MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

MCA 7-3

GLOSSÁRIO DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO NO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (STI)

2020

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

MCA 7-3

GLOSSÁRIO DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO NO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (STI)

2020

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

PORTARIA DTI Nº 12/SNOR, DE 7 DE OUTUBRO DE 2020.

Aprova a reedição do Glossário de Gestão de Serviços de Tecnologia da Informação do Comando da Aeronáutica.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA, no uso de suas atribuições, que lhe confere o art. 10 do Regulamento da Diretoria de Tecnologia da Informação da Aeronáutica, aprovado pela Portaria nº 472/GC3, de 12 de abril de 2018, resolve:

Art. 1º Aprovar a reedição do MCA 7-3 "Glossário de Gestão de Serviços de Tecnologia da Informação" que com esta baixa.

Art. 2º Esta Portaria entra em vigor em 3 de novembro de 2020.

Art. 3º Revoga-se a Portaria DTI nº 47/ANATI, de 17 de outubro de 2017, publicada no Boletim do Comando da Aeronáutica nº 181, de 20 de outubro de 2017.

Brig Int LUIZ FERNANDO MORAES DA SILVA
Diretor de Tecnologia da Informação da Aeronáutica

(Publicado no BCA nº 188 , de 16 de outubro de 2020)

SUMÁRIO

PREFÁCIO

Esta publicação contém, basicamente, termos, palavras, vocábulos e expressões de uso em Gestão de Serviços de Tecnologia da Informação, de governança de Tecnologia da Informação, em especial aqueles de uso comum no Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI), a fim de contribuir para a comunicação oficial em todos os níveis, aumentando a celeridade e a compreensão acerca dos principais termos técnicos utilizados na Gestão de Serviços de Tecnologia da Informação no STI.

Para a norma ABNT NBR 10719:20-15, glossário é "a relação de palavras ou expressões técnicas de uso restrito ou de sentido obscuro, utilizadas no texto, acompanhadas das respectivas definições, e elaborado em ordem alfabética".

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

É importante explicitar a terminologia adotada pelo COMAER neste tema, pois seus significados necessitam de um entendimento homogêneo por todos aqueles que interagem no âmbito do STI.

O conjunto de conceitos é o resultado de um trabalho de revisão da literatura especializada, em especial, tendo como base as normas técnicas ABNT NBR ISO/IEC 20000-1:2011, Tecnologia da Informação - Gestão de Serviços - Parte 1: Requisitos do sistema de gestão de serviços e ABNT NBR ISO/IEC 20000-2:2013, Tecnologia da Informação - Gerenciamento de serviços - Parte 1: Especificação e Parte 2: Código de prática que tratam do desenho, transição, entrega e melhoria de serviços que cumprem requisitos de serviço e fornecem valor para o cliente e para o provedor do serviço.

Tendo em vista a necessidade de atualização, intimamente relacionada ao tema, o presente Glossário será periodicamente revisado na medida em que novas definições e conceitos forem surgindo ou se tornando obsoletos.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O Glossário de Gestão dos Serviços de Tecnologia da Informação tem por finalidade padronizar a utilização de termos, palavras, vocábulos e expressões de uso corrente sobre o tema Governança de TI e Gestão dos Serviços de TI no Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI).

1.2 CONCEITUAÇÕES

Para os efeitos desta Instrução, aplicam-se os termos e expressões com os significados constantes no Glossário das Forças Armadas (MD-35-G-01/2007), no Glossário do Comando da Aeronáutica (MCA 10-4/2001), na legislação do Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI) em vigor e, quando aplicável, na legislação da Administração Pública Federal (APF) em vigor, bem como nas normas ABNT recomendadas pelo TCU em seus Acórdãos. Em especial aplicam-se os conceitos constantes da Norma ABNT NBR ISO/IEC 20000.

1.2.1 GESTÃO DOS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO NO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (GSTI)

1.2.1.1 Serviço de TI é o serviço baseado no uso da tecnologia da informação provido pelos Elos do STI para um ou mais clientes e usuários, oferecendo apoio aos processos de negócio do COMAER. É composto pela combinação de pessoas, processos e tecnologia da informação que devem ser definidas por meio de Acordo de Nível de Serviço entre o cliente do serviço de TI e o Eloresponsável por mantê-lo, além de Acordo de Nível Operacional firmado entre os elos que compõem o serviço e de Contratos com fornecedores.

1.2.1.2 Gestão de Serviços de Tecnologia da Informação no Sistema de Tecnologia da Informação do Comando da Aeronáutica (GSTI), compreende, obrigatoriamente, atividades de planejamento, elaboração, entrega, operação, monitoramento, avaliação e ajustes contínuos dos serviços de Tecnologia da Informação (TI) prestados pelos Elos do STI.

1.2.2 ÓRGÃO CENTRAL

O Órgão Central do STI é a Diretoria de Tecnologia da Informação da Aeronáutica (DTI).

1.2.3 ELOS

Os Elos do STI são Organizações ou frações de Organizações do COMAER responsáveis por atividades e ativos de TI em uma determinada instalação e subordinadas sistemicamente ao Órgão Central do STI.

A natureza de atividade-meio com alto grau de capilaridade que caracteriza o STI tem como consequência o fato de que uma variada gama de OM o integre, desde aquelas cuja missão precípua seja a atividade de tecnologia da informação – como os Centros de Computação – até outras cuja missão inclua também prestar o apoio de TI a um conjunto de OM em determinada região, tais como as Bases Aéreas e os Grupamentos de Apoio.

1.2.4 SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (STI)

Sistema reformulado pela Portaria nº 549/GC3, de 9 de agosto de 2010, com a finalidade de organizar, disciplinar e controlar as atividades de Tecnologia da Informação (TI), em consonância com as políticas específicas do Governo Federal e com a Política da Aeronáutica para a Tecnologia da Informação.

1.3 ÂMBITO

A presente Instrução aplica-seaoÓrgão Central do STIe aos Elos do Sistema de Tecnologia da Informação do Comando da Aeronáutica.

2 GLOSSÁRIO DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

2.1 LETRA A

2.1.1 ACESSO

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

2.1.2 ACESSO FÍSICO

Possibilidade de estar fisicamente próximo a um ativo.

2.1.3 ACESSO LÓGICO

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

2.1.4 AÇÃO CORRETIVA

Segundo a norma ISO 9000, ação corretiva é uma "ação para eliminar a causa de uma não-conformidade identificada ou outra situação indesejável".

2.1.5 AÇÃO PREVENTIVA

O item 8.5.3 da ISO 9001:2015 afirma que a ação preventiva determina e elimina a causa das não-conformidades em potencial para prevenir a sua ocorrência.Ao analisar que foi aberta uma ação preventiva, você percebe que houve uma inspeção com o objetivo eliminar as possibilidades de erros ou falhas, seja ele em um processo ou em um produto. Com essa ação, você consegue intervir para eliminar tais erros/falhas e evitar não-conformidades potenciais.

2.1.6 ACORDO DE NÍVEL DE SERVIÇO (ANS) OU SERVICE LEVEL AGREEMENT (SLA)

O ANS é um documento que descreve um serviço de TI, as suas metas de nível de serviço (em termos de desempenho, quantidade e qualidade) do ponto de vista do negócio da organização, características da carga de trabalho, papéis e responsabilidades dos atores envolvidos, prioridades e procedimentos de exceção, entre outros aspectos. Esse documento deve ser acordado entre os requisitantes ou interessados em um determinado serviço de TI, e o responsável pelos serviços de TI da organização, e deve ser revisado periodicamente para certificar-se de que continua adequado ao atendimento das necessidades de negócio da organização. A área de TI da instituição pública celebra acordos de nível de serviço com os seus clientes internos (áreas finalísticas, áreas administrativas etc.). As normas ABNT associam o conceito de ANS à relação existente entre os clientes internos e a área provedora de serviços de TI da própria organização.

2.1.7 ACORDO DE NÍVEL OPERACIONAL (ANO)

O acordo de nível operacional é o acordo firmado entre o provedor de serviço de TI da organização e um fornecedor interno da mesma organização cujos serviços são essenciais para viabilizar a entrega do serviço de TI ao cliente. A estrutura do ANO é semelhante à do ANS e define os produtos ou serviços a serem fornecidos e as responsabilidades de ambas as partes. A área de TI da instituição pública firma acordos de nível operacional com outras áreas da mesma organização (fornecedores internos).

2.1.8 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.

2.1.9 AGENTE RESPONSÁVEL PELA ETIR

Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Militar de carreira ou Servidor Público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, Direta ou Indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

2.1.10 ALERTA

É um sinal analisado e validado por um sensor na rede de identificação de ameaças e geração de alertas.

2.1.11 ALGORITMO DE ESTADO

Função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da Administração Pública Federal (APF), direta e indireta, não comercializável.

2.1.12 ALGORITMO REGISTRADO

Função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processos sejam passíveis de controle e auditoria.

2.1.13 ALTA ADMINISTRAÇÃO

Equivale ao conceito de “dirigente” do setor privado. No setor público, compõem a “Alta Administração” os principais dirigentes da organização. Como exemplos mais conhecidos, temos Ministros e Secretários de Estado, titulares de cargos de natureza especial, secretários executivos, secretários ou autoridades equivalentes ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS, nível seis, presidentes de tribunais, presidentes e diretores de agências nacionais, autarquias, fundações mantidas pelo Poder Público, presidentes de empresas públicas e sociedades de economia mista, bem como a diretoria executiva.

2.1.14 AMBIENTAÇÃO

Evento que oferece informações sobre a missão organizacional do órgão ou instituição, bem como sobre o papel do agente público nesse contexto.

2.1.15 AMBIENTE EXTERNO

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

2.1.16 AMEAÇA CIBERNÉTICA

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

2.1.17 AMEAÇA PERSISTENTE AVANÇADA (APT)

Operações de longo prazo projetadas para infiltrar ou exfiltrar o máximo possível de dados sem serem descobertas, sendo mais conhecidas pelo seu acrônimo em inglês Advanced Persistent Threat – APT. Possui ciclo de vida mais longo e complexo que outros tipos de ataque, sendo mais elaborados e necessitando de volume significativo de recursos para sua viabilização, o que exige forte coordenação. Em geral, são realizados por grupos com intenção de espionagem ou sabotagem.

2.1.18 AMEAÇAS

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

2.1.19 ANÁLISE DE IMPACTO NOS NEGÓCIOS (AIN)

Visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de SIC (Segurança de Informação e Comunicações) para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

2.1.20 ANÁLISE DE RISCO

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

2.1.21 ANÁLISE DINÂMICA

Tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução.

2.1.22 ANÁLISE ESTÁTICA

Tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários.

2.1.23 AP

Do Inglês Access Point é o dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

2.1.24 AQUISIÇÃO DE EVIDÊNCIA

Processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.

2.1.25 ÁREA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

Setor (ou conjunto de setores) da organização responsável (eis) pela coordenação e execução de ações e práticas de gestão de Tecnologia da Informação (ex.: gerenciamento de infraestrutura de TI, gerenciamento de projetos de TI, planejamento de TI, informatização de projetos organizacionais, gerenciamento de catálogo de serviços de TI, gestão de riscos de TI).

2.1.26 ÁREA DE NEGÓCIO

Diz respeito às unidades responsáveis pela execução de macroprocessos finalísticos e de apoio técnico ou administrativo. Os macroprocessos, neste contexto, podem ser entendidos como grandes conjuntos de atividades pelos quais a organização cumpre a sua missão, gerando valor.

2.1.27 ÁREA SIGILOSA

É aqueles 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.

2.1.28 ARQUITETURA DE SISTEMAS

Identificação e arranjo das estruturas físicas e lógicas de um sistema, abrangendo componentes de software, propriedades externamente visíveis destes componentes e as relações entre eles.

2.1.29 ARQUITETURA FÍSICA

Identificação e arranjo dos componentes físicos de um sistema, descrevendo estrutura física, funções técnicas, características de desenho e atributos técnicos que possam ser alcançados por qualquer componente e pelo sistema, sob determinadas restrições.

2.1.30 ARQUIVOS ELETRÔNICOS

Formato de armazenamento de informações (Fonte de armazenamento “Backup”.). Arquivos eletrônicos podem conter tanto informações de usuários quanto dados do sistema operacional e códigos de execução de programas.

2.1.31 ARTEFATO CIBERNÉTICO

Equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataques cibernéticos.

2.1.32 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 e/ou redes de computadores.

2.1.33 ASSINATURA DIGITAL

Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e-mail ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.

2.1.34 ASSINATURA ELETRÔNICA

Conjunto de dados, no formato eletrônico, que é anexado ou logicamente associado a outro conjunto de dados, também no formato eletrônico, para conferir-lhe autenticidade ou autoria. A assinatura eletrônica, portanto, pode ser obtida por meio de diversos dispositivos ou sistemas, como login/senha, biometria, impostação de PersonalIdentificationNumber (PIN) etc. Um dos tipos de assinatura eletrônica é a assinatura digital.

2.1.35 ASSUNTO SIGILOSO

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

2.1.36 ATACANTE

Pessoa responsável pela realização de um ataque.

2.1.37 ATAQUE

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

2.1.38 ATAQUE CIBERNÉTICO

Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais em dispositivos e redes computacionais e de comunicações do oponente.

2.1.39 ATIVIDADE

Processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

2.1.40 ATIVIDADES CRÍTICAS

Atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

2.1.41 ATIVO

Qualquer recurso ou habilidade que tenha valor para o COMAER. Os ativos de um provedor de serviço incluem qualquer coisa que pode contribuir para a entrega de um serviço. Ativos podem ser qualquer um dos seguintes tipos: gerência, organização, processo, conhecimento, pessoas, informações, aplicativos, infraestrutura e capital financeiro.

2.1.42 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.

2.1.43 ATIVO DE SERVIÇO

Qualquer recurso ou habilidade de um provedor de serviço. Ver também ativo.

2.1.44 AUDITORIA BASEADA EM RISCO

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

2.1.45 AUDITORIA DE CONFORMIDADE

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

2.1.46 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.

2.1.47 AUDITORIA DO SGSI

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

2.1.48 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.

2.1.49 AUTORIDADE CERTIFICADORA

Entidade responsável por emitir e gerenciar certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição etc.

2.1.50 AUTORIZAÇÃO

Processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

2.1.51 AVALIAÇÃO DE IMPACTO DE MUDANÇA

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

2.2 LETRA B

2.2.1 BACKDOOR

Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim. Normalmente esse programa é colocado de forma a não a ser notado.

2.2.2 BACKUP OU CÓPIA DE SEGURANÇA.

Cópia que se faz de cada arquivo do computador, como garantia para o caso em que se percam os dados originais gravados.

2.2.3 BALANCED SCORECARD (BSC)

Significa Indicadores Balanceados de Desempenho. É uma metodologia de medição, gestão de desempenho e de planejamento estratégico

2.2.4 BANCO DE DADOS DE GERENCIAMENTO DE CONFIGURAÇÃO (BDGC)

Dados armazenados para registrar atributos de itens de configuração e os relacionamentos entre itens de configuração durante o seu ciclo de vida.

2.2.5 BASE DE CONHECIMENTO

Um banco de dados que contém todos os registros de erros conhecidos. Este banco de dados é criado pelo gerenciamento de problema e é usado pelo gerenciamento de incidente e pelo gerenciamento de problema. O banco de dados de erro conhecido pode ser parte do sistema de gerenciamento de configuração ou pode ser armazenado em outro lugar do sistema de gerenciamento de conhecimento de serviço.

2.2.6 BASE DE REFERÊNCIA DE CONFIGURAÇÃO

Informação de configuração formalmente designada em um momento específico durante a vida do serviço ou componente do serviço.

2.2.7 BLOQUEIO DE ACESSO

Processo que tem por finalidade suspender temporariamente o acesso.

2.2.8 BLUE TEAM (TIME AZUL)

Equipe responsável por identificar e/ou prevenir ataques cibernéticos e responder adequadamente no caso de ocorrência desses ataques.

2.2.9 BOATO

É a mensagem 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.

2.2.10 BOT

Tipo de código malicioso. Programa que, além de incluir funcionalidades de*worms*,dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. O processo de infecção e propagação do*bot*é similar aodo*worm*, ou seja, o*bot*é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

2.2.11 BOTNET

Rede formada por centenas ou milhares de computadores infectados com *bot*. Permite potencializar as ações danosas executadas pelo bot e ser usada em ataques de negação de serviço, esquemas de fraude, envio de *spam* etc.

2.2.12 BOTS

Um *bot* (contração 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, ou seja, é uma forma automatizada de execução de uma determinada tarefa. Este tipo de programa de computador pode ter diversos usos, entre eles: ataques de DDoS, *downloaders* que ocupam toda a largura de banda dos links de comunicação, ataques coordenados do tipo *Botnet/zumbis* etc.

2.2.13 BUFFER OVERRUN/OVERFLOW

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

2.3 LETRA C

2.3.1 CADEIA DE CUSTÓDIA

Histórico ou documentação cronológica que registra a sequência de custódia, controle, transferência, análise e disposição de evidências físicas ou eletrônicas.

2.3.2 CAIXA BRANCA

Modalidade de Teste de Intrusão, na qual a equipe de teste possui acesso completo a informações internas de infraestrutura/modelagem/implementação do alvo do teste. Pode ser fornecido à equipe, credenciais de acesso e/ou código fonte da aplicação testada.

2.3.3 CAIXA CINZA

Modalidade de Teste de Intrusão, na qual equipe de teste possui acesso a algumas informações privilegiadas do alvo do teste. Neste caso são disponibilizadas mais informações do que teria um usuário comum, ou atacante externo.

2.3.4 CAIXA POSTAL

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

2.3.5 CAIXA PRETA

Modalidade de Teste de Intrusão, na qual equipe de teste não possui qualquer informação privilegiada com relação à infraestrutura/modelagem/implementação do alvo do teste.

2.3.6 CAPACIDADE DE GUERRA ELETRÔNICA

Somatório de meios e recursos de toda ordem que permita aos poderes naval, terrestre e aéreo empreender eficazmente ações e operações de guerra eletrônica, em proveito das operações de guerra.

2.3.7 CAPACITAÇÃO EM SIC

Atividade de ensino que tem como objetivo orientar sobre o que é SIC (Segurança de Informação e Comunicações), fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC.

2.3.8 CASOS DE TESTE

Descrevem uma situação que deverá ser testada, derivada diretamente dos Casos de Uso do sistema.

2.3.9 CASOS DE USO

Elemento gráfico/textual do processo de análise de sistemas que tem como objetivo o detalhamento dos comportamentos e respostas esperados entre os diversos atores do sistema e as ações plotadas. São constituídos pelos atores, pré-condições, fluxo principal - ou passos -, fluxos alternativos, exceções, pós-condições e requisitos.

2.3.10 CATÁLOGO DE DADOS

Um catálogo de dados é um serviço disponível para que o usuário tenha acesso aos dados publicados pelo órgão ou entidade. Segundo a Cartilha para Publicação de Dados Abertos no Brasil, todos os dados publicados pelo órgão/entidade devem estar acessíveis por meio do catálogo, sendo desejável que o referido catálogo possibilite a navegação e a busca simplificada dos dados. O catálogo deve ser acessível a partir do portal institucional do órgão ou entidade. Existem diversas formas de se implementar um catálogo de dados. Uma simples página contendo a lista de arquivos de dados publicados, em conjunto com as informações que possibilitem organizar, classificar e relacionar esses dados, pode ser considerada um catálogo.

2.3.11 CATÁLOGO DE REQUISIÇÃO

Visãodo catálogo de serviço que fornece detalhes das requisições de serviços existentes e novos que é disponibilizada para o usuário.

2.3.12 CATÁLOGO DE SERVIÇOS

O catálogo de serviços é um documento-chave para estabelecer expectativas de clientes e convém que ele seja de fácil acesso e amplamente disponível para o cliente e para as equipes de suporte. Convém que o catálogo de serviços inclua informações como: a) nome e descrição do serviço; metas do serviço; pontos de contato; horários de serviço;

acordos de segurança; serviços atuais; dependências entre o serviço e os serviços de apoio dos quais é dependente etc. Convém que o catálogo de serviços seja mantido e atualizado permanentemente.

2.3.13 CATÁLOGO DE SERVIÇOS DE TI

Informação estruturada sobre todos os serviços de TI disponíveis aos clientes desses serviços. Convém que o provedor de serviços defina todos os serviços em um catálogo, usando termos que estejam alinhados com a visão do cliente e seja compreensível por aqueles sem uma compreensão técnica detalhada. O catálogo de serviços é um documento-chave para estabelecer expectativas de clientes e convém que ele seja de fácil acesso e amplamente disponível para o cliente e para as equipes de suporte. Convém que o catálogo de serviços inclua informações como: a) nome e descrição do serviço; metas do serviço; pontos de contato; horários de serviço; acordos de segurança; serviços atuais; dependências entre o serviço e os serviços de apoio dos quais é dependente etc.

2.3.14 CATÁLOGO DE SERVIÇOS DE TI DO STI

É o catálogo de serviços de TI dos Elos do STI, onde constam quais serviços de TI são providos pelo STI para o Comando da Aeronáutica, compreendendo a administração dos serviços de TI.

2.3.15 CATÁLOGO DE SERVIÇOS DOS ELOS DO STI

É o catálogo de serviços de TI dos Elos do STI, onde constam todos os serviços de TI que são providos por estes Elos para o Comando da Aeronáutica, compreendendo a administração dos serviços de TI.

2.3.16 CAVALO DE TRÓIA

Tipo de código malicioso.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.

2.3.17 CENTRAL DE SERVIÇOS

A Central de Serviços funciona como o ponto de contato do dia a dia com os usuários.

2.3.18 CENTRAL DE SERVIÇOS DO SERVIÇO DE ATENDIMENTO AOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (SAUTI)

A Central de Serviços de TI do COMAER é uma função da Gestão de Serviços e é operada pelo Serviço de Atendimento aos Usuários de Tecnologia da Informação do Comando da Aeronáutica (SAUTI) e denomina-se Central de Serviços do SAUTI. É o canal único de comunicação dos Elos do STI com seus clientes e usuários que utilizam os serviços e produtos de TI disponibilizados de acordo com seus Catálogos de Serviços.

2.3.19 CERTIFICADO DIGITAL

Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

2.3.20 CERTIFICADO DIGITAL AUTOASSINADO

Certificado digital no qual o dono e o emissor são a mesma entidade.

2.3.21 CERTIFICAÇÃO DO COMAER

Processo pelo qual uma Organização Certificadora do COMAER se assegura do cumprimento dos requisitos estabelecidos para um Produto ou para um Sistema de Gestão da Qualidade, que se conclui com a emissão de um Certificado, de acordo com o item 1.2.5 da DCA 400-6/2007.

NOTA: este conceito aplica-se à Certificação de Tipo, de Integração, de Modificação, de Convalidação, de Organização Fornecedora, de Qualidade, de autorização de retorno à Operação e de Instalação do Produto.

2.3.22 CHAVE CRIPTOGRÁFICA

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

2.3.23 CHAMADO

Interação (por exemplo, uma chamada telefônica) com a central de serviço. Um chamado pode resultar no registro de um incidente ou de uma requisição de serviço.

2.3.24 CIBERNÉTICA

Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais.

2.3.25 CICLO DE VIDA DA INFORMAÇÃO

Compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação.

2.3.26 CLASSIFICAÇÃO

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

2.3.27 CLIENTE

O beneficiado por um produto ou um serviço proveniente do negócio. Por exemplo, se o negócio é fabricar carros, então o cliente do negócio será alguém que comprar um carro.

O cliente define os requisitos do produto ou serviço de TI para a solução de TI, no prazo e recursos disponíveis, que atenderá as demandas geradas pelo negócio. No STI este papel poderá ser exercido, em princípio, pelo Órgão Central de um Sistema, pelos ODGSA, pelo COMTI ou pelo GATI. Clientes são diferentes de usuários, pois os clientes definem os requisitos dos serviços de TI que serão utilizados pelos usuários.

2.3.28 CÓDIGOS MALICIOSOS

Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*etc.

2.3.29 COLABORADOR

É o órgão que tem capacidade de inserir sinais na rede de identificação de ameaças e geração de alertas.

2.3.30 CONFIGURAÇÃO

Disposição de itens de configuração (ICs) ou de outros recursos que trabalham em conjunto para fornecer um produto ou serviço. O termo também pode ser usado para descrever as configurações de parâmetros de um ou mais ICs.

2.3.31 COMISSÃO DE ANÁLISE DO ANS

É a comissão formada por técnicos especializados em TI para realizar a análise de ANS e seus respectivos ANO, conforme legislação de TI específica.

2.3.32 COMITÊ DIRETIVO DE TI

Comitê instituído por Portaria do Comandante da Aeronáutica com a finalidade de assessorar o EMAER no trato dos assuntos relacionados à governança de Tecnologia da Informação no COMAER, no mais alto nível.

2.3.33 COMPONENTE DO SERVIÇO

Unidade única de um serviço que, quando combinada com outras unidades, entregará um serviço completo. EXEMPLOS: Hardware, software.

2.3.34 COMPUTAÇÃO EM NUVEM

Modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

2.3.35 COMPUTADOR ZUMBI

Nome dado a um computador infectado por bot, pois pode ser controlado remotamente, sem o conhecimento do seu dono.

2.3.36 COMUNICAÇÕES DO RISCO

Troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

2.3.37 CONEXÃO SEGURA

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

2.3.38 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.

2.3.39 CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Cumprimento das legislações, normas e procedimentos relacionados à segurança da informação e comunicações da organização.

2.3.40 CONJUNTO DE DADOS

Os dados em formato aberto são organizados utilizando as estruturas de conjuntos de dados e recursos. Cada conjunto de dados possui uma descrição, um ou mais recursos, e uma série de metadados. Metadados são informações que descrevem características de determinado dado, explicando-o em certo contexto de uso. Metadados possibilitam organizar, classificar e relacionar os dados. São exemplos de metadados: o nome do conjunto de dados, uma explicação sobre os dados, periodicidade de atualização dos dados, identificação do órgão responsável pela publicação do conjunto de dados. Já um recurso

seria uma das formas como o conjunto de dados está disponível, ou seja, um conjunto de dados pode ser acessível por meio de várias fontes, pode ser uma planilha, um método de um serviço web, um documento etc.

2.3.41 CONTA DE SERVIÇO

Contas de acesso à rede corporativa de computadores, necessárias a um procedimento automático (aplicação, *script* etc.) sem qualquer intervenção humana no seu uso.

2.3.42 CONTA DE USUÁRIO

Identificação pessoal e intransferível, 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 COMAER.

2.3.43 CONTINUIDADE DE NEGÓCIOS

Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

2.3.44 CONTINUIDADE DO SERVIÇO

Capacidade de gerenciar riscos e eventos que poderiam ter sério impacto em um ou mais serviços, a fim de entregar continuamente os serviços nos níveis acordados.

2.3.45 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.

2.3.46 CONTROLE DE ACESSO

Conjunto de procedimentos, recursos ou meios utilizados com a finalidade de conceder ou bloquear o acesso. Conforme os meios utilizados para sua execução, classifica-se em três tipos: físico, técnico (ou lógico) e administrativo.

2.3.47 CONTROLES DE SEGURANÇA

Medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: a criptografia, as funções de "*hash*", a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os "*backups*" etc.

2.3.48 CORREIO ELETRÔNICO

Sistema de envio e recebimento de mensagens eletrônicas, mais conhecidas como "E-mail".

2.3.49 COVERT CHANNELS (CANAIS DE COBERTURA)

Os *covertchannels* são caminhos não previstos para conduzir fluxo de informações, mas que, no entanto, podem existir num sistema ou rede. Por exemplo, a manipulação de bits no protocolo de pacotes de comunicação poderia ser utilizada como um método oculto de sinalização. Devido à sua natureza, seria difícil, se não impossível, precaver-se contra a existência de todos os possíveis *covertchannels*. No entanto, a exploração destes canais

frequentemente é realizada por código troiano. A adoção de medidas de proteção contra código malicioso reduz, consequentemente, o risco de exploração de *covertchannels.*

2.3.50 CRACKER

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

2.3.51 CREDENCIAL DE SEGURANÇA

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

2.3.52 CREDENCIAMENTO

Autorização oficial concedida pela autoridade competente que habilita determinada pessoa a ter acesso a dados ou conhecimentos nos diferentes graus de sigilo, desde que esteja caracterizada a necessidade de conhecer.

2.3.53 CRIPTOGRAFIA

Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. 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.

2.3.54 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.

2.3.55 CSI – COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação.

2.3.56 CTIR GOV

Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.

2.3.57 CUSTÓDIA

Responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

2.3.58 CUSTODIANTE

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

2.3.59 CYBER KILL CHAIN

Conjunto de estágios de um ciberataque (tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo), que vão desde o reconhecimento até a infiltração de dados. Seu entendimento ajuda na prevenção de ameaças cibernéticas.

2.4 LETRA D

2.4.1 DADOS ABERTOS

Dados representados em meio digital em um formato sobre o qual nenhuma organização tenha controle exclusivo, passíveis de utilização por qualquer pessoa. Dados públicos representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na rede mundial de computadores e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento.

2.4.2 DADOS CORPORATIVOS

Dados provenientes de sistemas transacionais corporativos tipicamente voltados para automatizar processos referentes às diversas áreas setoriais, operacionais e administrativas do COMAER (e.g. SIGPES, SILOMS, OPERA, etc) ou qualquer dado externo que alimente esses sistemas transacionais (e.g. dados do SIAFI, SIASG, etc).

2.4.3 DADOS ESTRUTURADOS

Dados compostos por tipos claramente definidos, cujo padrão os torna facilmente pesquisáveis.

2.4.4 DADOS NÃO-ESTRUTURADOS

Dados sem um formato ou organização predefinidos, tornando-os muito mais difícil de coletar, processar e analisar.

2.4.5 DADO PÚBLICO

Qualquer dado gerado ou sob a guarda governamental que não tenha o seu acesso restrito por legislação específica.

2.4.6 DATA LAKE

Repositório centralizado e escalável de dados estruturados e não estruturados.

2.4.7 DATA MART

Subconjunto de um Data Warehouse, de visão departamental ou de área interesse bem definida, com o propósito de fornecer visão estratégica dos dados setorizados.

2.4.8 DATA WAREHOUSE

Repositório de dados estruturados que propicia às grandes organizações uma maneira flexível e eficiente de armazenar e recuperar, de forma efetiva, informações estratégicas necessárias aos processos decisórios de mais alto nível. Repositório histórico, não volátil, dos fatos operacionais de uma organização.

2.4.9 DDOS

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

2.4.10 DEFESA

O ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, reação contra qualquer ataque ou agressão real ou iminente.

2.4.11 DEFESA CIBERNÉTICA

Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.

2.4.12 DESASTRE

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

2.4.13 DESENVOLVIMENTO TECNOLÓGICO

Processo de pesquisa e produção de tecnologia. Os passos específicos do desenvolvimento dependem da tecnologia em questão.

2.4.14 DIAGRAMA DE PROCESSOS DE NEGÓCIO/BPMN

Representação gráfica através de fluxogramas com a identificação dos processos de negócio essenciais que existem dentro de uma organização. O modelo deve seguir uma notação gráfica específica e possuir descrição, métricas e outras informações de apoio. BPMN (*Business ProcessModelingNotation*): notação internacional padrão composta por uma série de ícones utilizados para o desenho de processos.

2.4.15 DISCIPLINA DE REDE

Forma de segurança das comunicações que compreende o uso adequado do material, a observância das frequências e regras de exploração prescritas, controle da rede, a fiscalização e a instrução.

2.4.16 DIRETRIZ

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

2.4.17 DIRIGENTE MÁXIMO

Membro da alta administração, sendo a maior autoridade administrativa do órgão ou entidade. Por exemplo: Chefes de Poderes, Presidentes dos Tribunais, Ministros de Estado, Secretário da RFB, Presidentes de Tribunais, presidentes de autarquias, comandantes militares, secretários-executivos, secretários-gerais, diretores-presidentes de estatais; reitores; presidentes de fundação e institutos; e ainda outros gestores ocupantes de cargo do Grupo-Direção e Assessoramento Superiores – DAS níveis seis e cinco.

2.4.18 DISPONIBILIDADE

Habilidade de um serviço de TI ou de outro item de configuração de executar sua função acordada quando necessário.

2.5 LETRA E

2.5.1 EFICÁCIA

Extensão na qual as atividades planejadas são realizadas e os resultados planejados são alcançados.

2.5.2 ELOS DO STI

Os Elos do STI são Organizações ou frações de Organizações do COMAER responsáveis por atividades e ativos de TI em uma determinada instalação e subordinadas sistemicamente ao Órgão Central do STI.

A natureza de atividade-meio com alto grau de capilaridade que caracteriza o STI tem como consequência o fato de que uma variada gama de OM o integre, desde aquelas cuja missão precípua seja a atividade de tecnologia da informação – como os Centros de Computação – até outras cuja missão inclua também prestar o apoio de TI a um conjunto de OM em determinada região, tais como as Bases Aéreas e os Grupamentos de Apoio.

2.5.3 EMPRESA ESTRATÉGICA DE DEFESA (EED)

Toda pessoa jurídica credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das seguintes condições:

a) ter como finalidade, em seu objeto social, a realização ou condução de atividades de pesquisa, projeto, desenvolvimento, industrialização, prestação dos serviços referidos no art. 10 da Lei nº 12.598/2012, produção, reparo, conservação, revisão, conversão, modernização ou manutenção de PED no País, incluídas a venda e a revenda somente quando integradas às atividades industriais supracitadas;

b) ter no País a sede, a sua administração e o estabelecimento industrial, equiparado a industrial ou prestador de serviço;

c) dispor, no País, de comprovado conhecimento científico ou tecnológico próprio ou complementado por acordos de parceria com Instituição

d) Científica e Tecnológica para realização de atividades conjuntas de pesquisa científica e tecnológica e desenvolvimento de tecnologia, produto ou processo, relacionado à atividade desenvolvida;

e) assegurar, em seus atos constitutivos ou nos atos de seu controlador direto ou indireto, que o conjunto de sócios ou acionistas e grupos de sócios ou acionistas estrangeiros não possam exercer em cada assembleia geral número de votos superior a 2/3 (dois terços) do total de votos que puderem ser exercidos pelos acionistas brasileiros presentes; e

f) assegurar a continuidade produtiva no País (Lei 12.598/2012).

2.5.4 ENDEREÇO DE CORREIO ELETRÔNICO

Nome único de uma caixa postal eletrônica, de uma pessoa, grupo ou organização, associado a um serviço de correio eletrônico. É formado por um identificador (nome, apelido, sigla ou código), um sinal "@" e o domínio do provedor do serviço.

2.5.5 ENDEREÇO IP (INTERNET PROTOCOL)

Refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

2.5.6 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.

2.5.7 ERRO

Falha ou vulnerabilidade que pode resultar em incidentes.

2.5.8 ERRO CONHECIDO

Problema que já foi analisado, porém ainda não foi resolvido.

2.5.9 ESCOPO DA AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

Partes da Organização Militar que serão auditadas.

2.5.10 ESPAÇO CIBERNÉTICO

Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

2.5.11 ESTAÇÕES DE TRABALHO

Computadoresdestinadosaosusuários.

2.5.12 ESTIMATIVA DE RISCO

Processo utilizado para atribuir valores à probabilidade e consequências de um risco.

2.5.13 ESTRUTURA DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (STI)

A estrutura do STI é formada pelo Órgão Central e Elos.

2.5.14 ETIR

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

2.5.15 EVENTO

Mudança de estado de relevância para o gerenciamento de um serviço ou de outro item de configuração.

2.5.16 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.

2.5.17 EVIDÊNCIA DE AUDITORIA

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

2.5.18 EVIDÊNCIA DIGITAL

Informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.

2.5.19 EVITAR RISCO

Uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco.

2.5.20 EXCLUSÃO DE ACESSO

Processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

2.5.21 EXERCÍCIO DE *RED TEAM* (Time Vermelho)

Atividade em que são utilizadas Táticas, Técnicas e Procedimentos (TTP) para emular uma ameaça cibernética real, com o objetivo de melhorar e medir a efetividade da equipe, dos processos e das tecnologias de defesa da organização.

2.5.22 EXPLOIT

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

2.5.23 EXPLORAÇÃO CIBERNÉTICA

Consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas.

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 FALHA

Ocorrência que implica na perda da habilidade de operar de acordo com requisitos especificados ou de entregar a saída ou o resultado esperado.

2.6.3 FILTRO DE PACOTES

Conjunto de regras que permitem ou bloqueiam o trânsito de pacotes entre redes distintas ou de qualquer rede com um determinado dispositivo. Comumente utilizado em sistemas de Firewall ou na proteção local de hosts.

2.6.4 FIREWALL

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

2.6.5 FONTE CIBERNÉTICA

Recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência.

2.6.6 FONTE DE RISCO

Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

2.6.7 FORMATO ABERTO

Formato de arquivo não proprietário, cuja especificação esteja documentada publicamente e seja de livre conhecimento e implementação, livre de patentes ou qualquer outra restrição legal quanto à sua utilização.

2.6.8 FORNECEDOR

Organização ou parte de uma organização que é externa à organização do provedor do serviço e regida em um contrato com o provedor de serviço para contribuir com o desenho, transição, entrega e melhoria de um serviço ou serviços ou processos.

2.6.9 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.

2.6.10 FUNÇÃO

Uma equipe ou grupo de pessoas e as ferramentas ou outros recursos que são utilizados para conduzir um ou mais processos ou atividades, por exemplo, a Central de Serviços. Também pode ser um propósito específico para um item de configuração, pessoa, equipe, processo ou serviço de TI.

2.6.11 FUNÇÃO DA CENTRAL DE SERVIÇOS DO SAUTI

A Central de Serviços do SAUTI deve ser utilizada para receber, registrar, encaminhar e monitorar os incidentes/problemas de TI registrados, interagindo com os Processos de fornecimento de serviço (Gerenciamento de incidentes, e requisições de serviços, Gerenciamento de Problemas), Gerenciamento de Serviços (Mudanças e Problemas).

2.7 LETRA G

2.7.1 GERENCIAMENTO DE INCIDENTE

Prática de minimizar o impacto negativo de incidentes restaurando a operação normal do serviço o mais rápido possível. Por esse motivo, o gerenciamento de incidente pode ter um enorme impacto na satisfação e de como o cliente e o usuário percebem o provedor de serviço.

2.7.2 GESTÃO DE CONTINUIDADE

Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

2.7.3 GESTÃO DE DADOS

O desenvolvimento, execução e supervisão de planos, políticas, programas e práticas que entreguem, controlem, protejam e aprimorem o valor dos ativos de dados e de informações ao longo de seus ciclos de vida.

2.7.4 GESTÃO DE MUDANÇAS

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

2.7.5 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.

2.7.6 GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Ações e métodos que visam à integração das 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 segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

2.7.7 GESTÃO DE SERVIÇOS DE TI NOS ELOS DO STI

O sistema de gestão de serviços de TI nos Elos do STI são Organizações ou frações de Organizações do COMAER responsáveis por atividades e ativos de TI em uma determinada instalação e subordinadas sistemicamente ao Órgão Central do STI.

2.7.8 GESTOR

Profissional que exerce formalmente função de gestão em qualquer nível hierárquico da organização. Profissional da organização que tem outros profissionais formalmente subordinados a ele (ex. gerentes, supervisores, chefes).

2.7.9 GESTOR DE SEGURANÇA DA INFORMAÇÃO

O Chefe da Assessoria de Segurança de Sistemas de Informação responsável pelas ações de segurança da informação.

2.7.10 GOVERNANÇA

Compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. É o sistema pelo qual as organizações são dirigidas e controladas. Pode ser entendido como o conjunto de ações e responsabilidades exercidas pela alta administração da empresa, órgão ou entidade, com o objetivo de oferecer orientação estratégica e garantir que os objetivos sejam alcançados, com simultânea gerência de riscos e verificação de que os recursos são utilizados de forma responsável.

2.7.11 GOVERNANÇA CORPORATIVA

É o sistema pelo qual as organizações são dirigidas e controladas. Pode ser entendido como o conjunto de ações e responsabilidades exercidas pela alta administração da empresa, órgão ou entidade, com o objetivo de oferecer orientação estratégica e garantir que os objetivos sejam alcançados, com simultânea gerência de riscos e verificação de que os recursos são utilizados de forma responsável.

2.7.12 GOVERNANÇA DE DADOS

Conjunto de políticas, processos, pessoas e tecnologias que visam a estruturar e administrar os ativos de informação, com o objetivo de aprimorar a eficiência dos processos de gestão e da qualidade dos dados, a fim de promover eficiência operacional, bem como garantir a confiabilidade das informações que suportam a tomada de decisão.

2.7.13 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 COMAER, atribuindo responsabilidade e capacidade de tomada de decisão, bem como respeitando as leis e regulamentos.

2.7.14 GOVERNANÇA DE TI OU GOVERNANÇA CORPORATIVA DE TI

É o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização. [

2.7.15 GOVERNANÇA DIGITAL

A utilização pelo setor público de recursos de tecnologia da informação e comunicação com o objetivo de melhorar a disponibilização de informação e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo.

2.7.16 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.

2.7.17 GRUPO INTERNO

Parte da organização do provedor de serviço que tem um acordo documentado com o provedor de serviço para contribuir com o desenho, transição, entrega e melhoria de um ou mais serviços.

2.7.18 GUERRA CIBERNÉTICA

Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC.

2.7.19 GUERRA ELETRÔNICA

Conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas.

2.7.20 GUERRA ELETRÔNICA ATIVA

Qualquer ação de guerra eletrônica que utilize emissão de energia eletromagnética.

2.7.21 GUERRA ELETRÔNICA PASSIVA

Qualquer ação de guerra eletrônica que consista em captar energia eletromagnética, sem emitir.

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. Tem conhecimento das falhas de segurança dos sistemas, estando sempre em busca de novos desafios e conhecimento, alémde evitar corromper informações intencionalmente.

2.8.2 HTML

Do Inglês *Hyper text Markup Language*. Linguagem universal utilizada na elaboração de páginas na Internet.

2.8.3 HTTP

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

2.8.4 HTTPS

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

2.9 LETRA I

2.9.1 IDS

Do Inglês *Intrusion Detection System* Programa, ou conjunto de programas,cuja função é detectar tráfego de rede malicioso.

2.9.2 IMPACTO

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

2.9.3 INCIDENTE

Qualquer evento que não faz parte do funcionamento padrão de um serviço e que causa, ou pode causar, uma interrupção no serviço ou uma redução de sua qualidade.

2.9.4 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.

2.9.5 INDÍCIOS

Vestígio, indicação de algo que pode se tornar uma ameaça.

2.9.6 INFORMAÇÃO

Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Conjunto de dados, processados ou não, utilizados para produção e transmissão de conhecimento entre indivíduos ou máquinas, contidos em qualquer meio, suporte ou formato, 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.

2.9.7 INFRAESTRUTURAS CRÍTICAS

Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

2.9.8 INTEGRIDADE

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

2.9.9 INTELIGÊNCIA DE NEGÓCIOS (BUSINESS INTELLIGENCE)

Análise e Inteligência de Negócios (*Analytics and Business Intelligence - ABI*) é um termo abrangente que inclui aplicativos, infraestrutura, ferramentas e melhores práticas que permitem o acesso e a análise de informações para melhorar e otimizar decisões e desempenhos.

2.9.10 INTERNET

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

2.9.11 INVASÃO

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

2.9.12 INVASOR

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

2.9.13 IPS

Do Inglês Intrusion Prevention System. Programa, ou um conjunto de programas, cuja função é detectar e bloquear tráfego de rede malicioso. Comumente utilizado em sistemas de Firewall juntamente com filtros de pacote e IDS.

2.9.14 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.

2.9.15 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 define formas de garantir a segurança da aplicação para o usuário final.

2.9.16 ITEM DE CONFIGURAÇÃO (IC)

Componente cuja gerência é necessária para a entrega de um serviço de TI.

2.10 LETRA K

2.10.1 KEYLOGGER

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

2.11 LETRA L

2.11.1 LEGALIDADE

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

2.11.2 LEGITIMIDADE

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

2.11.3 LEGALIDADE

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

2.11.4 LEGITIMIDADE

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

2.11.5 LGPD

Lei Geral de Proteção de Dados Pessoais, Lei nº 13,709 de 14 de agosto de 2018, que versa sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.11.6 LIBERAÇÃO

Agrupamento de um ou mais itens de configuração, novos ou modificados, implantados no ambiente de produção como resultado de uma ou mais mudanças.

2.12 LETRA M

2.12.1 MALWARE

Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm, bot, spyware, backdoor*, cavalo de tróia e *rootkit*.

2.12.2 MATERIAL SIGILOSO

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

2.12.3 MATURIDADE

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

2.12.4 MEDIDAS ESPECIAIS DE SEGURANÇA

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

2.12.5 METADADOS

Metadados são informações que descrevem características de determinado dado, explicando-o em certo contexto de uso; permitem organizar, classificar e relacionar os dados.

2.12.6 MELHORIA CONTÍNUA

Atividade recorrente para aumentar a habilidade de atender requisitos de serviço.

2.12.7 MEMÓRIA

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

2.12.8 MODELO DE BANCO DE DADOS

Representação gráfica que, através de uma linguagem de modelagem de dados, descreve os tipos de informações que serão armazenadas em um banco de dados. O modelo pode tanto ser conceitual, cuja representação é feita independente da implementação em um Sistema de Gerenciamento de Banco de Dados (SGBD), ou com um nível de abstração lógica, cujo modelo leva em consideração o tipo de SGBD utilizado.

2.12.9 MODELO OSI

Modelo de referência para que fabricantes de software e hardware desenvolvam produtos de rede compatíveis entre si. Normatizado através da ISO/IEC 7498-1, de 1994.

2.12.10 MODELO DE CLASSES

Diagrama de modelagem orientado a objetos que exibe o conjunto de classes e seus relacionamentos. Existem três perspectivas para o Diagrama de Classes: Modelo de Classes de Análise: representa as classes no domínio do negócio, sem levar em consideração detalhes referentes à tecnologia a ser utilizada na solução de um problema; Modelo de Classes de Projeto: é obtido através da adição de detalhes ao modelo anterior conforme a solução de software adotada; Modelo de Classes de Implementação: corresponde à implementação das classes em uma determinada linguagem de programação.

2.13 LETRA N

2.13.1 NÃO CONFORMIDADE

Não atendimento a um requisito.

2.13.2 NECESSIDADE DE CONHECER

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

2.13.3 NEGAÇÃO DE SERVIÇO

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

2.13.4 NEGÓCIO

Uma entidade corporativa em geral ou organização constituída por um determinado número de unidades de negócio. No contexto do GSTI, o termo inclui o setor público e organizações sem fins lucrativos, bem como empresas. Um provedor de serviço de TI provê serviços de TI para um cliente que é parte de um negócio. O provedor de serviço de TI pode fazer parte do mesmo negócio que seu cliente (provedor de serviço interno) ou fazer parte de outro negócio (provedor de serviço externo).

2.13.5 NECESSIDADE OPERACIONAL (NOP)

No contexto do Ciclo de Vida de um Sistema de TI, é uma carência de informação, deficiência ou oportunidade de inovação constatada, cuja solução depende da implantação de um Sistema de TI, a ser adquirido ou desenvolvido, ou da modificação/modernização de um Sistema já existente.

2.14 LETRA O

2.14.1 OBSERVAÇÃO DE AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

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

2.14.2 ÓRGÃO CENTRAL

O 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.

2.14.3 OSTENSIVO

Sem classificação, cujo acesso pode ser franqueado.

2.15 LETRA P

2.15.1 PADRONIZAÇÃO

Desenvolvimento e implementação de conceitos, doutrinas, procedimentos e propósitos para alcançar e manter o almejado nível de compatibilidade, intercambiabilidade no campo operacional, procedimental, material, técnico e administrativo.

2.15.2 PAPÉIS DE TRABALHO DOS AUDITORES

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

2.15.3 PARTES EXTERNAS

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

2.15.4 PARTE INTERESSADA

Pessoa ou grupo que tem um interesse específico no desempenho ou no sucesso da atividade ou atividades do provedor de serviço. Exemplo: Clientes, proprietários, gerência, pessoas na organização do provedor de serviço, fornecedores, banqueiros, sindicatos ou parceiros.

2.15.5 PATCHES

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

2.15.6 PDA

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

2.15.7 PDCA (PLAN-DO-CHECK-ACT)

Metodologia de melhoria contínua referenciada pela norma ABNT NBR ISO/IEC 27001.

2.15.8 PGP

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

2.15.9 PHISHING

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

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

2.15.10 PLANEJAMENTO DE TI

O Planejamento de TI é um processo gerencial destinado a atender às necessidades finalísticas e de informação de órgão ou entidade para determinado período. Para tanto, é necessário definir metas, ações e projetos para suprir tais necessidades. Constitui-se, ainda, em um importante complemento ao planejamento estratégico institucional, compreendendo diretrizes e ações transversais que suportam objetivos de negócio de todas as áreas da organização. Observe-se que não se trata do documento elaborado ao fim do processo, o qual pode ser chamado, por exemplo, de plano diretor de tecnologia da informação (PDTI) ou podem ser elaborados mais de um documento, como um Plano Estratégico de TI (PETI) e um PDTI. Tanto o PDTI quanto o PETI são exemplos de produtos resultantes do processo de Planejamento de TI.

2.15.11 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 influenciar diretamente na continuidade da instituição.

2.15.12 PLANO DE AUDITORIA

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

2.15.13 PLANO DE COMUNICAÇÃO DE MUDANÇA

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

2.15.14 PLANO DE CONTINGÊNCIA (PCG)

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

2.15.15 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. Sob o ponto de vista do Plano de Continuidade de Negócios, o funcionamento 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 sejam afetados.

2.15.16 PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Descreve o desenvolvimento de ações para garantir a continuidade operacional, considerando situações de desastre e de contingência.

2.15.17 PLANO DE GERENCIAMENTO DE INCIDENTES

Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

2.15.18 PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

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

2.15.19 PLANO DE RECUPERAÇÃO DE NEGÓCIOS

Documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.

2.15.20 PLANO DE RESTAURAÇÃO

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

2.15.21 PLANO DE TECNOLOGIA DA INFORMAÇÃO

É o plano resultante do processo de planejamento de TI, que contempla todas as atividades de planejamento estratégico e tático de TI.

2.15.22 PLANO DE TESTES

Planos que contêm os objetivos e metas globais do teste de software previsto.

2.15.23 CASOS DE TESTE

Descrevem uma situação que deverá ser testada, derivada diretamente dos Casos de Uso do sistema.

2.15.24 PODER CIBERNÉTICO

Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.

2.15.25 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento aprovado pelo Cmt do COMAER, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação no âmbito do COMAER.

2.15.26 PORTFÓLIO DE PROJETOS DE TECNOLOGIA DA INFORMAÇÃO

É a relação de projetos de Tecnologia da Informação que atendem os propósitos estratégicos da organização.

2.15.27 PRESTADOR DE SERVIÇO

Pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.

2.15.28 PRIMARIEDADE

Qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

2.15.29 PROBLEMA

Causa-raiz de um ou mais incidentes.

2.15.30 PROCEDIMENTO

Forma especificada de executar uma atividade ou um processo. Procedimentos podem ser documentados ou não.

2.15.31 PROCESSOS

Conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos.

Conjunto de atividades logicamente estruturadas que transformam insumos (entradas) em produtos (saídas). 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 COMAER.

2.15.32 PROCESSO DE GESTÃO DE PORTFÓLIO DE PROJETOS

O processo que proporciona o investimento de recursos físicos e financeiros adequados, e aprova as autoridades necessárias para o estabelecimento dos projetos selecionados. Realizar qualificação contínua de projetos, a fim de confirmar que eles justificam ou podem ser redirecionados a justificarem investimento contínuo. Seu propósito é iniciar e sustentar projetos adequados, suficientes e necessários a fim de satisfazer os objetivos estratégicos da organização.

2.15.33 PROCESSO DE GERENCIAMENTO DE CONFIGURAÇÃO E ATIVOS

É o processo responsável tanto pelo Gerenciamento da Configuração quanto pelo Gerenciamento de Ativos. Gerenciamento de Ativos é o processo de negócio responsável por rastrear e apresentar o valor e a responsabilidade financeira dos ativos durante o seu ciclo de vida. Já o Gerenciamento da Configuração é o processo responsável por manter as informações sobre os itens de configuração necessários para entrega de serviços de TI, incluindo seus relacionamentos.

2.15.34 PROCESSO DE GESTÃO DE ATIVOS

É o processo responsável por gerenciar e administrar qualquer recurso ou habilidade. Ativos de um Provedor de Serviço inclui qualquer coisa que pode contribuir para a entrega de um Serviço. Ativos podem ser qualquer um dos seguintes tipos: Gerência, Organização, Processo, Conhecimento, Pessoas, Informações, Aplicativos, Infraestrutura e Capital Financeiro.

2.15.35 PROCESSO DE GESTÃO DE INCIDENTES

É o processo responsável por gerir o ciclo de vida de todos os Incidentes. O principal objetivo da Gestão de Incidente é restabelecer o Serviço de TI aos Usuários o mais rápido possível. Conceito de incidente: 1) uma interrupção não planejada de um Serviço de TI ou uma redução da Qualidade de um Serviço de TI. Falha de um Item de

Configuração que ainda não tenha impactado um Serviço de TI é também um Incidente. 2) um evento ou uma série de eventos indesejados ou inesperados e que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

2.15.36 PROCESSO DE GESTÃO DE MUDANÇAS

É o processo responsável por controlar o ciclo de vida de todas as mudanças. O principal objetivo do Gerenciamento de Mudança é permitir que Mudanças que gerem benefícios sejam feitas, com a mínima interrupção aos Serviços de TI.

2.15.37 PROCESSO DE SOFTWARE

Processo de trabalho usado por uma organização na produção/aquisição de software e na gestão de seu ciclo de vida. Inclui atividades realizadas nas fases de definição, desenvolvimento, operação e retirada do software.

2.15.38 PROCESSO DE TRABALHO

Conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos/serviços (saídas) com valor agregado. Processos são geralmente planejados e realizados de maneira contínua para agregar valor na geração de produtos e serviços. Processos podem ser agrupados em macroprocessos e subdivididos em subprocessos.

2.15.39 PROCESSO PARA CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES

É o processo que visa garantir que cada informação tenha o tratamento de segurança adequado à sua importância para a organização. Convém que a informação seja classificada em termos de seu valor, requisitos legais, criticidade e sensibilidade para evitar modificação ou divulgação não autorizada.

2.15.40 PROCESSOS DE NEGÓCIO

Um processo que pertence e é executado pelo negócio. Um Processo de Negócio contribui para a entrega de um produto ou Serviço aos Clientes de negócio. Por exemplo: um comerciante que tenha um Processo de compra que ajude a entregar um serviço a seus Clientes de Negócio. Muitos Processos de Negócios dependem de Serviços de TI.

2.15.41 PRODUTO

Saída de uma organização que pode ser produzida sem transação alguma ocorrendo entre a organização e o cliente.

Nota: O elemento dominante de um produto é que ele geralmente é tangível.

2.15.42 PROJETO

Conjunto harmônico de ações definidas e quantificadas quanto ao propósito, características, metas, custos e tempo de realização, visando ao atendimento de uma necessidade específica.

2.15.43 PROJETO DE INTERFACE

É a documentação que representa a arquitetura da informação, detalhes de operação, requisitos e características de interface. O projeto pode ser um desenho informal, um conjunto de frames ou um protótipo, desde que proporcione uma melhor visão do sistema que será entregue, do ponto de vista do usuário.

2.15.44 PROTEÇÃO CIBERNÉTICA

Ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.

2.15.45 PROTÓTIPO

Modelo ou implementação preliminar de um produto ou sistema usado para avaliar sua arquitetura, desenho, performance, potencial de produção, documentação dos requisitos ou obter melhor entendimento sobre o mesmo.

2.15.46 PROVEDOR DE SERVIÇO

Organização ou parte de uma organização que gerencia e entrega um serviço ou serviços para o cliente.

2.15.47 PROVEDOR DE SERVIÇO DE TI

Um provedor de serviço que fornece serviços de TI para clientes internos ou externos.

2.15.48 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 LETRA Q

2.16.1 QUEBRA DE SEGURANÇA DA INFORMAÇÃO

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

2.17 LETRA R

2.17.1 RECLASSIFICAÇÃO

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

2.17.2 RECOMENDAÇÃO DE AUDITORIA

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

2.17.3 REDE SEM FIO

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

2.17.4 REDES SOCIAIS

Estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

2.17.5 REGISTRO

Documento que apresenta resultados obtidos ou fornece evidência de atividades realizadas. Exemplos: Relatórios de auditoria, relatórios de incidentes, registros de treinamento ou atas de reuniões.

2.17.6 RELATÓRIO DE AUDITORIA

Relatório formal com os principais resultados e conclusões da auditoria.

2.17.7 RELATÓRIO TÉCNICO DE ANÁLISE DO ANS

É o relatório que reflete os resultados da análise do ANS e do ANO do serviço de TI, prestado pelo provedor de serviço de TI, realizada por meio da comissão de análise do ANS, conforme legislação de TI específica.

2.17.8 RESILIÊNCIA

Capacidade coletiva e individual de absorver o impacto das adversidades, reagir com efetividade; recuperar-se e adaptar-se com rapidez; e perseverar, sem perder o foco no cumprimento da missão.

2.17.9 RESILIÊNCIA CIBERNÉTICA

Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa.

2.17.10 REQUISIÇÃO DE MUDANÇAS

Proposta para uma mudança a ser feita em um serviço, componente de serviço ou sistema de gestão de serviços.Uma mudança para um serviço inclui a provisão de um serviço novo ou a remoção de um serviço que não é mais requerido. [FONTE: ABNT NBR ISO 20000-1:2011].

2.17.11 REQUISITO OPERACIONAL (ROP)

É o documento emitido pelo EMAER, com base na NOP, que apresenta a descrição inicial das características de desempenho que o Sistema ou o Material deverá apresentar, em termos qualitativos e quantitativos, levando em conta a sua missão ou aplicação e a sua segurança em serviço.

2.17.12 REQUISITOS TECNICOS, LOGÍSTICOS E INDUSTRIAIS (RTLI)

É o documento que decorre do ROP e consiste na fixação das características técnicas, logísticas e industriais que o Sistema ou Material deverá ter para cumprir os requisitos operacionais estabelecidos.

2.17.13 REQUISITOS DE SEGURANÇA

Conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não

funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense.

2.17.14 REQUISIÇÃO DE SERVIÇO

Requisição de informação, aconselhamento, acesso a um serviço ou uma modificação pré-aprovada.

2.17.15 REQUISITOS DO SERVIÇO

Necessidade de um cliente e de usuários do serviço, incluindo requisitos do nível de serviço e as necessidades do provedor de serviço.

2.17.16 REQUISITOS DE SOFTWARE

Conforme estabelece a IN 04 em seu Cap. 1, Art. 2º. XI (atual: IN 01 de 05-04-2019 em seu Cap. 1, Art. 2º. IX), os requisitos constituem o "conjunto de características e especificações necessárias para definir a Solução de Tecnologia da Informação e Comunicação (TIC) a ser contratada"; Requisitos Funcionais: dizem respeito a características implementadas que serão traduzidas em funcionalidades do sistema; Requisitos Não-Funcionais: versam sobre características do sistema em termos de performance, usabilidade, confiabilidade, documentação, segurança e demais fatores não relacionados a funcionalidades.

2.17.17 RETER RISCOS

Uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

2.17.18 RISCO

Possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos (COSO, 2004); possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades (TCU, 2010f); efeito da incerteza nos objetivos (ABNT, 2009).

2.17.19 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 LETRA S

2.18.1 SATISFAÇÃO DO CLIENTE

Percepção do cliente no qual seus requisitos foram atendidos.

2.18.2 SCAN

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

2.18.3 SCANNER

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

2.18.4 SCREENLOGGER

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

2.18.5 SECURITY OFFICER

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

2.18.6 SEGURANÇA CIBERNÉTICA

Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas.

2.18.7 SEGURANÇA DA INFORMAÇÃO

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

2.18.8 SENHA

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

2.18.9 SENHA ADMINISTRATIVA

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

2.18.10 SENHA NÃO-ADMINISTRATIVA

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

2.18.11 SERVIÇO

Saída de uma organização, com pelo menos uma atividade necessariamente realizada entre a organização e o cliente. Nota: Os elementos dominantes de um serviço são geralmente intangíveis.

2.18.12 SERVIÇO DE TI

Um serviço fornecido por um provedor de serviço de TI. Um serviço de TI é composto de uma combinação de tecnologia da informação, pessoas e processos. Um serviço de TI voltado para o cliente suporta diretamente os processos de negócio de um ou mais clientes e convém que as suas metas de nível de serviço sejam definidas em um acordo de nível de serviço. Outros serviços de TI, chamados serviços de apoio, não são diretamente usados pelo negócio, porém são exigidos pelo provedor de serviço para entregar serviços voltados ao cliente.

2.18.13 SIGILO

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

2.18.14 SINAL

É chamado de sinal a informação baseada em um indício ou ameaça após ser parametrizada, consolidada e inserida por um sensor na rede de identificação de ameaças e geração de alertas.

2.18.15 SISTEMA

É o conjunto de elementos integrantes e interdependentes que têm por finalidade realizar uma tarefa de apoio em proveito da missão principal de uma organização. A vinculação desses elementos, entre si, ocorre por interesse de coordenação, orientação técnica e normativa.

2.18.16 SISTEMAS CRÍTICOS

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

2.18.17 SISTEMA DE GESTÃO DE SERVIÇOS (SGS)

Sistema de Gestão para dirigir e controlar as atividades de gerenciamento de serviço do provedor de serviços. O SGS inclui todas as políticas, objetivos, planos, processos, documentos e recursos de gerenciamento de serviço requeridos para o desenho, transição, entrega e melhoria dos serviços e para atingir os requisitos da Gestão de Serviços de TI.

2.18.18 SISTEMAS DE INFORMAÇÃO

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

2.18.19 SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (STI)

Sistema reformulado pela Portaria nº 549/GC3, de 9 de agosto de 2010, com a finalidade de organizar, disciplinar e controlar as atividades de Tecnologia da Informação (TI), em consonância com as políticas específicas do Governo Federal e com a Política da Aeronáutica para a Tecnologia da Informação.

2.18.20 SISTEMA INFORMATIZADO OU SISTEMA AUTOMATIZADO

Aplicativo de TI que implementa funcionalidade eletrônica que constitui parte de processo de negócio realizado pela TI ou com auxílio da TI.

2.18.21 SITE

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

2.18.22 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 (período de teste/avaliação) e, caso seja utilizado, o utilizador tem a obrigação moral de enviar o pagamento ao seu autor (na ordem de algumas - poucas - dezenas de dólares). Quando é feito o registro, é normal receber-se um manual impresso do programa, assim como uma versão melhorada, possibilidade de assistência técnica e informações acerca de novas versões.

2.18.23 SNIFFERS

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

2.18.24 SOFTWARE

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

2.18.25 SOFTWARE ANTIVÍRUS

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

2.18.26 SOLUÇÃO DE TI

Conjunto de bens e/ou serviços de TI que se integram para o alcance dos resultados pretendidos com a contratação.

2.18.27 SPAM

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

2.18.28 SPAMMER

Pessoa que envia spam.

2.18.29 SPYWARE

Sistema com comportamento malicioso destinado à coleta de informações sobre uma pessoa ou organização. Tal informação é enviada para outra entidade que poderá utilizá-la em prejuízo de seu proprietário.

2.18.30 SMS

Do Inglês *Short Message Service*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

2.18.31 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.

2.18.32 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.

2.18.33 SSL

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

2.18.34 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 LETRA T

2.19.1 TECNOLOGIA DA INFORMAÇÃO (TI)

Engloba todos os recursos necessários para adquirir, processar, armazenar e disseminar informações. Inclui "Tecnologia da Comunicação (TC)" e é sinônimo de "Tecnologia da Informação e Comunicação (TIC)".

2.19.2 TEMPO OBJETIVO DE RECUPERAÇÃO

É o tempo predefinido no qual uma atividade deverá estar disponível após uma interrupção ou incidente.

2.19.3 TESTE DE AUDITORIA

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

2.19.4 TESTE DE INTRUSÃO

O Teste de Intrusão consiste em atividade, previamente autorizada e com escopo definido, que busca identificar e explorar vulnerabilidades cibernéticas encontradas em determinado sistema, aplicação, ou infraestrutura de rede. O teste de intrusão tem por finalidade o levantamento das vulnerabilidades e da efetividade de sua exploração. O teste pode ocorrer nas modalidades "Caixa Branca", "Caixa Cinza", ou "Caixa Preta".

2.19.5 TOKENS

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

2.19.6 TRANSIÇÃO

Atividades envolvidas em mover um serviço novo ou modificado para ou a partir de um ambiente de produção.

2.19.7 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 a identificação de tendências.

2.19.8 TRATAMENTO DE RISCO

Processo de modificar um risco (ABNT, 2009). Consiste em selecionar e implementar uma ou mais opções de resposta a riscos para modificar os níveis de risco (INTOSAI, 2007). Definição das ações para reduzir a probabilidade de ocorrência dos eventos ou suas consequências (BRASIL, 2017).

2.20 LETRA U

2.20.1 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/.

2.20.2 USUÁRIO

Uma pessoa que usa o serviço de TI no dia-a-dia. Usuários são diferentes de clientes, pois alguns clientes não usam o serviço de TI diretamente.

2.21 LETRA V

2.21.1 VAZAMENTO

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

2.21.2 VISITA

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

2.21.3 VÍRUS

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

2.21.4 VPN

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

2.21.5 VULNERABILIDADE

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

2.21.6 VULNERABILIDADE DE 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 hackers em 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.

2.22 LETRA W

2.22.1 WEBMAIL

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

2.22.2 WEP

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

2.22.3 WI-FI

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

2.22.4 WIRELESS

Rede sem fio.

2.22.5 WORKSHOP

Atividade que, normalmente atrelada a uma conferência, busca aprofundar os conhecimentos sobre um assunto de forma mais prática e detalhada. A dinâmica, que conta com um moderador e um ou dois expositores de renome, divide-se em três etapas: exposição; discussão em grupos e conclusão.

2.22.6 WORLD WIDE WEB

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

2.22.7 WORM

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

2.22.8 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.

2.22.9 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 LETRA Z

2.23.1 ZERO-DAY VULNERABITLY

Veja Vulnerabilidade de Dia Zero.

3 DISPOSIÇÕES TRANSITÓRIAS

Caso descortine-se atualização relevante para o tema abordado nesta publicação, a mesma deverá ser revisada para atualização imediata pelo Órgão Central do STI, revogando-se as disposições em contrário

4 DISPOSIÇÕES FINAIS

A legislação complementar aopresente Manualserá posteriormente elaborada conforme a necessidade.

Os casos não previstos neste Manualserão submetidos à apreciação do Diretor de Tecnologia da Informação da Aeronáutica.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT).ABNT NBR 10719: 2015. *Informação e documentação — Relatório técnico e/ou científico — Apresentação.* 4ª edição: 25.05.2015. Válida a partir de: 25.06.2015.

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

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

_____. ABNT NBR ISO/IEC 12207:2009 – *Engenharia de sistemas e software – Processos de ciclo de vida de software.*

_____. ABNT NBR ISO/IEC 15504-1*, Tecnologia da informação – Avaliação de processo – Parte 1: Conceitos e Vocabulário.*

_____. ABNT NBR ISO/IEC 15504-2*, Tecnologia da informação – Avaliação de processo – Parte 2: Realização de uma avaliação.*

_____. ABNT NBR ISO/IEC 15504-3*, Tecnologia da informação – Avaliação de processo – Parte 3: Orientações para realização de uma avaliação.*

_____. ABNT NBR ISO/IEC 20000-1, *Tecnologia da Informação- Gestão de Serviços – Parte 1:Requisitos do sistema de gestão de serviços.*

_____. ABNT NBR ISO/IEC 20000-2, *Tecnologia da Informação- Gerenciamento de serviços - Parte 1:Especificação e Parte 2:Código de prática.*

_____. ABNT ISO/IEC 20000-3, *Tecnologia da Informação- Gerenciamento de serviços- Parte 3:Direcionamento para a definição do escopo e aplicabilidade da ABNT NBR ISO/IEC 20000-1.*

_____. ABNT NBR ISO 31000:2009 – Gestão de Riscos – Princípios e diretrizes. Rio de Janeiro, 2009.

_____. ABNT ISO/IEC TR 20000-5*, Tecnologia da informação – Gerenciamento de serviços- Parte 5: Exemplo de um plano de implementação da ABNT NBR ISO/IEC 20000-1*.

_____. ISO GUIA 73:2009 – *Gestão de Riscos* – Vocabulário. Rio de Janeiro, 2009.

BRASIL. Acórdão 2.585/2012 - TCU-Plenário. Relator: Ministro Walton Alencar Rodrigues. Disponível em: <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/pesquisa/acordao-completo>. Acesso em: 23 fev. 2017.

_____. Ato nº 233/2013. Institui a Política de Gerenciamento de Serviços de TI no âmbito do Tribunal Regional do Trabalho da 11ª. Região. Fortaleza, 2013.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica.*Gestão de Serviços de Tecnologia da Informação nos Elos Especializados do Sistema de Tecnologia da Informação do Comando da Aeronáutica*: **ICA 7-4**. Rio de Janeiro, RJ, 2016.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica.*Manual do Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo (DECEA),* de 2012: **MCA 7-1**. [Rio de Janeiro], 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Glossário *de Segurança da Informação.* Portaria Nº 93, de 26 de setembro de 2019 – DOU. Disponível em:<http://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 2020

_____. BTCU Administrativo | Ano 51 | n° 94 – Glossário.

_____. _____. Diretoria de Tecnologia da Informação da Aeronáutica. *Gestão de Serviçosde Tecnologia da Informação nos Elos de Serviço de Tecnologia da Informação de "nível 2"*:**ICA 7-6**. Rio de Janeiro, RJ, 2016.

_____. Comando da Aeronáutica. Gabinete do Comandante. *Implantação e Gerenciamento de Sistemas no Comando da Aeronáutica*:**ICA 700-1**. Brasília. 2006.

_____. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Atribuições Específicas para os Centros de Computação da Aeronáutica (CCA):***NSCA 7-6**.Rio de Janeiro, RJ,2005.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Estrutura e Competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI)*: **NSCA 7-7**.Brasília, DF, 2004.

_____. Comando da Aeronáutica. Comando-Geral de Apoio. *Funcionamento do Serviço de Atendimento ao Usuário de tecnologia da Informação do Comando da Aeronáutica:***NSCA7-8**. Brasília, DF, 2015.

_____. Decreto nº 8.777, de 11 de maio de 2016**.** Institui a Política de Dados Abertos do Poder Executivo federal. Diário Oficial da União, 12 mai. 2016.

_____. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal) - Glossário.

_____. Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações– versão 2.0 (2015-2018) - Glossário.

_____. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação– versão 01 (nov./2010) - Glossário.

_____. Glossário das Forças Armadas – **MD35-G-01** (5ª Edição/2015)

_____. Infraestrutura Nacional de Dados Abertos (INDA). Instrução Normativa nº 4, de 13 de abril de 2012. Diário Oficial da União, 13 abr. 2012. Seção 1, p. 67.

_____. Instrução Normativa 63, de 1º de setembro de 2010. Estabelece normas de organização e de apresentação dos relatórios de gestão e das peças complementares que constituirão os processos de contas da administração pública federal, para julgamento do Tribunal de Contas da União. Brasília, 2010.

_____. Levantamento de Governança de TI 2016 – Glossário.

_____. Levantamento Integrado de Governança Organizacional Pública - ciclo 2017 – Glossário.

_____. Padrões de Levantamento. Portaria-Segecex nº 11/2011.

_____. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa 01/DSIC/GSIPR. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Diário Oficial da União n 115, 18 jun. 2008, seção 1.

_____. Referencial Básico de Governança: Aplicável a Órgãos e Entidades da Administração Pública. Versão 2. Brasília, 2014. Disponível em: <http://portal.tcu.gov.br/comunidades/governanca/entendendo-a-governanca/referencial-de-governanca/>. Acesso em: 23 fev. 2017.

_____. Secretaria de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Cartilha Técnica para Publicação de Dados Abertos. Disponível em: <http://dados.gov.br/paginas/cartilha-publicacao-dados-abertos>. Acesso em: 23 fev. 2017.

_____. Secretaria de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Guia de Elaboração do PDTI do Sisp. Versão 2.0 beta. Brasília, 2015. Disponível em: <http://www.sisp.gov.br/guiapdti/wiki/download/file/Guia_de_PDTI_do _ SISP_v2_Beta.pdf >. Acesso em: 23 fev. 2017.

_____. Tribunal de Contas da União (TCU). Nota Técnica 6/2010-Sefti/TCU–versão 1.2.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para INTERNET – Glossário. Comitê Gestor da Internet no Brasil. 2ª edição. São Paulo, 2012.

Dicionário ITIL. Disponível em http://www.itsmf.com.br/portal/?page_id=90. Acesso em 05 out 2015.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). COBIT 5: *A Business Framework for the Governance and* Management *of Enterprise IT. United States of America*, 2012.

ISSAI 1003. Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI): Johannesburg, 2010. Disponível em: <http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm>. Acesso em: 23 fev. 2017.

OFFICE OF GOVERNMENT COMMERCE. *IT Service Management*. Glossário *Information Technology Infrastructure Library* (ITIL). Versão v3 1.2.