UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

CAMILA MÁRCIA SILVEIRA TEIXEIRA

# SEGURANÇA DA INFORMAÇÃO CORPORATIVA SOB A ÓTICA HUMANA

Belo Horizonte
2016

CAMILA MÁRCIA SILVEIRA TEIXEIRA

# SEGURANÇA DA INFORMAÇÃO CORPORATIVA SOB A ÓTICA HUMANA

Monografia apresentada ao programa de Especialização do Núcleo de Informação Tecnológica e Gerencial – NITEG, no curso Gestão da Informação e Pessoas da Escola de Ciência da Informação, da Universidade Federal de Minas Gerais, como requisito para a obtenção do certificado de Especialista em Gestão da Informação e Pessoas. Linha de Pesquisa: Segurança da Informação

Orientador: **PROF**. Jorge Tadeu Neves

BELO HORIZONTE

2016

Ficha catalográfica: elaborada pela biblioteca da ECI

Será impressa no verso da folha de rosto e não deverá ser contada.

**Universidade Federal de Minas Gerais**
**Escola de Ciência da Informação**
**Núcleo de Informação Tecnológica e Gerencial**

Trabalho de Conclusão de Curso de Especialização em Gestão de Informação e Pessoas, intitulado **"Segurança da Informação Corporativa sob a ótica humana"** autoria de ***Camila Márcia Silveira Teixeira,*** aprovado pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Jorge Tadeu de Ramos Neves
Curso Gestão de Informação e Pessoas
Escola de Ciência da Informação - UFMG
Orientador

Prof. Dr. Cláudio Paixão Anastácio de Paula
Curso Gestão de Informação e Pessoas
Escola de Ciência da Informação – UFMG

Data da aprovação: Belo Horizonte, 12 de dezembro de 2016

## RESUMO

Nesse trabalho será tratada a Engenharia Social. Atualmente os ambientes de negócios estão cada vez mais interconectados, de forma que ficam expostos a uma multiplicidade de ameaças, com potencial para violar a segurança das informações, em especial o engenheiro social[1]. Visto que as informações são um ativo vital para os negócios corporativos e o elemento humano é o elo mais vulnerável na segurança da informação, as organizações que almejam proteger suas informações necessitam definir estratégias de proteção adequadas que salvaguardem as pessoas e as informações. O desenvolvimento desta monografia foi feito por meio de uma revisão de literatura, estudo das boas práticas de segurança da informação do mercado, das principais vulnerabilidades humanas e estratégias de proteção. Constatou-se que para implementar a segurança da informação de forma efetiva em uma organização é importante que a estratégia de segurança da informação corporativa esteja alinhada com o negócio, cultura e necessidades organizacionais. Finalmente o estudo conclui com a constatação de que, uma vez que não existe segurança absoluta, é fundamental que a organização estabeleça um processo continuo de conscientização em segurança que leve em consideração que o elemento humano é o ponto de maior fragilidade e, tendo isso em mente, verifica-se constantemente que a segurança da informação é uma responsabilidade de todos.



**Palavras-chave:** Segurança da Informação. Engenharia Social. Vulnerabilidades. Ameaças. Persuasão.


[1] Golpistas que utilizam diferentes meios e discursos para enganar e persuadir potenciais vítimas a fornecerem informações sensíveis ou realizar ações, como executar códigos maliciosos e acessar páginas falsas.

## ABSTRACT

In this work will be treated the social engineering. The business environments is currently increasingly interconnected, so that the information is exposed to large set of threats with potential to violated the security, especially the social engineer[2]. Organizations that desire to protect your information need to define appropriate protection strategies that safeguard people and information because information is a vital asset for the corporate business and the human element is the most vulnerable element of the information security. The development of this monograph was done through a literature review, study of good information security practices of market, the major human vulnerabilities and protection strategies. It was concluded that to implement with effectively the information security in an organization is important that information security corporate strategy is aligned with the business, culture and organizational needs. Finally, the study concludes with the observation that, since there is no absolute security, it is fundamental that the organization establishes a continuous process of security awareness that takes into account that the human element is the most fragile point and, considering this constantly, information security is a responsibility of all.

**Keywords:** Information security. Social engineering. Vulnerabilities. Threats. Persuasion.

[2] Scammers who use different means and speeches to deceive and persuade potential victims to provide sensitive information or take action, such as executing malicious code and accessing fake pages.

## LISTA DE FIGURAS

Figura 1: Pirâmide ou tríade da Segurança da Informação. Figura retirada de (AFFONSO et al., 2008) ..... 20
Figura 2: Evolução do cenário da Segurança da Informação. Figura retirada de (AFFONSO et al., 2008). ..... 21
Figura 3: Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos de segurança e os aspectos complementares. Figura retirada de (Sêmola. 2003). ..... 29
Figura 4: Elementos básicos do processo de comunicação. Figura retirada de (AFFONSO et al., 2008). ..... 32
Figura 5: Universo social. Figura retirada de (AFFONSO et al., 2008). ..... 34
Figura 6: Modelo PDCA aplicado ao processo SGSI. Figura retirada de (BSI ISO 27001, 2009). ..... 40
Figura 7: Família de Produtos do Cobit 5. Figura retirada de (ISACA, 2016). ..... 41
Figura 8: Modelo PDCA aplicado ao processo BCMS. Figura retirada de (BSI ISO 22301, 2012). ..... 43

# SUMÁRIO

**1 INTRODUÇÃO ..... 14**

1.1 PROBLEMA ..... 17

1.2 OBJETIVOS ..... 17

1.2.1 Objetivo geral ..... 17

1.2.2 Objetivos específicos ..... 17

1.4 ESTRUTURA DA DISSERTAÇÃO ..... 17

1 CONCEITOS GERAIS E REVISÃO DA LITERATURA ..... 18

2.1 SEGURANÇA DA INFORMAÇÃO (SI) ..... 18

2.2 ENGENHARIA SOCIAL ..... 23

2.3 CICLO DE VIDA DA INFORMAÇÃO ..... 28

**3 METODOLOGIA ..... 46**

**5 CONSIDERAÇÕES FINAIS ..... 47**

**REFERÊNCIAS ..... 49**

# 1 INTRODUÇÃO

Informação é um ativo[3] essencial para os negócios de uma empresa e consequentemente necessita ser adequadamente protegida. Com o aumento da interconectividade no ambiente dos negócios, a informação fica exposta a ameaças, como por exemplo: fraudes eletrônicas, espionagem, sabotagem, vandalismo, desastres naturais, danos causados por código malicioso[4], hackers e ataque de negação de serviço, do inglês (DoS) *Denial of Service*[5] (AFFONSO et al., 2008; HILES, 2007).

É uma necessidade que todas as empresas se tornem mais ágeis, competitivas, modernas, lucrativas e de estarem preparadas para o crescimento. A informação é, portanto, um dos pivôs desta corrida e, como ativo, bem e patrimônio, precisa estar bem guardada como um segredo de negócio (SÊMOLA, 2003).

As redes de computadores em todas as partes do mundo estão sujeitas a desastres capazes de afetar a disponibilidade das informações. Geralmente para atender as solicitações de serviço, as organizações dependem de alguns requisitos tais como: estabelecimento sede, central de contato, web site, recursos[6]. Tais requisitos ficam expostos a desastres que podem comprometer os objetivos da empresa, ficando a cargo da empresa protegê-los para assegurar a competitividade no mercado, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem junto ao mercado (AFFONSO et al., 2008; HILES, 2007).

Toda organização é suportada por processos que mantêm relação de dependência com ativos físicos, tecnológicos, humanos que, inevitavelmente, possuem falhas de segurança.

Estas falhas podem ser potencialmente exploradas por ameaças as quais, ao obterem sucesso e gerarem um incidente, produzirão impactos nos ativos, tais impactos tendem a estenderem-se pelos processos e a atingirem todo o negócio, através, por exemplo, de prejuízos financeiros e de desgaste a imagem organizacional.

Neste contexto, a segurança da informação visa à proteção das informações contra diversas ameaças com o propósito de garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Ela

---

[3] Tudo aquilo que possui valor e, consequentemente, demanda proteção para uma organização.

[4] Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

[5] Técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

[6] Todos os bens, pessoas, tecnologias (incluindo instalações e equipamentos), suprimentos, informações (seja eletrônica ou não) que uma empresa tem que ter disponível para uso, quando necessário, a fim de operar e cumprir o seu objetivo.

pode ser aplicada em uma organização por meio de planos, políticas[7], procedimentos, processos, funções de software e hardware dentre outros.

Atualmente com o aumento crescente no volume de informações disponíveis e a grande dependência de sistemas para a realização dos negócios, a aplicação dos conceitos de segurança da informação na organização auxiliará a diminuir a exposição a riscos, prejuízos financeiros, comprometimento da imagem e ações de responsabilidade legal. Neste cenário, o desafio empresarial passa a ser extrair todos os benefícios da informatização e automação sem que os malefícios associados à falta de segurança sejam maximizados, colocando a empresa em um nível de risco inaceitável (ISO/IEC 27002, 2009; SÊMOLA, 2003).

As normas, guias e boas práticas relacionadas à segurança da informação podem ajudar a organização a desenvolver e mapear ações para atingir a chamada Maturidade na Gestão de Segurança da Informação. Deste modo, é recomendado às organizações que desenvolvam ações alinhadas com as melhores práticas de segurança a fim de evitar interrupções e assegurar a retomada em tempo hábil de suas atividades críticas, caso ocorra um desastre (AFFONSO et al., 2008). Como referências de mercado, que abordam boas práticas de segurança da informação, encontra-se a norma ISO/IEC 27001, o BS ISO 22301 e o COBIT 5.

É considerada uma boa prática que a segurança empresarial seja planejada com uma estratégia equilibrada quanto a segurança e a produtividade. Pouca ou nenhuma segurança pode implicar em um ambiente vulnerável, enquanto uma ênfase exagerada em segurança pode onerar demasiadamente a realização dos negócios e inibir o crescimento e a prosperidade da empresa. O desafio é identificar e alcançar um equilíbrio entre segurança e produtividade, com um foco especial no fator humano, considerado como a vulnerabilidade mais significativa para segurança da informação (MITNICK; WILLIAN, 2003).

Conforme (KARLINS; SCHAFER, 2015), existe um verdadeiro mar de oportunidades para buscar e encontrar pessoas que poderiam se tornar amigas ou mesmo parceiras de longo prazo, como: Facebook, Twitter, Instagram, e-mail, Skype, Dropbox, Linkedin, Lync, salas de bate-papo, comunidades, e-mail, blogs, mecanismos de busca, sites de namoro. Cabe aos internautas ficarem vigilantes quanto às informações sensíveis trafegados na rede, visto que terão um vínculo com a identidade do indivíduo pela eternidade, podendo ser utilizadas por um engenheiro social para descobrir informações sobre o indivíduo e tomar decisões sobre como tratá-lo.

A engenharia social é considerada a arte de obter informações de usuários para angariar vantagens, que representa uma ameaça séria, capaz de atacar de forma eficaz um usuário.

[7] Intenções e diretrizes globais formalmente expressas pela direção da empresa.

Os indivíduos geralmente não têm consciência do valor das informações que divulgam e compartilham, bem como dos impactos, caso venham a serem usadas de forma maliciosa, o que agrava as consequências de um ataque, visto que normalmente as pessoas não têm conhecimento da extensão das técnicas de engenharia social, têm dificuldade para perceberem que estão sendo atacadas e que podem vir a serem vítimas. Além disso, elas acreditam que são competentes para detectarem eventuais ataques (HOBEL et al., 2014; KIMPPA et al., 2015).

O crescimento de recursos para facilitar a comunicação, compartilhamento e uso de informações, como por exemplo: políticas de uso do seu dispositivo ou do inglês BYOD (*Bring Your Own Device*), ferramentas de comunicação on-line, ferramentas colaborativas, proveu automatização, facilitação de execução de tarefas diárias, eficácia na comunicação, entretanto proveu também insumos que podem ser utilizados para potencializar um ataque. O que é agravado pelo fato dos indivíduos geralmente publicarem e compartilharem informações, considerando que as interações estabelecidas são confiáveis e preocupando-se pouco com segurança e privacidade (HOBEL et al., 2014).

Vulnerabilidades em recursos de informação são geralmente exploradas para acesso a informações sensíveis; entretanto, as proteções podem ser reforçadas. Mas mesmo assim tais proteções são impotentes quando um usuário é manipulado por um engenheiro social (HOBEL et al., 2014).

Esta monografia visa realizar um levantamento bibliográfico e revisão de conceitos a respeito da segurança da informação, boas prática de segurança e da chamada engenharia social, enfatizando o fator humano, considerado como a parte mais frágil da segurança da informação.

Este trabalho de pesquisa é relevante devido a pertinência do tema (segurança da informação) no mundo atualmente. Dado que as informações são um ativo vital para os negócios corporativos, proteger as informações da forma adequada é essencial para a organização permanecer e progredir no mercado, assim sendo este trabalho é útil para a ampliação dos horizontes intelectuais a respeito da segurança da informação, com um enfoque especial na maior fragilidade da segurança da informação.

A principal razão para desenvolvimento de um trabalho cientifico neste tema é o fascínio e o entusiasmo da autora pela Segurança da Informação, que está presente no dia a dia, em termos pessoais e profissionais, e que permite vislumbrar e colaborar para um mundo mais protegido.

## 1.1 Problema

A informação é um ativo essencial para continuidade dos negócios corporativos, uma vez que todas as organizações dependem de informações para entrega de produtos e serviços. Com os avanços tecnológicos, os ambientes de negócios estão cada vez mais interconectados e expostos a uma gama de agentes nocivos. As ameaças, como por exemplo a engenharia social, a saber, técnica para enganar pessoas a fim de obter algum proveito, podem explorar as vulnerabilidades humanas, potencialmente susceptíveis a exploração, dado que o elemento mais frágil da segurança da informação são as pessoas.

## 1.2 Objetivos

Este estudo propõe atender ao objetivo geral e aos objetivos específicos a seguir.

### 1.2.1 Objetivo geral

Revisão de Literatura a respeito da segurança da informação e da chamada engenharia social, enfatizando o fator humano, considerado como o elo mais frágil da segurança da informação.

### 1.2.2 Objetivos específicos

- Discutir as principais políticas de iniciativas de segurança da informação de acordo com a norma ISO/IEC 27001 e demais referências relevantes para o assunto, com enfoque no elemento humano;
- Mapear os principais conceitos e ferramentas da engenharia social;
- Levantar as principais vulnerabilidades humanas;
- Identificar recomendações e boas práticas de segurança da informação, de acordo com a norma ISO/IEC 27001 e demais referências relevantes para o assunto, com enfoque na proteção do elemento humano.

## 1.4 Estrutura da dissertação

Este trabalho está dividido em 5 capítulos. Este capítulo apresentou uma introdução ao projeto tratado e desenvolvido nesta monografia, contextualizando a importância da segurança da informação as para redes coorporativas, bem como da fragilidade do elemento humano. O capítulo 2 apresenta o referencial teórico e mapeamento dos

conceitos e boas práticas estudados. O capitulo 3 relata a metodologia utilizada para desenvolver o trabalho. O capítulo 4 expõe a análise de resultados. E o capítulo 5 trata das conclusões do trabalho futuros.

# 1 CONCEITOS GERAIS E REVISÃO DA LITERATURA

## 2.1 Segurança da Informação (SI)

A ISO/IEC 27.001 define segurança da informação como preservação da confidencialidade (propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados), integridade (propriedade de salvaguarda da exatidão e completeza de ativos) e disponibilidade (propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada) da informação; adicionalmente, outras propriedades, tais como autenticidade (garantia de que a fonte da informação é quem diz ser), não repúdio (evitar que uma entidade possa negar que foi ela quem executou uma ação) e confiabilidade (capacidade de uma pessoa ou sistema de realizar e manter seu funcionamento em circunstâncias de rotina, bem como em circunstâncias hostis e inesperadas), podem também estar envolvidas (ISO/IEC 27001, 2009). No mesmo viés, o Guia de Governança Corporativa e Gestão de TI (Cobit 5) define que a implementação da Segurança da Informação em uma organização garante que a informação é protegida contra a divulgação a usuários não autorizados (confidencialidade), modificação inadequada (integridade) e não-acesso quando necessário (disponibilidade) (COBIT 5, 2012).

As organizações que almejam proteger seus ativos de forma efetiva podem implantar no ambiente corporativo algumas boas práticas de mercado referentes a segurança da informação, tais como COBIT e a ISO/IEC 27.001, supracitados. A adoção destas boas práticas é um facilitador na aculturação dos colaboradores e estabelecimento continuo de controles de segurança eficazes, uma vez que proveem modelos reconhecidas internacionalmente como boas práticas de mercado.

Aquilo que se procura proteger está em todo lugar, distribuído por todos os perímetros físicos e lógicos de uma organização, sendo enviado e recebido por diversos meios, representado por conhecimento tácito ou explicito. As organizações que almejam um estado seguro buscam cercar-se de mecanismos que preservem o conhecimento que detêm e que lhes garantam tranquilidade, obtida pela não exposição ao perigo exagerado ou simplesmente por estarem livres dele (SEMOLA, 2003).

Mecanismos de proteção para as informações alinhados com as necessidades dos negócios são preponderantes para sobrevivência das organizações, e além disso, para

minimização de riscos, maximização de retorno sobre investimentos e oportunidades, solidificação da imagem e reputação organizacional, atendimento a requisitos legais e regulatórios. Tais fatores, por sua vez, influenciaram efetivamente na alocação de recursos direcionados a segurança, agregando em visibilidade do retorno no investimento em segurança.

Conforme Affonso et al. (2008), a SI pode ser definida como um estado no qual os ativos[8] de informação[9] [10]estão livres de perigos e incertezas. Geralmente, dentro de uma organização, está segurança costuma se aplicar a tudo aquilo que possui valor e, consequentemente, demanda proteção.

As organizações que almejam implementar a gestão de segurança da informação, precisam entender a real criticidade dos ativos para o negócio e aplicar estratégias adequadas de segurança para salvaguardar tais ativos.

De acordo com a Cartilha para Segurança na Internet, ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos, por meio de variadas técnicas e motivados por distintas questões, como por exemplo: prestigio, golpes financeiros, demonstração de poder, dentre outros. Qualquer serviço, computador ou rede que seja acessível através da Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque (CERT.BR, 2012).

Os ativos acessíveis por meio da internet estão expostos a uma gama de ameaças, dentre elas o engenheiro social, que pode vir a atuar no cenário organizacional a qualquer momento, cabendo a organização aceitar o risco de conviver com esta ameaça, consequentemente colher as consequências, ou tomar ações para tratativa, tais como evitar, minimizar ou transferir o risco.

Affonso et al. (2008) também relatam que há muita dificuldade para alcançar a segurança absoluta, pois é muito improvável conseguir endereçar todas as possíveis situações de prejuízo e também há limitações de recursos financeiros, sendo que à medida que os investimentos em segurança vão crescendo, existe um momento em que o recurso gasto é maior que o valor do próprio ativo a ser protegido. A segurança próxima de 100% é uma meta normalmente buscada dentro do meio militar, onde falhas podem custar vidas, ativo de valor imensurável.

[8] Tudo aquilo que possui valor para uma organização.

[9] Ativos que geram, processam, manipulam, transmitem e armazenam informações, além das informações em si.

É importante que a estratégia e controles de segurança corporativos estejam alinhada com os requisitos de negócio; bem como que o custo/benefício tenha sido avaliado e atenda às necessidades corporativas.

Para conferir e estabelecer um tratamento de segurança a uma informação é necessário garantir seus três atributos ou conceitos principais: **confidencialidade, integridade e disponibilidade.** A confidencialidade é a propriedade da informação de se manter acessível aos agentes autorizados e, ao mesmo tempo, inacessível aos agentes não autorizados. A integridade é a propriedade da informação de se manter sob controle e poder ser alterada por agentes autorizados e, ao mesmo tempo, impedida de sofrer alterações por agentes não autorizados. E a disponibilidade é a propriedade da informação de se manter acessível a agentes autorizados a qualquer momento que se precise dela. A Figura 1 ilustra a pirâmide da Segurança da Informação, composta pelos três atributos neste parágrafo citados.

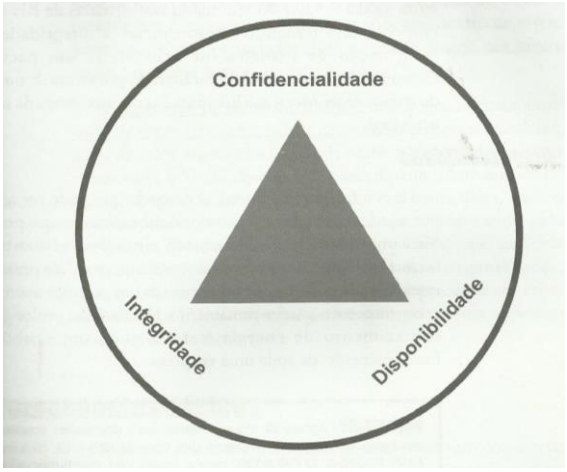


**Figura 1: Pirâmide ou tríade da Segurança da Informação. Figura retirada de (AFFONSO et al., 2008)**

Entre as décadas de 1970 e 1980, na época dos mainframes, enquanto a informática fazia parte da retaguarda dos negócios, os aspectos de segurança tinham como foco principal a confidencialidade dos dados. Nas décadas de 1980 e 1990, com o surgimento dos ambientes de rede, os aspectos de segurança tinham como foco principal a confidencialidade e integridade dos dados e informações. Já entre as décadas de 1980 e 1990, os aspectos de segurança tinham como foco principal a confidencialidade, integridade e disponibilidade dos dados, informação e conhecimento.

Nesta época a informática passou a fazer parte direta dos negócios, e a proteção passou a priorizar o capital intelectual. Uma análise simplificada deste cenário pode ser visto na Figura 2.

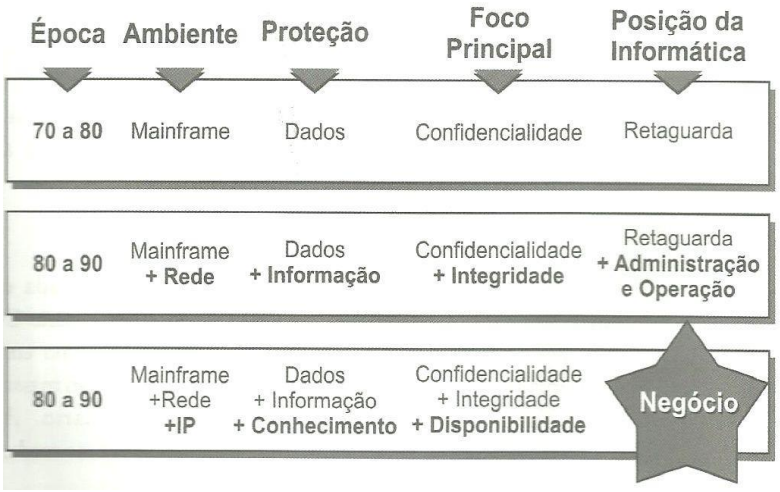


**Figura 2: Evolução do cenário da Segurança da Informação. Figura retirada de (AFFONSO et al., 2008).**

A partir do século XXI, a segurança da informação tornou-se mais importante para o sucesso empresarial, transcendendo o limite da produtividade e da funcionalidade. Como exemplo de acontecimento que aumentou a importância da segurança nesta época pode-se citar o ataque do vírus "*I Love You*" e o ataque de 11 de setembro de 2001 às Torres Gêmeas em Nova York.

O ataque do "11 de setembro" representou um marco na história do impacto de um desastre inesperado. Desastre este, cuja a probabilidade era muito remota, não era factível que uma ameaça humana, colocasse em cheque a segurança e soberania dos Estados Unidos. Contudo, esta ameaça obteve sucesso na sua exploração, desfrutando de uma vulnerabilidade existente, a saber, o ambiente de contingência de diversas organizações era próximo do ambiente principal (as torres gêmeas). Apesar, da probabilidade deste desastre ser considerada, na época de 2011, remota o impacto classificou-se como inquantificavel, acarretando no fim de muitas empresas, e em termos mais críticos, na perda de vidas, ativo de valor inestimável. Assim sendo, este desastre, difundiu mundialmente a importância de as organizações cuidarem dos seus ativos, entendendo o cenário de riscos que permeiam o ambiente de negócios e implementando estratégias de segurança eficientes.

Conforme a ISO/IEC 27001 (2009), para se atingir o sucesso na implementação da segurança da informação em uma organização deve-se levar em consideração os seguintes fatores:

1. Política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

2. Uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;
3. Comprometimento e apoio visível de todos os níveis gerenciais;
4. Um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;
5. Divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;
6. Distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;
7. Provisão de recursos financeiros para as atividades da gestão de segurança da informação;
8. Provisão de conscientização, treinamento e educação adequados;
9. Estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;
10. Implementação de um sistema de medição, que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

Ainda de acordo com a ISO/IEC 27001 (2009), para se estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) a organização deve:

1. Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo.
2. Definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia que:

    a) Inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas com a segurança da informação;
    b) Considere requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;
    c) Esteja alinhada com o contexto estratégico de gestão de riscos da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer;
    d) Estabeleça critérios em relação aos quais os riscos serão avaliados;
    e) Tenha sido aprovada pela direção.
    c) Definir a abordagem de análise/avaliação de riscos da organização.

3. Identificar uma metodologia de análise/avaliação de riscos que seja adequada ao SGSI e aos requisitos legais, regulamentares e de segurança da informação, identificados para o negócio;
4. Desenvolver critérios para a aceitação de riscos e identificar os níveis aceitáveis de risco;
   A metodologia de análise/avaliação de riscos selecionada deve assegurar que as análises/avaliações de riscos produzam resultados comparáveis e reproduzíveis.
   a) Identificar os riscos;
   b) Analisar e avaliar os riscos;
   c) Identificar e avaliar as opções para o tratamento de riscos.

## 2.2 Engenharia Social

De acordo com CERT.br (2012), a engenharia social é uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes, como, por exemplo, o conhecido “conto do vigário”.

Conforme (MITNICK; WILLIAM, 2003), geralmente não é simples obter informações sigilosas de instituições de nichos de serviços críticos tais como bancário, comercial, contudo as fragilidades dos usuários podem ser facilitadores para obtenção destas informações. Através de técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

A engenharia social é uma técnica que utiliza a influência e a persuasão ou manipulação para enganar as pessoas e convencê-las de que o “engenheiro social” é alguém que na verdade ele não é, através desta técnica o engenheiro social pode aproveitar-se das pessoas para alcançar os seus objetivos. Para facilitar o alcance dos objetivos ele apresentara um comportamento favorável ao aumento da probabilidade de que ele e a vítima sejam atraídos um pelo outro e experimentem um resultado positivo quando interagirem.

De acordo com (KARLINS; SCHAFER, 2015) as “Leis da Atração” são ferramentas que melhoram a eficácia de uma relação, podendo ser utilizadas por um engenheiro social para moldar relações humanas. Segue lista das leis da atração:

1. A Lei da Semelhança (“Algo em Comum”): pessoas que compartilham as mesmas perspectivas, princípios, crenças, atitudes e atividades tendem a desenvolver relações próximas e reforçarem umas às outras, o que aumenta a probabilidade de atração mútua. Podendo trazer vários benefícios como elevação da autoestima, sensação maior de felicidade e bem-estar, de ser entendido e estar seguro.
2. Farinha do Mesmo Saco: semelhanças conectam as pessoas. Encontrar coisas em comum rapidamente estabelece uma conexão e um ambiente fértil para desenvolver amizades. Aristóteles escreveu: “Nós gostamos daqueles que se parecem conosco e que possuem os mesmos objetivos… Gostamos daqueles que desejam as mesmas coisas que nós”.
3. A Lei da Atribuição Equivocada: quando as pessoas se sentem bem consigo mesmas e não atribuem a sensação boa a uma causa específica, tendem a associar a causa com quem está fisicamente mais perto.
4. A Lei da Curiosidade: quando alguém se comporta de um jeito que produz curiosidade em outra pessoa, isso aumenta significativamente as chances de que ela queira interagir com a outra pessoa numa tentativa de satisfazer essa curiosidade. Portanto, uma “isca de curiosidade” se torna uma ferramenta eficaz para conhecer alguém de interesse e desenvolver uma amizade.
5. A Lei da Reciprocidade: as normas sociais ditam que se alguém lhe dá algo ou faz um favor para você, pequeno ou grande, então você fica predisposto a retribuir o gesto na mesma medida ou num gesto ainda maior.
6. A Lei da Revelação Prévia: indivíduos que revelam uma quantidade maior de informações pessoais possuem mais chances de receber em troca o mesmo nível de informação. Revelação prévia promove a atração. As pessoas sentem proximidade com outros que revelam suas vulnerabilidades, pensamentos íntimos e fatos sobre si mesmos.

É comum que os engenheiros sociais retratem o máximo de normalidade possível no contato, conhecimento da terminologia interna da organização, interesses comuns aos da vítima, remoção de barreiras e obstáculos, a fim de não levantarem suspeitas e criarem uma conexão com a vítima, tal conexão constrói uma ponte psicológica entre os indivíduos e abre caminho para que vários níveis de amizade se desenvolvam, facilitando a conquista da confiança da vítima e a obtenção de informações. Situações e estados do ambiente ou das pessoas, tais como pressão para atender demandas, escassez de tempo, estado emocional, fadiga mental, falta de conhecimento, representam um fator favorável ao atacante, visto que

estes podem distrair a vítima, que pode utilizar um atalho mental para resolução das demandas sem analisar cuidadosamente as informações.

A esse respeito, o cientista mais respeitado do mundo no século XX, Albert Einstein, afirmou: “Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro”. Já Mitnick e William (2003) ressalvam que os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas (devido, por exemplo, a credulidade, a inocência ou a ignorância) ou, em geral, apenas desconhecem as boas práticas de segurança.

Os engenheiros sociais utilizam de traços sociais favoráveis para estabelecer a afinidade e a confiança (como por exemplo: simpatia, educação, gentileza, charme), eles têm habilidade em lidar com as pessoas, intimidá-las, manipulá-las, estimulando emoções tais como medo, agitação ou culpa para obterem as informações que almejam. A intimidação pode criar o medo de ser punido e influenciar as pessoas para que cooperem, podendo também criar o medo de uma situação embaraçosa ou de ser desqualificado para uma próxima promoção.

A manipulação tem sido estudada pelos cientistas há pelo menos 60 anos. Robert B. Cialdini[11], ao escrever para a revista Scientific American (edição de fevereiro de 2001), resumiu a sua pesquisa apresentando “seis tendências básicas da natureza humana”, as quais estão envolvidas em uma tentativa de obter o consentimento para uma solicitação, estas podem ser utilizadas pelos engenheiros sociais para suas tentativas de manipulação. Segue relação a seguir:

1. Autoridade

   As pessoas têm a tendência de atender a uma solicitação que é feita por uma pessoa com autoridade. Uma pessoa pode ser convencida a atender uma solicitação se ela acreditar que o solicitante é uma pessoa com autoridade ou que está autorizada a fazer tal solicitação.
2. Afabilidade

   As pessoas têm a tendência de atender uma pessoa que faz uma solicitação quando ela conseguiu se fazer passar por alguém agradável ou com interesses, crenças, atitudes semelhantes aos da vítima.
3. Reciprocidade

   As pessoas podem atender automaticamente a uma solicitação quando recebem ou têm a promessa de receber algo de valor. O presente pode ser um item material, um conselho ou ajuda. Quando alguém faz algo para um indivíduo, o indivíduo sente uma inclinação em retribuir. Essa forte tendência

[11] Psicólogo social, professor, escritor e empresário dentre os mais respeitados nos estudos da persuasão.

de retribuir existe nas situações em que a pessoa que recebe o presente não pediu por ele.

4 Consistência

As pessoas têm tendência de atender após fazer um comprometimento público ou adotar uma causa. Depois que prometem, fazem qualquer coisa, não querem parecer pouco confiáveis ou indesejáveis e tendem a seguir as instruções para serem coerentes com a declaração ou promessa.

5 Validação social

As pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado.

6 Escassez

As pessoas têm a tendência de cooperar quando acreditam que o objetivo procurado está em falta e que outras pessoas estão competindo por ele, ou que ele só está disponível por um período de tempo curto.

Mitnick e William (2003) recomendam que as organizações utilizem as etapas a seguir para protegerem-se contra a divulgação de informações aparentemente inofensivas:

1. O departamento de segurança da informação precisa realizar treinamentos de conscientização, no qual deve detalhar os métodos de ataque utilizados pelos engenheiros sociais;
2. Cada um dos empregados precisa ter consciência que a fala de um interlocutor ter conhecimento dos procedimentos da empresa, da linguagem e dos identificadores internos não dá de maneira nenhuma a forma ou a autenticação para o solicitante, nem o autoriza a ter a necessidade de saber as informações;
3. Cada organização tem a responsabilidade de determinar o método adequado de autenticação a ser usado quando os empregados interagem com as pessoas que eles não conhecem pessoalmente ou pelo telefone;
4. As pessoas que têm a responsabilidade e o papel de criar uma política de classificação de dados devem examinar os tipos de detalhes que parecem inofensivos e podem levar a informações sigilosas;
5. O simples conhecimento da terminologia interna da organização pode fazer com que um engenheiro social pareça assumir autoridade e conhecimento;

6. Implementar uma política que proíbe a divulgação dos números internos dos funcionários, contratados, consultores e temporários para as pessoas que não são da empresa;
7. Desenvolver um procedimento passo a passo para identificar positivamente se um interlocutor que está pedindo os números de telefone é de fato um empregado;
8. Os códigos contábeis e ás cópias dos diretórios corporativos (uma cópia impressa, um arquivo de dados ou uma lista eletrônica de telefones na intranet) são alvos frequentes dos engenheiros sociais. Cada empresa precisa ter uma política escrita e bem divulgada sobre a revelação desse tipo de informação. As salvaguardas devem incluir a manutenção de um registro de auditoria que estabelece os casos em que as informações sigilosas para as pessoas de fora da empresa;
9. Informações, tais como número de empregado, por si só, não devem ser usadas como nenhum meio de autenticação. Todo empregado deve ser treinado para verificar não apenas a identidade do solicitante, como também a necessidade que o requisitante tem de saber da informação;
10. No treinamento de segurança, deve-se ensinar essa abordagem aos funcionários: sempre que um estranho pedir um favor, saiba primeiro como negar educadamente até que a solicitação possa ser verificada. Seguir as políticas e os procedimentos da empresa com relação a verificação e a divulgação das informações não públicas;
11. O treinamento de segurança com relação a política da empresa criado para proteger os ativos de informação precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao ativo de TI da empresa.

Para aqueles autores os ataques de engenharia social geralmente têm o mesmo elemento comum: a fraude. A vítima é levada a acreditar que o atacante é um colega ou alguma outra pessoa que está autorizada a acessar informações confidenciais ou que está autorizada a dar a vítima instruções que envolvam a tomada de ações com um computador ou com um equipamento relacionado com o computador.

A maioria dos ataques poderia ser evitada se a vítima seguisse estas etapas quando um indivíduo o solicitasse informações:

1. Verificar a identidade da pessoa que faz a solicitação: essa pessoa é realmente quem diz ser?
2. Verificar se a pessoa esta autorizada: A pessoa tem a necessidade de saber ou tem autorização para fazer a solicitação?

De acordo com a Cartilha para Segurança na Internet o que define as chances de um ataque na Internet ser ou não bem-sucedido é o conjunto de medidas preventivas tomadas pelos usuários, desenvolvedores de aplicações e administradores dos computadores, serviços e equipamentos envolvidos. De forma que se cada uma das partes envolvidas fizer a sua parte na proteção dos ativos, um ataque pode ser evitado ou pelo menos os impactos minimizados (CERT.BR, 2012).

O cenário de risco zero, não existe, nem em ambientes militares ou financeiros, que lidam com ativos inestimáveis, e que consequentemente a rigidez em segurança é maior. Todavia, podem ser adotados diferentes mecanismos e controles de segurança, que se complementem e que proporcionem um nível de segurança adequado, de forma que a organização tenha conhecimento dos principais riscos que permeiam o ambiente de negócio e faça a gestão destes riscos, implementando soluções de segurança adequadas. Ademais, é imprescindível que as soluções apresentem um caráter sistêmico, considerando essencialmente o elemento humano, considerado o elemento mais frágil da segurança informacional.

## 2.3 Ciclo de vida da informação

Conforme Sêmola (2003), as fases do ciclo de vida da informação representam os momentos nos quais a informação é submetida ao tratamento, seja pela ação direta de ativos físicos, tecnológicos ou humanos, incluindo os procedimentos associados a cada um deles. São fases críticas, comumente, momentos de exposição ao risco e que, por isso, devem ser diagnosticadas e trabalhadas pela empresa como parte de um desafio único e integrado de gerenciamento. Segue descrição sucinta das fases:

1. Manuseio
   Momento em que a informação é criada e manipulada;
2. Armazenamento
   Momento em que a informação é armazenada;
3. Transporte
   Momento em que a informação é transportada;
4. Descarte
   Momento em que a informação é descartada.

O referido autor faz uma analogia entre as fases do ciclo de vida da informação com os elos de uma corrente. Cada fase do ciclo de vida deve resistir à força contrária de ameaças, tornando-se peças igualmente importantes para o todo; a fase mais ineficaz pode comprometer a eficácia da proteção de todo o ciclo de vida. Um comportamento semelhante é identificado em uma corrente; o elo mais fraco poderá comprometer a eficácia da proteção da corrente. O poder de proteção de uma corrente está diretamente associado ao poder de resistência do seu elo mais fraco, da mesma forma o poder de proteção de uma informação está diretamente associado ao poder de resiliência a ameaças da sua fase mais ineficaz.

A Figura 3 ilustra a interação entre as fases sob uma ótica da segurança da informação.

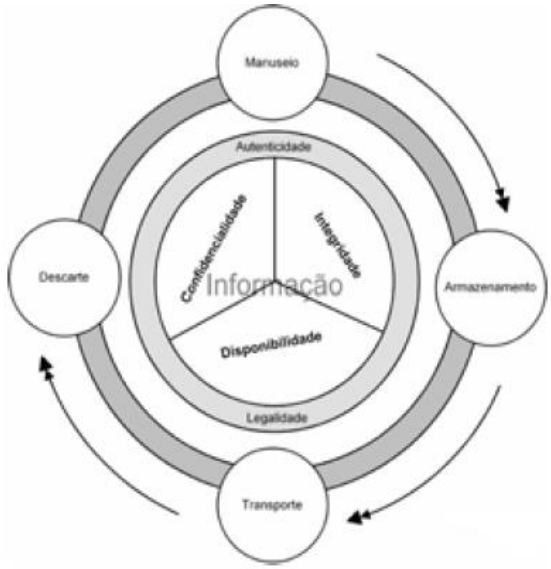


**Figura 3: Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos de segurança e os aspectos complementares. Figura retirada de (Sêmola. 2003).**

Para proteger as informações de forma eficaz é de suma importância que todas as fases do ciclo de vida da informação (manuseio, armazenamento, transporte e descarte) sejam providas de proteções adequadas, uma vez que uma falha na proteção de uma destas fases pode comprometer a segurança de todo o ciclo de vida da informação. Além disso, nas estratégias de proteção é primordial que sejam atendidos os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, considerando os aspectos humanos, tecnológicos e processuais.

É considerada uma boa prática as organizações planejarem estratégias de proteção informacional equilibradas quanto a segurança e produtividade, englobando todo o ciclo de vida da informação e alinhadas com as melhores práticas de segurança do mercado.

Considerando que não existe segurança 100% é importante que a estratégia de segurança corporativa seja personalizada para o contexto organizacional, alinhada com atributos tais como cultura, negócio, necessidades, missão, visão e objetivo corporativo.

## 2.3 Ameaça, Incidente e Desastre

Conforme Sêmola (2003), ameaça é uma atitude ou dispositivo com potencialidade para explorar e provocar danos à segurança da informação, atingindo um ou mais de seus atributos: confidencialidade, integridade, disponibilidade. Exemplos de potenciais ameaças são: concorrente, sabotador, especulador, hacker[12], cracker[13], erro humano (como a deleção de arquivos digitais acidentalmente), acidentes naturais (como inundação, terremoto) funcionário insatisfeito, técnicas (como engenharia social[14], trashing[15]), ferramentas de software (vírus[16], sniffer[17], trojan horse[18], e-mailspoofing[19]). De forma análoga, AFFONSO et al. (2008), define ameaças como eventos ou ações que tem potencial de causar algum tipo de dano aos ativos. Quando uma ameaça se concretiza, ela recebe o nome de incidente (situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises), ou a um desastre, que é um incidente de maior magnitude, como por exemplo o "11 de setembro".

## 2.4 Vulnerabilidade

De acordo com a Cartilha para Segurança na Internet, uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação

---

[12] Invasor de sistemas.

[13] Também conhecido como "Hacker Black-Hat" ou "Hacker do mal" invasor de sistemas que utiliza seus conhecimentos para roubar senhas, documentos, causar danos, espionagem industrial.

[14] Utiliza-se de meios não técnicos para obter informações privilegiadas. Geralmente o engenheiro social é habilidoso em enganar e iludias as pessoas.

[15] Vasculhar o lixo para encontrar informações descartadas que tenham valor ou que forneçam uma ferramenta a ser usada em um ataque de engenharia social, tal como números de telefones internos, cargos.

[16] Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

[17] Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegados em uma rede de computadores.

[18] Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

[19] Técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

de segurança. Por exemplo: falhas em projetos, falha na configuração de softwares, falha na implantação de equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante, explorando uma vulnerabilidade, tenta executar ações maliciosas, tais como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores, tornar um serviço inacessível. (CERT.BR, 2012).

A vulnerabilidade é uma evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio e aumenta a probabilidade de que uma investida de ameaça tenha sucesso. Por exemplo: falhas de infraestrutura física (como carência de mecanismos de controle de acesso físico na sala de servidores), falhas tecnológicas (erros em projeto de software básico de sistemas operacionais), falhas de mídias (como fitas de backup impróprias para a restauração em função de deterioração), falhas humanas (como ausência de conscientização que provoca displicência ao criar e manter em sigilo a senha pessoal) (SÊMOLA, 2003).

Para AFFONSO et al. (2008) as vulnerabilidades criam situações que podem ser exploradas por uma ameaça, acarretando prejuízos. Elas podem ser causadas por várias circunstâncias, mas, no geral, podem ser classificadas como a ausência de um mecanismo de proteção ou uma falha de funcionamento em um mecanismo de controle existente; como por exemplo, ausência de mecanismo de detecção de incêndio, uma falha em um mecanismo de controle de acesso, a ausência de um procedimento de troca periódica de senhas.

É importante que uma organização estabeleça um processo de gestão de vulnerabilidades, técnicas, humanas e processuais e que este processo seja continuo e com ações de identificação, analise, tratativa, correção periódicos, de forma a manter um nível de segurança adequado.

## 2.5 Impacto

No contexto da Segurança da Informação o impacto pode ser definido como o resultado da ação bem-sucedida de uma ameaça ao explorar uma vulnerabilidade de um ativo e atingir, assim, um ou mais atributos da pirâmide da Segurança da Informação. Por exemplo: prejuízo financeiro, perda de competitividade, perda de mercado, danos à imagem, depreciação da marca, descontinuidade. (SÊMOLA, 2003).

## 2.6 Comunicação

Conforme AFFONSO et. al. (2008), a comunicação engloba o processo para estabelecê-la, bem como o universo interior tanto de quem emite a mensagem como de quem

a recebe, podendo ser realizada através do olhar, pelo jeito de vestir, escrever ou falar. A Figura 4 exibe os elementos envolvidos no processo de comunicação, conforme:

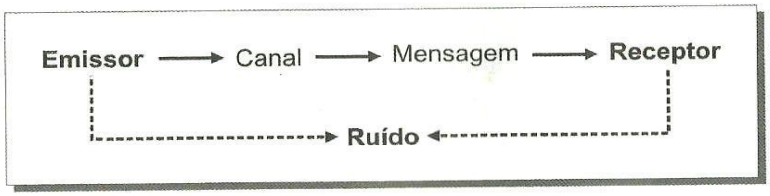


**Figura 4: Elementos básicos do processo de comunicação. Figura retirada de (AFFONSO et al., 2008).**

O emissor é quem envia a mensagem; o canal é o meio pelo qual ela é enviada; a mensagem é a informação que se transmite; e o receptor é aquele que a recebe. Os ruídos são todas as interferências que podem existir entre um extremo e outro e que podem prejudicar a compreensão. Exemplos de ruídos: aspectos emocionais, desconforto interno ou externo. De acordo com o autor existem três tipos de comunicação:

1. Comunicação não verbal: simbólica e sonora;
2. Comunicação oral: códigos que expressam sensações e sentimentos;
3. Comunicação escrita: representação gráfica, como os desenhos e a escrita propriamente dita.

O processo de comunicação é influenciado pelo universo interior dos envolvidos, influenciado diretamente por estado de humor, tensão, sentimentos, receios, dentre outros fatores do indivíduo, de caráter subjetivo, que terão um efeito de ruído na comunicação. Um engenheiro social, por sua vez, pode utilizar estes fatores a seu favor, a fim de facilitar a obtenção de um resultados positivos com a vítima. Para isso, ele poderá fazer uma leitura do perfil da vítima, entender os principais fatores individuais e prováveis ruídos na comunicação, que podem ser utilizados para potencializar e ou criar um terreno fértil para um ataque.

Para estabelecer uma comunicação segura é importante a adoção de procedimentos de segurança: conhecer a identidade do receptor, conhecer a identidade do emissor, identificar se o receptor tem autorização de acesso as informações e necessidade de conhecimento das informações, o canal de comunicação e os ruídos na comunicação. Tais procedimentos são importantes para evitar e minimizar impactos de ataques de engenharia social. Um engenheiro social com acesso a informações e juntamente com habilidades, técnicas e ferramentas, pode criar uma ponte psicológica com a vítima e explorar vulnerabilidades humanas, visando a conquista da confiança da vítima para obter vantagens, acarretando impactos inestimáveis para a vítima e para a organização.

Em um grupo social ou profissional o relacionamento se constrói pelos seus agentes, a partir de suas realidades, referencias e objetivos. Os laços de amizade, de simpatia ou antipatia podem unir ou afastar as pessoas, estes são influenciados por fatores pessoais tais como: capacidade intelectual, cultura, aspirações, interesses, temperamento e caráter e estão sujeitos a conflitos, tais como: interesses, valores, sentimentos e emoções. Segundo Affonso et al. (2008), algumas questões humanas interferem na comunicação, conforme descrito a seguir:

1. Soberba: manifestação arrogante de um orgulho às vezes ilegítimo, excessivo;
2. Inveja: desejo violento de possuir o bem alheio; desgosto ou pesar pelo bem ou pela felicidade de outrem;
3. Insegurança: falta de segurança em si próprio, em seus conhecimentos e experiências;
4. Medo: sentimento de grande inquietação ante a noção de um perigo real ou imaginário, de uma ameaça, temor, pavor;
5. Mentira: impostura, fraude, falsidade. Engano dos sentimentos ou do espírito; erro, ilusão, ideia, opinião, doutrina ou juízo falso;
6. Depressão: abatimento moral;
7. Vaidade: desejo imoderado de atrair admiração ou homenagens;
8. Avareza: apego exagerado ao dinheiro, falta de generosidade, mesquinhez;
9. Cobiça: desejo veemente de alguma coisa. Avidez. Ambição desmedida de riquezas;
10. Ira: cólera, raiva, indignação. Desejo de vingança.
11. Luxúria: lascívia, sensualidade, corrupção de costumes;
12. Preguiça: pouca disposição para o trabalho, demora ou lentidão em fazer qualquer coisa; moleza. Negligência, indolência;
13. Entusiasmo: veemência, vigor no falar e escrever. Exaltação criadora;
14. Decepção: desilusão; desengano; desapontamento. Surpresa desagradável, contrariedade.

Quando um indivíduo quer obter uma informação de outrem utilizando a engenharia social, geralmente busca informações a respeito da vítima tais como: caráter, personalidade, valores, vulnerabilidades; estas serão úteis para o estabelecimento de uma comunicação que lhe permita obter o que quer explorando as fraquezas de um dos ativos humanos da organização. Affonso et. al. (2008) recomendam para proteção das informações de uma comunicação:

1. Usar códigos conhecidos;
2. Usar meios adequados aos tipos de mensagens e usuários;
3. Adotar estilo simples e claro;
4. Respeitar o interlocutor, não super ou subestimá-lo;
5. Respeitar a cultura organizacional e a do país;
6. Evitar “ruídos” nos processos.

## 2.7 Análise de componentes estruturais

Conforme Affonso et. al (2008) a Segurança da Informação está diretamente ligada à compreensão do contexto, seu significado e sua importância. O universo humano (que inclui questões sócio familiar, de nutrição, saúde, economia, religiosidade, lazer, segurança, educação, justiça, política, integração social) de uma organização pode ser analisado como um todo ou por perímetros pré-estabelecidos, podendo ser definidos conforme o contexto situacional, como, por exemplo, nos departamentos.

A Figura 5 exibe o universo-social e os aspectos a ele relacionados.

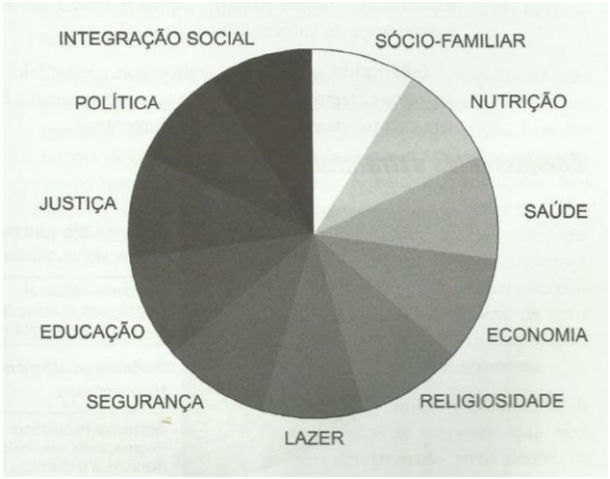


**Figura 5: Universo social. Figura retirada de (AFFONSO et al., 2008).**

A complexidade do mundo interior individual está diretamente relacionada com aspectos individuais tais como percepção, afeição, realidade, sonhos, medos, desejos que são influenciados por aspectos do universo social tais como integração-social, sócio familiar, educação. Tais aspectos individuais refletem-se no coletivo, influenciam as relações e podem também influenciar ou determinar medidas de controle de segurança mais ou menos rígidas.

## 2.9 Educação e Conscientização

Conforme Mitnick e William (2003), a aprendizagem implica em mudança de hábitos (comportamentos). Segundo Aristóteles, o hábito é de importância básica para a moralidade. Pode-se tratar a habituação distinguindo-a em adaptativa e estabilizadora. Entende-se por adaptativa quando um indivíduo se acomoda a determinadas circunstâncias ao ponto que a ausência delas se fará sentir como um transtorno, e por estabilizadora quando o indivíduo estabiliza em si uma atitude determinada de tal como que fique preferida e conservada.

Práticas de conscientização em segurança da informação são consideradas um processo de aprendizagem, que implica em mudança de hábitos. Em tais práticas é importante atenção especial quanto à forma como o conhecimento será disseminado; é conveniente educar pela compreensão das ideias e fatos e não coagir ou trabalhar o medo, visto que a coação e o medo podem desencadear comportamentos ofensivos a segurança da informação.

Conforme a ISO/IEC 27001 (2009) o treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação e respondam de acordo com as necessidades do seu trabalho. Esta norma recomenda que os participantes do SGSI estejam conscientes da necessidade de segurança de sistemas de informação e redes e do que eles podem fazer para aumentar a segurança.

Prover atenção especial ao fator humano, principalmente quanto ao universo social das populações do contexto organizacional, é imprescindível para aquelas organizações que almejam um estar em um estado seguro, visto que este fator representa a vulnerabilidade mais significativa para segurança da informação e requer devida proteção.

Um Plano de Conscientização em Segurança (PCS) tem como propósito focar a conscientização coletiva da corporação a respeito dos problemas de segurança, visando influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informação da organização.

É recomendado a criação e planejamento deste plano conforme a seguinte ordem e sequência de atividades:

1. Definição do objetivo;

2. Compreensão do universo que envolve o público alvo (atores desse cenário, seu status e papel, suas aspirações, padrões de comportamento, criatividade cultural[20]);
3. Análise histórica da evolução da segurança na organização. E paralelamente estudo e compreensão do plano de negócios, do inglês *business plan*[21], da empresa, sua missão e valores corporativos;
4. Seleção e ordenamento, quanto a prioridade, dos conteúdos;
5. Definição de metodologia de abordagem;
6. Definição do intervalo de tempo entre a apresentação dos conteúdos.

Todos os profissionais de uma organização são responsáveis pela segurança das informações corporativa, está responsabilidade não é apenas do departamento de segurança, da auditoria ou da alta direção, mas de toda população organizacional, sendo de suma importância o apoio, comprometimento e participação da alta direção no planejamento e execução deste processo, a fim de facilitar a mobilização e sensibilização de todos os colaboradores.

A ISO/IEC 27.001 (2009) define que a organização deve assegurar que todo o pessoal que tem responsabilidades atribuídas definidas no SGSI seja competente para desempenhar as tarefas requeridas:

1. Determinando as competências necessárias para o pessoal que executa trabalhos que afetam o SGSI;
2. Fornecendo treinamento ou executando outras ações (por exemplo, contratar pessoal competente) para satisfazer essas necessidades;
3. Avaliando a eficácia das ações executadas; e
4. Mantendo registros de educação, treinamento, habilidades, experiências e qualificações.

A norma também orienta que em uma organização todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do SGSI.

A tecnologia pode ser utilizada em prol de dificultar os ataques de engenharia social, retirando as pessoas do processo de tomada de decisão, entretanto apenas a tecnologia não

[20] Caminho alternativo, a forma como as pessoas resolvem os seus problemas quando o caminho oficial não responde em tempo.

[21] Plano com diretrizes formais quanto aos objetivos de negócio, justificativas quanto a viabilidade de alcance dos objetivos e planos para alcança-los.

previne totalmente um ataque de engenharia social. O meio verdadeiramente mais efetivo de amenizar a ameaça da engenharia social é realizar constantemente práticas de conscientização para a população organizacional, aliada com políticas de segurança eficazes, que definam as principais regras para o comportamento de todos os profissionais. Quanto mais bem instruídos em segurança da informação estiverem os profissionais de uma organização, mais atentos estarão ao assédio de um engenheiro social e uma melhor resposta eles serão capazes de elaborar e transmitir em um ataque. Contudo, é recomendado avaliação constante quanto aos estados de ânimo, necessidades e interesses da população organizacional, (a análise de clima [22]pode ser utilizada como um recurso facilitador para este propósito) a fim de precaver que a população organizacional estará preparada adequadamente a um ataque de um engenheiro social, que possa vir a ocorrer a qualquer momento.

A conscientização em segurança da informação tem por objetivo assegurar que a segurança seja inserida na cultura corporativa, sendo primordial o apoio ostensivo da alta direção. O sucesso do ataque de uma ameaça, tal como um engenheiro social, pode ser evitado ou pelo menos reduzido através de uma conscientização efetiva, com a participação de todos os colaboradores da organização, com comportamento seguro, consciente e alerta e por meio da implantação efetiva de um conjunto de medidas de proteção tais como plano de conscientização em segurança da informação, políticas de segurança da informação, tecnologias de proteção, práticas contra divulgação de informações aparentemente inofensivas.

## 2.10 Política de Segurança da Informação

De acordo com a Cartilha para Segurança na Internet a política de segurança da informação organizacional define os direitos e as responsabilidades de cada profissional em relação à segurança dos recursos computacionais que utiliza e as penalidades ás quais está sujeito, caso não a cumpra. Ela é considerada como um importante mecanismo de segurança tanto para as instituições como para os usuários, visto que por meio dela é possível definir e esclarecer o comportamento esperado de cada um. Por conseguinte, casos de mau comportamento ou uso abusivo, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas. Exemplos de situações de uso abusivo:

[22] Ferramenta que visa proporcionar a análise da organização com o seu ambiente, bem como o conjunto de condições que caracterizam o estado de satisfação e ou insatisfação dos colaboradores profissionais na empresa e das demais pessoas que com eles interagem.

compartilhamento de senhas, divulgação de informações confidenciais, ataques a computadores, comprometimento de computadores (CERT.BR, 2012).

Conforme Affonso et al, (2008) a política de segurança da informação de uma organização é um conjunto de documentos que descreve quais são os objetivos que todas as áreas ligadas a segurança da informação devem trabalhar para atingir.

A ISO/IEC 27001 (2009) define que a política de segurança da informação prove uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A norma recomenda que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização. Ela recomenda que a política contenha declarações relativas aos itens abaixo listados:

1. Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação;
2. Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;
3. Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco; breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:
4. Conformidade com a legislação e com requisitos regulamentares e contratuais;
5. Requisitos de conscientização, treinamento e educação em segurança da informação;
6. Gestão da continuidade do negócio;
7. Consequências das violações na política de segurança da informação.
8. Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;
9. Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

## 2.11 Boas Práticas de Segurança da Informação

Existem diversas boas práticas, normas e exigências regulatórias relacionadas à segurança da informação, aplicáveis a diferentes segmentos de mercado, como financeiro, hospitalar, energético, automotivo, que tratam informações sensíveis e precisam protege-las da forma adequada. Segue descritivo de algumas boas práticas com orientações com relação à segurança informacional:

### 2.11.1 Norma ISO/IEC 27.001:2009

A família de normas ISO 27.000 objetiva auxiliar as organizações a manter a segurança dos ativos organizacionais, como por exemplo: informações financeiras, propriedade intelectual, informações de colaboradores (ISO STANDARTS, 2016).

A ISO/IEC 27.001 é uma norma internacional que prove um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos e tamanho e estrutura da organização.

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas. As empresas que almejam certificar que as recomendações da ISO/IEC 27.001 estão sendo seguidas no âmbito organizacional podem certificarem-se nesta norma (ISO STANDARTS, 2016; ISO/IEC 27001, 2009).

A abordagem de processo para a gestão da segurança da informação apresentado nesta norma enfatiza a importância do:

1. Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;
2. Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
3. Monitoração e análise crítica do desempenho e eficácia do SGSI; e
4. Melhoria contínua baseada em medições objetivas.

O modelo de Planejar, Fazer, Verificar e Agir (PDCA), do inglês *Plan-Do-Check-Act* é aplicado ao SGSI e neste contexto este modelo tem por objetivo manter e melhorar continuamente a eficácia do SGSI organizacional. A fase de planejamento refere-se a estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Já a segunda fase é referente a implementar e operar a política, controles, processos e procedimentos do SGSI. A terceira fase contempla avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção. E a última fase contempla executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A Figura 6 ilustra o fluxo do SGSI, a partir de entradas relacionadas a partes interessadas e requisitos para gestão de segurança da informação, ações e processos são executados e é produzida como saída uma gestão de segurança da informação alinhada com os requisitos estabelecidos.

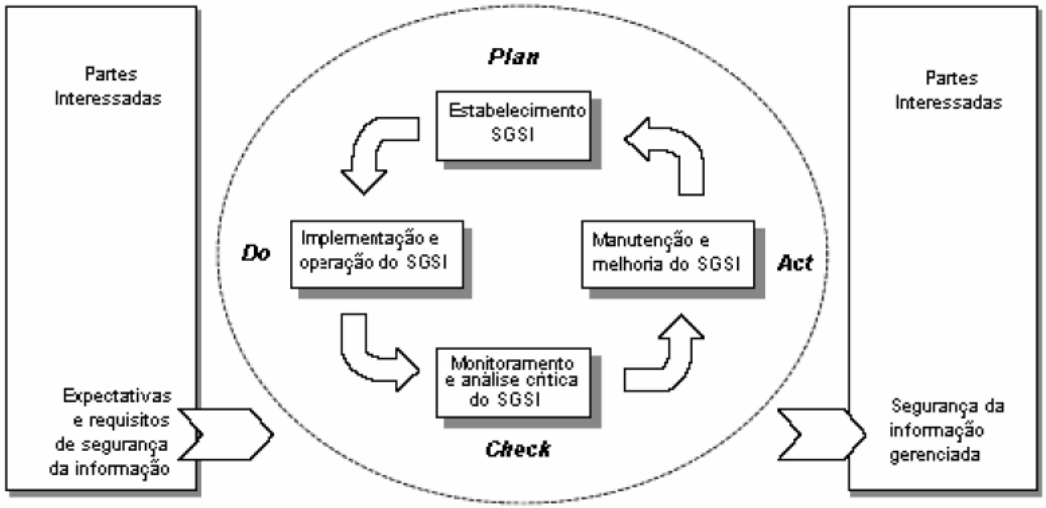


**Figura 6: Modelo PDCA aplicado ao processo SGSI. Figura retirada de (BSI ISO 27001, 2009).**

### 2.11.2 COBIT 5

O Cobit 5 provê orientação da ISACA (Fundada em 1969, a ISACA é uma entidade independente e sem fins lucrativos que organiza conferências internacionais, publica o ISACA *Journal* e desenvolve padrões internacionais de controle e auditoria de SI que ajudam seus usuários a garantir a confiança e o valor dos sistemas de informação) sobre governança corporativa e gestão de TI. Este guia pode ser utilizado por muitas organizações e usuários das comunidades de negócios, TI, riscos, segurança e garantia.

Este guia apresenta uma orientação para segurança da informação, abordando aspectos de muitos padrões e práticas bem aceitos globalmente na atualidade, pode ser utilizado por profissionais de segurança, de negócios e usuários de TI em geral. A Figura 3 apresenta a família de produtos do Cobit 5:

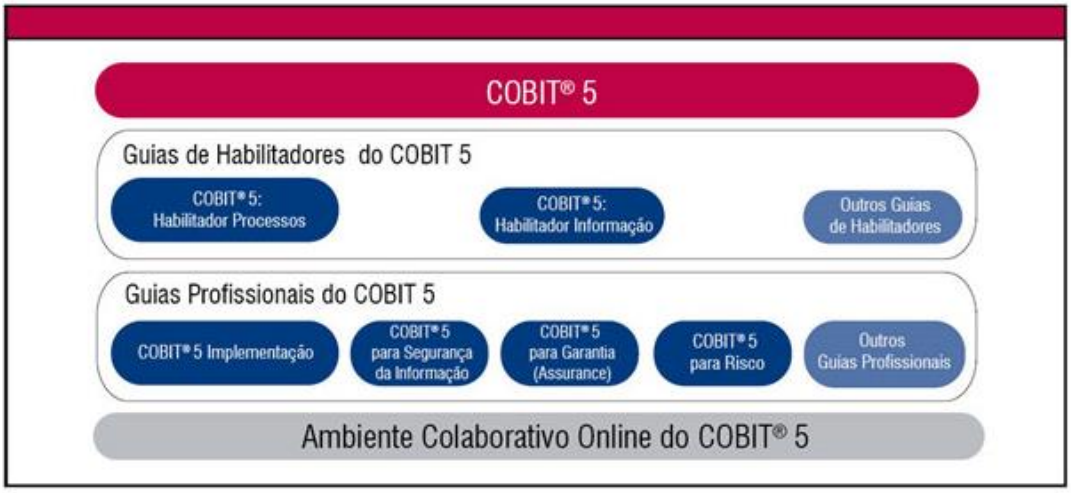


**Figura 7: Família de Produtos do Cobit 5. Figura retirada de (ISACA, 2016).**

De acordo com o Cobit 5 o processo de Gerenciar Segurança contribuirá:

1. Diretamente, para a consecução dos objetivos de TI:
   a) Conformidade de TI e apoio para conformidade do negócio com leis e regulamentos externos;
   b) Gestão de risco organizacional de TI;
   c) Transparência dos custos, benefícios e riscos de TI;
   d) Segurança da informação, infraestrutura de processamento e aplicativos;
   e) Disponibilidade de informações úteis e confiáveis para tomada de decisão.
2. Em menor grau, para a consecução dos objetivos de TI:
   a) Prestação de serviços de TI em consonância com os requisitos de negócio;

b) Uso adequado de aplicativos, informações e soluções tecnológicas.

### 2.11.3 BS ISO 22301:2012

A Norma internacional BS ISO 22301 especifica requisitos para implementar e gerenciar um Sistema de Gestão de Continuidade de Negócios (BCSM) do inglês (*Business Continuity Management System*). Esta norma define a continuidade de negócios como a capacidade da organização de continuar entregando seus produtos e serviços a níveis aceitáveis e pré-definidos, mediante situação de um incidente devastador. Ela define a gestão de continuidade de negócios como um processo de gestão holístico que identifica potenciais ameaças a uma organização e os impactos as operações do negócio, que estas ameaças podem causar, caso se concretizem e provê uma estrutura para construção de uma resiliência organizacional com capacidade de responder de forma efetiva, protegendo os interesses dos *stakeholders*, reputação, marca e as atividades organizacionais de valor agregado. Conforme a BS ISO 22301 (2012), uma BCMS enfatiza a importância de:

1. Entender as necessidades organizacionais e a necessidade de implementação de políticas e objetivos de gestão de continuidade de negócios;
2. Implementar e manter controles e medidas para gestão da capacidade organizacional de gerenciar incidentes devastadores;
3. Monitorar e auditar a eficácia do BCMS;
4. Melhoria contínua baseada na medição dos objetivos estabelecidos.

Os componentes principais do BCMS são:

1. Politica;
2. Pessoas com responsabilidades definidas;
3. Processos de gestão relacionados com:
   a) Politica;
   b) Planejamento;
   c) Implementação e Operação;
   d) Avaliação de desempenho;
   e) Auditoria;
   f) Melhoria.
4. Documentação que provisione evidencias auditáveis;
5. Qualquer processo de gestão de continuidade de negócios relevantes para a organização.

O modelo de Planejar, Fazer, Verificar e Agir (PDCA), do *inglês Plan-Do-Check-Act* é aplicado ao BCMS é neste contexto este modelo tem por objetivo manter e melhorar continuamente a eficácia do BCMS organizacional. A fase planejamento é referente ao estabelecimento de políticas, objetivos, controles, processos e procedimentos relevantes para continuidade de negócios, a fim de entregar resultados alinhados com as políticas e objetivos organizacionais. Já a segunda fase é relativa a implementação e operação de políticas, controles, processos e procedimentos de continuidade de negócios. A terceira fase está relacionada ao monitoramento e avaliação de performance das políticas e objetivos da gestão de continuidade de negócios, reportando resultados a gerência e determinando ações para recuperação e melhoria. E a última fase é referente a execução de ações corretivas, com base na avaliação dos resultados por parte da gerência e reavaliação do escopo, políticas e objetivos do BCMS. A Figura 1 ilustra o fluxo do BCMS, a partir de entradas relacionadas a partes interessadas e requisitos para gestão de continuidade de negócios, ações e processos são executados e são produzidos saídas e é produzida como saída uma gestão de continuidade de negócios alinhada com os requisitos estabelecidos.

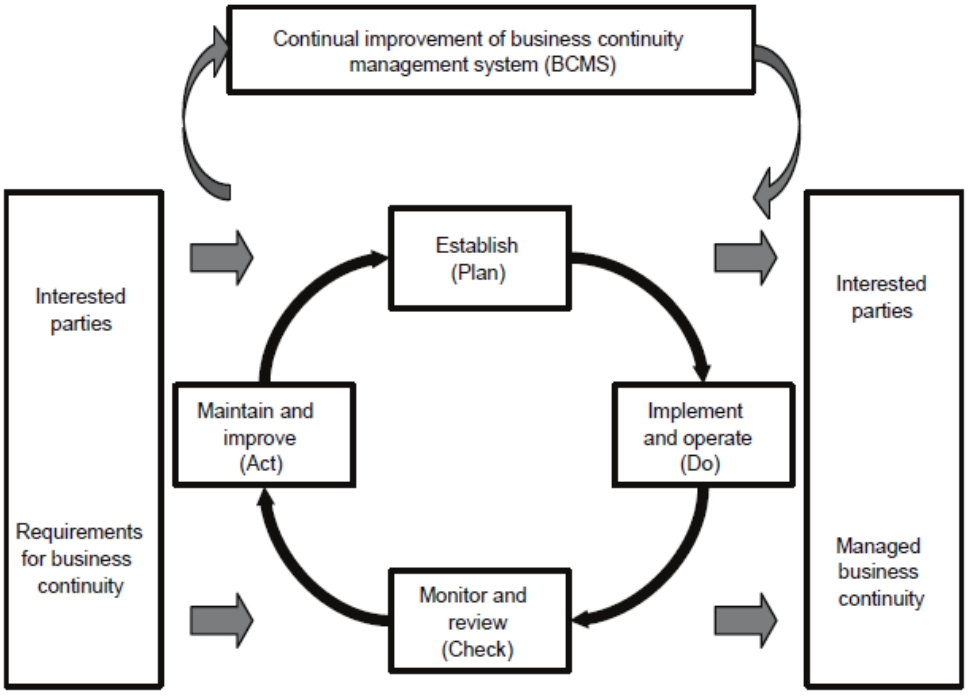


**Figura 8: Modelo PDCA aplicado ao processo BCMS. Figura retirada de (BSI ISO 22301, 2012).**

### 2.11.4 Resolução 3.380 do Banco Central do Brasil

A resolução n° 3380 do Banco Central do Brasil, que se tornou pública em 29 de junho de 2006, dispõe sobre a implementação da estrutura de gerenciamento do risco operacional. A saber o risco operacional é definido como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. O seu Art. 1 determina que às instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem implementar uma estrutura de gerenciamento do risco operacional. Como exemplos de eventos de risco operacional relacionados à segurança da informação: danos a ativos físicos próprios ou em uso pela instituição, aqueles que acarretem a interrupção das atividades da instituição, falhas em sistemas de tecnologia da informação, fraudes internas e externas.

Com relação ao âmbito da segurança da informação, em especifico no que tange a continuidade de negócios, ela é definida como capacidade da organização de continuar entregando seus produtos e serviços a níveis aceitáveis e pré definidos, mediante situação de um incidente devastador, a resolução define no art. 3 item IV que a estrutura de gerenciamento de risco operacional deve prever existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional.

### 2.11.5 Circular 3.681 do Banco Central do Brasil

A circular 3.681, que se tornou pública em 4 de novembro de 2013, dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências. Através do art. 4 ela define que a estrutura de gerenciamento de riscos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil deve prever, no que tange ao risco operacional, no mínimo:

I - Plano de contingência e outros mecanismos que garantam a continuidade dos serviços de pagamento prestados;

II - Mecanismos de proteção e segurança dos dados armazenados, processados ou transmitidos;

III - Mecanismos de proteção e segurança de redes, sítios eletrônicos, servidores e canais de comunicação com vistas a reduzir a vulnerabilidade a ataques;

IV - Procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas, bases de dados e módulos de segurança;

V - Monitoramento das falhas na segurança dos dados e das reclamações dos usuários finais a esse respeito;

VI - Revisão das medidas de segurança e de sigilo de dados, especialmente depois da ocorrência de falhas e previamente a alterações na infraestrutura ou nos procedimentos;

VII - Elaboração de relatórios que indiquem procedimentos para correção de falhas identificadas;

VIII - Realização de testes que assegurem a robustez e a efetividade das medidas de segurança de dados adotadas.

# 3 METODOLOGIA

Para atingir os objetivos definidos, este trabalho foi realizado de acordo com as seguintes etapas metodológicas:

1. Revisão de literatura em profundidade sobre os principais temas tratados no trabalho.

2. Estudo e mapeamento de conceitos da ISO/IEC 27001, Cartilha de Segurança da Informação, Guia Oficial para formação de gestores em Segurança da Informação, Manual de Persuasão do FBI, A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação e Gestão da Segurança da Informação: Uma Visão Executiva, COBIT 5, BS ISO 22301, Resolução Bacen 3380, Circular Bacen 3681.

- Pesquisa de conceitos de informação, comunicação, ciclo de vida da informação, segurança da informação, vulnerabilidades, ameaças, engenharia social, impactos, conscientização, política de segurança da informação.

3. Identificação e mapeamento das principais vulnerabilidades humanas:

- Pesquisa e mapeamento das vulnerabilidades humanas no contexto da segurança da informação, englobando técnicas e métodos de exploração de vulnerabilidades, a arte da engenharia social, ferramentas utilizadas por engenheiros sociais, métodos de proteção contra ataques de engenharia social.

4. Identificação e mapeamento de boas práticas para proteger as informações, com enfoque nas pessoas;

- Pesquisa e mapeamento de recomendações e ferramentas para proteção das informações e do elemento mais vulnerável da segurança da informação (as pessoas).

# 5 CONSIDERAÇÕES FINAIS

A informação é um ativo, bem e patrimônio fundamental para prosperidade dos negócios organizacionais. Este ativo provê um diferencial de competitividade, agilidade, modernidade, lucratividade, expansibilidade e de imagem.

Com a era da informação e com os avanços tecnológicos, os recursos de tecnologia para proteção de informações apresentam soluções cada vez mais robustas, entretanto somente a tecnologia não é uma solução suficiente. Recursos tecnológicos dificultam que uma ameaça tenha êxito ao tentar explorar uma vulnerabilidade de um ativo, com tudo eles não provém uma proteção de forma sistêmica ao ativo, por exemplo: uma organização pode utilizar um software de alta tecnologia para guarda de senhas de usuários administradores, contudo a configuração para visualizar a senha pode não ter sido desabilitado pela equipe de administração da ferramenta e um usuário não conscientizado pode copiar a senha para um papel, exemplo este mostra a importância de estabelecer a segurança de forma global, analisando e definindo controles referentes a processos, pessoas e tecnologias.

Em prol de se estabelecer uma segurança mais eficiente é importante que o planejamento da estratégia de segurança organizacional alinhe os controles para proteção dos ativos com a cultura, negócio, objetivo, missão, visão e necessidades organizacionais. Adquirir proteções que provêm mais que o necessário, acarreta gastos desnecessários, podendo extrapolar o valor do próprio ativo e inviabilizar a aquisição da proteção e ou prover funcionalidades que não são essenciais ou necessárias, por outro lado proteções que provêm menos que o necessário podem deixar o ativo vulnerável a exploração de ameaças, podendo acarretar uma série de prejuízos, como por exemplo, financeiro e depreciação da marca. Para definição das proteções dos ativos é importante considerar tecnologia, processos e pessoas, estando todos estes alinhados com o negócio da organização e levando em consideração que não existe segurança absoluta.

A instrução e o treinamento a respeito das diretrizes e procedimentos de segurança corporativos devem capacitar os indivíduos para que tenham o conhecimento de como detectar, evitar e agir diante de um evento, incidente ou qualquer situação que eles entendam que possa vir a comprometer a segurança das informações. Se cada profissional atuar como um indivíduo consciente quanto a segurança da informação e a alta direção praticar, apoiar e prover suporte a gestão de segurança da informação, provavelmente a aculturação da segurança será mais eficiente e, possivelmente, a integridade, disponibilidade e a confidencialidade de informações sensíveis serão mais bem preservadas de potenciais ameaças, tais como um engenheiro social.

Como oportunidade de trabalho futuro seria interessante a realização de pesquisas a respeito de modelos de sucesso de planos de conscientização em segurança da informação, visto que para proteger as informações corporativas um passo essencial é conscientizar a população organizacional. Além disso, existem outros vieses humanos, também referentes a segurança, a serem explorados em outros trabalhos, tais como segurança no processo de recursos humanos que poderia tratar da gestão de acessos lógicos e físicos, englobando o recrutamento, a contratação; a transferência entre áreas organizacionais e o desligamento tanto para funcionários, estagiários, aprendizes e terceiros. Existem boas práticas para proteção das informações no contexto de acesso lógico e físico; assim, provavelmente um estudo mais exploratório culminaria em uma relevante pesquisa.

## REFERÊNCIAS


Affonso, C.; Alevate, W.; Andrucioli, A.; Bastos, A.; Blum, R. O.; Marinho, Z.; Pinto, E.; Poggi, E.; Ramos, A.; e. ***Security Officer*** **- 1: Guia Oficial para Formação de Gestores em Segurança da Informação**. Zouk: Porto Alegre, 2008. 351p.

Affonso, C.; Alevate, W.; Andrucioli, A.; Bastos, A.; Blum, R. O.; Marinho, Z.; Pinto, E.; Poggi, E.; Ramos, A.; e. ***Security Officer*** **- 2: Guia Oficial para Formação de Gestores em Segurança da Informação**. Zouk: Porto Alegre, 2008. 363p.

Banco Central do Brasil; Luiz Edson Feltrim. **Circular n° 3681**. Brasília: Banco Central do Brasil, 2013. 08 p.

Banco Central do Brasil; Henrique de Campos Meirelles. **Resolução n° 3380**. Brasília: Banco Central do Brasil, 2006. 04 p.

BSI Standart Publication. **BS ISO 22301 - Societal Security - Business Continuity Management Systems - Requirements**. UK: BSI Standart Publication, 2012. 36p.

CERT.BR - Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para a internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 142p.

Gestão de Crises e Continuidade dos Negócios. **Gestão de Continuidade dos Negócios**. Disponível em: http://www.gcnbrasil.com/index.php?option=com_content&view=section&id=5&Itemid=54. Acesso em: outubro. 2016.

Hiles, Andrew. **The Definitive Handbook of Business Continuity Management**. Inglaterra: John Wiley and Sons Ltd, 2007. 668p.

Hobel, H.; Huber, M.; Krombholz, K.; Weippl, E. Advanced social engineering attacks.**Journal of Information Security and Applications**, Elsevier, Vienna, Austria, n.22, 24 out. 2014.

International Organization for Standardization; International Electrotechnical Commission. **ISO/IEC 27001 - Information technology - Security techniques - Information security management system – Requeriments**. Berlin: ISO/IEC, 2009. 25p.

International Organization for Standardization; International Electrotechnical Commission. **ISO/IEC 27002 - Information technology - Security techniques – Code of practice for information security management**. Berlin: ISO/IEC, 2010. 129p.

ISACA. **COBIT 5 – Modelo Corporativo para Governança e Gestão de TI na Organização**. EUA: ISACA, 2012. 98p.

ISACA**. Publicações centrais do COBIT: Uma rápida visão**. Mark Thomas. Disponível em: <http://www.isaca.org/COBIT/focus/Pages/the-core-cobit-publications-a-quick-glance-portuguese.aspx>**.** Acesso em: 12 out. 2016.

ISO Standarts. **ISO/IEC 27001 - Information security management**. Melhoramentos. Disponível em: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>. Acesso em: 09 out. 2016.

Karlins, M.; Schafer, J. **Manual de Persuasão do FBI**. Universo dos Livros: São Paulo, 2015. 274p.

Kimppa, K.K.; Malan, M.M; Mounton, F.; Venter, S. H. Necessity for ethics in social engineering research. **Computer & Security**, Elsevier, Indiana, USA, n. 55, 9 set. 2015.

Mitnick D. Kevin; Simon L.William. **A Arte de Enganar. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. Perason Education: São Paulo, 2003. 588p.

Sêmola, M. **Gestão da Segurança da Informação: Uma Visão Executiva**. Campus Elsevier: Rio de Janeiro, 2003. 154p.