CENTRO UNIVERSITÁRIO DE ANÁPOLIS – UniEVANGÉLICA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

CÍNTIA DA SILVA GALVÃO
SAMARA DE LOURDES MIRANDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: PROPOSTA DE UMA SEÇÃO ABORDANDO ENGENHARIA SOCIAL PARA A NORMA ISO/IEC 27002

ANÁPOLIS - GO
2020

CÍNTIA DA SILVA GALVÃO
SAMARA DE LOURDES MIRANDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: PROPOSTA DE UMA SEÇÃO ABORDANDO ENGENHARIA SOCIAL PARA A NORMA ISO/IEC 27002

Trabalho de Conclusão de Curso II apresentado como requisito parcial para a conclusão da disciplina de Trabalho de Conclusão de Curso II do curso de Bacharelado em Engenharia de Computação do Centro Universitário de Anápolis – UniEVANGÉLICA.

Orientador(a): Prof. Me. Millys Fabrielle Araújo Carvalhaes.

Anápolis - GO
2020

CÍNTIA DA SILVA GALVÃO
SAMARA DE LOURDES MIRANDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: PROPOSTA DE UMA SEÇÃO ABORDANDO ENGENHARIA SOCIAL PARA A NORMA ISO/IEC 27002

Trabalho de Conclusão de Curso II apresentado como requisito parcial para a obtenção de grau do curso de Bacharelado em Engenharia de Computação do Centro Universitário de Anápolis – UniEVANGÉLICA.

Aprovado(a) pela banca examinadora em [dia] de [mês] de 2020, composta por:

_____
Prof. Millys Fabrielle Araujo Carvalhaes
Orientador

_____
Prof. [nome do professor]

_____
Prof. [nome do professor]

RESUMO

Esta pesquisa tem como objetivo identificar os principais tipos de ataques a segurança da informação que envolvam técnicas de engenharia social. Para isso foram realizadas pesquisas bibliográficas acerca do assunto em busca do que leva o usuário a ser uma vítima deste tipo de técnica e se atualmente existem Políticas de Segurança da Informação (PSI) direcionadas a engenharia social. Foi feita uma análise das normas ISO (*the International Organization for Standardization*) / IEC (*the International Electrotechnical Commission*) 27001 e 27002 sobre a importância de um Sistema de Gestão a Segurança da Informação (SGSI) e da implementação de uma Política de Segurança da Informação. Como resultado do estudo realizado não foi encontrado nenhum tópico abordando especificamente a engenharia social na norma ISO 27002. Diante disto este trabalho tem como objetivo propor uma seção para complementar a ISO 27002 que aborde diretamente a engenharia social, incluindo procedimentos e contramedidas para evitar tais ataques.

Palavras-chave: Segurança da Informação; Ataques; Engenharia Social; Políticas de Segurança da Informação; ISO 27002.

ABSTRACT

This research aims to identify the main types of attacks on information security that involve social engineering techniques. For this purpose, bibliographic research about the subject was conducted in search of what makes the user a victim of this kind of technique and if exists Information Security Policy (ISP) towards social engineering. An analysis of ISO (International Organization for Standardization) and IEC (International Electrotechnical Comission) 27001 and 27002 was made, about the importance of a Information Security Management System (ISMS) and the creation of an Information Security Policy. As a result of this study, no topic was found specifically about social engineering in the ISO 27002 standard. Given this, this work aims as an objective to propose an section to complement the ISO 27002 standard, that address directly to social engineering, including procedures and countermeasures to prevent such attacks.

Keywords: Information Security; Attacks; Social Engineering; Information Security Policy; ISO 27002.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

ABNT/CB-21 - Comitê Brasileiro de Computadores e Processamento de Dados

C.I.D - Confidencialidade, Integridade e Disponibilidade

IEC - *The International Electrotechnical Commission*

ISO - *The International Organization for Standardization*

LGPD - Lei Geral da Proteção de Dados

NBR - Norma Técnica Brasileira

PSI - Políticas de Segurança da Informação

SGSI - Sistema de Gestão a Segurança da Informação

SUMÁRIO

1. INTRODUÇÃO

Volumes maciços de informações digitalizadas são gerados, armazenados, manipulados e compartilhados a todo instante. Esta forma de utilizar a tecnologia para manipular informações traz facilidade para o usuário, contudo também traz um risco à segurança da informação. Somente em 2017 o Brasil perdeu cerca de 22 bilhões de dólares devido a crimes cibernéticos, e no mesmo ano cerca de 62 milhões de brasileiros foram vítimas de cibercrime. (SYMANTEC, 2017).

Diversos autores apontam que a principal ameaça para qualquer segurança é o ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema. A instrução é importante na segurança da informação, pois segurança também pode ser considerada uma questão comportamental. (SANTOS, 2011 apud COELHO; RASMA; MORALES, 2013).

Segundo Mitnick e Simon (2003) a evolução das tecnologias de segurança da informação dificulta a exploração de vulnerabilidades técnicas, com isso os atacantes irão buscar a exploração do elemento humano. Dessa forma o atacante engana, influência ou manipula o indivíduo para obter o acesso a informações sigilosas, este tipo de ação é denominado como engenharia social.

O uso de técnicas de engenharia social para a realização de ataques é de difícil prevenção, pois não é possível utilizar um *antimalware* que a impeça, dado que a engenharia social coloca o próprio indivíduo no circuito de brechas de segurança e o utiliza como arma. (KIM; SOLOMON, 2014).

De acordo com Agostinho (2004), a popularização da internet e do acesso a microcomputadores facilitou as práticas de delitos digitais, considerados crimes virtuais, sendo assim necessário ajustar a norma penal. Visto que, os responsáveis pela ação criminosa não são agentes físicos, mas sim agentes virtuais e devem ser penalizados pelo evento criminoso.

Foram desenvolvidas diferentes normas com a intenção de garantir a segurança da informação, uma delas é a ISO 27002. De acordo com Correia (2016) ela faz parte de um grupo de oito normas ISO que fornecem diretrizes com orientações visando a introdução, implementação e manutenção do Sistema de Gestão de Segurança da Informação, gestão de riscos e métricas. Considerando os diferentes meios e cenários a Política de Segurança da Informação indica as melhores práticas a serem seguidas para a gestão da informação.

A Política da Segurança da Informação é um documento que auxilia empresas e pessoas a gerenciar a segurança de dados no qual é estabelecido um conjunto de técnicas, métodos, regras e boas práticas. Deve ser desenvolvida com base nas recomendações propostas pela norma Associação Brasileira de Normas Técnicas (ABNT) Norma Técnica Brasileira (NBR) ISO/IEC 27001.

De acordo com Marciano e Lima-Marques (2006), para uma gestão de segurança da informação correta todos os usuários devem assumir a responsabilidade de seus atos com a aplicação de normas e procedimentos. Sendo assim, como uma seção complementar a norma ISO/IEC 27002, tratando de engenharia social, pode auxiliar usuários a evitar ataques cibernéticos que fazem o uso dessa técnica?

Considerando que para a melhoria da gestão da segurança da informação é importante o uso de boas práticas, foi elaborado este trabalho com o objetivo geral de propor uma seção complementar a norma ISO/IEC 27002 com ênfase em engenharia social, tratando de boas práticas, métodos e técnicas para a sua prevenção. O processo para alcançar este objetivo foi estabelecido de acordo com os seguintes objetivos específicos: Identificar os tipos de ataques a segurança da informação, analisar as principais técnicas de engenharia social, analisar os motivos que levam o usuário a ser vítima da engenharia social e analisar as normas da família ISO/IEC 27000.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada uma introdução geral a segurança da informação, onde serão abordados assuntos como a diferença entre dado e informação, o conceito de ativos e o seu valor para indivíduos e organizações. Para melhor compreensão da importância da segurança da informação serão apresentados os seus princípios básicos e como cada um deles contribui para a segurança dos dados. Será apresentada a definição de vulnerabilidades, ameaças, ataques, e a relação entre eles, onde serão abordados os tipos de ataques a segurança da informação existentes, assim como alguns dos programas maliciosos mais utilizados nestes ataques e sua forma de agir. Adiante será abordada a técnica de ataque chamada engenharia social, explicando como o fator humano e suas vulnerabilidades favorecem o uso desta técnica, e como agem os engenheiros sociais que a utilizam para explorar as vulnerabilidades humanas de modo que consigam acesso a informações sem autorização.

Além disso, será apresentada a necessidade de se manter a informação segura e o conjunto de normas ISO da família 27000, que auxiliam as organizações nessa segurança, expondo o objetivo de cada uma delas. O assunto será aprofundado especificamente nas normas ISO 27001 e ISO 27002, que contribuem para a criação de uma Política de Segurança da Informação. Complementando a ideia das normas serão apresentados os conceitos de políticas, diretrizes e procedimentos, assim como as medidas de segurança existentes para a proteção dos ativos e os passos necessários para a implementação de um Sistema de Gestão de Segurança da Informação.

2.1 SEGURANÇA DA INFORMAÇÃO

Como afirma Machado (2014), a “Era da Conectividade” é representada pela importância das informações, sejam elas físicas ou virtuais, localizadas em um banco de dados de uma empresa ou em seu próprio computador. Um momento em que o acesso à internet, redes sociais ou e-mail se torna crucial para a comunicação e para o acesso a informações.

Segundo Cunha e Fenato (2013), antes a administração nas organizações era baseada em um modelo industrial, mas agora mudou o seu rumo baseando-se em conhecimento. Uma vez que, para acompanharem o cenário econômico mundial as empresas passaram a dar um valor e importância cada vez maior a informação. Devido a isso a

informação é considerada um bem vital dentro de uma organização, mas é importante ressaltar que ela precisa ter qualidades, ser confiável e estar disponível na hora certa, dessa forma, a partir das pessoas presentes em uma organização e da informação disponível a elas é gerado o conhecimento, portanto a informação é o combustível dessa nova economia.

2.2 DADO E INFORMAÇÃO

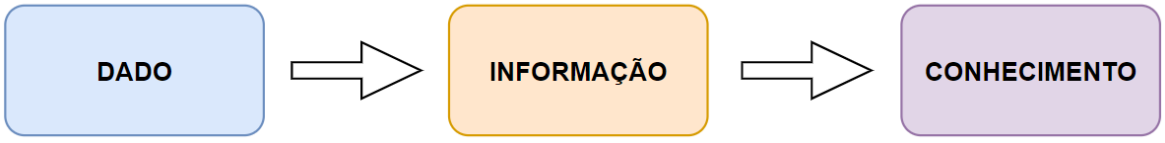
Os dados são a matéria prima da informação, eles são a menor unidade dentro da informação. Sendo assim todo sistema de informação é considerado um agrupamento de dados. Gravações e imagens podem ser citadas como exemplo de dados. (NOVO, 2010).

De acordo com Chiavaneto (2008 apud CUNHA; FENATO, 2013) os dados isolados têm pouco valor, pois sozinhos não constituem uma informação, entretanto quando são agrupados e relacionados eles permitem a obtenção da informação e passam a ter valor. Para que possam ganhar significado, e como resultado informar, é necessário efetuar o processamento dos dados (classificação, armazenamento e relacionamento), que pode ser feito de forma manual ou computacional, dependendo de como está sendo utilizado o dado.

Após o processamento de dados eles passam a constituir uma informação. Depois desse processo a informação pode gerar o conhecimento, como apresentado na Figura 1, e apresentar uma grande importância para quem faz o uso dela. Atualmente a informação integra o patrimônio de uma empresa, pois pode ser considerada um ativo valioso da mesma. (NOVO, 2010).

Diariamente tem-se contato com inúmeras informações diferentes, estas apresentadas em formatos diversos, como em texto, vídeo, áudio. E a forma como essa informação é apresentada impõe restrições sobre os seus métodos de proteção. (BAARS et al., 2018).

Figura 1: Relação entre dado, informação e conhecimento



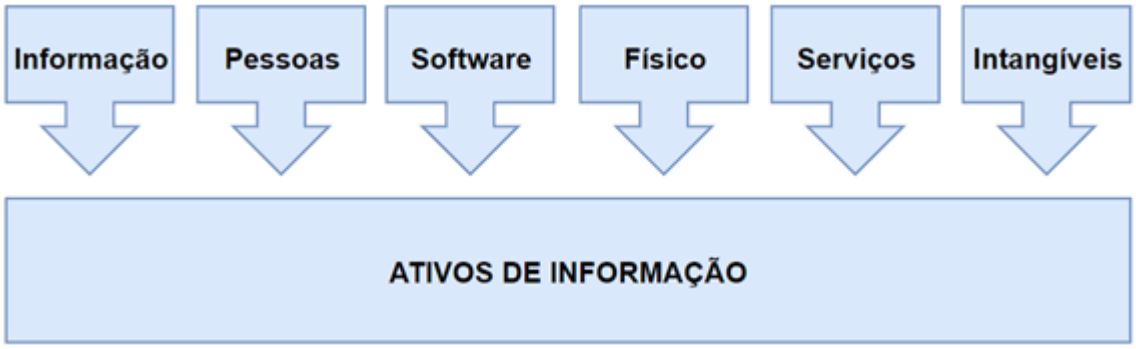
Fonte: Adaptado de Carvalho (2012 apud PAZ, 2019, p. 13).

2.3 ATIVOS

Segundo Kim e Solomon (2014, p. 65) “um ativo é qualquer item que tenha valor”. Dentro de uma organização todos os itens possuem valor, mas são considerados como ativos aqueles itens mais importantes, e por isso, devem ser protegidos. Qualquer informação que possui valor para um indivíduo ou organização pode ser chamado de ativo, tais como relatórios financeiros, discos rígidos, documentos impressos, etc. (NOVO, 2010).

Para a NBR ISO/IEC 27002:2005 os ativos relacionados a sistemas de informação são categorizados em: ativos de informação, ativos de software, ativos físicos, serviços, pessoas e intangíveis, conforme pode ser visualizado na Figura 2.

Figura 2: Ativos de Informação



Fonte: (LYRA, 2015, p. 12).

2.4 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

Abordado o conceito de informação, agora será apresentado o que é a segurança da informação.

> Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada. (FONTES, 2006, p. 10).

Para ser utilizada a informação deve garantir as seguintes características fundamentais: confidencialidade, integridade e disponibilidade. Estes são os três princípios básicos da segurança da informação, conforme pode ser verificado na Figura 3, eles também podem ser chamados de qualidades da informação. Tais princípios devem ser preservados, uma vez que qualquer ação que comprometa um deles estará afetando a segurança de toda informação. (DANTAS, 2011).

A confidencialidade, integridade e disponibilidade são definidas como o acrônimo C.I.D do inglês C.I.A., *confidentiality*, *integrity*, *availability*. (GOODRICH; TAMASSIA, 2013). Cada empresa tem a sua combinação de objetivos, requisitos de negócio e de segurança que adotam para executar estes princípios, devido a isso o nível de segurança necessário para implementá-los pode ser diferente de empresa para empresa, mas é fundamental que sejam utilizados em todos os programas de segurança. (BAARS et al., 2018).

Figura 3: Triângulo CID (Confidencialidade, Integridade, Disponibilidade)

Fonte: (PALMA, 2014, p.20).

2.4.1 Confidencialidade

A confidencialidade, ou exclusividade, assegura quem pode ter acesso a determinado tipo de informação, pois a informação deve ser acessada e utilizada exclusivamente por aqueles que possuem autorização. (BAARS et al., 2018).

Baars et al. (2018) ainda complementa que a confidencialidade deve ser mantida durante todo o processo dos dados, pois a segurança da informação deve ser garantida no sistema em que os dados estão armazenados, quando estiverem sendo transmitidos e também quando chegarem ao destino.

Entretanto Novo (2010, p. 36) afirma que “é importante lembrar que não existe mecanismo 100% confidencial, durante 100% do tempo”.

2.4.2 Integridade

A integridade é responsável por evitar que a informação seja modificada sem autorização, pois ela deve ser correta e não estar corrompida. Além disso, ela também garante que a informação esteja protegida de ameaças involuntárias ou intencionais, dessa forma ela é considerada uma informação íntegra. (MACHADO, 2014).

O sistema ou pessoa que emitiu uma informação deve ter a garantia que a informação chegará ao receptor da mesma forma que foi enviada, sem acessos desautorizados ou modificações, e o receptor dessa mensagem também deve ter a segurança que a informação repassada a ele não foi modificada durante o caminho. (NOVO, 2010).

2.4.3 Disponibilidade

O objetivo da disponibilidade é possibilitar, sem interrupções, o acesso ou modificação da informação, pelas pessoas que possuem autorização prévia a isso, sempre que for necessário utilizá-la. (NOVO, 2010).

Segundo Machado (2014, p. 51) “a disponibilidade da informação se refere a toda estrutura física e tecnológica necessária para permitir o acesso, o tráfego e o armazenamento das informações e dados.” E para a garantia da disponibilidade das informações os recursos tecnológicos utilizados para gerenciamento das mesmas devem estar sempre funcionando corretamente, e caso ocorra algum desastre eles devem ser capazes de se recuperar de forma rápida e completa.

Problemas na disponibilidade podem acontecer por falhas de segurança no software ou hardware, como ataques e contaminação por vírus, ou até mesmo causas ambientais, como enchentes, incêndios, entre outros. Os sistemas de informação devem estar sempre protegidos contra estes possíveis perigos. Para isso devem ser utilizadas medidas de segurança para recuperação de dados caso ocorra algum problema de disponibilidade. (MACHADO, 2014).

2.5 VULNERABILIDADES, AMEAÇAS E ATAQUES

2.5.1 Vulnerabilidades

Para Kim e Solomon (2014) uma vulnerabilidade pode ser considerada como qualquer falha existente em um sistema que torne um ativo mais propenso a sofrer ameaças que lhe causarão dano. Para proteger um ativo de ameaças e ataques é necessário tentar eliminar o máximo possível as vulnerabilidades de um sistema.

Em uma organização podem existir diversas vulnerabilidades, mas elas sozinhas não causam nenhum tipo de incidente, porém, se forem encontradas por pessoas com objetivos ilícitos podem tornar-se uma ameaça. (KONZEN, 2013).

Uma vulnerabilidade pode ser um bug em um sistema operacional, arquivos desprotegidos, desatualização de aplicações ou sistemas, e até mesmo um funcionário que divulga a sua senha pode ser considerado como uma vulnerabilidade. (MORAES, 2010).

2.5.2 Ameaças

A exploração de uma vulnerabilidade existente é denominada de ameaça. Para a NBR ISO/IEC 27002:2005 ameaça pode ser considerada como qualquer possibilidade da existência um incidente indesejado, este sendo capaz de causar algum tipo de dano para os ativos de um sistema ou organização.

De acordo com Kim e Solomon (2014), não é possível eliminar todas as ameaças, mas é possível se proteger tratando as vulnerabilidades existentes, de modo que mesmo que existam ameaças elas não conseguirão explorar a vulnerabilidade.

Segundo Santos e Soares (2019), para se proteger é possível fazer uma análise individual de cada ameaça identificando alguns itens como: O agente que poderá realizar a ameaça, qual a motivação de tal ameaça e qual seria o dano causado por ela. Com essas informações é possível fazer uma listagem das ameaças que cada ativo pode estar suscetível e a definição das vulnerabilidades que este ativo pode possuir.

2.5.3 Ataques

Uma ameaça concretizada se torna um ataque, ou seja, é considerado ataque quando uma vulnerabilidade é explorada com sucesso por uma ameaça inteligente, e em consequência disto é causado algum incidente ao ativo vulnerável. (BARRETO et al., 2018).

Para Kim e Solomon (2014) os ataques podem ser divididos em:

- Ataques ativos: Neste caso ocorre uma intrusão física e além do acesso às informações do usuário também ocorre a modificação da mesma.
- Ataques passivos: São aqueles em que não há nenhuma modificação, o atacante apenas tem acesso às informações, interceptando ou monitorando transmissões.

Kim e Solomon (2014) complementa ainda que esses são alguns dos programas maliciosos utilizados em ataques:

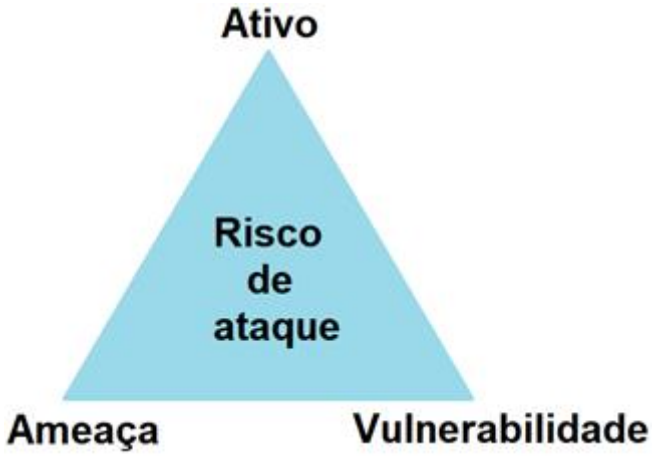
- Vírus: É um tipo de programa que age criando cópias iguais a ele e alocando-as em programas ou arquivos de um sistema, podendo aumentar o tamanho de arquivos, desativar funções do antivírus do computador, entre outros.
- Verme: Este se assemelha ao vírus, mas se replica e envia cópias de si mesmo a outros computadores e não a outros programas no mesmo computador, um verme pode reduzir a disponibilidade gerando um grande tráfego na rede, utilizando sua largura de banda, chegando até impossibilitar a navegação na internet.
- Cavalo de Troia: O cavalo de Troia é um programa aparentemente normal, mas age de forma maliciosa assim que o usuário o executa, ele pode coletar informações confidenciais, baixar arquivos e ocultar programas.
- *Rootkit:* É utilizado após um atacante invadir um sistema de computador, ele esconde os vestígios dos ataques, para isso ele modifica ou substitui outros programas presentes no computador, por exemplo, se um vírus está sendo rodado no computador o *rootkit* pode substituir o gerenciador de tarefas deste computador por uma versão modificada que oculta esse vírus de modo que ele não seja perceptível.
- Programa espião: É semelhante ao cavalo de Troia, é utilizado para roubar informações dos usuários sem que eles saibam, ele age por meio da internet monitorando as atividades dos usuários e colhendo informações.

2.5.4 Relação entre vulnerabilidades, ameaças e ataques

Segundo a NBR ISO/IEC 27002:2005 as vulnerabilidades exploradas por uma ameaça podem causar a perca dos princípios da segurança da informação, deixando assim uma porta aberta para que um invasor possa entrar e ter acesso sem autorização aos ativos de um ambiente. Na Figura 4 podemos observar a relação entre vulnerabilidade, ameaça e ativo. (MACHADO, 2014).

As vulnerabilidades e ameaças andam lado a lado, pois a existência de uma vulnerabilidade no sistema consequentemente o deixará suscetível a uma ameaça e a ocorrência de um ataque. (BARRETO et al., 2018).

Figura 4: Ativo, ameaça e vulnerabilidade



Fonte: (HOEPERS; STEDING-JESSEN, 2014, p. 19).

2.6 ENGENHARIA SOCIAL

Uma das técnicas de ataque a segurança da informação mais poderosas e difícil de evitar, que não faz o uso apenas da tecnologia, é a Engenharia Social. (FONTES, 2006). Nessa técnica o atacante faz o uso da persuasão e manipulação para ganhar a confiança da vítima, ele abusa da sua ingenuidade e falta de habilidade em busca de conseguir informações que não são do seu direito, a partir disso ele poderá utilizá-las para realizar acessos não autorizados a outras informações ou computadores. (BARRETO et al., 2018).

2.6.1 O fator humano

Para Barreto et al. (2018) o ponto mais importante para que a segurança da informação funcione corretamente é o fator humano, pois a segurança começa e termina no ser humano. Lyra (2015) diz ainda que os seres humanos são guiados pelo seu psicológico e é normal que mudem seus comportamentos de acordo com as situações tomando decisões baseadas em confiança, mesmo que inconscientemente, e é essa falha humana que é utilizada na engenharia social. Devido a isso é necessário que as pessoas sejam bem informadas sobre a segurança da informação de modo que estejam cientes das vulnerabilidades e perigos a quais podem estar expostas.

Machado (2014) diz que o ser humano é tido como a maior vulnerabilidade da segurança da informação, visto que por meio da exploração humana é possível conseguir acesso até as informações mais protegidas.

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).

Os seres humanos são vulneráveis e um engenheiro social age em cima disso explorando sua ingenuidade e fragilidade. Uma pessoa pode ser vítima de um ataque de engenharia social por não ter conhecimento do que se trata, acreditando que está agindo da maneira correta sem causar nenhum risco ela acaba cedendo ao engenheiro social informação que não deveria, e muitas das vezes ela nem percebe que foi vítima da engenharia social. (BARRETO et al., 2018).

De acordo com Santos, Moura e Silva (2010) estas são algumas características de vulnerabilidades humanas:

- Autoconfiança: O ser humano gosta de demonstrar confiança e sabedoria em seus diálogos, tentando assim transmitir conhecimento e segurança, mostrando ser alguém eficiente.
- Formação profissional: O ser humano está sempre em busca de reconhecimento pessoal, mesmo que inconscientemente, ele procura sempre estar no controle de uma situação.

- Vontade de ser útil: Naturalmente o ser humano busca sempre ser útil em determinadas situações, ele age com gentileza para ajudar os outros em suas necessidades.
- Busca por novas amizades: O ser humano gosta de ser elogiado, ele costuma se sentir bem ao ouvir coisas a seu respeito que o agradam.
- Propagação de responsabilidade: Geralmente o ser humano acredita não ser o único encarregado por uma atividade, pressupondo que outra pessoa também pode ter acesso a mesma.
- Persuasão: As pessoas naturalmente possuem traços comportamentais que as tornam suscetíveis a manipulação.

Na Tabela 1 são apresentadas algumas tendências básicas do comportamento humano que os tornam vulneráveis as técnicas de engenharia social segundo Gartner (2002 apud BALDIM, 2007).

Tabela 1: Comportamentos humanos que os tornam vulneráveis

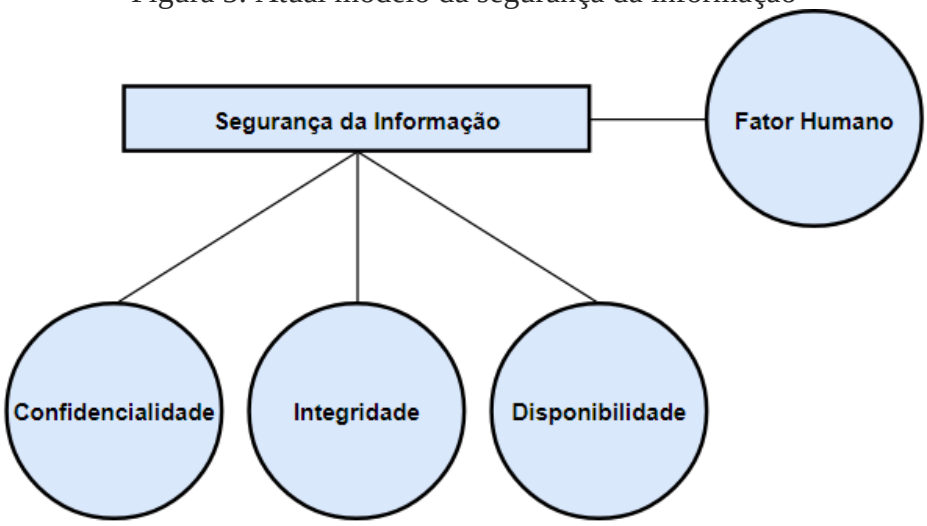
Comportamento	Definição	Exemplo
Reciprocidade	Uma pessoa é incentivada a fazer alguma coisa em troca de algo.	Você compra uma rodada de queijo quando eles te dão desconto.
Coerência	Certos comportamentos moldados são coerentes de uma pessoa a outra.	Se você perguntar algo e esperar o outro vai se sentir obrigado a te responder.
Aceitação social - Medo	Alguém sente a necessidade de fazer o que todo mundo faz.	Se uma pessoa estiver parada no em um local movimentado olhando para cima eventualmente outras pessoas irão fazer o mesmo.
Simpatia	Pessoas tendem a dizer sim para aqueles que elas gostam ou se sentem atraídas.	Modelos bonitas são usadas em publicidade.

Autoridade	Pessoas tendem a escutar ou prestar atenção nos avisos de quem tem posição de autoridade.	"Quatro entre cinco médicos recomendam..."
Escassez	Se alguém está com poucos suplementos, isso se torna mais "precioso" e, portanto, mais apelativo.	Furby ou Sony Playstation 2.

Fonte: Adaptado de Gartner (2002 apud BALDIM, 2007, p. 47)

Para Alves (2010) o fator humano é primordial como um dos elementos base da segurança da informação. Ainda hoje ele não é considerado como um nível base da segurança da informação, não fazendo parte dos três pilares fundamentais, como apresentado na Figura 5.

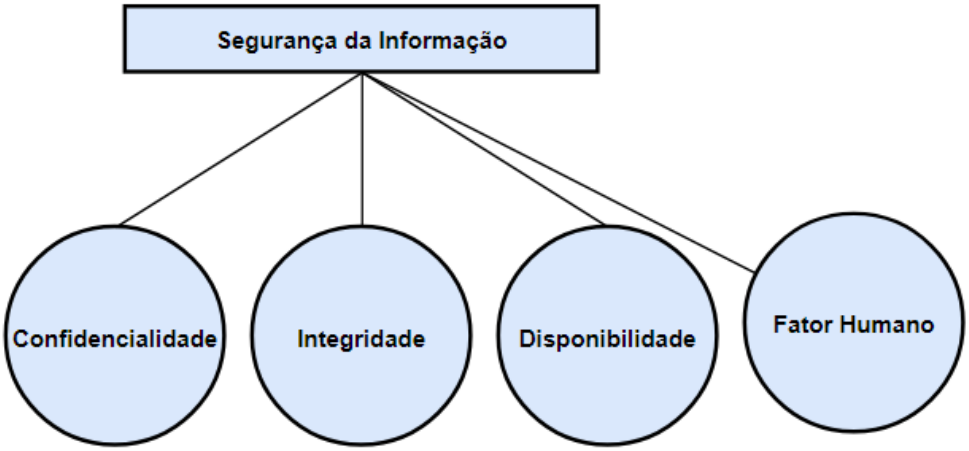
Figura 5: Atual modelo da segurança da informação



Fonte: (SILVA; COSTA, 2009 apud ALVES, 2010, p. 33).

Alves (2010) propõe ainda que o fator humano seja incluído como um dos pilares fundamentais da segurança da informação, conforme apresentado na Figura 6, pois ele é um dos maiores causadores de problemas a segurança, possibilitando a ocorrência de diversos tipos de ataques, sendo assim é necessário que seja dada uma maior atenção a este fator no nível base da segurança da informação.

Figura 6: Proposta de novo modelo para Segurança da Informação



Fonte: (SILVA; COSTA, 2009 apud ALVES, 2010, p. 34).

2.6.2 O engenheiro social

Para Alves (2010) o engenheiro social faz o uso de técnicas de manipulação e persuasão para enganar alguém psicologicamente de modo que a pessoa aja de acordo com o que ele espera. Ele é uma pessoa criativa que pode se passar por outras pessoas, utilizar o carisma, apelo sentimental e diversas outras formas de ganhar a confiança da vítima para que ela caia no seu golpe.

Um engenheiro social é uma pessoa tão habilidosa que na maioria das vezes nem precisa encontrar a vítima para realizar o ataque, mesmo sem nem saber como a vítima se parece e apenas por meio de uma chamada telefônica o engenheiro social já consegue as informações que procura. (SOUSA, 2016).

> Os ataques de engenharia social podem ser divididos em dois grupos:
> Os ataques diretos: Como o próprio nome já diz, são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, fax e até mesmo pessoalmente. Este exige do engenheiro social, um planejamento antecipado e bem detalhado, além de um segundo plano para caso o primeiro não dê certo, além de muita criatividade e articulação para que o plano seja bem sucedido.
> Os ataques indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir como, por exemplo, vírus, Cavalos de Troia ou através de sites e e-mails falsos para assim obter informações desejadas. (ALVES, 2010, p. 15-16)

Segundo Barreto et al. (2018), normalmente a estratégia mais comum utilizada pelo engenheiro social é juntar todas informações a respeito da vítima antes do ataque, e após conseguir o máximo possível de informações ele faz o uso deste conhecimento para arquitetar o seu plano de ataque. O engenheiro social pode realizar o ataque via telefone,

redes sociais, pessoalmente, e de diversas outras formas que ele achar que é provável conseguir sucesso.

2.6.2.1 Técnicas de ataque de um Engenheiro Social

De acordo com Fontes (2006), para obtenção das informações o engenheiro social pode fazer o uso das seguintes técnicas:

- Falam com conhecimento: Por meio das informações que o engenheiro social já sabe a respeito da vítima ele consegue falar com propriedade sobre os assuntos que aborda para aplicar o seu golpe.
- Adquirem a confiança do interlocutor: Após o engenheiro social citar essas informações na conversa com a vítima mostrando ter propriedade e conhecimento do que fala, a vítima passe a crer que ele é quem diz ser conquistando assim a confiança dela.
- Prestam favores: O engenheiro social pode fingir apenas que deseja ajudar a vítima a solucionar algum problema para depois conseguir concretizar o seu ataque.

Também deve-se dar destaque as seguintes técnicas apresentadas pela Microsoft (2006 apud MOREIRA, 2019):

- Intimidação: O engenheiro social finge ser uma pessoa com autoridade e de maior nível hierárquico que a sua vítima.
- Persuasão: O engenheiro social tem como objetivo induzir a vítima para que ela faça exatamente o que ele quer.

Até os sistemas de segurança de computadores mais fortes podem ser quebrados por meio da engenharia social. Devido a isso, os projetistas devem manter sempre o cuidado a respeito dos riscos de ataques de engenharia social que os usuários dos sistemas poderão sofrer. (GOODRICH; TAMASSIA, 2013).

Segundo Peixoto (2006 apud MOREIRA, 2019), as técnicas de ataque dos engenheiros sociais estão em constante evolução, sempre em busca de novas ideias, saindo do tradicional, para obter sucesso nos seus golpes. Porém, mesmo com todas as transformações, modificações e incrementações nos ataques e nos métodos de enganar suas vítimas os engenheiros sociais sempre fazem o uso de algum aspecto ou característica clássica durante seu ataque.

2.7 NECESSIDADE DA SEGURANÇA DA INFORMAÇÃO

Paralelamente ao avanço das tecnologias de informação, na forma de armazenar e compartilhar as informações, também houve um aumento nos crimes relacionados a mesma, pois estão vulneráveis a diversas formas de ameaças físicas ou virtuais. Surgiu então a necessidade da segurança dessas informações, empresariais e pessoais, de forma que fiquem livres de riscos e perigos. (OLIVEIRA; MOURA; ARAÚJO, 2014). De acordo com Cunha e Fenato (2013) para ajudar neste problema de proteção de dados, há uma área na tecnologia da informação especializada neste assunto, ela é chamada de segurança da informação.

> A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplicam-se tanto as informações corporativas quanto as pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição. (ARAUJO, 2008 apud OLIVEIRA; MOURA; ARAÚJO, 2014, p. 4).

Oliveira, Moura e Araújo (2014) afirma que no passado era mais fácil garantir a segurança da informação, como estavam contidas em papéis eles podiam ser trancados em locais seguros, garantindo assim que a informação fosse modificada apenas por pessoas com autorização e evitando que fosse danificada ou roubada. Mas em razão da evolução tecnológica também houve um aumento na conectividade com à rede de internet, dessa forma as informações passaram a ser armazenadas cada vez mais em mídias digitais, consequentemente pelo fato dos dados armazenados em formato digital serem portáteis esses ativos acabaram despertando cada vez mais o interesse de ladrões.

2.8 NORMA ISO

Segundo Correia (2016), a finalidade das normas da família ISO/IEC 27000 é auxiliar as organizações a manterem seus ativos seguros, com o objetivo de propiciar o monitoramento contínuo dos dados, a integridade de informações financeiras, dados pessoais de colaboradores, dos clientes e propriedades intelectuais (conjunto de direitos autorais, compreendido como patente de invenção). A Tabela 2 apresenta resumidamente o objetivo de cada norma da família ISO/IEC 27000.

Tabela 2 – Características das normas da família ISO/IEC 27000.

Normas ISO	Objetivo da norma
27000	Aborda o vocabulário da segurança da informação e tem como objetivo reduzir os riscos de perda, roubo ou alteração da informação, visando a garantia de qualidade e confidencialidade comercial.
27001	Aborda a gestão de segurança da informação e tem como objetivo verificar se está de acordo com um padrão que define os requisitos para se obter um SGSI.
27002	Aborda o controle para segurança da informação, é a única norma em gestão da segurança para qual existe certificação profissional, é recomendada a utilização em conjunto com a norma ISO 27001.
27003	É composta de um conjunto de normas para realizar a implementação do SGSI, ou seja, ela apenas demonstra uma orientação detalhada sobre a norma ISO 27001.
27004	Aborda o gerenciamento de métricas e relatórios para um SGSI, tem como objetivo auxiliar na definição dos níveis de serviço para a segurança da informação.
27005	Aborda a gestão de riscos de segurança da informação e tem como objetivo detalhar a perspectiva dos riscos.
27006	Aborda os requisitos para auditoria externas em um SGSI, tem como objetivo definir os requisitos na perspectiva da empresa, investigar o seu cliente, para validar um SGSI.
27007	Aborda as referências para auditorias em um SGSI e deve ser utilizada em conjunto com a ISO 27006 guiando a verificação do sistema de segurança da informação.
27008	Aborda a auditoria nos controles de um SGSI e tem como objetivo auditoria dos controles em segurança da informação.
27010	Aborda a gestão de segurança da informação para comunicações interempresariais.
27011	Aborda a gestão de segurança da informação para empresas de telecomunicações baseada na ISO 27001.

Fonte: Adaptado de Sansigolo (2015).

De acordo com o Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21) a norma ISO 27001 indica requisitos para facilitar a aplicabilidade do Sistema de Gestão da Segurança da Informação, a norma determina um modelo para estabelecer, implementar, manter e melhorar o SGSI, englobando também os conceitos de avaliação e tratamento de riscos em um ambiente organizacional. Todos os tipos de organizações podem ser resguardados pela norma, pois os requisitos contidos na mesma são genéricos com a pretensão de aplicá-los a quaisquer organizações.

A NBR ISO/IEC 27002 tem o seguinte objetivo:

> Fornecer as diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, essa norma foi elaborada com seções que tratam a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. (Editora ABNT, 2013a, p. 1 apud RIOS, 2017, p. 136).

Para Peixoto et al. (2015), uma das principais funções do processo de implementação das normas ISO/IEC 27001 e ISO/IEC 27002 é a criação da Política de Segurança da Informação. Para que ISO/IEC 27001 seja implementada é fundamental que a ISO/IEC 27002 seja utilizada em conjunto, pois é ela que fornece o guia de melhores práticas, as seções de controle que são citadas na ISO/IEC 27001 são detalhadas na ISO/IEC 27002 possibilitando uma correta implementação do SGSI.

A ISO/IEC 27002 dispõe de 15 capítulos, sendo 133 controles que estão separados em 11 capítulos chamados seções de controles de segurança da informação, ela inclui também um capítulo onde é apresentada uma seção introdutória, que aborda análise, avaliação e tratamento de riscos.

Segundo Peck (2010 apud PEIXOTO et al., 2015), a ISO/IEC 27002 define os seguintes passos para a implantação da segurança da informação:

- Inventariar os ativos;
- Realizar análise de risco;
- Classificar as informações;
- Criar um Comitê de Segurança;
- Elaborar uma PSI;
- Auditar os controles que foram criados ou não;
- Criar planos de contingência

A distinção entre políticas, diretrizes, normas e procedimentos é fundamental, uma vez que elas compõem um conjunto de determinações formais que servem como ferramentas

para a avaliação e execução dos processos organizacionais e auditorias periódicas. (PONTES, 2014 apud FERREIRA, F. 2015).

2.8.1 Política de Segurança da Informação

A Política de Segurança da Informação está relacionada a um conjunto de normas e instruções, onde sua tarefa principal é estabelecer orientações para prevenção de incidentes relacionados à segurança da informação. (ARTHUR, 2009 apud COIMBRA, 2018).

Segundo Zúquete (2013 apud COIMBRA, 2018), as políticas de segurança fazem parte de um agrupamento medidas de segurança cibernética, sendo assim, a PSI trata-se de requisitos que devem ser seguidos para garantir a segurança da informação

Para Chiavenatto (2010 apud HUMMES, 2017), política é um guia que delimita ações, ela é composta por definições de propósitos de uma empresa, estabelece orientações e limites para os indivíduos. As políticas são princípios que constituem regras a serem seguidas e contribuem para alcançar objetivos definidos.

Tipos de políticas podem ser descritas como:

- Política Regulatória: É um documento criado cujo objetivo é fornecer para as organizações uma série de especificações legais, na qual são muito bem detalhadas, deixando definido o que deve ser feito e quem deve fazer. Esta política apresenta os requisitos legais que as organizações devem seguir.
- Política Consultiva: Indica quais são as ações ou métodos que devem ser adotados para concretização de determinadas tarefas. O principal propósito desta política é conscientizar os funcionários da organização sobre as atividades do cotidiano.
- Política Informativa: Caracteriza-se por não haver riscos, caso nenhuma ação seja cumprida ou realizada. Esta política tem a função apenas de informar, sendo assim, não é rigorosa. (FERREIRA, F. N., 2003 apud FERREIRA, F. S., 2015).

2.8.2 Diretrizes

Como afirma Ferreira, F. (2015), diretriz trata-se de regras genéricas, na qual são elaboradas normas e procedimentos. Ela desempenha um papel relevante na organização, pois auxilia a política da organização.

Segundo o Tribunal de Contas da União (2012), na seção “Organizando a Segurança da Informação”, são apresentadas diretrizes para a segurança da informação, detalhando aspectos da organização interna, como o comprometimento da direção, coordenação, atribuição de responsabilidades, processo de autorização para recursos de processamento da informação, acordos de confidencialidade, análise crítica independente, contato com autoridades e com grupos de interesses. Possuí também diretrizes responsáveis por lidar com relacionamentos de partes externas, identificação dos riscos e dos requisitos de segurança da informação necessários no relacionamento com clientes e terceiros.

De acordo com Ferreira, F. (2015), as normas fazem parte de alguma diretriz dentro da organização. Se tratando de normas é possível observá-las com características específicas pois são elas que definem quais comportamentos devem ser seguidos dentro de uma organização, com um foco específico de acordo com a diretriz na qual faz parte.

2.8.3 Procedimentos

Procedimentos encontram-se no nível operacional, é descrito de acordo com a norma que o mesmo faz parte, pois seguindo a hierarquia, as diretrizes são compostas de normas que em seguida são compostas por procedimentos e os procedimentos mostram como deve ser feito, ou seja, são apresentados os passos de forma clara e detalhada. (CAMPOS, 2007 apud FERREIRA, F. 2015).

2.9 MEDIDAS DE SEGURANÇA

Segundo Sêmola (2014) as medidas de segurança são práticas, procedimentos e mecanismos usados na proteção dos ativos, visando impedir que ameaças explorem as vulnerabilidades e possibilitando também a redução das mesmas, e caso exista alguma deve-se limitar o seu impacto minimizando ou evitando os riscos de acesso às informações de valor. As medidas de segurança possuem as seguintes características:

Preventivas: Tem como objetivo evitar o acontecimento de acidentes por meio de mecanismos que estabeleçam conduta e ética. Podem ser políticas de segurança, instruções e procedimentos, conscientização, equipamentos adequados, configurações de rede e demais práticas que objetivam o controle de segurança da camada física, camada lógica e camada humana.

Detectivas: Tem como objetivo identificar as condições ou os indivíduos que causam ameaças, este tipo de medida pode ser feita através da análise de risco, ou alertas de exploração da vulnerabilidade.

Corretivas: Tem a função de agir em prol da correção da estrutura tecnológica e humana para que sejam adaptadas às condições de segurança estabelecidas. Planos emergenciais como: Restauração de *backup*, plano de continuidade operacional, plano de recuperação de desastres.

2.10 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Sistema de Gestão de Segurança da Informação é um conjunto de informações que tem como finalidade garantir o controle de segurança para assegurar a proteção dos ativos e a confiabilidade de dados internos, externos ou de terceiros. (ABNT/CB-21, 2013).

Segundo Baars et al. (2018), o sistema de gerenciamento inclui um conjunto de controles, sendo eles, estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. Ao serem estabelecidos e implementados é necessário que sejam monitorados, revisados e melhorados para assegurar que os requisitos especificados na norma ISO 27001 estão sendo atendidos.

Estes são os seguintes pilares de um Sistema de Gestão de Segurança da Informação: Preservação da confidencialidade, confiabilidade, autenticidade, integridade, disponibilidade, não repúdio.

Segundo a ABNT NBR ISO/IEC 207001 para a implantação de um Sistema de Gestão da Segurança da Informação é necessário seguir os seguintes passos:

- Estabelecer o SGSI, ou seja, definir o escopo e os limites do SGSI de acordo com as características do negócio, da organização, da localidade, dos ativos e da tecnologia, deve se incluir também aspectos que serão excluídos do escopo de forma detalhada e com justificativas.

- Implementar e operar o SGSI, ou seja, formular plano de tratamento, implementá-lo, definir como serão medidas a eficácia, e gerenciar operações e recursos.
- Monitor e analisar criticamente o SGSI, ou seja, manter a execução de procedimentos de monitoração e análise crítica para identificar erros no procedimento, tentativas de violação a segurança, prevenir incidentes, realizar análises regulares a respeito da eficácia do SGSI, conduzir auditorias internas e por fim atualizar planos de segurança.
- Manter e melhorar o SGSI, ou seja, implementar melhorias no SGSI, manter execução de ações preventivas e corretivas, comunicar as ações as devidas partes interessadas, e garantir que as melhorias atinjam os objetivos que foram determinados.

- Requisitos de documentação, ou seja, documentações requeridas pelo SGSI, para garantir que ações sejam rasteáveis, políticas e decisões sejam documentadas e para certificar que registros sejam reproduzíveis.
  - Controle de documentos, ou seja, documentos gerados pelo SGSI devem ser protegidos e controlados.
  - Controle de registros, ou seja, os registros devem ser estabelecidos e devem fornecer evidências da conformidade, do processo, e da eficácia da operação.
- Responsabilidade da direção, ou seja, a direção deve se responsabilizar pelo andamento do SGSI.
  - Comprometimento da direção, ou seja, a direção deve mostrar comprometimento com o que foi estabelecido, implementado, operado, monitorado, realizado análise crítica, e na manutenção e melhoria do SGSI.
- Gestão de recursos, ou seja, o ato de gerenciar os recursos necessários para seguir o processo do SGSI.
  - Provisão de recursos, ou seja, a organização deve prover os recursos necessários para que o sistema de gestão da segurança da informação seja realizado com conformidade e para que os resultados sejam eficientes.
  - Treinamento, conscientização e competência, ou seja, a organização deve assegurar que todo o time tenha responsabilidades definidas no SGSI e que se comprometam em realizar as devidas tarefas.

- Auditorias internas do SGSI, ou seja, as auditorias devem ser realizadas para certificar-se que os objetivos, controles, processos e procedimentos do SGSI atendem os requisitos da norma, da legislação, da segurança da informação, verificar se são mantidos e se estão sendo executados de acordo com o esperado.
- Análise crítica do SGSI pela direção, ou seja, a direção deve analisar criticamente para determinar necessidades de melhorias ou mudança no SGSI.
    - Entradas para análise crítica, ou seja, resultados de auditorias, resultados de análise crítica, técnicas, procedimentos usados para melhorar o desempenho e a eficácia da SGSI, ações preventivas e corretivas, vulnerabilidades ou ameaças à segurança, acompanhamento e recomendações.
    - Saídas da análise crítica, ou seja, decisões e ações referente à melhoria do SGSI, requisitos de segurança da informação, obrigações, requisitos legais ou regulamentares, necessidades de recursos, e requisitos de negócio.
- Melhoria do SGSI, ou seja, as formas de preservar a melhoria e a eficiência do SGSI.
    - Melhoria contínua, ou seja, a organização deve aprimorar o SGSI continuamente por meio de políticas de segurança da informação, objetivos de segurança, resultados da auditoria, análises, monitoramentos, e ações preventivas e corretivas junto a análise crítica da organização.
    - Ação corretiva, ou seja, a organização deve resolver falhas de não-conformidade com os requisitos do SGSI, e o procedimento deve ser documentado.
    - Ação preventiva, ou seja, a organização deve determinar ações que serão realizadas para evitar não-conformidade, e o procedimento deve ser documentado.

De acordo Avancini (2018), para a implementação de um Sistema de Gestão de Segurança da Informação correto e efetivo é necessário um levantamento de aplicações da legislação local, que pode ser distinto para cada país, a proteção dos dados não deve obstruir informações de uma investigação policial ou encobrir atos ilícitos. As diferenças culturais devem ser consideradas, pois os aspectos locais podem ser abordados de diferentes formas

considerando os costumes, o nível de conhecimento, experiências, idioma, então a partir deste levantamento devem ser adaptadas às capacitações, treinamentos e boas práticas de segurança que não sejam ilegais para o país e outros requisitos presentes na SGSI. Um dos critérios que impactam no SGSI são os requisitos legais e regulamentares que fazem parte da saída da análise crítica, sendo um evento externo ou interno.

Segundo Roque (2019), a Lei n.º 13.709/2018, ou Lei Geral da Proteção de Dados (LGPD), é responsável por regulamentar a proteção de dados no Brasil, entre as finalidades da Lei é possível citar “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º). A violação à privacidade representa ameaças a direitos da personalidade, sendo recorrente de forma presencial ou virtual, a LGPD entrará em vigor no Brasil em 2020.

3. METODOLOGIA

Inicialmente, o tema deste trabalho foi escolhido devido à grande demanda por requisitos de segurança da informação, principalmente relacionados a engenharia social, além do interesse pessoal para maior aprendizado na área.

Após a definição do tema, foi realizada uma pesquisa bibliográfica a respeito dos principais pontos da segurança da informação, incluindo seus princípios básicos, vulnerabilidades, ameaças e ataques, foram investigadas as principais técnicas utilizadas por um engenheiro social para executar um ataque. Em seguida foi realizada uma identificação de quais os motivos que levam o usuário a ser vítima deste tipo de ataque.

Posteriormente foi efetuada uma pesquisa exploratória qualitativa por Políticas de Segurança da Informação e das normas ISO 27001 e 27002. A partir das normas foi possível entender a importância de um Sistema de Gestão a Segurança da Informação, e que para implementá-lo é preciso de uma Política de Segurança da Informação. A norma ISO 27001 contempla os requisitos para que o SGSI seja implementado com facilidade e assertividade, já a norma ISO 27002 detalha as diretrizes e disponibiliza um guia com boas práticas.

Com estes dados foi criada uma seção cujo objetivo é abordar os tipos de ataques que fazem uso da engenharia social, boas práticas, métodos e técnicas que poderão evitar esses ataques. A estrutura da norma ISO 27002 é o pilar para a construção da seção, a norma ISO 27002-2013 é estruturada com os seguintes aspectos; inicialmente é descrito o tópico que será abordado, exemplo: “Organização da Segurança da Informação”, em seguida são apresentados subtópicos que retratam o assunto de forma clara, juntamente com os meios de prevenção e/ou sugestões práticas de como conduzir os dados de forma segura, por exemplo: a norma diz que todas as responsabilidades para com a segurança da informação sejam devidamente atribuídas; e lança o subtópico “Responsabilidades e papéis pela segurança da informação”, dentro do subtópico é subdivido o guia de boas práticas de “a” á “e”, em cada letra possui uma sugestão que convém ser colocada em prática para que os papéis pela segurança seja feito de forma adequada.

Alguns dos procedimentos apresentados no desenvolvimento deste trabalho não estão ligados explicitamente as técnicas de engenharia social, porém, estão indiretamente relacionados a métodos utilizados nos ataques que fazem o uso da engenharia social.

4. RESULTADOS

Neste capitulo será apresentada a proposta da seção desenvolvida, como um guia de boas práticas, com ênfase em engenharia social. A seção está separada em tópicos, assim como na norma ISO 27002, onde cada tópico aborda um problema ou vulnerabilidade a ser tratada que pode ser explorada por um engenheiro social, mas que ainda não foi diretamente discutida e relacionada as técnicas de engenharia social na família de normas ISO 27000. Além disso, dentro de cada tópico são apontados métodos de como minimizar os problemas e vulnerabilidades apresentados e se proteger das técnicas de engenharia social.

4.1 PROPOSTA DE UMA SEÇÃO COMPLEMENTAR A NORMA ISO 27002 – ENGENHARIA SOCIAL

4.1.1 Senhas

Uma senha curta, com vários caracteres repetidos, apenas com letras ou números, com datas importantes como o aniversário e número de documentos, ou nomes importantes como o próprio nome ou nome de familiares pode ser uma brecha para um engenheiro social. Apenas por meio de uma conversa o engenheiro social pode fazer com que a vítima informe sua senha sem perceber, além disso, uma senha como a data de nascimento pode ser descoberta até mesmo por meio de uma rede social. (ALVES, 2010).

De acordo com Rodrigues (2018 apud Rodrigues B. et al., 2017) usuários costumam seguir padrões de senhas. Na Tabela 3 é possível identificar que a sequência numérica é recorrente e palavras associadas ao contexto da senha (linkedin e password) também.

Tabela 3: Dez senhas mais frequentes da lista LinkedIn.

Senha	Frequência
123456	753.305
linkedin	172.523
password	144.458
123456789	94.314
1234567	63.769
111111	57.210
1234567	49.652
sunshine	39.118
qwerty	37.538
654321	33.854

Fonte: Adaptado de Rodrigues (2018 apud RODRIGUES B. et al., 2017).

Como se proteger:

a) Convém elaborar senhas com no mínimo oito caracteres;

Considere uma senha de 7 caracteres formada apenas pelas letras do alfabeto (26 letras), se utilizado um algoritmo de força bruta, capaz de fazer 100.000 tentativas de senha por segundo, essa senha seria quebrada em 22h. Já uma senha de 8 caracteres, também formada apenas pelas 26 letras do alfabeto, sendo o utilizado o mesmo algoritmo levariam 24 dias para que ela fosse quebrada. (ALMEIDA, 2019).

b) Convém alternar os caracteres entre letras minúsculas, letras maiúsculas, números e caracteres especiais (*, &, $, #, @, !);

Uma senha contendo apenas letras e números é menos segura do que uma senha que contém caracteres especiais e variados, pois quanto maior a variedade de caracteres mais forte será a senha. Porém, a senha de letras e números pode se tornar mais forte de que uma senha de caracteres especiais caso ela seja maior, por exemplo, uma senha de apenas letras e números contendo 15 caracteres é 33.000 vezes mais forte do que uma senha de apenas 8 caracteres especiais e variados. O ideal é uma senha com maior variedade e quantidade de caracteres, o recomendado são 14 caracteres. (ALVES, 2010).

c) Convém utilizar senhas novas e diferentes em cada conta;

É bastante comum que um usuário volte a reutilizar uma senha em outras contas quando ele a decora, principalmente se for uma senha forte. Porém, esta é uma falha grave a segurança, caso alguém consiga descobrir a senha de uma única conta também terá descoberto a senha de outras contas do usuário, portanto mesmo que uma senha seja considerada forte ela não deve ser reutilizada em outras contas. (NOVO, 2010).

d) Convém não utilizar datas importantes ou nomes como senha, por exemplo a data de nascimento, nome próprio ou de familiares próximos;

Utilizar este tipo de dado como senha é uma brecha para um engenheiro social, pois informações pessoais do usuário ou de pessoas próximas a ele são as primeiras a serem testadas por um engenheiro social. (ALVES, 2010). Além de atualmente ser possível encontrar diversas informações pessoais por meio de redes sociais, caso o engenheiro social faça

uma abordagem direta a vítima ele pode descobrir a senha por meio de uma simples conversa.

e) Convém memorizar a senha em vez de anotá-la. Caso seja registrada em um papel convém guardá-lo em local seguro;

É recomendado que as senhas jamais sejam anotadas, e se anotadas deve-se armazená-las em um local seguro minimizando assim as chances de um acesso não autorizado. O mais adequado para que não se esqueça as senhas sem anotá-las é utilizar um gerenciador de senhas, nele é escolhida uma senha mestre que guarda todas as senhas de outras contas. (NOVO, 2010).

f) Convém utilizar na senha palavras que não são encontradas no dicionário.

Senhas com palavras existentes no dicionário podem ser quebradas utilizando softwares que fazem a busca e comparação de palavras do dicionário com a senha do usuário, eles buscam até mesmo palavras escritas de trás para frente ou com erros mais comuns de digitação, desse modo conseguem encontrar a combinação correta entre a senha e a palavra do dicionário. (ALVES, 2010).

4.1.2 Redes Sociais

O crescimento no número de usuários das redes sociais traz como consequência o compartilhamento e disponibilização de uma grande quantidade de dados pessoais. Com o acesso aos dados compartilhados um engenheiro social pode traçar as suas informações para arquitetar e realizar o seu golpe, estes dados podem ir desde a data de nascimento, onde trabalha, onde estuda e até mesmo as músicas favoritas e a orientação política. Com todas essas informações um engenheiro social consegue aproximar-se da sua vítima com maior facilidade, pois já possuindo conhecimento sobre os seus interesses e informações pessoais ele consegue iniciar um contato aparentando apenas uma conversa casual. (CAPISTRANO, 2013).

Como se proteger:

a) Convém adicionar em redes sociais apenas pessoas que já conhece pessoalmente;

Uma pesquisa realizada pelo autor Capistrano (2013) com trinta usuários da rede social *Facebook* ele constatou que 86,6% deles não conhecem pessoalmente todos os seus amigos do *Facebook*. Diante disso, um usuário pode vir a ter em sua lista de amigos um engenheiro social que tem como objetivo apenas obter acesso as suas informações pessoais e atividades do dia a dia, informações estas que podem ser utilizadas para os mais diversos fins.

b) Convém privar ou não informar dados pessoais como: data de nascimento, local onde mora, onde estuda ou onde trabalha;

Este tipo de informação pode facilitar ao engenheiro social uma aproximação, onde por meio destas informações ele pode iniciar uma conversa com a vítima com objetivo de conquistar a sua confiança, e por meio da manipulação e influência consegue acesso a mais informações a seu respeito. (SILVA; ARAÚJO; AZEVEDO, 2013).

c) Convém não participar de grupos de compras, vendas ou trocas nas redes sociais;

Expor uma informação deste tipo pode fazer com que um engenheiro social entre em contato demonstrando interesse sobre uma negociação, essa é uma forma que ele utiliza para se aproximar sem levantar suspeitas. Nessa situação o engenheiro social pode trabalhar para ganhar a confiança da vítima e obter mais informações, ele pode por exemplo, oferecer a vítima uma venda parcelada com o objetivo de manter contatos futuros para obter maiores informações. (CAPISTRANO, 2013).

d) Convém não expor relacionamentos pessoais como marcação de familiares ou companheiro(a) de relacionamento;

Expor este tipo de dado favorece ao engenheiro social o enriquecimento das informações críticas a respeito do usuário e a criação de estratégias para cometer um ataque, como criar perfis falsos, realizar chantagens, entre outros. Os usuários não se dão conta que a cada dia estão se expondo cada vez mais nas redes sociais e uma informação como o nome de um familiar próximo pode trazer um risco a segurança. (SILVA; ARAÚJO; AZEVEDO, 2013).

e) Convém não fazer check-in em lugares aonde vai ou compartilhar os locais que frequenta;

Este tipo de informação fornece ao engenheiro social em tempo real o local onde o usuário está, assim como o lugar onde ele não está. O engenheiro social pode se aproveitar desta informação para se aproximar do usuário de maneira mais casual e até presencialmente indo ao local compartilhado. Além disso, o usuário está compartilhando a informação de que não está em casa, o que pode levar alguém ao local efetuar alguma ação, como mexer na caixa de correios em busca de uma correspondência que conste o CPF ou dados sensíveis do usuário. (CAPISTRANO, 2013).

f) Convém não clicar em qualquer link postado na rede social, seja matéria de jornal, links de lojas, aplicativos e etc.

Mesmo que um link seja compartilhado por uma pessoa confiável não há garantia de que está pessoa também pegou este link de uma fonte confiável. Este tipo de link pode estar camuflado com uma informação interessante, mas que na verdade tem como objetivo expor o usuário a vulnerabilidades e obter suas informações. É recomendado observar o que está escrito no endereço do link para a identificação do site, porém, existem redutores de link que fazem com que este endereço seja alterado dificultando sua identificação. (CAPISTRANO, 2013).

4.1.3 Phishing

O *Phishing* é um tipo de técnica de engenharia social que tem como objetivo obter dados sigilosos das vítimas utilizando sites falsos ou clonados. O meio mais comum de realização desse ataque é por e-mail, o atacante se passa por outra pessoa ou instituição informando uma situação emergencial que seja convincente para que a vítima clique no link informado. Outro modo de realizar o ataque é anexar junto ao e-mail um arquivo contendo um programa mal intencionado, como um vírus, que irá roubar as informações da vítima. (SANTOS, Daniel, 2016).

Existe também um grupo variante do *Phishing* chamado de *Spear Phishing*. Neste grupo o ataque é mais específico e direcionado, são golpes mais elaborados onde os atacantes primeiro investigam cuidadosamente o destinatário, e a partir das informações obtidas

arquitetam o seu plano para adequar especificamente àquele destinatário. (STALLINGS; BROWN, 2014).

Como se proteger:

a) Convém ter atenção a e-mails de fontes desconhecidas;

A maior parte dos ataques de *Phishing* ocorrem por spam, que é o envio em massa de mensagens eletrônicas genéricas direcionadas a um grande grupo de vítimas, então o usuário deve ter bastante atenção ao receber e-mails de fontes desconhecidas além de não clicar em links ou baixar arquivos deste tipo de e-mail. (EL PESCADOR, 2017).

b) Convém verificar e conferir o remetente do e-mail;

Caso o usuário receba algum e-mail solicitando informações pessoais é importante antes conferir o endereço de remetente com a mensagem enviada. Se houver dúvidas de que é uma mensagem legitima o mais adequado é entrar em contato com a organização que enviou o e-mail para confirmação. (KIM; SOLOMON, 2014).

c) Convém ter atenção a e-mails que solicitam uma ação urgente;

Muitos ataques de *Phishing* o atacante envia um e-mail se passando por um banco onde afirma que deve ser feita uma atualização urgente do aplicativo do banco para que o usuário não fique vulnerável, ou então se passa pela Receita Federal informando que existem pendencias no CPF da vítima e lhe fornece um link para uma página falsa. (BARRETO et al., 2018). Deve-se ter bastante cuidado com qualquer e-mail que solicite alguma ação ou informação urgente, pois este é um método muito utilizado pelos engenheiros sociais para influenciar o usuário a fornecer seus dados.

d) Convém não enviar informações pessoais por e-mail;

A melhor maneira de se proteger é evitar fornecer qualquer informação pessoal quando solicitada por e-mails ou mensagens. (KIM; SOLOMON, 2014). Bancos, instituições e outras empresas não irão solicitar dados pessoais dos usuários ou informações de login por e-mail, e caso ocorra deve-se seguir a orientação do tópico “b”.

e) Convém evitar clicar em links enviados por e-mail;

Algumas mensagens podem vir acompanhadas de um link onde o remetente orienta o usuário a clicar para executar alguma ação, nesse caso o mais

adequado é o próprio usuário digitar no seu navegador o endereço do link recebido na mensagem. (KIM; SOLOMON, 2014). Pois nesse tipo de e-mail o atacante também pode utilizar a técnica de ofuscamento de URL, onde aparentemente o endereço do link é de um site confiável, mas quando o usuário clica é direcionado a um site de *Phishing*. (GOODRICH; TAMASSIA, 2013).

f) Convém verificar o rodapé do e-mail;

E-mails legítimos de organizações, empresas e etc. costumam sempre conter dados no rodapé. É importante verificar se existe um endereço físico do local no rodapé ou uma opção com link para cancelar a inscrição do usuário. Caso não exista um desses itens deve-se ficar atento, pois pode se tratar de um e-mail falso. (INTEGRASUL, 2017). Além disso, deve-se verificar se no rodapé existe uma logo do remetente ou mais informações de contato, como número de telefone. Se houver dúvidas a respeito da legitimidade do e-mail exclua-o imediatamente.

g) Convém verificar a gramática e pontuação.

Os e-mails legítimos enviados por instituições e organizações são escritos por redatores profissionais que se esforçam ao máximo para escrever um texto correto e revisado, sem erros gramaticais ou de pontuação e com uma linha de assunto correta. Um e-mail deste tipo contendo erros gramaticais, de pontuação ou uma sequência ilógica de ideias provavelmente é uma fraude escrita por alguém inexperiente. (SILVA, 2019).

4.1.3.1 Vishing

Segundo Santos, Daniel (2016), o termo *vishing* é a combinação de "*voice*" e "*phishing*". Este é um tipo de ataque baseado no *phishing* tradicional onde o atacante tem como objetivo obter dados sigilosos das vítimas, mas no *vishing* o engenheiro social entra em contato com a vítima via chamada telefônica. Utilizando-se das técnicas de manipulação e persuasão durante a conversa o engenheiro tenta ganhar a confiança da vítima de modo que ela forneça seus dados pessoais ou execute determinada ação. (SILVA, 2019).

Como se proteger:

a) Convém ter atenção a ligações de números desconhecidos;

No ataque de *vishing* o atacante pode fazer o uso de técnicas para alterar a identificação do número que está ligando, ou até mesmo criar perfis falsos de identificação de chamadas fazendo parecer com que os números de telefones pareçam verdadeiros. (SILVA, 2019).

b) Convém ter atenção a ligações oferecendo grandes prêmios ou vantagens;
No Brasil a técnica de *vishing* é bastante utilizada nos presídios, os presos entram em contato com a vítima do lado de fora informando que ela é ganhadora de um grande prêmio, mas para recebê-lo antes deve ser pago um valor mínimo para a liberação do prêmio, normalmente esse valor deve ser colocado em créditos em outro celular. Porém, o prêmio informado não existe e esta é apenas uma maneira que os atacantes utilizam para ganhar vantagens financeiras em cima das vítimas. (SANTOS, Daniel, 2016).

c) Convém ter atenção a ligações informando que uma conta será suspensa;
Utilizando-se das técnicas de engenharia social o atacante pode entrar em contato com a vítima amedrontando-a informado que usa conta telefônica ou de algum outro serviço está suspensa, mas para reativa-la é necessário apenas confirmar alguns dados pelo telefone. Caso a vítima caia no golpe e informe os dados o atacante pode posteriormente utilizar estes dados para aplicar outros golpes como clonagem de cartões e transações financeiras. (PEREIRA, 2012).

d) Convém ter atenção a ligações de sistemas bancários;
Assim como nas ligações de suspensão de contas, nas ligações de sistemas bancários o atacante pode se passar por um funcionário do banco solicitando que a vítima fale ou digite os seus dados bancários, como número da conta, no seu telefone celular para que seja realizado determinado serviço. (CRESPO; SYDOW, 2007). Porém, os dados informados podem ser utilizados pelo atacante para a aplicação de golpes financeiros.

e) Convém ter atenção a ligações de falso sequestro.
Este é outro tipo de golpe também bastante utilizado de dentro de presídios. Os presos entram em contato com uma a vítima alegando que sequestraram um ente querido e através de ameaças tentam convencer a vítima a pagar um falso resgate. Para convencer a vítima a pagar o resgate no momento de desespero os atacantes fazem o uso das técnicas de engenharia social em

chantagens e ameaças, normalmente descrevem a cena em que o suposto sequestrado está, ameaçam a vida do mesmo e manipulam a vítima de modo que ela acredite que está responsável pela vida do seu ente querido. (SILVA; MELO, 2015).

4.1.3.2 Smishing

O termo *smishing* é a combinação de *Short Message Service* "(SMS)" e "*phishing*". Este é outro tipo de ataque baseado no *phishing* tradicional, mas neste caso o atacante faz o uso de SMS ou aplicativos de mensagens instantâneas para realizar o ataque. Normalmente nestas mensagens de texto os atacantes fazem o uso da engenharia social para influenciar a vítima a acessar um link enviado. (SILVA, 2019).

Como se proteger:

a) Convém não abrir links enviados por SMS ou aplicativos de mensagens vindos de fontes desconhecidas;

O atacante pode se passar por uma pessoa ou organização e por meio da mensagem de texto faz o envio de um link para a vítima, assim que este link é acessado ela é direcionada a um arquivo ou site malicioso, caso a vítima baixe o arquivo ou forneça informações no site o ataque poderá ser efetivado. (SANTOS, Daniel, 2016).

b) Convém verificar, caso o link seja aberto, se ele se comporta de forma diferente do smartphone no navegador do computador;

Em ataques de *smishing* o atacante pode enviar um link para a vítima via mensagem de texto que quando aberto no smartphone acessa uma página falsa solicitando dados, por exemplo a página de um banco, porém, quando esse mesmo link é acessado no navegador do computador pode ser forjado um erro informando que a página está indisponível. Este tipo de situação é um grande indício de um ataque de *smishing*. (SILVA et al., 2018).

c) Convém ter atenção a mensagens de texto solicitando dados pessoais;

É bastante comum neste tipo de ataque o envio de mensagens de texto solicitando dados pessoais das vítimas onde o atacante se passa por um funcionário ou instituição tentando convencer a vítima a acreditar na mensagem e fornecer os seus dados, por exemplo, o atacante pode se passar

por um banco que necessita da confirmação dos dados de uma conta bancária da vítima. (ESPÍNOLA; CRUZ, 2020).

d) Convém ter atenção a mensagens com conteúdo alarmante;
Utilizando-se da engenharia social os atacantes podem enviar mensagens informando que a conta da vítima foi invadida, ou que está expirando e ela pode até mesmo perder benefícios críticos devido a isso. Então aproveitando-se de mensagens que alertam a vítima de condições extremas o atacante faz com que ela em um momento de pânico faça uma ação imediata fornecendo a ele os seus dados pessoais. (SILVA, 2019).

e) Convém ter atenção a mensagens com grandes recompensas financeiras.
Neste tipo de mensagem o atacante pode alegar que a vítima ganhou na loteria, oferecer um grande desconto em um produto ou até mesmo dizer que ela foi ganhadora de um sorteio, mas o seu objetivo é fazer com que a vítima seja influenciada pela mensagem e acesse o link enviado fornecendo assim os seus dados pessoas e financeiros em busca do tal prêmio. (SILVA, 2019).

4.1.4 *Pretexting* (Representação)

O *pretexting* é uma das técnicas mais importantes e mais utilizadas na engenharia social, segundo Baer (2008 apud SILVA, F. 2013), o *pretexting* é a criação de um falso pretexto para a obtenção de informações das vítimas, é mais do que uma mentira. O atacante cria e utiliza um cenário específico induzindo a vítima a acreditar que ele é outra pessoa fazendo com que ela forneça determinada informação ou faça uma ação que não faria em outra circunstância. Geralmente o atacante faz uma pesquisa minuciosa, muitas vezes pela internet, sobre a vítima de modo que consiga construir um personagem convincente para o ataque de modo que ele não falhe, pois um menor passo falho pode fazer com que a vítima desconfie do golpe. (HADNAGY, 2011 apud SOUZA, 2015).

Como se proteger:

a) Convém não expor informações pessoais na internet;
Conforme o tópico de 4.1.2 de redes sociais trata, deve-se ter muito cuidado ao expor informações pessoais na internet, principalmente em redes sociais onde normalmente as pessoas compartilham muitas informações sem se preocuparem com os riscos. De acordo com Hadnagy (2011 apud SOUZA, 2015), os atacantes que fazem do *pretexting* encontram na internet um

ambiente bastante propício para encontrar informações a respeito das suas vítimas, informações estas que são utilizadas para a construção do seu personagem e do pretexto para o ataque.

b) Convém ter atenção a presentes e agrados vindos de desconhecidos;

Em busca de criar o cenário perfeito para o ataque, o engenheiro social busca inventar uma situação plausível e construir um personagem detalhado. Segundo os autores a engenharia social está bastante envolvida ao sentimento das vítimas, então o atacante pode enviar presentes ou agrados em busca de conseguir conquistar a sua confiança. (WATSON; MASON; ACKROYD, 2014 apud SOUZA, 2015).

c) Convém ter atenção a desconhecidos se passando por autoridades;

O engenheiro social que faz o uso do *pretexting* cria diversos papéis ao longo da sua vida, ele pode se passar por uma autoridade ou alguém de alta patente para manipular e influenciar a vítima a cair no seu golpe, normalmente um empregado não questiona alguém nesta posição, então os engenheiros sociais costumam fazer o uso desta mentira para ganhar a confiança da sua vítima. (HENRIQUES, 2016).

d) Convém ter atenção aos padrões de fala e tipo de linguagem utilizadas;

Muitas vezes os engenheiros sociais em busca de realizar o golpe perfeito chegam a estudar os padrões de fala e tipo de linguagem utilizadas nas organizações, pois cada organização costuma possuir suas próprias linguagens e expressões. O atacante ao conversar com alguém utilizando-se da mesma linguagem consegue persuadi-lo mais facilmente, pois a vítima se sente mais segura deste modo. (ALVES, 2010). Porém, observar o modo de abordagem pode fazer com que a vítima desconfie do golpe, pois caso o engenheiro social não consiga adotar perfeitamente esses padrões de linguagem ele pode vir a cometer um deslize.

e) Convém ter atenção a funcionários que se dizem terceirizados.

Tomando certo conhecimento sobre o funcionamento da empresa o atacante pode de passar por um funcionário terceirizado, enquanto o verdadeiro funcionário terceirizado não está disponível, para conseguir acesso ao sistema de computadores alegando possuir permissão para tal acesso. (HENRIQUES, 2016). Em outra situação o atacante pode se passar por um técnico de suporte

corporativo, a vítima acreditando na identidade falsa é induzida a fornecer dados de funcionários ou aceitar uma falsa manutenção de sistemas. (FERREIRA, M. 2016).

4.1.5 *Baiting* (Isca)

O *baiting*, do inglês isca, é uma técnica de ataque que explora a curiosidade da vítima. (GOODRICH; TAMASSIA, 2013). O atacante faz o uso de algum tipo de mídia física, como *pendrive*, CD, DVD, entre outros. Estes dispositivos são infectados com algum software malicioso por um engenheiro social e deixados em um local fácil de ser encontrado, por exemplo um estacionamento, elevador ou banheiro. Assim que a vítima insere o dispositivo em seu computador o software malicioso é instalado dando acesso ao atacante. (HENRIQUES, 2016).

Como se proteger:

a) Convém não utilizar dispositivos desconhecidos;

O objetivo do atacante nesta técnica é fazer com que a vítima encontre o dispositivo e insira-o em seu computador mesmo sem ter conhecimento da sua procedência. O atacante deixará estes dispositivos “esquecidos” em um local visível e normalmente de grande movimentação para que a vítima o encontre e já tenha a curiosidade de inseri-lo em seu computador. Porém, apenas o fato de inserir este dispositivo no computador já faz com que o software malicioso seja instalado, ele funciona como um Cavalo de Troia e pode dar ao atacante acesso ao computador da vítima, roubar dados confidenciais ou até mesmo dar brecha para uma invasão no sistema. (FERREIRA, M. 2016).

b) Convém ter atenção a dispositivos com títulos “atraentes” escritos;

Para despertar a curiosidade da vítima o atacante pode escrever no dispositivo um título atraente como nomes de softwares populares ou jogos. Por exemplo, o atacante pode deixar alguns desses dispositivos no estacionamento de uma empresa que possuí um sistema de computação seguro, um funcionário passando pelo local pode encontrar o dispositivo e, mesmo sem saber a sua procedência, conectá-lo em seu computador acreditando ser legítimo, devido ao nome que está escrito nele, fazendo com que a máquina seja infectada. (GOODRICH; TAMASSIA, 2013).

c) Convém ter atenção a dispositivos entregues por outras pessoas.
Uma outra estratégia que o atacante pode utilizar para realizar o ataque é criar uma situação hipotética e entregar o dispositivo infectado a uma pessoa alvo. Por exemplo, ele entrega a sua vítima um dispositivo infectado e pede para que sejam passados arquivos para ele, como músicas ou filmes, e a pessoa em boa vontade sem imaginar que o dispositivo está infectado pode conectá-lo em seu computador e instalar o software malicioso sem perceber. (GUAREZI, 2019).

4.1.6 *Quid Pro Quo* (Algo por algo)

Segundo o Goodrich e Tamassia (2013), outra técnica de ataque de engenharia social é o *quid pro quo*, que em latim significa "uma coisa pela outra". Neste tipo de ataque o engenheiro social oferece para vítima um benefício, como um presente, em troca de acesso ou informações, de modo que a vítima receberá esse benefício caso efetue determinada ação solicitada por ele. (HENRIQUES, 2016). De acordo com Collins (2019 apud LEITE, 2019), o objetivo deste ataque é criar uma confusão na cabeça da vítima de modo que ela caia no golpe.

Como se proteger:

a) Convém ter atenção a ligações do suporte de TI;
O método mais comum utilizado para a realização do ataque é o contato do suporte técnico de TI. O engenheiro social entra em contato com diversas vítimas dentro da empresa alegando ser do suporte técnico e oferecendo ajuda com algum problema, ele faz isso até encontrar uma vítima que realmente está passando por um problema de TI, então em busca de solucionar o seu problema a vítima dá acesso a credenciais e pode até chegar desabilitar programas importantes e instalar softwares maliciosos sem perceber. Caso seja aberto um chamado no suporte técnico é importante sempre conferir com o suposto atendente a qual problema se refere o atendimento antes de ceder informações. (ROCHA, 2018).

b) Convém ter atenção as ofertas de supostas atualizações de sistema;
Este é um método parecido com o apresentado acima, nele o engenheiro social também se passa por um técnico de TI e entra em contato com diversas vítimas de uma empresa oferecendo-lhes uma suposta atualização do sistema,

ele informa que é necessário que a vítima permita o seu acesso ao sistema para que seja efetuada a atualização. (VAULT, 2017 apud HENRIQUES, 2016). Porém, está suposta atualização é apenas uma desculpa para que o atacante tenha acesso a informações confidenciais.

c) Convém ter atenção a formulários de pesquisas;
O atacante pode fazer o uso de formulários ou supostas pesquisas nas ruas ou em ambientes de trabalho em busca de obter dados das vítimas. (JUNIOR, 2020). É comum ver pessoas sendo abordadas nas ruas por indivíduos que alegam estarem fazendo uma pesquisa, normalmente para alguma instituição, perguntando se elas podem informar alguns dados, como nome, telefone, idade, formação e outras informações pessoais que serão preenchidas em um formulário. Então, ainda segundo Junior (2020), para evitar ser mais uma vítima deste método é importante questionar antes de responder qualquer formulário ou pesquisa.

d) Convém ter atenção a formulários com promessas de prêmios e sorteios.
O atacante em busca de obter os dados da vítima pode simular uma pesquisa onde ele oferece brindes vantajosos, como canecas e canetas, para convencer a vítima a preencher o suposto formulário de pesquisa com seus dados sensíveis. (ROCHA, 2018). Outra forma de convencer a vítima a fornecer seus dados são as promessas de prêmios e sorteios onde a vítima deve preencher um formulário com suas informações pessoais para participar.

4.1.7 *Hoax* (Boato)

O *hoax*, do inglês boato, é uma técnica de ataque onde o engenheiro social faz o uso de um conteúdo alarmante que gere grande comoção a vítima, semelhante à técnica de ataque "*smishing*" que faz o uso de falsas mensagens para enganar a vítima. As mensagens enviadas pelos atacantes podem simular ter como remetente alguma instituição, empresa importante ou órgão governamental. (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012). Segundo Santos, Daniel, (2016) elas são recebidas como forma de spam em redes sociais e e-mails, mensagens telefônicas e por meio de mensageiros instantâneos, como o *Whatsapp*. Além de promover a desinformação as mensagens também podem conter algum link que quando acessado pela vítima instala um software malicioso em seu dispositivo.

Esta técnica é muito utilizada para disseminação das famosas *fake news*, do inglês notícias falsas, como o engenheiro social faz o envio de um conteúdo alarmante, quem recebe muitas vezes acaba compartilhando para os seus contatos sem confirmar a veracidade da história, fazendo com que a notícia se espalhe cada vez mais rápido.

Como se proteger:

a) Convém ter atenção a mensagens dramáticas ou apelativas;

Para comover a vítima e fazê-la compartilhar a mensagem o atacante constrói uma história dramática, às vezes acompanhada de uma imagem chocante, de modo que a vítima seja facilmente enganada acreditando naquele falso conteúdo e compartilhando com os seus contatos. (BONAFIN, 2014). Um exemplo deste tipo de mensagem são falsas histórias comoventes acompanhadas da imagem de uma criança doente que precisa de ajuda.

b) Convém ter atenção a mensagens de prêmios ou sorteios;

O atacante poderá enviar uma mensagem para a vítima alegando que ela foi a ganhadora de um grande prêmio ou sorteio. (SANTOS, Daniel, 2016). Este é um método semelhante ao que ocorre na técnica de ataque "*vishing*", porém, em vez de solicitar uma ação financeira da vítima o atacante informa que ela deve compartilhar essa mensagem com um número mínimo de pessoas para que possa receber o prêmio.

c) Convém ter atenção a mensagens que desvalorizam determinado mecanismo de segurança;

O atacante poderá fazer o uso de um discurso convincente para mudar a opinião e atitude das pessoas sobre um determinado mecanismo de segurança, por meio dele o atacante alega que aquele mecanismo é desvalorizado e ineficiente. (SILVA, F. 2013). Acreditando no falso discurso as vítimas poderão deixar de utilizar importantes medidas de segurança em seus dispositivos ficando ainda mais vulneráveis a ameaças externas.

d) Convém ter atenção a notícias chocantes muito compartilhadas;

Em busca de despertar a curiosidade da vítima o atacante poderá criar notícias falsas, como "rato encontrado em coca-cola" ou "loja famosa distribuindo produtos de graça". (BONAFIN, 2014). Este tipo de notícia é facilmente encontrada em redes sociais, pois muitas pessoas acabam compartilhando a informação sem checar se é verdadeira.

e) Convém ter atenção a informações e notícias sobre política.

Nas eleições presidenciais do Brasil em 2014, 10% das interações feitas no *Twitter* eram falsas e geradas por meio de robôs, que são perfis falsos criados nas redes sociais passando-se por seres humanos para compartilhar *hashtags*, participar de debates e disseminar informações falsas, conforme informa o estudo do Departamento de Análise de Políticas Públicas – DAPP da Fundação Getúlio Vargas: O uso de robôs em redes sociais e a política no brasil. (LIMA; AMARAL, 2018). Portanto, para evitar ser vítima ou compartilhar falsas informações é importante sempre checar antes em fontes confiáveis se àquela é uma informação verídica.

4.1.8 Sextorsão

Segundo Sydow e Castro (2015), a palavra sextorsão vem da junção da palavra "sexo" com "extorsão". É uma área da engenharia social onde o atacante busca obter favores sexuais por meio da extorsão, geralmente realizada de maneira virtual. (GASTALDO, 2020). De acordo com Santos, Débora (2018), o atacante pode ser um conhecido, com quem a vítima convive ou já teve algum tipo de relacionamento, alguém que ela conheceu apenas virtualmente, ou até mesmo um hacker que obteve acesso as suas contas ou dispositivos. Ele faz o uso fotos, vídeos ou outros conteúdos de cunho sexual da vítima para chantageá-la em busca de obter vantagens, sendo o famoso "*nudes*", do inglês "sem roupa ou pelado", o conteúdo mais popular utilizado pelos atacantes.

Em 2012 foi aprovada a lei 12.737/2012, apelidada de "Lei Carolina Dieckman", que prevê a criminalização em caso de violação do dispositivo informático da vítima com o objetivo de obter, adulterar ou destruir seus dados ou informações. Porém, a lei é limitada já que repreende apenas em casos de invasão (violação indevida), excluindo situações de envio espontâneo durante algum tipo de relacionamento e outras situações em que há uma exposição da vítima, mas sem ocorrer a invasão. (SYDOW; CASTRO, 2015).

Como se proteger:

a) Convém não enviar fotos íntimas;

Os principais casos de sextorsão ocorrem por causa fotos, vídeos ou outros conteúdos sexuais enviados pela vítima a outra pessoa. Logo, a melhor forma de evitar ser vítima desta técnica é não fazer o envio de deste tipo de conteúdo para ninguém. A pessoa que solicita o envio explora a boa vontade e

confiança da vítima, e nem sempre a sextorsão é premeditada, por exemplo pode vir a ocorrer após um relacionamento que não deu certo. (GASTALDO, 2020).

b) Convém não enviar a mesma foto íntima para diferentes pessoas;

Caso o tópico acima não tenha sido seguido e uma foto já tenha sido enviada para alguém, como uma pessoa de um relacionamento passado, não deve ser feito o envio desta mesma foto para mais ninguém. Deste modo, se a foto vir a ser exposta é possível saber exatamente quem é a única pessoa que a possuía. Além disso é importante guardar para quem enviou, como enviou e quando enviou caso seja necessário tomar medidas legais contra alguém. (GASTALDO, 2020).

c) Convém ter maior atenção a redes sociais;

Conforme o tópico de 4.1.2 de redes sociais trata, por meio das redes sociais os atacantes tem a possibilidade de se manter anônimos, logo é importante ter atenção e não confiar em qualquer pessoa que entra em contato buscando aproximação e principalmente pedindo informações pessoais ou fotos. (MORGADO, 2019). Muitas vezes o atacante cria um perfil falso, se passando por outra pessoa, em uma rede social com intuito de alcançar alguém, ele se passa por outra pessoa e faz o uso da sedução e técnicas de exploração emocional para obter a confiança da vítima e pedir o envio de fotos íntimas. (GASTALDO, 2020).

d) Convém habilitar a autenticação de dois fatores.

A autenticação de dois fatores é um mecanismo adicional de segurança presente em algumas contas. É importante habilitá-la, pois caso o atacante consiga acesso a senha sem permissão ele ainda não conseguirá acessar a conta sem o segundo fator de autenticação. (MORGADO, 2019).

5. CONCLUSÃO

Portanto o estudo acerca de Políticas de Segurança da Informação e normas ISO 27001 e 27002, foi possível entender a importância de um Sistema de Gestão a Segurança da Informação.

De acordo com o proposto foram conceituados os pontos mais importantes da segurança da informação, também foram apresentados os tipos ataques relacionados a mesma e os principais programas maliciosos utilizados, além da abordagem das principais técnicas utilizadas por um engenheiro social na realização dos ataques e as vulnerabilidades humanas que levam uma pessoa a ser vítima da engenharia social.

A partir das informações obtidas foi observado que ao implementar a norma ISO 27002 é pertinente que a empresa crie Políticas de Segurança da Informação, pois são métodos utilizados para a implementação de um Sistema de Gestão de Segurança da Informação, considerando a importância de proteger ativos internos e externos das organizações, assegurar que dados pessoais sejam mantidos em sigilo, e a segurança da privacidade individual. Os métodos citados acima são responsáveis por estabelecerem requisitos e instruções para os indivíduos, e podem ser definidos como um conjunto de normas, eles diferem de acordo com a organização, porém todas concluem a função de orientar indivíduos, auxiliando assim na prevenção de incidentes a segurança da informação.

Foi elaborado um guia onde apresenta-se os tipos de ataques que fazem uso da engenharia social, boas práticas, métodos e técnicas que poderão evitar esses ataques. Este guia segue o padrão da norma ISO 27002 no qual a abordagem está dividida em tópicos e subtópicos com tipos de ataques e boas práticas.

No entanto o guia não será implementado, fica como sugestão para trabalhos futuros a validação do guia onde possivelmente seria implementado em empresas, startups, instituições, entre outros.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT/CB-21. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos**. 2013.

AGOSTINHO, Denilson Aparecido. **Leis de Segurança da Informação.** Universidade Federal de Santa Catarina, Santa Catarina, 2004. Disponível em: <http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/Trabalhos%202004-2/artigo-LeisDeSeguranca.pdf>. Acesso em: 10 out. 2019.

ALMEIDA, Paulo Ricardo Lisboa de. **Autenticação Segura**. Curitiba: Universidade Positivo - Unidade Praça Santos Andrade, 2019. 57 slides, color. Disponível em: http://www.prlalmeida.com.br/posTestesRiscosSegurancaUP-2019-01/Aula1Parte4.pdf. Acesso em: 17 set. 2020.

ALVES, Cássio Bastos. **SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL**: Como se proteger para não ser mais uma vítima. 2010. 120 f. TCC (Graduação) - Curso de Sistemas de Informação, Centro Universitário do Distrito Federal, Brasília, 2010. Disponível em: <https://docplayer.com.br/3136545-Cassio-bastos-alves-seguranca-da-informacao-vs-engenharia-social-como-se-proteger-para-nao-ser-mais-uma-vitima.html>. Acesso em: 22 abr. 2020.

AVANCINI, F. **Implementação De Um Sistema Unificado De Gestão Da Segurança Da Informação Em Data Centers De Diversos Países**. 2018. Disponível em: <https://riuni.unisul.br/bitstream/handle/12345/5787/AD6_Fabricio_Avancini_versao_final.pdf?sequence=1&isAllowed=y>. Acesso em: 05 de abril 2020.

BAARS, Hans et al. **Fundamentos de Segurança da Informação**: Com base na ISO 27001 e na ISO 27002. 3. ed. Rio de Janeiro: Brasport, 2018. 237 p. Tradução de: Alan Sá.

BALDIM, Natália Pimenta. **ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO**: Uma análise focada nos profissionais de secretariado executivo. 2007. 127 f. Monografia (Especialização) - Curso de Secretariado Executivo Trilíngue, Departamento de Letras, Universidade Federal de Viçosa, Minas Gerais, 2007. Disponível em: <http://www.secretariadoexecutivo.ufv.br/docs/anexo8.pdf>. Acesso em: 22 abr. 2020.

BARRETO, Jeanine dos Santos et al. **Fundamentos de segurança da informação**. Porto Alegre: Sagah Educação S.A, 2018. 198 p.

BONAFIN, Leandro Marcos. **Análise Teórica da Segurança no Uso da Linguagem PHP com Banco de Dados MySQL Aplicado ao Comércio Eletrônico**. 2014. 10 f. Monografia (Doutorado) - Curso de Mba em Gestão da Tecnologia da Informação e Internet, Universidade Nove de Julho, São Paulo, 2014. Disponível em: https://bonafin.com.br/Artigo_Analise_Teorica_da_Seguranca_PHP_MySQL_no_ecommerce_%5bLeandro_Marcos_Bonafin_2014%5d_final.pdf. Acesso em: 22 out. 2020.

CAPISTRANO, Ramon dos Santos. **REDES SOCIAIS VIRTUAIS COMO AMBIENTE DE EXPOSIÇÃO DE DADOS PESSOAIS PARA A ENGENHARIA SOCIAL**. 2013. 36 f. TCC (Graduação) - Curso de Bacharel em Sistemas de Informação, Universidade Federal do Ceará, Quixadá, 2013. Disponível em: http://www.repositoriobib.ufc.br/000012/00001226.pdf. Acesso em: 05 out. 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet:** Versão 4.0. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 142 p. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 23 set. 2019.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO. **Exatas & Engenharia**, v. 3, n. 05, mar. 2013. ISSN 2236-885X. Disponível em: <http://www.seer.perspectivasonline.com.br/index.php/exatas_e_engenharia/article/view/87/59>. Acesso em: 23 set. 2019.

COIMBRA, Sara Alexandra Magalhães Pereira. **AMEAÇAS E VULNERABILIDADES À SEGURANÇA DA INFORMAÇÃO DOS SISTEMAS DE INFORMAÇÃO DA FORÇA AÉREA. POLÍTICA DE SEGURANÇA E PREVENÇÃO**. 2018. 60 f. - Curso de Promoção a Oficial Superior, Instituto Universitário Militar, Pedrouços, 2018. Disponível em:
<http://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSaraCoimbra_TII_VF.pdf>.
Acesso em: 18 jun. 2020.

CORREIA, Carlos Manuel Rosa. **Plano de Implementação da Norma ISO/IEC 27001:2013 na organização INEM-Instituto Nacional de Emergência Médica**, I. P**.** 2016. 95f. Dissertação de Mestrado-Universidade Nova de Lisboa, Lisboa, 2016. Disponível em: <https://run.unl.pt/bitstream/10362/19605/1/TGI0069.pdf>. Acesso em: 23 set. 2019.

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. Novas Tendências da Criminalidade Telemática. **Revista de Direito Administrativo**, Rio de Janeiro, v. 246, p. 162-180, set. 2007. ISSN 2238-5177. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/41656. Acesso em: 09 out. 2020.

CUNHA, Dalvan; FENATO, Marcos Alexandre. A SEGURANÇA DA INFORMAÇÃO E A SUA IMPORTÂNCIA PARA A AUDITORIA DE SISTEMAS. **Revista Científica**

Semana Acadêmica, Fortaleza, v. 1, n. 29, p. 1-16, 26 jul. 2013. Disponível em: <https://semanaacademica.org.br/system/files/artigos/dalvancunha-asegurancadainformacaoeasuaimportanciaparaaauditoriadesistemas.pdf>. Acesso em: 30 mar. 2020.

DANTAS, Marcus Leal. **SEGURANÇA DA INFORMAÇÃO**: Uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 152 p. Disponível em: <http://www.marcusdantas.com.br/files/seguranca_informacao.pdf>. Acesso em: 29 mar. 2020.

EL PESCADOR. **Ataques de Phishing**: Tudo que você precisa saber para não ser fisgado. Brasil: Tempest Security Intelligence, 2017. Disponível em: https://www.elpescador.com.br/ebook/ELPESCADOR-EBOOK-PHISHING.PDF. Acesso em: 03 out. 2020.

ESPÍNOLA, Samuel Guimarães; CRUZ, Letícia Cerqueira Menezes. SEGURANÇA NA INTERNET: PROBLEMAS E SOLUÇÕES PARA O USUÁRIO COMUM. **ConSciências**, Belo Horizonte, v. 1, n. 11, p. 1-6, jan. 2020. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/17081. Acesso em: 12 out. 2020.

FERREIRA, Fabiano Santana. **A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TRIBUNAL DE JUSTIÇA DA PARAÍBA**: Uma análise baseada na NBR ISO 27002. 2015. 78 f. Monografia (Especialização) - Curso de Sistemas de Informação, Centro de Ciências Aplicadas e Educação, Universidade Federal da Paraíba, Rio Tinto, 2015. Disponível em: <https://repositorio.ufpb.br/jspui/bitstream/123456789/17141/1/FSF24032015.pdf>. Acesso em: 05 maio 2020.

FERREIRA, Marvin. A Engenharia Social e os crimes cibernéticos. **Centro de Estudos Sociedade e Tecnologia (CEST)**, São Paulo, v. 1, n. 5, p. 1-2, mar. 2016. Disponível em: http://www.cest.poli.usp.br/wp-content/uploads/2018/08/V1N5-A-engenharia-social-e-os-crimes-cibernéticos.pdf. Acesso em: 14 out. 2020.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. 1. ed. São Paulo: Editora Saraiva, 2006. 173 p.

GASTALDO, Gabriel. Sextortion – Sextorsão. **Medium**, 2018. Disponível em: https://medium.com/arddhu/sextorsao-1d682c02cc89. Acesso em: 29 out. 2020.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança e Computadores**. 1. ed. Porto Alegre: Bookman, 2013. 550 p. Tradução de: Maria Lúcia Blanck Lisbôa.

GUAREZI, Júlio. **ENGENHARIA SOCIAL: AVALIAÇÃO DE RISCOS E VULNERABILIDADES TENDO O FATOR HUMANO COMO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO Trabalho**. 2019. 68 f. TCC (Doutorado) - Curso de Graduação em Sistema da Informação, Universidade do Sul de Santa Catarina, Palhoça, 2019. Disponível em: https://riuni.unisul.br/bitstream/handle/12345/8487/TCC_EngSocial_JulioGuarezi_atual.pdf?sequence=1&isAllowed=y. Acesso em: 15 out. 2020.

HENRIQUES, Francisco de Assis Fialho. **A influência da Engenharia Social no fator humano das organizações**. 2016. 112 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2016. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/25353/1/DISSERTAÇÃO%20Francisco%20de%20Assis%20Fialho%20Henriques.pdf. Acesso em: 13 out. 2020.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. **Fundamentos de Segurança da Informação**. São Paulo: Escola de Governança da Internet no Brasil, 2014. 47 slides, colorido. Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 17 abr. 2020.

HUMMES, Alex Artur. **PROPOSTA DE IMPLANTAÇÃO DE UMA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE SEGURANÇA NACIONAL**. 2017. 17f. Monografia (Especialização) – Curso de Governança de Tecnologia da Informação, Unisul Virtual, Montenegro, 2017. Disponível em: <https://riuni.unisul.br/handle/12345/3043>. Acesso em: 17 jun. 2020.

INTEGRASUL. **COMO EVITAR DE CAIR EM ATAQUES DE PHISHING**. **Integra News**, Caxias do Sul, v. 2, n. 6, p. 5-5, mar. 2017. Disponível em: https://www.integrasul.com.br/imagens/informativo/informativo-06.pdf. Acesso em: 03 out. 2020.

JUNIOR, Ricardo Cestari. Engenharia Social: Sua Empresa Está Protegida?. **Medium**, 2020. Disponível em: https://medium.com/compugraf-cyberwars/engenharia-social-sua-empresa-está-protegida-9502b893cfe7. Acesso em: 21 out. 2020.

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação**. 1. ed. Rio de Janeiro: LTC, 2014.

KONZEN, Marcos Paulo. **GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA**. 2013. 119 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal de Santa Maria, Santa Maria, 2013. Disponível em: <https://repositorio.ufsm.br/bitstream/handle/1/8276/KONZEN%2c%20MARCOS%20PAULO.pdf?sequence=1&isAllowed=y>. Acesso em: 17 abr. 2020.

LEITE, Iago Piccoli. **Engenharia Social: Não seja mais uma vítima**. 2019. 35 f. TCC (Doutorado) - Curso de Tecnológico em Redes de Computadores, Faculdade de Tecnologia Alcides Maya, Porto Alegre, 2019. Disponível em: http://raam.alcidesmaya.com.br/index.php/projetos/article/view/59. Acesso em: 18 out. 2020.

LIMA, P.; AMARAL, ÉRICO. EXISTEM FERRAMENTAS DIGITAIS CAPAZES DE REDUZIR A DISSEMINAÇÃO DAS FAKE NEWS?. **Anais do Salão Internacional de Ensino, Pesquisa e Extensão**, v. 10, n. 2, 6 nov. 2018. Disponível em: https://guri.unipampa.edu.br/uploads/evt/arq_trabalhos/17804/seer_17804.pdf. Acesso em: 28 out. 2020.

LYRA, Mauricio Rocha (org.). **Governança da Segurança da Informação**. 1. ed. Brasília: Edição do Autor, 2015. 173 p.

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação Princípios e Controle de Ameaças**. 1. ed. São Paulo: Érica, 2014. 176 p.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. **Ciência da Informação**, Brasília, v. 35, n. 3, p. 89-98, Dez. 2006. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000300009&lng=en&nrm=iso>. Acesso em: 15 maio. 2020.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Education, 2003. 286 p. Tradução de: Kátia Aparecida Roque. Disponível em: <https://www.docdroid.net/Mq0Edkm/kevin-mitnick-a-arte-de-enganar.pdf>. Acesso em: 13 out. 2019.

MORAES, Alexandre Fernandes de. **Segurança em Redes**: Fundamentos. 1. ed. São Paulo: Érica, 2010. 265 p.

MOREIRA, Eurico dos Santos. O uso de ataques diretos e pessoais da engenharia social para a obtenção de informações de uma corporação. **Revista Inteligência Competitiva**, v. 9, n. 1, p. 55-72, jan./mar. 2019. Disponível em: <https://www.inteligenciacompetitivarev.com.br/ojs/index.php/rev/article/view/302/pdf_177>. Acesso em: 22 abr. 2020.

MORGADO, Gabriela – O que é Sextorsão?. **PSafe**, 2019. Disponível em: https://www.psafe.com/blog/o-que-e-

sextorsao/#:~:text=Caracterizado%20como%20um%20tipo%20de,troca%20de%20dinheiro%20ou%20favores.. Acesso em: 30 out. 2020.

NOVO, Jorge Procópio da Costa. **Softwares de Segurança da Informação**: Curso Técnico em Manutenção e Suporte em Informática. Manaus: Centro de Educação Tecnológica do Amazonas – CETAM, 2010. 116 p. Disponível em: <http://ead.ifap.edu.br/netsys/public/livros/LIVRO%20MANUTEN%C3%87%C3%83O/Modulo%20III/software_seguran%C3%A7a_informa%C3%A7%C3%A3o.pdf>. Acesso em: 3 out. 2019.

OLIVEIRA, G. D. DE; MOURA, R. K. G. DE; ARAÚJO, F. DE A. N. G. DE. Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação (T.I.). **Múltiplos Olhares em Ciência da Informação**, v. 3, n. 2, 29 maio 2014. Disponível em: <https://periodicos.ufmg.br/index.php/moci/article/view/17382/14164>. Acesso em: 30 mar. 2020.

PALMA, Fernando. **Overview da Certificação ISO 27002**. Bahia: Portal GSTI & PMG Education, 2014. 32 slides, colorido. Disponível em: <https://pt.slideshare.net/fernando.palma/certificao-profissional-iso-27002>. Acesso em: 10 maio 2020.

PAZ, Fábio Alves. **A IMPORTÂNCIA DA IMPLEMENTAÇÃO DE UM PROGRAMA DE SEGURANÇA DA INFORMAÇÃO NOS FUNDOS DE PENSÃO**. 2019. 56 f. Monografia (Especialização) - Curso de Auditoria e Controladoria, Universidade Candido Mendes, Rio de Janeiro, 2019. Disponível em: <http://www.avm.edu.br/docpdf/monografias_publicadas/K238791.pdf>. Acesso em: 10 maio 2020.

PEIXOTO, S. C, et al. Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 06, n. 2, p. 37-49, 2015. Disponível em: <http://periodicos.unifacef.com.br/index.php/resiget/article/view/1065/848>. Acesso em: 20 maio 2020.

PEREIRA, Cleber Guedes. **PHISHING: CONCEITOS E AÇÕES PREVENTIVAS APLICADAS À EMPRESA**. 2012. 55 f. Monografia (Especialização) - Curso de Pós-Graduação Lato Sensu em Redes de Computadores Com Ênfase em Segurança, Centro Universitário de Brasília, Brasília, 2012. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/8136/1/50910909.pdf. Acesso em: 10 out. 2020.

RIOS, O. K. L.; RIOS, V. P. S.; FILHO, J. G. A. T. Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições

Federais do Ensino Superior. **Revista Gestão & Tecnologia, Pedro Leopoldo,** v. 17, n. 1, p. 130-153, jan./abr. 2017. Disponível em: <http://revistagt.fpl.edu.br/get/article/view/1084/728>. Acesso em: 20 maio 2020.

ROCHA, Douglas da Fonseca. Engenharia Social: Compreendendo ataques e a importância da conscientização. Brasil Escola, 2018. Disponível em: https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm. Acesso em: 19 out. 2020.

RODRIGUES, Bernardo Araujo. **CORINDA: HEURÍSTICAS CONCORRENTES PARA QUEBRA DE SENHAS**. 2018. 130 f. Dissertação (Mestrado) - Curso de Pós-Graduação em Engenharia Elétrica e de Computação, Universidade Federal de Goiás, Goiânia, 2018. Disponível em: https://repositorio.bc.ufg.br/tede/bitstream/tede/8936/5/Dissertação%20-%20Bernardo%20Araujo%20Rodrigues%20%20-%202018.pdf. Acesso em: 14 dez. 2020.

ROQUE, André. A TUTELA COLETIVA DOS DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). **Revista Eletrônica de Direito Processual – REDP**, v.20, n. 02, p. 01-19, maio/ago. 2019. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270>. Acesso em: 20 maio 2020.

SANSIGOLO, Gabriel. **A IMPORTÂNCIA DA SÉRIE ISO 27000.** Faculdade de Tecnologia de São José dos Campos, São Paulo, 2015. Disponível em: <https://docs.academicoo.com/user/gsansigolo/importancia-iso-2700.pdf>. Acesso em: 10 out. 2019.

SANTOS, Daniel Pitanga dos. **A ENGENHARIA SOCIAL NO BRASIL E SEUS RISCOS**. 2016. 121 f. Monografia (Especialização) - Curso de Especialização em Gestão da Tecnologia da Informação e Comunicação, Universidade Tecnológica Federal do Paraná, Curitiba, 2016. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/13297/1/CT_GETIC_V_2015_05.pdf. Acesso em: 03 out. 2020.

SANTOS, Débora Gomes dos. **SEXTORSÃO COMO ESTUPRO VIRTUAL: ESTUPRO REALIZADO NA ERA TECNOLÓGICA**. 2018. 23 f. Curso de Graduação em Direito, Centro de Ciências Humanas e Sociais Aplicadas, Centro Universitário de Maringá, Maringá, 2018. Disponível em: http://rdu.unicesumar.edu.br/bitstream/123456789/5460/1/TRABALHO%20DE%20CONCLUSÃO%20DE%20CURSO.pdf. Acesso em: 30 out. 2020.

SANTOS, Edenilza Pereira dos; MOURA, Eulene Cruz; SILVA, Jandira de Morais. Segurança da Informação: como garantir a integridade, a confidencialidade e a disponibilidade das informações em uma organização educacional privada de Teresina: como garantir a integridade, a confidencialidade e a disponibilidade das informações em

uma organização educacional privada de Teresina. **Revista Científica da FSA**, Teresina, v. 7, n. 1, p. 77-92, jan. 2010. Disponível em: <http://www4.fsanet.com.br/revista/index.php/fsa/article/view/409/194>. Acesso em: 08 abr. 2020.

SANTOS, Eduardo Esteves dos; SOARES, Tamires Mariana Mayumi Kurosaki. RISCOS, AMEAÇAS E VULNERABILIDADES: o impacto da segurança da informação nas organizações. **Revista Tecnológica da Fatec Americana**, São Paulo, v. 7, n. 2, p. 43-51, 16 dez. 2019. Disponível em: <https://fatecbr.websiteseguro.com/revista/index.php/RTecFatecAM/article/view/188>. Acesso em: 17 abr. 2020.

SÊMOLA, Marcos. **Gestão da segurança da informação: Uma visão executiva.** 2º Edição. Rio de Janeiro: Elsevier, 2014.

SILVA, Carlo. M. R. et al. **Suscetibilidade através da forja de fidedignidade: uma abordagem sobre ataques de Phishing**. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2019, São Paulo. XIX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2019), 2019. Disponível em: https://sbseg2019.ime.usp.br/anais/195693.pdf. Acesso em: 11 out. 2020.

SILVA, Francisco José Albino Faria Castro e. **Classificação Taxonómica dos Ataques de Engenharia Social**: caracterização da problemática da segurança de informação em portugal relativamente à engenharia social. 2013. 132 f. Dissertação (Mestrado) - Curso de Segurança dos Sistemas de Informação, Faculdade de Engenharia, Universidade Católica Portuguesa, Lisboa, 2013. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf. Acesso em: 25 out. 2020.

SILVA, Iury Pereira da. **ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA**. 2019. 79 f. TCC (Graduação) - Curso de Graduação em Engenharia de Software, Universidade Federal do Ceará, Quixadá, 2019. Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/49703/1/2019_tcc_ipsilva.pdf. Acesso em: 07 out. 2020.

SILVA, N. B. X.; ARAÚJO, W. J. DE; AZEVEDO, P. M. DE. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Informação**, v. 6, n. 2, p. 37-55, ago./dez. 2013. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782. Acesso em: 02 out. 2020.

SILVA, Welton Pereira e; MELO, Mônica Santos de Souza. A análise de gêneros discursivos na Linguística Forense: um estudo sobre os Golpes do Falso Sequestro: a análise de gêneros discursivos na linguística forense: um estudo sobre os golpes do falso sequestro. **Gragoatá**, Niterói, v. 38, n. 1, p. 73-90, mar. 2015. Disponível em: https://www.researchgate.net/profile/Welton_Silva/publication/330703876_A_Analise_de_Generos_Discursivos_na_Linguistica_Forense_um_estudo_sobre_os_Golpes_do_Falso_Sequestro/links/5ca37354a6fdcc12ee8d8769/A-Analise-de-Generos-Discursivos-na-Linguistica-Forense-um-estudo-sobre-os-Golpes-do-Falso-Sequestro.pdf. Acesso em: 15 out. 2020.

SOUSA, Natan Lima Ferreira Fernandes de. **ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO**. 2016. 12 f. Trabalho acadêmico (Graduação) - Curso de Tecnologia em Análise e Desenvolvimento de Sistemas, Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro, Paracatu, 2016. Disponível em: <https://roitier.pro.br/wp-content/uploads/2016/11/Natan-Fernandes_3600_assignsubmission_file_Engenharia-Social-vs-Segurança-da-Informação-Natan-Lima-F-F-Sousa.pdf>. Acesso em: 22 abr. 2020.

SOUZA, Raul Carvalho de. **Prevenção para ataques de engenharia social:**: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos raul. 2015. 187 f. Dissertação (Mestrado) - Curso de Ciência da Informação, Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, 2015. Disponível em: https://core.ac.uk/download/pdf/33551742.pdf. Acesso em: 12 out. 2020.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores**: princípios e práticas. 2. ed. Rio de Janeiro: Elsevier Editora Ltda, 2014. 744 p. Tradução de: Arlete Simille Marques.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. Sextorsão. **Revista dos Tribunais**, São Paulo, v. 104, n. 959, p. 167-182, set. 2015. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.959.09.PDF. Acesso em: 29 out. 2020.

SYMANTEC. **2017 Norton Cyber Security Insights Report Global Results**. 2017. Disponível em: <https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf>. Acesso em: 10 ago. 2019.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas Práticas em Segurança da Informação**. 4. ed. Brasília: Tribunal de Contas da União, 2012. 108 p. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 01 maio 2020.