do tipo "nome_usuario@decea.gov.br" (sem aspas, por exemplo) que identifica univocamente um determinado utilizador dentro da Internet e, em particular, a sua caixa de correio eletrônica. Qualquer envio de correio eletrônico para esse utilizador deve ser feito para o seu endereço eletrônico.

2.5.2 ENDEREÇO IP

Este endereço é um número único para cada computador conectado à Internet, composto por uma seqüência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

2.5.3 ENGENHARIA SOCIAL

Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

2.5.4 ESCOPO DA AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

Partes da Organização Militar que serão auditadas.

2.5.5 ESTAÇÕES DE TRABALHO

Computadores destinados aos usuários.

2.5.6 ETIR

Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes de telecomunicações e sistemas de informação.

2.5.7 EVENTO DE SEGURANÇA DA INFORMAÇÃO

É a ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

2.5.8 EVIDÊNCIA DE AUDITORIA

Informações recolhidas da unidade auditada tais como: registros, documentos escritos, impressos de computador, entrevistas e observações.

2.5.9 *EXPLOIT*

Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.

2.6 LETRA F

2.6.1 FALSA IDENTIDADE

Ato onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como, por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

2.6.2 *FIREWALL*

Um sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes.

2.6.3 *FREEWARE*

Software distribuído em regime gratuito, mas segundo alguns princípios gerais como a impossibilidade de alteração de qualquer parte para posterior distribuição, impossibilidade de venda, etc.

2.7 LETRA G

2.7.1 GESTÃO DE MUDANÇAS

Processo de gerenciamento de mudanças em sistemas operacionais, serviços, sistemas, aplicativos e outros.

2.7.2 GESTÃO DE RISCOS

Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos..

2.7.3 GESTOR DE SEGURANÇA DA INFORMAÇÃO

É O Chefe da Assessoria de Segurança de Sistemas de Informação responsável pelas ações de segurança da informação no âmbito do DECEA e está ligado hierarquicamente ao Diretor Geral do DECEA.

2.7.4 GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

A Governança da Segurança da Informação contribui para alcançar o alinhamento estratégico das atividades de segurança da informação com objetivos de negócio do DECEA, atribuindo responsabilidade e capacidade de tomada de decisão, bem como respeitando as leis e regulamentos.

2.7.5 GRAU DE SIGILO

Gradação atribuída a dados, informações, áreas ou instalações considerados sigilosos em decorrência de sua natureza ou conteúdo, que são: ultra-secreto, secreto, confidencial e reservado.

2.8 LETRA H

2.8.1 *HACKER*

Indivíduo com profundos conhecimentos de sistemas operacionais, linguagens de programação, técnicas e ferramentas que potencializam as tentativas de acesso indevido. Comumente buscam mais conhecimento e evitam corromper informações intencionalmente.

2.8.2 HTML

Do Inglês HyperText Markup Language. Linguagem universal utilizada na elaboração de páginas na Internet.

2.8.3 HTTP

Do Inglês *HyperText Transfer Protocol*. Protocolo usado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o navegador de internet).

2.8.4 HTTPS

Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

2.9 LETRA I

2.9.1 IDS

Do Inglês *Intrusion Detection System*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

2.9.2 IMPACTO

Abrangência dos danos causados por um incidente de segurança da informação sobre um ou mais processos de negócio.

2.9.3 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar à perda dos princípios de segurança da informação.

2.9.4 INFORMAÇÃO

Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos ou máquinas em processos comunicativos ou transacionais. A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvos de proteção da segurança da informação.

2.9.5 *IP SPOOFING*

No contexto de redes de computadores, IP spoofing é uma técnica de subversão de sistemas informáticos que consiste em mascarar (spoof) pacotes IP utilizando endereços de remetentes falsificados.

2.9.6 *ISO/IEC 15408* OU *COMMON CRITERIA*

Fornece conjunto de critérios fixos que permitem especificar a segurança de uma aplicação, de forma não ambígua, a partir de características do ambiente da aplicação e defini formas de garantir a segurança da aplicação para o usuário final.

2.9.7 INTEGRIDADE

Característica da informação de manter-se na mesma condição em que foi disponibilizada pelo seu proprietário.

2.9.8 INTERNET

Rede mundial de computadores, que compartilham diversos tipos de informação ao mesmo tempo.

2.9.9 INVASÃO

Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

2.9.10 INVASOR

Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

2.10 LETRA K

2.10.1 *KEYLOGGER*

Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

2.11 LETRA L

2.11.1 LEGALIDADE

"1º Conforme a lei. 2º Relativo à lei. 3º Prescrito pela lei".O uso da tecnologia da informação e comunicação deve estar de acordo com as leis vigentes no local ou país.

2.11.2 LEGITIMIDADE

Asseveração de que o emissor e o receptor de dados ou informações são legítimos e fidedignos tanto na origem quanto no destino.

2.11.3 LISTA DE VERIFICAÇÃO

Questionário estruturado ou Plano de Trabalho para orientar e auxiliar os auditores nos testes das Organizações Militares a serem auditadas.

2.11.4 *LOG*

Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

2.11.5 *LOGIN*

Identificação de um utilizador perante um computador. Fazer o *login* é o ato de dar a sua identificação de utilizador ao computador ou sistema de informação.

2.12 LETRA M

2.12.1 MATERIAL SIGILOSO

É toda matéria, substância ou artefato que, por sua natureza, deva ser de conhecimento restrito.

2.12.2 MATURIDADE

Capacidade de uma organização definir, gerenciar, medir, controlar e verificar a eficácia de seus processos.

2.12.3 MEDIDAS ESPECIAIS DE SEGURANÇA

Medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações sigilosos. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais a esses dados e informações.

2.12.4 MEMÓRIA

Área de armazenamento de programas que estão sendo executados ou ainda serão executados pelo computador.

2.12.5 MP3

Tecnologia que permite a compressão de músicas em até 1/11 do seu tamanho original sem perda significativa de qualidade.

2.13 LETRA N

2.13.1 NECESSIDADE DE CONHECER

Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa, possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos.

2.13.2 NEGAÇÃO DE SERVIÇO

Atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

2.13.3 NEGÓCIO

Atividade fim de uma organização.

2.13.4 *NOTEBOOK*

Computador portátil.

2.14 LETRA O

2.14.1 OBSEVAÇÃO DE AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

Recomendação da auditoria opcional ou consultiva que tem objeto de melhorar o processo avaliado.

2.14.2 OSTENSIVO

Sem classificação, cujo acesso pode ser franqueado.

2.15 LETRA P

2.15.1 PAPÉIS DE TRABALHO DOS AUDITORES

Documentos escritos, gravações e qualquer outra evidência gerada pelos auditores durante a auditoria, incluindo a lista de verificação.

2.15.2 PARTES EXTERNAS

São os ativos de informação que estão no mundo externo ao DECEA.

2.15.3 *PATCHES*

Um *patch* é um programa criado para atualizar ou corrigir um *software*.

2.15.4 PDA

Minicomputadores de bolso usados para armazenar informações de estações de trabalho e editá-las para posteriormente serem sincronizadas com a estação.

2.15.5 PGP

Do Inglês *Pretty Good Privacy*. Programa que implementa criptografia de chave única, de chave pública e privada e assinatura digital. Possui versões comerciais e gratuitas.

2.15.6 *PHISHING*

Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros.

Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

2.15.7 PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Documento que visa à redução de impacto de incidente ou desastre no processo produtivo de determinada organização. O sucesso de sua aplicação pode influir diretamente na continuidade da instituição.

2.15.8 PLANO DE AUDITORIA

Planejamento da auditoria, contemplado datas, envolvidos, unidades e auditores.

2.15.9 PLANO DE COMUNICAÇÃO DE MUDANÇA

Definição da forma de comunicação e das pessoas que devem ser alertadas de alguma mudança.

2.15.10 PLANO DE CONTINGÊNCIA (PCG)

Documento que descreve os procedimentos e as capacidades necessárias para recuperar uma aplicação computadorizada específica ou um sistema complexo. Foco em interrupções nos sistemas de TI com efeitos de curto prazo.

2.15.11 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O Plano de Continuidade de Negócios é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento do DECEA e de suas Organizações Subordinadas no contexto das atividades previstas por sua missão. Sob o ponto de vista do Plano de Continuidade de Negócios, o funcionamento do DECEA se refere a dois condicionantes: aos ativos e aos processos.

O Plano de Continuidade de Negócios é constituído pelos seguintes planos: Plano de Administração de Crises (PAC), Plano de Recuperação de Desastres (PRD), Plano de Continuidade Operacional (PCO) e Planos de Contingência (PCG). Todos estes planos têm como objetivo principal formalizar as ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio do DECEA e de suas Organizações Subordinadas sejam afetados.

2.15.12 PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Descreve o desenvolvimento de ações para garantir a continuidade operacional do DECEA ou de suas Organizações Militares subordinadas, considerando situações de desastre e de contingência.

2.15.13 PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Documento que descreve procedimentos detalhados necessários para dar continuidade às operações do DECEA ou de uma de suas Organizações Militares Subordinadas, considerando terem sido destruídos ou ficarem inacessíveis a sua infraestrutura computacional, facilidades principais ou uma combinação de ambos.

2.15.14 PLANO DE RESTAURAÇÃO

Documento que indique os passos que devem ser realizados para recuperação de um ativo em caso de falha.

2.15.15 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento aprovado pelo Diretor Geral do DECEA, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação no âmbito do DECEA e suas Organizações Militares subordinadas.

2.15.16 PROCESSO

Conjunto de atividades logicamente estruturadas de modo a transformar uma entrada em uma saída. Além disso, a interpretação aplicável para o caso dos Planos de

Continuidade é a de que processos são as atividades realizadas para operar e garantir o cumprimento da missão do DECEA.

2.15.17 PROTETOR DE TELA

Programa que impede a visualização do conteúdo mostrado no monitor, após um determinado período de tempo. Pode ainda restringir ou não o acesso ao computador ao término deste período.

2.15.18 P2P

Acrônimo para *peer-to-peer*. Arquitetura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, onde alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.

2.15.19 *PROXY*

Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte a Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

2.15.20 PROGRAMAÇÃO DA AUDITORIA

Diário das auditorias planejadas por Organização Militar.

2.16 LETRA Q

2.16.1 QUEBRA DE SEGURANÇA DA INFORMAÇÃO

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

2.17 LETRA R

2.17.1 RECOMENDAÇÃO DE AUDITORIA

Ação corretiva que se propõe a abordar um ou mais itens de auditoria identificados, que devem ser abordados antes da certificação ou recertificação do SGSI.

2.17.2 REDE SEM FIO

Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

2.17.3 RELATÓRIO DE AUDITORIA

Relatório formal com os principais resultados e conclusões da auditoria.

2.17.4 RESILIÊNCIA

Capacidade concreta de retornar ao estado natural, superando uma situação crítica.

2.17.5 RECLASSIFICAÇÃO

Alteração, pela autoridade competente, da classificação de dado, informação, área ou instalação sigilosos.

2.17.6 RISCO

Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, de integridade e de disponibilidade nos ativos de informação, causando, possivelmente, impactos ao negócio.

2.17.7 RISCO DE AUDITORIA

Potencial de uma auditoria não cumprir os seus objetivos, por exemplo, pelo uso de informações não confiáveis, incompletas ou imprecisas.

2.17.8 *ROOTKIT*

Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

2.18 LETRA S

2.18.1 *SCAN*

Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores.

2.18.2 *SCANNER*

Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

2.18.3 *SCREENLOGGER*

Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

2.18.4 *SECURITY OFFICER*

Profissional responsável pela segurança das informações de uma organização. Deve conhecer bem o negócio da organização, ter bom relacionamento com os colaboradores e trânsito livre junto às chefias.

2.18.5 SEGURANÇA DA INFORMAÇÃO

Preservação da confidencialidade, da integridade e da disponibilidade da informação. Adicionalmente, podem ser requeridas outras propriedades tais como: autenticidade, responsabilidade, não repúdio e confiabilidade.

2.18.6 SENHA

Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

2.18.7 SENHA ADMINISTRATIVA

Associadas às tarefas de manutenção e administração de sistemas e ambientes computacionais, que permite um acesso irrestrito a um computador, aplicativo e etc.

2.18.8 SENHA NÃO-ADMINISTRATIVA

São utilizadas para as atividades rotineiras e sem os privilégios de acesso concedidos às tarefas de manutenção e administração de sistemas

2.18.9 SIGILO

Segredo; de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada.

2.18.10 SISTEMAS CRÍTICOS

Sistema de informação em que a falha pode causar graves consequências humanas, econômicas ou de imagem para o DECEA.

2.18.11 SISTEMAS DE INFORMAÇÃO

Sistema de informação é a expressão utilizada para descrever um sistema, seja ele automatizado (que pode ser denominado como Sistema de Informação Computadorizado), seja ele manual, que abrange pessoas, máquinas, ou métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário ou cliente.

2.18.12 *SITE*

Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

2.18.13 *SHAREWARE*

Software que é distribuído livremente, desde que seja mantido o seu formato original, sem modificações, e seja dado o devido crédito ao seu autor. Normalmente, foi feito para ser testado durante um curto período de tempo (período de teste/avaliação) e, caso seja utilizado, o utilizador tem a obrigação moral de enviar o pagamento ao seu autor (na ordem de algumas - poucas - dezenas de dólares). Quando é feito o registro, é normal receber-se um manual impresso do programa, assim como uma versão melhorada, possibilidade de assistência técnica e informações acerca de novas versões.

2.18.14 SNIFFERS

Espécie de programa que tem por função capturar todo o tráfego que circula em uma rede local. Muito usado por administradores de rede para resolução de problemas e por *Hackers* para obter informações ilicitamente.

2.18.15 *SOFTWARE*

Programa de computador, parte lógica do computador. São os programas que fazem o computador funcionar ou realizam uma função específica.

2.18.16 *SOFTWARE* ANTIVÍRUS

Programa de computador que realiza a detecção e remoção de vírus de computador.

2.18.17 SPAM

Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*).

2.18.18 *SPAMMER*

Pessoa que envia *spam*.

2.18.19 SMS

Do Inglês *Short Message Service.* Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS permite apenas dados do tipo texto e cada mensagem são limitados em 160 caracteres alfanuméricos.

2.18.20 SSH

Do Inglês *Secure Shell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

2.18.21 SSID

Do Inglês *Service Set Identifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

2.18.22 SSL

Do Inglês *Secure Sockets Layer*. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Veja também HTTPS.

2.18.23 *SWITCH*

Equipamento de conectividade de rede, com capacidade de comutação em alta velocidade entre as portas, possibilitando a utilização de toda a banda disponível para a comunicação entre dois equipamentos.

2.19 LETRA T

2.19.1 TESTE DE AUDITORIA

Verificação realizada pelos auditores para verificar se um controle é eficaz e adequado para mitigar um ou mais riscos para a organização.

2.19.2 TECNOLOGIA DA INFORMAÇÃO (TI)

Conjunto formado por recursos humanos técnicos especializados, processos, serviços, infraestrutura tecnológica e recursos computacionais, que é empregado na geração, armazenamento, veiculação, processamento, reprodução e uso da informação pelo DECEA e OM subordinadas.

2.19.3 *TOKENS*

Pequenos dispositivos eletrônicos que geralmente armazenam um certificado digital de forma que a posse do dispositivo por uma pessoa autorizada possa garantir a sua autenticidade em transações eletrônicas

2.19.4 TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

É o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

2.19.5 TRATAMENTO DO RISCO

Processo de seleção e implantação de medidas para modificar um risco.

2.20 LETRA U

2.20.1 URL

Do Inglês *Universal Resource Locator*. Seqüência de caracteres que indica a localização de um recurso na Internet, como por exemplo, http://decea.gov.br/.

2.20.2 USUÁRIO

Alguma pessoa que interagir diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.

2.21 LETRA V

2.21.1 VAZAMENTO

É a divulgação não autorizada de conhecimento e/ou dado sigiloso.

2.21.2 VISITA

Pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa.

2.21.3 VÍRUS

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

2.21.4 VPN

Do Inglês *Virtual Private Network*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

2.21.5 VULNERABILIDADE

Fragilidade (presente ou associada) de ativos que manipulam ou processam informações que, uma vez explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação.

2.22 LETRA W

2.22.1 *WEBMAIL*

Sistema *web* que permite o usuário acessar sua caixa postal de e-mail a partir de um navegador de Internet.

2.22.2 *WEP*

Do Inglês *Wired Equivalent* Privacy. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

2.22.3 *WI-FI*

Do Inglês *Wireless Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

2.22.4 *WIRELESS*

Rede sem fio.

2.22.5 *WORLD WIDE WEB*

Rede de alcance mundial também conhecida como *web* e WWW é um sistema de documentos em hipermídia que são interligados e executados na Internet.

2.22.6 *WORM*

Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

2.22.7 *WLAN*

Do Inglês *Wireless Local-Area Network*. Refere-se a um tipo de rede que utiliza ondas de rádio de alta freqüência, ao invés de cabos, para a comunicação entre os computadores.

2.22.8 *WPA*

Do Inglês *Wi-Fi Protected Access*. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Esta tecnologia foi projetada para, através de atualizações de *software*, operar com produtos *Wi-Fi* que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica**.** Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica, de 2006: **RCA 205-1**. [Rio de Janeiro], 2006.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano Diretor de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo*: **PCA 7-14**. [Rio de Janeiro], 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo*: **PCA 7-11**. [Rio de Janeiro], 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27001. *Tecnologia da Informação – Sistemas de gestão de segurança da informação – Requisitos*. 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. Tecnologia da Informação – Código de Práticas para a Gestão da Segurança da Informação. 2005.