

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



TECNOLOGIA DA INFORMAÇÃO

MCA 7-1

**GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO
DO DEPARTAMENTO DE CONTROLE DO ESPAÇO
AÉREO**

2023

**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**

2023



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

PORTARIA DECEA Nº 745/DGCEA, DE 14 DE FEVEREIRO DE 2023.
Protocolo COMAER nº 67600.002903/2023-31

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

**O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO
ESPAÇO AÉREO**, de conformidade com o previsto no art. 21, inciso I, da Estrutura
Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 11.237, de 18 de outubro
de 2022, e considerando o disposto no art. 10, inciso IV, do Regulamento do DECEA,
aprovado pela Portaria nº 2.030/GC3, de 22 de novembro de 2019, resolve:

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

Art. 2º Revogar a Portaria DECEA nº 4/SDTE, de 16 de março de 2012,
publicada no Boletim do Comando da Aeronáutica nº 63, de 30 de março de 2012.

Art. 3º Este Manual entra em vigor em 1º de março de 2023.

(a)Ten Brig Ar ALCIDES TEIXEIRA BARBACOV
Diretor-Geral do DECEA

(Publicado no BCA nº , de de 2023.)

SUMÁRIO

1	DISPOSIÇÕES PRELIMINARES	9
1.1	<u>FINALIDADE</u>	9
1.2	<u>ÂMBITO</u>	9
2	GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO.....	10
2.1	<u>LETRA A</u>	10
2.2	<u>LETRA B</u>	15
2.3	<u>LETRA C</u>	17
2.4	<u>LETRA D</u>	23
2.5	<u>LETRA E</u>	26
2.6	<u>LETRA F</u>	28
2.7	<u>LETRA G</u>	29
2.8	<u>LETRA H</u>	30
2.9	<u>LETRA I</u>	32
2.10	<u>LETRA J</u>	35
2.11	<u>LETRA K</u>	35
2.12	<u>LETRA L</u>	35
2.13	<u>LETRA M</u>	36
2.14	<u>LETRA N</u>	38
2.15	<u>LETRA O</u>	40
2.16	<u>LETRA P</u>	41
2.17	<u>LETRA Q</u>	45
2.18	<u>LETRA R</u>	45
2.19	<u>LETRA S</u>	47
2.20	<u>LETRA T</u>	51
2.21	<u>LETRA U</u>	52
2.22	<u>LETRA V</u>	53
2.23	<u>LETRA W</u>	54
2.24	<u>LETRA X</u>	55
2.25	<u>LETRA Z</u>	55
2.26	<u>NÚMERO 2</u>	56
2.27	<u>NÚMERO 3</u>	56
	REFERÊNCIAS	57

PREFÁCIO

Esta publicação tem como objetivo fornecer ao Departamento de Controle do Espaço Aéreo os termos, conceitos, palavras, vocábulos e expressões mais 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.

Para maior facilidade no manuseio deste manual, os termos, conceitos, palavras, vocábulos e expressões aqui contidos foram dispostos, respectivamente, em ordem alfabética e em números inteiros de ordem crescente para facilitar o manuseio deste manual.

Por fim, cabe ressaltar que este Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo está em consonância com a Portaria nº 93 GSI/PR, de 18 de outubro de 2021, o qual sempre deverá ser revisado e atualizado quando 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 AAA

Sigla que representa autenticação, autorização e auditoria.

2.1.2 AC

Sigla que representa autoridade certificadora.

2.1.3 AC-RAIZ

Sigla que representa autoridade certificadora raiz.

2.1.4 ACESSO FÍSICO

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

2.1.5 ACESSO LÓGICO

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

2.1.6 ACL

Sigla que representa uma lista de controle de acesso (*Access Control List*).

2.1.7 ACCOUTABILITY

Conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações.

2.1.8 ACEITAÇÃO DO RISCO

É a decisão de conviver com as consequências, caso um cenário de risco se materialize.

2.1.9 ADMINISTRADOR DE REDE

Pessoa física que tem como atribuição principal o gerenciamento da rede local da Unidade/Órgão, bem como dos recursos computacionais a ela conectados direta ou indiretamente.

2.1.10 ADVANCED ENCRYPTION STANDARD (AES)

Algoritmo de criptografia de chave simétrica escolhido em 1997 como padrão pelo NIST (*National Institute of Standards and Tecnology*) e que se tornou o padrão efetivo do governo federal americano em 2002. O AES (*Advanced Encryption Standard*), como

passou a ser chamado, trabalha com blocos de dados de 128 bits e pode utilizar chaves de 128, 192 e 256 bits.

2.1.11 ADVERTISING SOFTWARE (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.

2.1.12 ALERTA

É o resultado da correlação de milhões de logs, o alerta é um potencial incidente. É necessário passar por uma triagem para excluir os falsos positivos e identificar os reais incidentes que devem ser tratados.

2.1.13 ALTA ADMINISTRAÇÃO

Corpo dos dirigentes máximos da organização com poderes para estabelecer as políticas, os objetivos e a direção geral da organização.

2.1.14 AMBIENTE EXTERNO

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

2.1.15 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, conseqüentemente, causando impactos aos negócios de uma organização.

2.1.16 AMEAÇAS AVANÇADAS PERSISTENTES (APTS)

Referem-se a uma categoria de ameaças associadas a violações cibernéticas, cujos autores perseguem e comprometem os alvos escolhidos de maneira agressiva. As APTs ocorrem muitas vezes em campanhas, uma série de tentativas fracassadas, ou bem-sucedidas, com o objetivo de atingir um alvo em ambiente de rede protegido e, portanto, não são incidentes isolados. Além disso, embora o malware seja usado normalmente como ferramenta de ataque, a ameaça real consiste no envolvimento de operadores humanos que podem adaptar, ajustar e aprimorar os seus métodos com base nas defesas das vítimas.

2.1.17 ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

É um processo usado para avaliar e mapear as atividades e recursos que possam ser afetados nos órgãos ou entidades da administração pública em cenários de desastres. Visa entender o impacto causado, identificar o tempo tolerável de interrupção, calcular a infraestrutura de contingência mínima, bem como definir as prioridades de recuperação, a fim de subsidiar o desenvolvimento de estratégias para minimizar os riscos.

2.1.18 ANÁLISE DE INCIDENTES

Visa identificar as causas dos incidentes, incluindo artefatos e outras evidências relacionadas ao evento. O objetivo dessa análise é identificar o escopo do incidente, sua extensão, sua natureza e os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação por meio de um Plano de Análise de Incidente a partir do momento que foi identificado um incidente de segurança da informação.

2.1.19 ANÁLISE DE RISCO

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

2.1.20 ANÁLISE DE TRÁFEGO

Consiste no atacante monitorar passivamente transmissões para identificar padrões de comunicação e de comportamento do usuário.

2.1.21 ANÁLISE DE VULNERABILIDADES

Consiste na avaliação e identificação de falhas e potenciais ameaças de segurança numa infraestrutura tecnológica.

2.1.22 AP

Sigla oriunda do Inglês *Access Point*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede cabeada.

2.1.23 APETITE AO RISCO

Nível de risco que uma organização está disposta a aceitar.

2.1.24 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.

2.1.25 ARP SPOOFING

Ataque também conhecido como envenenamento das tabelas ARP, ou *ARP Poisoning*, no qual o atacante inunda a rede com pacotes ARP que contém informação maliciosa, associando seu endereço MAC ao IP do equipamento da vítima e recebendo qualquer pacote direcionado para ele, podendo realizar modificações e novos envios praticamente sem ser detectado.

2.1.26 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.

2.1.27 ARTEFATO MALICIOSO

Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores.

2.1.28 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.

2.1.29 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.

2.1.30 ASSUNTO SIGILOSO

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

2.1.31 ATACANTE

Pessoa responsável pela realização de um ataque.

2.1.32 ATAQUE

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

2.1.33 ATAQUE DE SENHA

A utilização de senhas relativamente simples facilita a quebra de senhas por *hackers*, que possibilitam o acesso a redes e sistemas.

2.1.34 ATIVIDADE MALICIOSA

Qualquer atividade que infrinja a política de segurança de um órgão ou entidade da administração pública ou que atente contra a segurança de um sistema.

2.1.35 ATIVO

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

2.1.36 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.

2.1.37 ATIVO DE REDE

Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores, como roteadores e *switches*.

2.1.38 ATIVO DE SERVIÇO

Qualquer recurso ou conhecimento que pode contribuir para a entrega de um serviço de Tecnologia da Informação e Comunicações.

2.1.39 AUDITORIA BASEADA EM RISCO

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

2.1.40 AUDITORIA DE CONFORMIDADE

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

2.1.41 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.

2.1.42 AUDITORIA DO SGSI

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

2.1.43 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.

2.1.44 AUTORIDADE CERTIFICADORA (AC)

Entidade responsável por emitir e gerenciar certificados digitais.

2.1.45 AUTORIDADE CERTIFICADORA RAIZ (AC-RAIZ)

Situa-se no topo da hierarquia da cadeia de certificação, portanto sendo a primeira autoridade. Sua função é executar as normas técnicas e operacionais e as políticas de certificados estabelecidas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP). Isso significa que a AC-Raiz pode emitir, distribuir, expedir, revogar e gerenciar os certificados das autoridades que estão abaixo de seu nível hierárquico, que são as autoridades certificadoras. A autoridade certificadora raiz da ICP Brasil é o Instituto Nacional de Tecnologia da Informação (ITI).

2.1.46 AUTORIDADE DE REGISTRO (AR)

Estabelece a interface entre o usuário e a autoridade certificadora (AC). A AR vincula-se à AC e tem como principal objetivo ser o intermediário presencial entre a AC e o interessado pelo certificado digital, recebendo, validando e encaminhando as solicitações de emissão ou revogação dos certificados digitais, além de identificar os solicitantes de certificados digitais de forma presencial.

2.1.47 AVALIAÇÃO DE IMPACTO DE MUDANÇA

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

2.1.48 AVALIAÇÃO DE RISCOS

Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

2.2 LETRA B

2.2.1 *BACKDOOR*

É geralmente uma porta de acesso não documentada que permite ao administrador entrar no sistema, solucionar problemas ou fazer manutenção. Alguns *backdoors* são deliberadamente e amplamente conhecidos, como fornecer ao fabricante uma maneira de restaurar as senhas dos usuários. Em outras situações, *backdoors* podem ser usados para acessar um sistema infectado e seu controle remoto, como forma de permitir que o atacante modifique ou exclua arquivos, execute programas, distribua uma quantidade massiva de e-mails ou instale outras ferramentas maliciosas.

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 BACKUP COMPLETO

É um ponto de partida para outros tipos de backup. Ele faz a cópia completa de todos os arquivos, pastas ou volumes para destinos estabelecidos como servidores, sistemas de discos ou fitas como tapes LTO e *autoloaders*.

2.2.4 BACKUP DIFERENCIAL

Cópia realizada depois de um *backup* completo ou outro diferencial. Inicialmente é feito após o backup completo e realiza apenas cópia dos arquivos já alterados em sua primeira execução. Na segunda realização, ele faz o armazenamento dos documentos que foram alterados após o último backup completo, mais os arquivos modificados depois do primeiro diferencial.

2.2.5 BACKUP INCREMENTAL

Cópia realizada depois de um *backup* completo ou outro incremental. Inicialmente é feito após o backup completo e realiza apenas a cópia dos arquivos já alterados em sua primeira execução. Na segunda realização, ele faz o armazenamento dos documentos que apenas foram alterados após o último backup incremental. Com isso, o *backup* incremental é mais rápido e demanda menos espaço de armazenamento.

2.2.6 BASELINE DE SEGURANÇA

O conjunto de controles mínimos de segurança definidos para um sistema de informações de baixo impacto, impacto moderado ou alto impacto.

2.2.7 BIA (BUSINESS IMPACT ANALYSIS)

Vide ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA).

2.2.8 BIBLIOTECA DE SOFTWARE

É um conjunto de rotinas, que já podem ser compiladas e prontas para serem utilizadas pelos programas. As bibliotecas são salvas em arquivos semelhantes ou mesmo idênticos aos arquivos de programa, na forma de uma coleção de arquivos de código-objeto agrupados com um índice para fácil recuperação de cada rotina.

2.2.9 BIG DATA

Conjuntos de dados extremamente amplos e que, por este motivo, necessitam de ferramentas especialmente preparadas para lidar com grandes volumes, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil.

2.2.10 BIOMETRIA

Verificação da identidade de um indivíduo por meio de uma característica física.

2.2.11 BLACKLIST

Lista de itens aos quais é negado o acesso a certos recursos, sistemas ou protocolos.

2.2.12 BLINDAGEM

Também chamada de *hardening*, trata-se de um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco em infraestrutura, com o principal objetivo de torná-la preparada para enfrentar tentativas de ataque.

2.2.13 BLUETOOTH

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

2.2.14 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.

2.2.15 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.

2.2.16 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.

2.2.17 BRING YOUR OWN DEVICE (BYOD)

Trata-se de uma política de segurança de uma organização, que permite que os dispositivos pessoais dos funcionários sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa.

2.2.18 BUFFER OVERRUN/OVERFLOW

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

2.2.19 BUG BAR

É usada para definir os limites de severidade das vulnerabilidades de segurança, por exemplo: nenhuma vulnerabilidade conhecida na aplicação com uma classificação “crítica” ou “importante” no momento da liberação.

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 CHAVE CRIPTOGRÁFICA

Valor que trabalha com um algoritmo criptográfico para cifração ou decifração.

2.3.5 CHECKSUM

Verificar se um arquivo é exatamente o mesmo arquivo depois de uma transferência, ou seja, se não foi alterado por terceiros ou se não está corrompido.

2.3.6 CIFRAÇÃO

Ato de codificar sinais de linguagem em claro, mediante uso de algoritmo criptográfico simétrico ou assimétrico, com o intuito de transformá-los em sinais ininteligíveis para pessoas não autorizadas a conhecê-la.

2.3.7 CLASSIFICAÇÃO

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

2.3.8 CLI

A sigla em inglês *command-line interface* (CLI), tradução para Interface de Linha de Comando. É um programa que funciona através de linhas de comando de texto dando instruções a um computador para fazer funções específicas.

2.3.9 CLICKJACKING

Técnica maliciosa em que uma vítima é induzida a clicar em URL, botão ou outro objeto de tela que ela não tenha percebido e nem pretendido clicar. O *clickjacking* pode ser realizado de muitas maneiras, uma delas seria carregar uma página *web*, de forma transparente, atrás de outra página visível, de forma que os *links* e objetos para clicar são apenas fachadas, ou seja, quando o usuário clicar em um *link* aparentemente óbvio, ele, na verdade, estará selecionando o *link* de uma página oculta.

2.3.10 CLOUD BROKER

É uma empresa ou indivíduo que atua como um agente intermediário entre um provedor de serviços na nuvem e um cliente final. O Cloud Broker busca identificar qual será o uso do ambiente e o espaço necessário de armazenamento para o cliente. Ele faz uma consultoria e disponibiliza um serviço customizado de infraestrutura utilizando recursos dos melhores fornecedores do mercado;

2.3.11 CLOUD JACKING

Forma de ataque cibernético em que *hackers* se infiltram nos programas e nos sistemas armazenados em ambiente de computação em nuvem, a fim de utilizar esses recursos para minerar criptomoedas.

2.3.12 CLOUD SECURITY ALLIANCE (CSA)

Uma das principais organizações do mundo dedicada à definição e conscientização das melhores práticas, com a finalidade de ajudar a garantir um ambiente seguro de computação em nuvem, por meio de trabalhos de pesquisa, educação, eventos e produtos específicos para segurança em nuvem. Ela também opera um dos programas mais populares de certificação de provedor de segurança na nuvem, o *CSA security, trust and assurance registry* (STAR).

2.3.13 CMDB (CONFIGURATION MANAGMENT DATA BASE)

Tradução para Banco de Dados de Gerenciamento de Configuração. É um banco de dados que ajuda a gerenciar os ICs. Ele armazena registros de configuração dos ICs, incluindo atributos como: tipo, proprietário, versão, *status* etc., e seus relacionamentos com outros ICs.

2.3.14 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 troia, *rootkits*, etc.

2.3.15 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

2.3.16 COMITÊ GESTOR DA ICP BRASIL

Vinculado à Casa Civil da Presidência da República, possui como principal competência determinar as políticas que a AC-Raiz executará. É composto por cinco representantes da sociedade civil, integrantes de alguns setores afetos ao tema e representantes de órgãos da administração pública federal.

2.3.17 COMMON CRITERIA

Norma internacional (ISO/IEC 15.408, 2009) que fornece uma base de critérios comuns para a avaliação das propriedades de segurança de produtos e sistemas de TI.

2.3.18 COMMON VULNERABILITIES AND EXPOSURES (CVE)

Sigla em inglês traduzido para Exposições e Vulnerabilidades Comuns (CVE), possui um número do CVE, que é um identificador usado por fornecedores como a Microsoft, RedHat e Adobe para catalogar vulnerabilidades individuais dos quais patches são providos como solução. Muitas vezes, novos ataques e explorações são documentados em um CVE

muito antes do fornecedor admitir o problema ou liberar uma atualização ou *patch* para resolver a situação. Estas exposições e vulnerabilidades, disponibilizadas e mantidas pela MITRE Corporation, podem ser acessadas pelo público no link <https://cve.mitre.org/>.

2.3.19 COMPUTAÇÃO EM NUVEM

É o fornecimento sob demanda de recursos de TI através da Internet. Em vez de usar softwares ou hardwares que estão no local, você usa tecnologia hospedada em um banco de dados remoto por meio de um provedor do serviço de nuvem.

2.3.20 CONEXÃO SEGURA

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

2.3.21 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.

2.3.22 CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

É o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização.

2.3.23 CONSCIENTIZAÇÃO

Atividade que tem por finalidade orientar os usuários da organização sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros.

2.3.24 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.

2.3.25 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.

2.3.26 CONTROLE DE ACESSO

Conjunto de procedimentos, recursos e meios utilizados com o objetivo de garantir a segurança de dados sigilosos, dos bens e das pessoas. impedindo assim, o acesso de pessoas não-autorizadas aos ambientes;

2.3.27 CÓPIAS DE SEGURANÇA

É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso de perda dos dados originais com o objetivo de manter a integridade e disponibilidade da informação e dos recursos de processamento de informação

2.3.28 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.

2.3.29 COVERT CHANNELS

Os *covert channels* são caminhos não previstos para conduzir fluxo de informações, mas que 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*.

2.3.30 CRACKER

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

2.3.31 CREDENCIAMENTO

É o ato de concessão de Credencial de Segurança.

2.3.32 CREDENCIAL DE SEGURANÇA

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

2.3.33 CRIME CIBERNÉTICO

Também conhecido como crime digital, informático ou cibercrime, é a atividade criminosa em que se utiliza de um computador ou uma rede de computadores como instrumento ou base de ataque para causar incidente, desastre cibernético ou obter lucro financeiro.

2.3.34 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.

2.3.35 CRIPTOGRAFIA ASSIMÉTRICA

Também conhecida como criptografia de chave pública, é qualquer sistema criptográfico que usa pares de chaves, sendo as chaves públicas, que podem ser divulgadas amplamente, e as chaves privadas, que são apenas conhecidas pelo proprietário. Este sistema realiza duas funções, a autenticação, em que a chave pública verifica se um portador da chave privada aparelhada enviou a mensagem; e encriptação, em que apenas o portador da chave privada aparelhada pode decryptar a mensagem encriptada com a chave pública. São exemplos de algoritmos assimétricos para esta implementação: RSA, ElGamal, DSS.

2.3.36 CRIPTOGRAFIA SIMÉTRICA

Criptografia que usa algoritmo com a mesma chave criptográfica para encriptação de texto puro e decryptação de texto cifrado. São exemplos de algoritmos simétricos: AES, Blowfish, TwoFish e 3DES.

2.3.37 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.

2.3.38 CROSS-SITE REQUEST FORGERY (CSRF)

Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o *cookie* da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação *Web* vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima (OWASP, 2013).

2.3.39 CROSS-SITE SCRIPTING (XSS)

Método de ataque que explora vulnerabilidades de *scripting* entre *sites*, que visa contornar controles de acesso, como a política de mesma origem. Ao injetar um *script* malicioso em uma entrada desprotegida ou não validada do navegador, o invasor faz com que o *script* seja devolvido pelo aplicativo e executado no navegador. Um ataque XSS bem-sucedido pode permitir ao invasor assumir o controle das funcionalidades do aplicativo, manipular dados ou implantar códigos maliciosos adicionais. Os ataques XSS também permitem que os invasores injetem *scripts* do lado do cliente, em páginas da *web* visualizadas por outros usuários.

2.3.40 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.

2.3.41 CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)

Sigla internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público-alvo específico;

2.3.42 CTIR.FAB

Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de computadores da Força Aérea Brasileira, subordinado ao Órgão Central do Sistema de Tecnologia da Informação (STI) do COMAER e mantido pelo Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER). (Fonte: ICA 7-42/2016 e DCA 11-130/2020).

2.3.43 CTIR GOV

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

2.3.44 CUSTÓDIA

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

2.3.45 CUSTODIANTE DA INFORMAÇÃO

Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação.

2.3.46 CVE

Sigla de *Common Vulnerabilities and Exposures*.

2.3.47 CVSS

Sigla de Common Vulnerability Scoring System, tradução para sistema comum de pontuação de vulnerabilidade.

2.4 LETRA D**2.4.1 DATA CENTER**

Local físico onde se concentram os computadores corporativos, rede, armazenamento e outros equipamentos de TI que dão suporte às operações de negócios.

2.4.2 DDoS

Da sigla em 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.

2.4.3 DECIFRAÇÃO

Ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

2.4.4 DEFACEMENT

É uma técnica que consiste na realização de modificações de conteúdo e estética de uma página da web.

2.4.5 DEEPFAKE

É uma tecnologia que usa inteligência artificial (IA) para criar vídeos falsos, mas realistas, de pessoas fazendo coisas que elas nunca fizeram na vida real. Esta técnica permite fazer montagens de vídeo com celebridades, bem como realizar discursos fictícios de políticos influentes.

2.4.6 DEEP WEB

Termo usado para denotar uma classe de conteúdo na Internet que, por várias razões técnicas, não é indexada pelos mecanismos de pesquisa.

2.4.7 DEFESA CIBERNÉTICA

É o conjunto de práticas que tem como objetivo proteger servidores, computadores, sistemas eletrônicos, redes, dispositivos e dados contra os ataques de pessoas mal-intencionadas que atuam no mundo virtual.

2.4.8 DESASTRE

Evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações, inclusive pela tomada de controle, destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

2.4.9 DESCARTE

Procedimento que tem por objetivo a eliminação correta de informações, documentos, mídias e acervos digitais.

2.4.10 DESCREDENCIAMENTO DE SEGURANÇA

Processo utilizado para desabilitar órgão ou entidade, pública ou privada, ou para revogar a credencial de pessoal natural, para o tratamento da informação classificada.

2.4.11 DIRETRIZ

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

2.4.12 DISPONIBILIDADE

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

2.4.13 DISCO RÍGIDO

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

2.4.14 DLT

Sigla de livro razão distribuído (*Distributed Ledger Techonology*).

2.4.15 DLP

Sigla de prevenção de perda de dados (*Data Loss Prevention*).

2.4.16 DMZ (*DEMILITARIZED ZONE*)

Sigla de zona desmilitarizada (*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.

2.4.17 DNS

Da sigla do Inglês *Domain Name System*. Serviço que traduz nomes de domínios para endereços IP e vice-versa;

2.4.18 DOCUMENTO SIGILOSO

É aquele que contém assunto classificado como sigiloso e que, portanto, requer medidas especiais de segurança para evitar a ocorrência de comprometimento.

2.4.19 DOCUMENTO SIGILOSO CONTROLADO

É aquele que, por sua importância, requer medidas adicionais de controle em relação aos documentos sigilosos.

2.4.20 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.

2.4.21 DoS

Da sigla em inglês *Denial of Service*. É um ataque a um sistema ou servidor ou rede de computadores, que tem por objetivo torná-lo inacessível. É um ataque feito por apenas um invasor que envia vários pacotes.

2.4.22 DOWNLOADS

É a transferência de arquivos de um computador para outro.

2.4.23 DROPPERS

São programas projetados para extrair outros arquivos de seu próprio código. Geralmente, esses programas extraem vários arquivos no computador para instalar um pacote de programas mal-intencionados. Além da extração de arquivos, os *droppers* podem possuir outras funções.

2.4.24 DUMP

Registro da estrutura de tabela e ou dados de um banco de dados e que normalmente está na forma de uma lista de declarações SQL.

2.5 LETRA E

2.5.1 EAVESDROPPING

Atacante passivamente monitora comunicações de rede de dados, incluindo credenciais de autenticação.

2.5.2 E-MAIL

Sigla de correio eletrônico (*Electronic MAIL*).

2.5.3 ELIMINAÇÃO

Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

2.5.4 ELOS DE COORDENAÇÃO DO STI

São setores pertencentes aos Órgãos de Direção-Geral, de Direção Setorial (ODGS) e aos Órgãos de Assistência Direta e Imediata ao Comandante da Aeronáutica, responsáveis pela coordenação de suas atividades de TI junto ao Órgão Central do STI.

2.5.5 ELOS ESPECIALIZADOS DO STI

São aqueles que, por atribuições regimentais ou por terem sido instituídos em ato específico, executam atividades ou serviços especializados de TI de interesse do COMAER.

2.5.6 ELOS DE SERVIÇOS DO STI

São setores de TI das OM do COMAER que executam atividades rotineiras de manutenção de TI, reportando-se aos seus respectivos Elos de Coordenação.

2.5.7 ELOS USUÁRIOS DO STI

São todos os militares e servidores civis que utilizam as ferramentas disponibilizadas pelo STI, nos seus locais de trabalho ou nas operações, para o tratamento das

informações de interesse do COMAER, tendo a sua autorização, credenciamento e apoio técnico, coordenadas pelos seus respectivos Elos de Serviço.

2.5.8 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.

2.5.9 ENDEREÇO IP

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

2.5.10 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.

2.5.11 ESCOPO DA AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

Partes da Organização Militar que serão auditadas.

2.5.12 ESTAÇÕES DE TRABALHO

Computadores destinados aos usuários.

2.5.13 ETIR

Sigla de Equipe de Tratamento de Resposta a Incidentes Cibernéticos. Este termo foi alterado pelo Decreto nº 10.641, de 2 de março de 2021, para denominação Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, que significa um 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.

2.5.14 EVENTO

Qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Pode também ser definida como qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente.

2.5.15 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.

2.5.16 EVIDÊNCIA DE AUDITORIA

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

2.5.17 EVITAR O RISCO

Forma de tratamento de risco, na qual a alta administração decide não realizar a atividade, não se envolver ou não agir, a fim de se retirar de uma situação de risco. Pode também ser definida como a eliminação da causa raiz do risco, implementando ações para levar a probabilidade do risco a zero.

2.5.18 EXFILTRAÇÃO DE DADOS

Movimento não autorizado de dados, também chamado de *data exfil*, exportação de dados, extrusão de dados, vazamento de dados e roubo de dados.

2.5.19 EXFIL

Vide exfiltração de dados.

2.5.20 EXPLOIT

Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador. Entre os tipos mais comuns de *exploits* estão o *SQL injection*, o *cross-site scripting*, o abuso de configuração de autenticação fraca e o abuso de falhas de configuração de segurança.

2.5.21 EXPLORAÇÃO DE DIA ZERO

É um ataque digital que faz uso das "Vulnerabilidades de Dia Zero" para instalar *software* malicioso em um dispositivo ou 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 FORÇA BRUTA

Método de quebra de senhas que utiliza uma lista de palavras, ou dicionário, que simplesmente faz a repetição de todas as combinações possíveis.

2.6.4 FORENSE DIGITAL

É um ramo da ciência forense que abrange a recuperação e investigação de material encontrado em dispositivos digitais, geralmente em relação a crimes computacionais.

2.6.5 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 CONTINUIDADE DE NEGÓCIOS

Processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.

2.7.2 GESTÃO DE INCIDENTES

Processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação.

2.7.3 GESTÃO DE MUDANÇAS

É o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do Órgão ou entidade da Administração Pública Federal, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

2.7.4 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.

2.7.5 GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação.

2.7.6 GESTÃO DE VULNERABILIDADES

Sistemática para obter informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliando a exposição da Organização Militar a estas vulnerabilidades e tomar as medidas apropriadas para lidar com os riscos.

2.7.7 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.

2.7.8 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.

2.7.9 GRAU DE SIGILO

Gradação atribuída a dados, informações, áreas ou instalações consideradas sigilosas em decorrência de sua natureza ou conteúdo, que são: ultrassecreto, secreto, confidencial e reservado.

2.7.10 GUERRA CIBERNÉTICA

Termo utilizado a conflitos que acontecem na esfera digital, onde armas e soldados dão lugar a *malwares* e *hackers*. Estes ataques buscam atingir variados setores digitais de seus adversários, como as estruturas financeiras, os controladores de infraestruturas públicas, como as usinas de energia, e as estruturas governamentais ou militares.

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 HARDENING

Também conhecido como blindagem, trata-se de um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco em infraestrutura, com o principal objetivo de torná-la preparada para enfrentar tentativas de ataque.

2.8.3 HASH

Resultado único e de tamanho fixo, gerado por uma função de resumo. O *hash* pode ser utilizado, entre outras possibilidades, para verificar a integridade de arquivos e gerar assinaturas digitais. Ele é gerado de forma que não é possível realizar o processamento inverso para recuperação da informação original. Além disso, qualquer alteração na informação original produzirá um *hash* distinto. Apesar de ser teoricamente possível que informações diferentes gerem *hashes* iguais, a probabilidade de isso ocorrer é bastante baixa.

2.8.4 HONEYPOT

É um sistema de computador configurado com o objetivo de atrair ciberataques, como uma emboscada. Ele emula um alvo para os *hackers* e usa suas tentativas de intrusão para obter informações sobre cibercriminosos e a maneira como eles estão operando ou para distraí-los de outros alvos. Existem dois tipos de *honeypots*: os de baixa interatividade e os de alta interatividade. Em um *honeypot* de baixa interatividade são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir; desta forma, o sistema operacional real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. Nos *honeypots* de alta interatividade, os atacantes interagem com sistemas operacionais, aplicações e serviços reais.

2.8.5 HOST

Um computador ou dispositivo de TI como, por exemplo, estação de trabalho, roteador, *switch*, *gateway* e *firewall*.

2.8.6 HOTSPOT

É o nome dado ao local onde a tecnologia de redes sem fio está disponível, onde é possível conectar-se à INTERNET, ou a qualquer outro tipo de rede, utilizando um equipamento portátil que esteja preparado para se comunicar em uma Rede sem Fio.

2.8.7 HTML

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

2.8.8 HTTP

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

2.8.9 HTTP GET E POST

O protocolo de transferência de hipertexto (HTTP) é projetado para permitir a comunicação entre clientes e servidores. Dois métodos comumente usados para uma solicitação entre um cliente e servidor são: GET e POST. GET é menos seguro comparado ao POST porque dados são enviados como parte da URL.

2.8.10 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 ICP-BRASIL

Sigla de infraestrutura de chaves públicas brasileira. É a cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais, para identificação virtual do cidadão.

2.9.2 IDE CVE

Identificação para um CVE específico (ver CVE).

2.9.3 IDS/IPS (INTRUSION DETECTION SYSTEM / INTRUSION PREVENTION SYSTEM)

Um IDS/IPS é um equipamento ou *software* que inspeciona o tráfego e procura assinaturas de ataques ou padrões de comportamento incomum. Um IDS alerta o administrador do sistema por *pager*, *e-mail*, ou telefone celular quando um evento que aparece na lista de eventos de segurança da empresa é acionado. Sistemas de prevenção de intrusão (IPS) iniciam contramedidas, tais como o bloqueio do tráfego quando um tráfego suspeito é detectado.

2.9.4 IMPACTO

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

2.9.5 IMPACTO DO RISCO

Reflete a severidade dos efeitos da ocorrência do risco nos objetivos da Organização, do Projeto ou da Atividade.

2.9.6 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.

2.9.7 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.

2.9.8 INFORMAÇÃO CLASSIFICADA

Informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo.

2.9.9 INCERTEZA

É a incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

2.9.10 INCIDENTE

Interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

2.9.11 INJEÇÃO SQL (SQL INJECTION)

É um tipo de ameaça que se aproveita de vulnerabilidades nos sistemas que interagem com bases de dados via SQL (*Structured Query Language*). Injeção de SQL ocorre quando o atacante consegue inserir uma série de instruções dentro de uma *query* através da manipulação das entradas de dados de uma aplicação.

2.9.12 INTEGRIDADE

Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

2.9.13 INTERNET

Sistema global de Redes de computadores interligadas que utilizam um conjunto próprio de protocolos (*Internet Protocol Suite* ou *TCP/IP*) com o propósito de servir progressivamente usuários no mundo inteiro.

2.9.14 INTERNET DAS COISAS (IoT)

Infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade. Vide Decreto nº 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas.

2.9.15 INTERNET PROTOCOL(IP)

Protocolo que permite o endereçamento e o transporte de pacotes de dados (datagramas) na Internet, sem, contudo, assegurar que estes pacotes sejam entregues;

2.9.16 INTEROPERABILIDADE

Característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.

2.9.17 INTRANET

Rede privada, acessível apenas aos membros da organização a que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta, por meio de firewalls.

2.9.18 INVASÃO

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

2.9.19 INVASOR

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

2.9.20 IOT

Sigla de Internet das coisas (*Internet of things*). É a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas, com dispositivos baseados em tecnologias da informação existentes e nas suas evoluções, com interoperabilidade, conforme disposto no Decreto nº 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas.

2.9.21 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.

2.9.22 IPS

Um Sistema de Prevenção de Intrusão é uma abordagem preventiva da segurança de rede, usada para identificar ameaças em potencial e responder rapidamente aos ataques.

2.9.23 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.

2.9.24 ITEM DE CONFIGURAÇÃO (IC)

São todos os componentes de TI e os serviços prestados com eles. Podem incluir computador, software, componentes de rede, servidores, documentação, procedimentos e todos os outros componentes de TI que a Organização utiliza.

2.10 LETRA J

2.10.1 JUICE JACKING

É um ataque cibernético em seu dispositivo móvel, onde um software malicioso é instalado nele, ou dados sensíveis é copiado a partir dele enquanto o dispositivo é carregado. Geralmente ocorre quando você tenta carregar seu dispositivo móvel em locais públicos, como aeroportos ou cafeterias. Esse tipo de ataque envolve cibercriminosos tentando enganar seu dispositivo e converter o cabo de carregamento USB simples em um cabo de compartilhamento de dados.

2.11 LETRA K

2.11.1 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.

2.11.2 KIT DE DESENVOLVIMENTO DE SOFTWARE (SDK)

Conjunto de ferramentas de desenvolvimento e de códigos pré-gravados, que podem ser usados pelos desenvolvedores para criar aplicativos. Geralmente, ajudam a reduzir a quantidade de esforço e de tempo que seria necessário para os profissionais escreverem seus próprios códigos.

2.12 LETRA L

2.12.1 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.

2.12.2 LEGITIMIDADE

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

2.12.3 LGPD

Sigla de Lei Geral de Proteção de Dados Pessoais.

2.12.4 LISTA DE CONTROLE DE ACESSO (ACL)

Sigla em inglês *Access Control List*. É uma lista que define as permissões de acesso de um usuário a um determinado componente ou serviço de um sistema, como um

arquivo ou diretório. Os roteadores e *firewalls* também fazem uso de listas de controle de acesso para a filtragem de pacotes de entrada e de saída.

2.12.5 LISTA DE BLOQUEIO

Vide *blacklist*.

2.12.6 LISTA DE VERIFICAÇÃO

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

2.12.7 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.

2.12.8 LOG DE AUDITORIA

Fornecem eventos no nível do sistema que mostram vários horários de início e término de processo do sistema, travamentos etc. São nativos dos sistemas e exigem menos configurações para ativarem.

2.12.9 LOG DE SISTEMA

Incluem eventos no nível do usuário, ou seja, quando um usuário faz login, acessa um arquivo etc.

2.12.10 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.

2.13 LETRA M

2.13.1 MAC

Significa *Media Access Control*, ou controle de acesso ao meio. É o endereço físico de 48 bits da estação, ou, mais especificamente, da interface de rede. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet.

2.13.2 MAIN-IN-THE-MIDDLE

É um ataque sofisticado e usualmente praticado em redes sem fio, pois não há a necessidade de atacante estar conectado a uma rede cabeada. Permite ainda ao atacante interceptar as comunicações entre um AP e um cliente, obtendo assim as credenciais de autenticação e dados.

2.13.3 MALVERSITING

Do inglês *malicious advertsing*. Tipo de golpe que consiste em criar anúncios maliciosos e, por meio de serviços de publicidade, apresentá-los em diversas páginas *Web*.

2.13.4 MALWARE

Denominação em inglês como *malicious software*, é qualquer software malicioso feito com a intenção de roubar dados ou causar danos a um computador, servidor, cliente, ou a uma rede de computadores. Entre os exemplos de *malware* estão os vírus, *worms*, *trojans* (ou cavalos de troia), *spyware*, *adware* e *rootkits*.

2.13.5 MÁQUINA VIRTUAL (VM)

São computadores de software com a mesma funcionalidade que os computadores físicos. Assim como os computadores físicos, elas executam aplicativos e um sistema operacional. Podemos dizer que a máquina virtual funciona como um computador dentro do computador.

2.13.6 MASQUERADING

O atacante se faz passar por um usuário autorizado para obter acesso a privilégios não autorizados.

2.13.7 MATERIAL SIGILOSO

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

2.13.8 MATRIZES DE INSTALAÇÃO

Arquivos executáveis e de configuração que, independentemente do meio de armazenamento (DVD-ROM, Flash Drives, Discos Rígidos etc.), são utilizados para a instalação de sistemas de software nos equipamentos de TI (computadores).

2.13.9 MATRIZ RACI

É uma ferramenta que possibilita aos membros da equipe visualizarem suas responsabilidades no ciclo de vida do projeto. A sigla RACI significa: R (*Responsible*), A (*Accountable*), C (*Consulted*) e I (*Informed*), em português: o Responsável, a Autoridade, o Consultado e o Informado.

2.13.10 MATRIZ DE RISCO

Ferramenta utilizada para avaliar os processos que envolvam riscos na organização, permitindo um enquadramento dos riscos dentro dos parâmetros estabelecidos.

2.13.11 MATURIDADE

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

2.13.12 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.

2.13.13 MELHORIA CONTÍNUA

É uma prática que as empresas adotam quando buscam ininterruptamente aperfeiçoar seus produtos, serviços e processos.

2.13.14 MEMÓRIA

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

2.13.15 METADADOS

Representam os dados sobre outros dados, onde as informações estruturadas descrevem e permitem localizar, gerenciar, controlar e preservar outras informações, ou seja, os dados ao longo do tempo. Todos os dados descritivos de um documento, físico ou digital, sobre autor, data de criação, local de criação, conteúdo, forma, dimensões e outras informações são metadados.

2.13.16 MFA

Sigla de autenticação de multifatores (*MultiFactor Authentication*).

2.13.17 MÍDIAS

Meios difundidos de cópias de segurança que incluem CD-ROM, DVD, disco rígido externo, fitas magnéticas, flash de memórias, *pendrives*, entre outros que porventura surjam com o avanço tecnológico.

2.13.18 MODIFICAÇÃO DE MENSAGEM

O atacante altera uma mensagem legítima, excluindo, adicionando ou alterando-a.

2.13.19 MUDANÇA

Transição ou alteração de uma situação atual.

2.14 LETRA N

2.14.1 NÃO CONFORMIDADE

Significa o quanto a organização não está adequada a normas, legislações, procedimentos e boas práticas, recomendáveis ou obrigatória. Significa o quanto a organização não está adequada a estes requisitos através da implantação, monitoramento e auditoria de controles.

2.14.2 NÃO REPÚDIO

Habilidade de provar a ocorrência de um evento ou ação e suas entidades originárias.

2.14.3 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.

2.14.4 NEGAÇÃO DE SERVIÇO (DoS)

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

2.14.5 NEGAÇÃO DE SERVIÇO DISTRIBUÍDA (DDoS)

Atividade maliciosa, coordenada e distribuída, em que um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

2.14.6 NEGÓCIO

Atividade fim de uma organização.

2.14.7 NORMALIZAR DADOS

Conjunto de regras que visa minimizar as anomalias no armazenamento e modificação dos dados, além de proporcionar maior flexibilidade na sua utilização. esses passos reduzem a redundância e a chance dos logs se tornarem inconsistentes quando forem analisados pela equipe responsável por identificar os incidentes de segurança da informação.

2.14.8 NOTEBOOK

Computador portátil.

2.14.9 NTP

Significa *Network Transfer Protocol* ou Protocolo de Tempo para Redes. É o padrão que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos a partir de referências de tempo confiáveis.

2.14.10 NUVEM COMUNITÁRIA

Infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos.

2.14.11 NUVEM HÍBRIDA

Infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações.

2.14.12 NUVEM PRIVADA (OU INTERNA)

Infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos.

2.15 LETRA O

2.15.1 OBSERVAÇÃO DE AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

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

2.15.2 ONE-TIME PASSWORD

Denominada de senha descartável, é a senha que é válida somente para uma sessão de *login* ou transação, em um sistema de computadores ou outros dispositivos digitais

2.15.3 ÓRGÃO CENTRAL DO STI

É a Diretoria de Tecnologia da Informação da Aeronáutica (DTI), ao qual compete: disciplinar a atividade-meio por intermédio de Normas de Sistemas do Comando da Aeronáutica (NSCA); suprir e manter os elos, no que se refere às necessidades para o funcionamento do sistema; administrar a atividade sistematizada; e fiscalizar a aplicação das legislações do STI pertinentes.

2.15.4 OSTENSIVO

Sem classificação, cujo acesso pode ser franqueado.

2.15.5 OWASP

A *Open Web Application Security Project* (OWASP) é uma entidade sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança de softwares aplicativos reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da Internet. Os estudos e documentos da OWASP são disponibilizados para toda a comunidade internacional, e adotados como referência por entidades como *U.S. Defense Information Systems Agency* (DISA), *U.S. Federal Trade Commission*, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo *PCI Council*.

2.15.6 OWASP TOP 10

O trabalho mais conhecido da OWASP é sua lista “The Top 10 Most Critical Web Application Security Risks” ou “OWASP TOP 10”, que reúne os riscos de ataque mais críticos exploráveis a partir de vulnerabilidades nas aplicações *Web*.

Atualizadas a cada três anos, estas listas ficam disponíveis no seguinte site:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

2.16 LETRA P

2.16.1 PAPÉIS DE TRABALHO DOS AUDITORES

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

2.16.2 PARTES EXTERNAS

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

2.16.3 PATCHES

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

2.16.4 PDA

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

2.16.5 PENTEST

Acrônimo de teste de penetração (*penetration test*).

2.16.6 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.

2.16.7 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.

2.16.8 PIN

Sigla de número de identificação pessoal (*Personal Identification Number*). É um número exclusivo, conhecido somente pelo usuário e pelo sistema, para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para realização de transações bancárias e em *chips* telefônicos.

2.16.9 PIVOTEAMENTO

Técnica usada pelos pen-testers que pretendem acessar o computador-alvo conectado a uma rede, porém não é diretamente acessível a partir da localização atual do atacante. Por exemplo, se um atacante invadir um servidor da Web em uma rede corporativa, o atacante poderá então utilizar o servidor da Web comprometido para atacar outros sistemas diferentes na rede, como um firewall.

2.16.10 PKI

Sigla de infraestrutura de chave pública (*public key infrastructure*).

2.16.11 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.

2.16.12 PLANO DE AUDITORIA

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

2.16.13 PLANO DE COMUNICAÇÃO DE MUDANÇA

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

2.16.14 PLANO DE CONTIGÊNCIA (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.

2.16.15 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.

2.16.16 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.

2.16.17 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.

2.16.18 PLANO DE RESTAURAÇÃO

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

2.16.19 PMTP (TEMPO MÁXIMO DE TOLERÂNCIA A PARALISAÇÃO)

Tempo máximo decorrido após o início de uma interrupção para que uma atividade seja reiniciada.

2.16.20 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.

2.16.21 PONTO DE RECUPERAÇÃO OBJETIVO (RPO)

Ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perde dados no caso de um incidente.

2.16.22 PORT SCAN

Denominada também de *port scanning*, é um processo de varredura para determinar quais portas em uma rede estão abertas e que podem estar recebendo ou enviando dados.

2.16.23 PREMISSAS

Fatores que, para fins de planejamento, são considerados verdadeiros, reais ou certos sem prova ou demonstração. Toda premissa tem um risco associado, pois, se não for válida, poderá causar impacto nos objetivos do projeto.

2.16.24 PREPARED STATEMENT

Um modelo de instrução usado, por exemplo, em consultas ou atualizações em SQL, no qual certos valores constantes são substituídos durante cada execução.

2.16.25 PREVENÇÃO DE PERDA DE DADOS (DLP)

Termo em inglês denominado *Data Loss Prevention* (DLP), é um conjunto de práticas e produtos que garantem que os dados confidenciais ou críticos de uma organização permaneçam disponíveis para os usuários autorizados e não sejam compartilhados ou disponibilizados para usuários não autorizados.

2.16.26 PROBABILIDADE DE OCORRÊNCIA DO RISCO

É a chance de ocorrência de um evento que pode afetar o alcance dos objetivos organizacionais.

2.16.27 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.

2.16.28 PROGRAMAÇÃO DA AUDITORIA

Diário das auditorias planejadas por Organização Militar.

2.16.29 PROPRIETÁRIO DAS INFORMAÇÕES

É o responsável pela autorização de acesso às informações, considerando as normas vigentes no DECEA.

2.16.30 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.

2.16.31 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*.

2.16.32 PSN

Sigla de provedor de serviço de nuvem.

2.16.33 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 implementado 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.

2.17 LETRA Q

2.17.1 QUEBRA DE SEGURANÇA DA INFORMAÇÃO

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

2.18 LETRA R

2.18.1 RANSOMWARE

Tipo de *malware*, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados.

2.18.2 RECLASSIFICAÇÃO

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

2.18.3 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.

2.18.4 REDE PRIVADA VIRTUAL (VPN)

É uma rede privada que estabelece uma conexão de rede protegida ao usar redes públicas, a *Internet*. As VPNs criptografam seu tráfego de *Internet*, que dificultam terceiros rastrear suas atividades online e roubar seus dados.

2.18.5 REDE SEM FIO

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

2.18.6 REDES AD HOC

Em telecomunicações, as redes *ad hoc* são uma especificação de rede que não possui um nó ou terminal especial, geralmente designado como ponto de acesso, para o qual

todas as comunicações convergem de onde são encaminhadas aos respectivos destinos. Assim, uma rede de computadores *ad hoc* é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas dos terminais vizinhos.

2.18.7 REDES SOCIAIS

São sites e aplicativos usados por pessoas e organizações que se conectam com clientes, familiares, amigos e pessoas que compartilham seus interesses e objetivos em comum.

2.18.8 RELATÓRIO DE AUDITORIA

Relatório formal com os principais resultados e conclusões da auditoria.

2.18.9 REPRODUÇÃO DE MENSAGEM

O atacante monitora passivamente transmissões e retransmissões de mensagens, agindo como se o atacante fosse um usuário legítimo.

2.18.10 RESILIÊNCIA

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

2.18.11 RESTAURAÇÃO

Procedimento de restaurar os dados a partir de um dispositivo de cópia de segurança.

2.18.12 RETER RISCO

Tipo de tratamento de risco, em que a alta administração decide realizar a atividade, assumindo as responsabilidades, caso ocorra o risco identificado.

2.18.13 RISCO

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

2.18.14 RISCO INERENTE

Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

2.18.15 RISCO RESIDUAL

Risco a que a Organização, o projeto ou a atividade estão expostos, após a implementação de ações gerenciais para o tratamento do risco.

2.18.16 RISCO DE AUDITORIA

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

2.18.17 ROGUE ACCESS POINT

Um *Rogue Access Point* (*Rogue AP*) é um ponto de acesso *wireless* que foi instalado em uma rede sem autorização explícita do administrador da rede local. O *Rogue AP* pode ter sido instalado por um usuário legítimo que desconheça as implicações desta conduta ou deliberadamente instalado por alguém com o intuito de atacar a Rede sem Fio. Em qualquer caso, um *rogue AP* representa uma séria ameaça à segurança da rede.

2.18.18 ROLLBACK

Um *rollback* ou procedimento de *rollback* é uma estratégia de retorno às condições anteriores que deve ser disponibilizada antes que mudanças sejam implementadas no sistema.

2.18.19 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.

2.18.20 RPO

Vide Ponto de Recuperação Objetivo.

2.18.21 RTO

Vide Tempo de Recuperação Objetivo.

2.19 LETRAS

2.19.1 SALT

É um dado aleatório que é usado como uma entrada adicional para a função unidirecional que cria o *hash* de uma senha.

2.19.2 SANITIZAÇÃO DE DADOS

Eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

2.19.3 SCAN

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

2.19.4 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.

2.19.5 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.

2.19.6 SDK

Sigla de kit de desenvolvimento de *software* (*software development kit*).

2.19.7 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.

2.19.8 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.

2.19.9 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.

2.19.10 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.

2.19.11 SENHA NÃO-ADMINISTRATIVA

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

2.19.12 SERVICE PACK

É coleção de atualizações de *software* ou sistema operacional, disponibilizada pelo fabricante deste em um único pacote. Em geral, os fabricantes utilizam este método de atualização quando o número de correções atinge um limite arbitrário.

2.19.13 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.

2.19.14 SIGILO

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

2.19.15 SINGLE SIGN-ON (SSO)

É uma tecnologia de autenticação que permite que um usuário use um único *login* para acessar vários aplicativos de forma transparente e segura.

2.19.16 SISTEMAS CRÍTICOS

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

2.19.17 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.

2.19.18 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.

2.19.19 SMART CARD

É um cartão que funciona como mídia armazenadora. Em seus chips são armazenadas as chaves privadas dos usuários. O acesso às informações neles contidas é feito por meio de senha pessoal, determinada pelo titular.

2.19.20 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.

2.19.21 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.

2.19.22 SNMP

Simple Network Management Protocol – Protocolo Simples de Gerência de Rede é um protocolo de gerência típica de redes UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (*switches*). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, fornecer informações para o planejamento de sua expansão, dentre outras.

2.19.23 SOC

Denominado de Centro de Operações de Segurança, o SOC representa a combinação perfeita de recursos humanos, processuais e tecnológicos para, juntos, formarem uma estrutura de gerenciamento forte para a segurança da informação.

2.19.24 SOFTWARE

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

2.19.25 SOFTWARE ANTIVÍRUS

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

2.19.26 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 é conhecida também como UCE (do Inglês *Unsolicited Commercial E-mail*).

2.19.27 SPAMMER

Pessoa que envia diversos emails ou mensagens, geralmente propaganda eletrônica, sem autorização do receptor. Estas mensagens são denominadas de *spam*.

2.19.28 SPEAN PHISHING

É uma forma direcionada de *phishing* em que e-mails fraudulentos visam organizações específicas em um esforço para obter acesso a informações confidenciais.

2.19.29 SPOOFING

Ato de falsificar a identidade da fonte de uma comunicação ou interação. É possível falsificar endereço IP, ARP, DNS (conhecido com envenenamento do cache de DNS), endereço MAC, *site* da *web*, endereço de *e-mail*, id de chamador, entre outros.

2.19.30 SPYWARE

Tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e *adware* são alguns tipos específicos de *spyware*.

2.19.31 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.

2.19.32 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.

2.19.33 SSL/TLS (SECURE SOCKETS LAYER / TRANSPORT LAYER SECURITY)

Ambos são protocolos criptográficos que conferem segurança de comunicação na Internet para serviços como *e-mail* (SMTP), navegação por páginas (HTTPS) e outros tipos de transferência de dados.

2.19.34 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.

2.19.35 SYSLOG

Sistema de registro de evento que tem como objetivo armazenar mensagens de eventos ocorridos no sistema, permitindo ao administrador, localizar possíveis falhas ou tentativas de invasão no sistema.

2.20 LETRA T

2.20.1 TCP/IP

Significa protocolo de controle de transmissão/protocolo da internet (Transmission Control Protocol/Internet Protocol). TCP/IP é um conjunto de regras padronizadas que permitem que os computadores se comuniquem em uma rede como a internet.

2.20.2 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.

2.20.3 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.

2.20.4 TEMPO OBJETIVO DE RECUPERAÇÃO (RTO)

Tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente.

2.20.5 TERMO DE RESPONSABILIDADE

Termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

2.20.6 TESTES DE INVASÃO

Denominada também de teste de penetração, ou simplesmente *pentest*, são conjuntos de processos e procedimentos utilizando *softwares* específicos para verificar as vulnerabilidades e avaliar seus riscos em um sistema ou rede.

2.20.7 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.

2.20.8 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.

2.20.9 TRATAMENTO DO RISCO

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

2.21 LETRA U

2.21.1 URL

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

2.21.2 USUÁRIO

Alguma pessoa que interage 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.

2.21.3 USUÁRIO DAS INFORMAÇÕES

Entende-se como usuário das informações qualquer indivíduo com acesso às informações originadas no DECEA e em suas Organizações Subordinadas.

2.22 LETRA V

2.22.1 VAZAMENTO

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

2.22.2 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.

2.22.3 VISITA

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

2.22.4 VM

Sigla de máquina virtual (*Virtual Machine*).

2.22.5 VPN

Sigla de rede privada virtual (*Virtual Private Network*).

2.22.6 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.

2.22.7 VULNERABILIDADE DIA ZERO

Falha na segurança de um *software*, que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma vulnerabilidade de dia zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um *patch* de segurança para essa falha, ela pode ser explorada por *hacker* sem explorações de dia zero. A correção de uma vulnerabilidade de dia zero geralmente é tarefa do fabricante do *software*, que precisará lançar um pacote de segurança para consertar a falha.

2.23 LETRA W

2.23.1 WATERING HOLE

Tipo de ataque em que os cibercriminosos conhecem o comportamento de navegação na internet de um grupo de usuários e infectam os sites mais visitados com links ou conteúdos maliciosos. A chance de sucesso aumenta, já que as ameaças ficam "escondidas" em um ambiente aparentemente seguro

2.23.2 WEBMAIL

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

2.23.3 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.

2.23.4 WHITELIST

Lista de itens aos quais é garantido o acesso a certos recursos, sistemas ou protocolos. Utilizar uma *whitelist* para controle de acesso significa negar o acesso a todas as entidades, exceto àquelas incluídas na *whitelist*.

2.23.5 WI-FI

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

2.23.6 WIRELESS

Rede sem fio.

2.23.7 WLAN

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

2.23.8 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.

2.23.9 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.

2.23.10 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.

2.23.11 WPA2

O WPA2 ou 802.11i foi uma substituição da *Wi-Fi Alliance* em 2004 à tecnologia WPA, pois, embora fosse bem seguro em relação ao padrão anterior WEP, a *Wi-Fi Alliance* teve a intenção de fazer um novo certificado para redes sem fio mais confiável, bem como necessitava continuar o investimento inicial realizado sobre o WPA. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio.

2.23.12 WPA3

É um protocolo de segurança anunciado em 2018 pela *Alliance*, que fornece um método muito mais seguro e confiável em substituição ao WPA2 e aos protocolos de segurança mais antigos. O WPA3-Empresarial aumenta a criptografia mínima para 192 bits, sendo a criptografia de 128 bits no modo WPA3-Pessoal, o que aumenta a segurança nas redes sem fio contra os ataques de força bruta. Além de prover uma comunicação mais segura, com melhor criptografia, possui métodos que impedem as pessoas que se conectam à rede de conhecerem as senhas.

2.24 LETRA X

2.24.1 XSS

Ver *cross-site scripting*.

2.25 LETRA Z

2.25.1 ZERO-DAY EXPLOIT

Vide exploração de dia zero.

2.25.2 ZERO-DAY VULNERABILITY

Vide vulnerabilidade de dia zero.

2.25.3 ZONA DESMILITARIZADA (DMZ)

Vide DMZ (DESMILITARIZED ZONE).

2.25.4 ZUMBI

Dispositivo ou computador infectado por *bot* e conectado à internet usado para realizar determinada tarefa com fins maliciosos, sem que o proprietário saiba.

2.26 NÚMERO 2

2.26.1 2FA

Sigla que significa autenticação de dois fatores (*2Factor Authentication*).

2.27 NÚMERO 3

2.27.1 3DES

Sigla para *Triple Data Encryption Standard*, é um padrão de criptografia baseado em outro algoritmo de criptografia simétrica, o DES, desenvolvido pela IBM em 1974 e adotado como padrão em 1977. O 3DES usa 3 chaves de 64 bits. O tamanho máximo da chave é de 192 bits, embora o comprimento utilizado seja de 56 bits. Os dados são encriptados com a primeira chave, decryptados com a segunda chave e finalmente encriptados novamente com uma terceira chave.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT NBR ISO/IEC 27001**. *Tecnologia da Informação – Sistemas de gestão de segurança da informação – Requisitos*. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT NBR ISO/IEC 27002**. *Tecnologia da Informação – Código de Práticas para a Gestão da Segurança da Informação*. 2013.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Instrução para Salvaguarda de Assuntos Sigilosos Aeronáutica: **ICA 205-47**. Brasília, DF, 2015.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Diretriz de Segurança da Informação do DECEA*: **DCA 7-2**. Rio de Janeiro, RJ, 2022.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. *Glossário de Gestão de Serviços de Tecnologia da Informação do Comando da Aeronáutica (STI)*: **MCA 10-3**. Rio de Janeiro, RJ, 2020.

BRASIL. **Instrução Normativa conjunta CGU/MP N° 1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

BRASIL. **Portaria N° 93 GSI/PR, de 18 de outubro de 2021**. Glossário de Segurança da Informação. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370>. Acesso em: 17/08/2022.