FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Paulo Henrique Romualdo

SEGURANÇA DA INFORMAÇÃO, ENGENHARIA SOCIAL:

Principais ataques às organizações e o elo mais fraco da Segurança.

Americana, SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Paulo Henrique Romualdo

SEGURANÇA DA INFORMAÇÃO, ENGENHARIA SOCIAL:

Principais ataques às organizações e o elo mais fraco da Segurança.

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Profª. Especialista Juliane Borsato Beckedorff Pinto.

Área de concentração: Segurança da Informação.

Americana
2020

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

R674s ROMUALDO, Paulo Henrique

Segurança da informação, engenharia social: principais ataques ás organizações e o elo mais fraco da segurança. / Paulo Henrique Romualdo. – Americana, 2020.

70f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Esp. Juliane Borsato Beckedorf Pinto

1 Segurança em sistemas de informação 2. Engenharia social I. PINTO, Juliane Borsato Beckedorf II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU

Paulo Henrique Romualdo

SEGURANÇA DA INFORMAÇÃO, ENGENHARIA SOCIAL:

Principais ataques às organizações e o elo mais fraco da Segurança.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 11 de dezembro de 2020.

Banca Examinadora:

_____
Prof ª Juliane Borsato Beckedorff Pinto (Presidente)
Especialista
CEETEPS – FATEC – Americana Ministro Ralph Biasi

_____
Prof. Alberto Martins Júnior (Membro)
Mestre
CEETEPS – FATEC – Americana Ministro Ralph Biasi

_____
Prof. Maxwel Vitorino da Silva (Membro)
Mestre
CEETEPS – FATEC – Americana Ministro Ralph Biasi

RESUMO

O crescente aumento do uso de dispositivos na área de Tecnologia da Informação – TI – e do uso da Internet, bem como a utilização cada vez maior de sistemas de informação desenvolvidos para *web*, fez com que a Segurança da Informação- SI - seja um aspecto importante para organizações de maneira geral. A SI tem como principal objetivo preservar um dos ativos mais importantes das organizações, que é a informação, visando a continuidade de negócios de instituições, entre outros objetivos. As ameaças à informação englobam aspectos de desastres naturais, *hardware, software*, instalações físicas, falhas humanas e ataques feitos por indivíduos como *crackers* e engenheiros sociais. O estabelecimento e uso de normas e regulamentos que compõem políticas de SI podem mitigar muitos efeitos provocados pelas ameaças e ataques, mas questões relacionadas à vulnerabilidade de colaboradores de organizações, no que diz respeito a ataques de engenheiros sociais, formam um conjunto de desafios às políticas de SI. Este trabalho apresenta um estudo sobre alguns tipos de ataques de engenheiros sociais e sobre o elo mais fraco da cadeia de SI que é o ser humano, com o objetivo de propor possíveis ações para mitigar a vulnerabilidade dos colabores das instituições. Para alcançar este objetivo, o autor deste trabalho realizou pesquisas bibliográficas detalhadas sobre SI e políticas de SI, perfis de atacantes e características do ser humano considerado como elo mais fraco da cadeia de SI. Elaborou e aplicou uma pesquisa quantitativa sobre estes aspectos, apresentando os resultados obtidos, bem como sugestões para reduzir a vulnerabilidade dos colaboradores de organizações.

Palavras-chave: segurança da informação; engenheiro social; fator humano.

ABSTRACT

The growing increase in the use of devices in Information Technology - IT - and the use of the Internet, as well as the increasing use of information systems developed for the web, makes Information Security - SI - an aspect important for organizations in general. SI's main objective is to preserve one of the most important assets of organizations, which is information, aiming at the business continuity of institutions, among other objectives. Information threats encompass aspects of natural disasters, hardware, software, physical installations, human failures, and attacks by individuals such as crackers and social engineers. The establishment and use of rules and regulations that make up IS policies can mitigate many effects caused by threats and attacks, but issues related to the vulnerability of employees of organizations, with respect to attacks by social engineers, form a set of policy challenges. of SI. This work presents a study on some types of attacks by social engineers and on the weakest link in the IS chain, which is the human being, with the aim of proposing possible actions to mitigate the vulnerability of the institutions' collaborators. To achieve this goal, the author of this work has carried out detailed bibliographic research on IS and IS policies, profiles of attackers and characteristics of the human being considered as the weakest link in the IS chain. Prepared and applied a quantitative research on these aspects, presenting the results obtained, as well as suggestions to reduce the vulnerability of employees of organizations.

Keywords*: information security; social engineer; human factor.*

AGRADECIMENTO

Em primeiro lugar quero agradecer a Deus por permitir estar realizando este curso e me dar a oportunidade de adquirir conhecimento na área de Segurança da Informação, aprimorando-o durante esses anos de curso. Foi um tempo muito precioso, com muitos desafios, conquistas e um período de muito “networking”, comunicação e relacionamento interpessoal com diversos tipos de pessoas, colegas de profissão que muito contribuíram para o meu desenvolvimento ao longo do curso.

Em segundo lugar agradeço aos meus pais, que foram os maiores conselheiros, incentivadores e contribuidores para que eu chegasse até aqui. Sem eles confesso que teria desistido curso; não chegaria até o fim.

Em terceiro lugar eu agradeço aos meus amigos e familiares, que me deram muito apoio e incentivo no decorrer desses anos.

Finalmente, através dos incentivos que de todos recebi e, em especial, aqueles que recebi de minha professora e orientadora, Profª Juliane Borsato Beckedorff Pinto, consegui persistir até o fim. Eu não chegaria aonde consegui chegar, se não fosse pela minha dedicação e esforço.

Foi um grande desafio para mim, mas valeu a pena persistir e concluir com êxito. A palavra que fica é gratidão.

DEDICATÓRIA

Aos meus pais, Paulo Rogério Felisberto Romualdo e Shirlei Antonia da Silva Romualdo, dedico este trabalho de graduação, pois tudo o que conquistei foi por conta deles.

Também dedico ao meu avô Jair Romualdo, por ser um exemplo de pessoas em minha vida.

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Desde o uso do primeiro computador em larga escala, no início da década de 1940, os avanços tecnológicos relacionados ao *hardware* e ao *software* das máquinas têm evoluído de forma muito rápida. Sistemas computacionais foram desenvolvidos, com o objetivo de processar dados e produzir informações. Essas informações eram reunidas pelos dirigentes das organizações, para melhorar a produtividade, os lucros e reduzir custos.

Com o surgimento da Internet, tornando-se disponível a todos em pouco espaço de tempo, a evolução das máquinas e dos sistemas computacionais tornou-se mais dinâmica. Sistemas computacionais tornaram-se mais complexos e receberam a denominação de sistemas de informação. E as organizações passaram a ter os resultados do processamento de seus dados de forma mais rápida e organizada. Seus negócios puderam ser apresentados a um maior número de pessoas físicas e jurídicas. Passaram, também, a desenvolver aplicações utilizando a Internet.

A partir da implementação do *e-commerce*, em 1995 nos EUA, e após cinco anos estabelecendo-se no Brasil, as vendas por *e-commerce* têm crescido sistematicamente, aumentando o faturamento das instituições. O número crescente de potenciais consumidores, de diversas faixas etárias, utilizando a Internet e a facilidade de se realizar transações, são os dois principais motivos para o aumento de faturamento das organizações (TOREZANI, 2008).

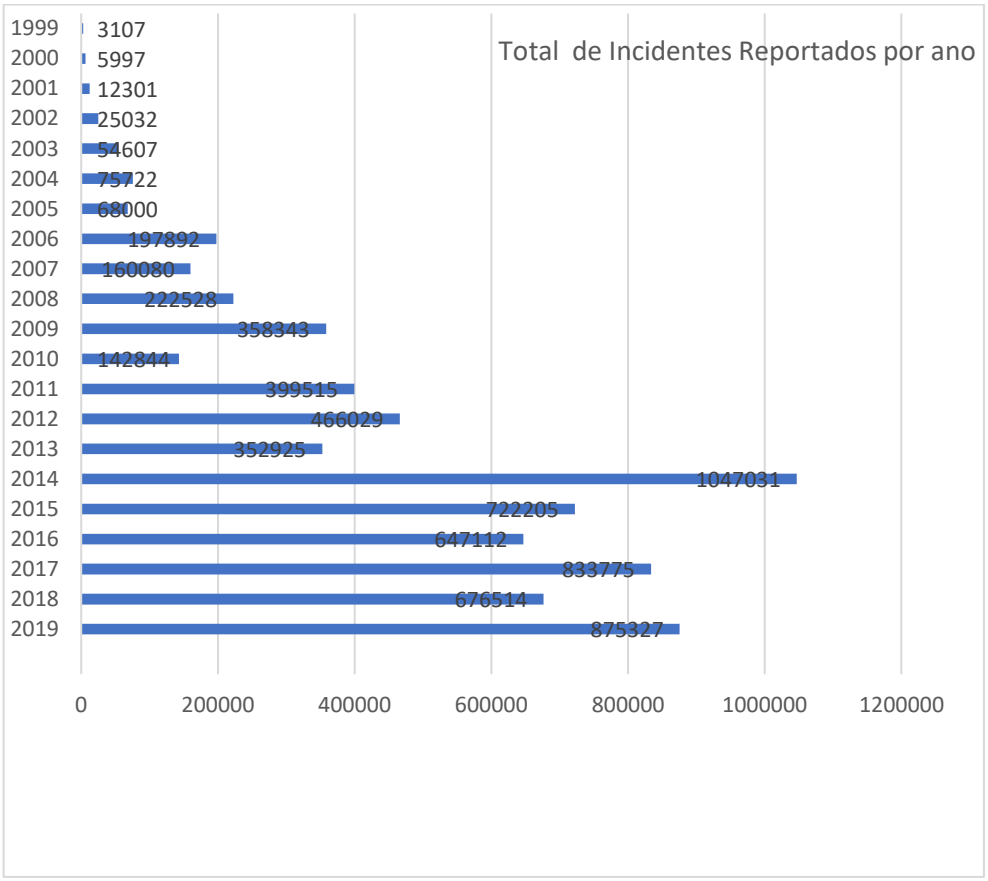
O uso da Internet e sua disponibilidade cada vez maior às pessoas provocaram a necessidade de proteção de informações de pessoas físicas e jurídicas.

O crescimento e a evolução de ameaças e ataques, bem sucedidos ou não, realizados por *hackers, crackers* e engenheiros sociais, indivíduos especialistas nesses tipos de ações, mostraram a necessidade de adoção de políticas de segurança da informação (SI), de monitoramento e aprimoramento dos controles dessas ameaças ou ataques, pois se bem sucedidos podem provocar prejuízos expressivos para as instituições e para as pessoas usuárias da rede, de maneira geral (MAULAIS, 2016).

Os incidentes relacionados a ataques a organizações são reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Grupo de Respostas a Incidentes de Segurança para a Internet Brasileira, mantido pelo Comitê

Gestor da Internet no Brasil), CERT.br. O Gráfico 1, a seguir, mostra a evolução dos incidentes, no período entre 1999 e 2019.

Gráfico 1 – Incidentes reportados ao CERT.br, entre 1999 e 2019.



Fonte: CERT.br, 2019

Maulais (2016), tem suas afirmações reforçadas pelos números apresentados no Gráfico 1.

As informações sobre o aumento de ataques às instituições e às pessoas, despertou o interesse do autor deste trabalho. Principalmente por saber da existência de políticas de segurança para mitigação desses ataques, bem como saber que muitos pesquisadores da área de segurança de Sistemas de Informação – SI afirmam que o elo mais fraco da segurança é o ser humano (FONSECA, 2017).

O escopo deste trabalho aborda questões da segurança da informação e os principais tipos de ataques sofridos pelas organizações atualmente, perfis dos indivíduos que provocam esses ataques e as principais técnicas utilizadas por eles,

bem como aspectos relacionados ao elo mais fraco da cadeia de segurança, ou seja, o ser humano.

O problema proposto pelo trabalho é obter informações para tentar responder uma questão sobre SI, que persiste. Mesmo com a existência e evolução de ferramentas utilizadas para contenção de ataques à segurança da informação de organizações em geral, além da existência de políticas de segurança da informação adotadas pelas instituições.

A questão pode ser expressa na pergunta: é possível mitigar os ataques às organizações, abordando formas de educação e treinamento contínuos, propostos aos colaboradores das instituições?

O objetivo geral deste trabalho é analisar as principais técnicas de ataques relatadas na literatura, usadas principalmente por engenheiros sociais, sabendo que o elo mais fraco da cadeia de segurança é o ser humano, buscando recursos na bibliografia estudada, para melhorar a mitigação desses ataques.

Pretende-se alcançar o objetivo geral deste trabalho através dos objetivos específicos relacionados a seguir:

- Apresentar os conceitos de segurança da informação;
- Identificar os principais tipos de ataques relatados que ocorrem nas organizações;
- Analisar as principais técnicas de ataques às organizações utilizadas atualmente;
- Apresentar os principais aspectos de perfis de atacantes, principalmente engenheiros sociais;
- Analisar a questão da segurança da informação focando o ser humano, pois é considerado o elo mais fraco na cadeia de segurança;
- Realizar e analisar os resultados de uma pesquisa quantitativa, aplicando um questionário, focando em um universo potencialmente sujeito a ataques (Apêndice A);
- Usar os resultados obtidos na pesquisa para sugerir formas de controle às pessoas e às organizações, na tentativa de melhorar a mitigação de ataques.

O tipo de metodologia utilizada neste trabalho é a metodologia exploratória descritiva. Serão realizadas pesquisas bibliográficas sobre segurança da informação, políticas de segurança da informação, perfis de atacantes (*hackers, crackers* e engenheiros sociais) e perfil do elo mais fraco da cadeia de SI.

A abordagem utilizada na metodologia é a pesquisa quantitativa, para obter resultados indicativos de ataques e perfis dos indivíduos que sofreram esses ataques.

O universo da pesquisa é composto por pessoas que responderam questionário elaborado pelo autor (Apêndice A), visando a responder à questão apresentada na problematização deste trabalho.

A estrutura deste trabalho prevê:

- Capítulo 1, a apresentação do referencial teórico utilizado no trabalho, envolvendo conceitos de segurança da informação e principais tipos de ataques que ocorrem atualmente;
- Capítulo 2 apresenta o referencial teórico sobre conceitos dos perfis de atacantes, características e técnicas utilizadas por engenheiros sociais, bem como características do elo mais fraco da cadeia de SI;
- O Capítulo 3 descreve a pesquisa quantitativa realizada, apresentando e discutindo os resultados obtidos;
- O Capítulo 4 destaca questões de SI, engenharia social e indivíduos que sofreram ataques, relatados na pesquisa, apresentando sugestões para a mitigação de ataques à SI;
- O Capítulo 5 apresenta as considerações finais deste trabalho.

1 SOBRE SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta conceitos sobre informação, segurança da informação (SI), ocorrência de ataques às organizações, principais ataques praticados atualmente, conforme literatura estudada e normas da ABNT relacionadas à SI.

1.1 Sobre Segurança da Informação

O surgimento de computadores de grande porte, a rápida evolução destes equipamentos para os chamados micro computadores e o aparecimento de diversas linguagens de programação, adequadas para diversos tipos de aplicações, provocaram constante e rápida mudança nas áreas de *software* e de *hardware.*

O aparecimento da Internet (na década de 1980) é uma das consequências dessa dinâmica.

Inicialmente a Internet era usada para troca de dados em pesquisas acadêmicas, sendo utilizada por instituições universitárias e de pesquisa. Rapidamente evoluiu para a comunicação e troca de informações entre organizações e pessoas (SIPAHI, 2012).

Segundo Michaelis (2016), a informação é o resultado produzido pelo conhecimento de fatos e de dados, sendo fornecida a alguém com finalidade específica. A informação de organizações produzida pelo processamento de dados é o ativo mais importante dessas organizações, recomendando-se sua proteção, como todos os outros ativos das instituições (CHIAVENATO, 2005).

O processo de evolução das ferramentas ligadas à informação continuou e persiste até hoje.

A utilização da Internet ampliou-se para outros tipos de equipamentos, tais como telefones celulares, *notebooks, tablets, Smart* TV.

A Internet passou a ser usada, também, em diversas áreas e por diversos tipos de perfis de pessoas físicas e jurídicas. Algumas delas são: medicina, sistemas de trânsito e educação. A utilização da rede cresceu rapidamente, não apenas nas organizações, mas pessoas de diversas faixas etárias têm mais facilidades de acesso à Internet (SILVA, T.; SILVA, L., 2017).

Uma das consequências mais sérias, com o crescente uso da rede para as mais diversas aplicações, foi o aparecimento de ataques à rede, focando organizações de diferentes perfis, bem como usuários da rede de maneira geral.

Esses ataques são feitos, geralmente, por pessoas mal intencionadas, com os mais diversos objetivos (HENRIQUES, 2016).

Os ataques são realizados na tentativa de obterem facilidades pessoais, tais como acesso indevido a contas bancárias, objetivando recursos alheios; venda (em proveito próprio) de informações confidenciais obtidas irregularmente, golpes aplicados a pessoas, para obtenção dos mais diversos recursos. As pessoas que realizam esses ataques são chamadas de *hackers, crackers* e engenheiros sociais (MITNICK; SIMON, 2003). Os tipos de ataques são diversificados e a próxima seção trata sobre este tema.

1.2 Tipos de Ataques às redes de organizações

Os ataques realizados aos sistemas de informação das organizações podem ser classificados de diversas formas. Uma delas é considerar dois grandes conjuntos de ataques: ataques cibernéticos (específicos, relacionados às políticas internacionais e seus respectivos governantes) e os ataques cibernéticos relacionados às redes de organizações que não fazem parte do conjunto anterior.

Registros relacionados a ataques cibernéticos e à guerra cibernética mostram que o primeiro ataque deste tipo ocorreu em 1982, provocado pelos Estados Unidos contra a então União Soviética (COMPUGRAF, 2020). O escopo deste trabalho não engloba questões relacionadas a esses tipos de ataques, portanto não serão abordados no trabalho.

Após diversas pesquisas bibliográficas realizadas, encontrou-se a informação sobre o registro do primeiro ataque (não relacionado à guerra cibernética) ocorrido a redes de computadores de organizações. Mitnick e Simon (2006), relatam o primeiro ataque a redes de computadores das organizações com ocorrência no final da década de 1980.

Em 2017 uma empresa brasileira ligada à Segurança da Informação, *GoCache next-gen CDN*, realizou uma pesquisa listando os dez países que mais ataques sofreram naquele ano. Os ataques foram feitos por diversos motivos e o resultado da pesquisa é visto na Tabela 1, a seguir.

Tabela 1 - Dez países que sofreram mais ataques na área de S.I.

1	**CHINA**
2	**ESTADOS UNIDOS**
3	**TURQUIA**
4	**RÚSSIA**
5	**TAIWAN**
6	**BRASIL**
7	**ROMÊNIA**
8	**INDIA**
9	**ITÁLIA**
10	**HUNGRIA**

Fonte: *GoCach*e, 2017

Em 2019 essa classificação foi atualizada por outra empresa brasileira, denominada *AllEasy*, especializada na área de SI e localizada na cidade de São Paulo, SP. A empresa fez uma publicação mostrando que o Brasil está em terceiro lugar entre os países que mais ataques sofreram na área de SI. China e Estados Unidos continuam liderando essa lista (ALLEASY, 2020).

Os ataques documentados por essas empresas são diversificados, mas a predominância desses ataques é apresentada na Tabela 2, a seguir.

Tabela 2 – Principais tipos de ataques aplicados às organizações

1	*PHISHING*
2	*SPEAR PHISHING*
3	*BAITING*
4	*PRETEXTING*
5	*QUID PRO QUO*
6	*TAILGATING*

Fonte: POSITIVO TECNOLOGIA, 2018

O primeiro tipo de ataque, *phishing,* é bastante conhecido. Os primeiros registros deste tipo de ataque são de 1997. É uma técnica que utiliza *e-mails* falsos estimulando quem os recebe a executar algum tipo de ação que será prejudicial a alguém (pessoa física ou jurídica) (GUISSO, 2017).

O ataque *spear phishing* é similar ao *phishing,* porém o objetivo do atacante é sempre algum tipo de organização. O atacante utiliza um *e-mail* para colaboradores

do foco de seu ataque e na suposição de que conseguirá enganar algum deles, tenta obter os benefícios pretendidos.

Baiting é um tipo de ataque bastante conhecido, cujo registro de utilização desta técnica indica o início da década de 2000. É uma técnica na qual o atacante finge esquecer um *pen drive* ou outro tipo de dispositivo de armazenamento de informação no local que é o foco de seu ataque. Geralmente algum colaborador curioso utiliza o dispositivo para conhecer seu conteúdo. E o objetivo do atacante é alcançado, pois consegue que seja instalado algum tipo de *malware* através do dispositivo (POSITIVO TECNOLOGIA, 2018).

Pretexting (palavra que pode ser traduzida como pretexto) é uma abordagem na qual o atacante utiliza uma ou mais técnicas para convencer alguma pessoa a fornecer informação importante e que tenha alguma utilidade para o atacante. A pessoa que sofre o ataque pode trabalhar em alguma organização na qual o atacante esteja interessado ou pode ser uma pessoa sofrendo um ataque para fornecer algo de interesse do atacante (POSITIVO TECNOLOGIA, 2018).

A técnica T*ailgating* é uma técnica anterior ao uso da Internet. O atacante consegue obter a forma de entrada em locais controlados eletronicamente, usando alguma técnica de persuasão junto à pessoa responsável pelo acesso ao local (POSITIVO TECNOLOGIA, 2018).

O ataque Q*uid pro Quo* é uma técnica na qual o atacante oferece algum tipo de benefício muito atraente à pessoa que está sendo atacada, como por exemplo, um tipo de prêmio (viagens, produtos geralmente de alto custo, entre outros). Caso a pessoa aceite, precisa preencher um tipo de formulário. Nos campos a serem preenchidos há informações que são confidenciais e a pessoa não percebe que as forneceu. A propósito, o termo Q*uid pro Quo* deriva do latim e tem um significado semelhante a trocar alguma coisa por alguma coisa (MAGALHÃES, 2020).

Os ataques são realizados por pessoas (ou grupos de pessoas) com bons conhecimentos na área de tecnologia da informação - TI e cujo principal objetivo é ter acesso às informações confidenciais, tirando proveito do uso dessas informações de diversas maneiras.

Há razões menos frequentes, tais como vencer desafios, invadindo sistemas de informação conhecidos como seguros ou até mesmo por questões sociais, podendo divulgar posteriormente seus feitos aos grupos aos quais pertencem (AGUADO; CANOVAS, 2017).

Geralmente os ataques são feitos por códigos maliciosos, *malware,* objetivando algum tipo de interesse pessoal do atacante (lucro com dados confidenciais obtidos por roubo; vaidade pessoal do atacante, entre outros). Há diversos tipos de códigos maliciosos e sua característica principal é a capacidade de acesso a dados e execução de comandos na máquina infectada por esses códigos (CERT.br, 2012).

A Tabela 3, a seguir, mostra os incidentes reportados em 2019 ao CERT.br.

Tabela 3 – Incidentes reportados ao CERT.br (classificados por tipo de ataque)

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019

Tabela: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)		**dos** (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**62481**	7796	12	4191	6	19	0	2594	4	46038	73	1744	2	99	0
fev	**70069**	7707	11	2192	3	27	0	4179	5	54401	77	1459	2	104	0
mar	**85409**	4476	5	29309	34	19	0	2006	2	47966	56	1521	1	112	0
abr	**59900**	7624	12	2718	4	37	0	1555	2	45774	76	2119	3	73	0
mai	**52129**	6555	12	15773	30	74	0	1425	2	25521	48	2633	5	148	0
jun	**221231**	6598	2	191593	86	52	0	1337	0	19289	8	2230	1	132	0
jul	**48836**	8230	16	3884	7	27	0	1308	2	32054	65	2994	6	339	0
ago	**61006**	11421	18	5892	9	51	0	1561	2	37521	61	4400	7	160	0
set	**52027**	9599	18	7326	14	28	0	1876	3	27654	53	5388	10	156	0
out	**53253**	10568	19	8313	15	45	0	2219	4	26153	49	5859	11	96	0
nov	**59735**	7032	11	25701	43	80	0	625	1	20450	34	5795	9	52	0
dez	**49251**	12871	26	4416	8	68	0	1649	3	26927	54	3277	6	43	0
Total	**875327**	100477	11	301308	34	527	0	22334	2	409748	46	39419	4	1514	0

Fonte: Cert.br, 2019

Em relação à Tabela 3, o relatório de totais de incidentes apresentados por CERT.br tem uma legenda que resume os conceitos de cada um dos tipos de ataques, a saber:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores (CERT.br, 2019).

1.2.1 Tipos de Ataque *Ransomware*

Este tipo de ataque ganhou destaque com a pandemia, aumentando em mais de 350% no primeiro trimestre de 2020. Os dados são da organização Kaspersky (2020), especialista em segurança digital. A organização atribui este aumento ao regime de trabalho *home-office*, adotado pelas organizações de maneira geral, em função da pandemia (CANALTECH, 2020).

Vale lembrar que a tradução da palavra *ransom* é resgate. Os primeiros ataques do tipo *Ransomware* surgiram em 2005, através de denúncias feitas na Rússia. Um ataque do tipo *Ransomware* ocorre quando o computador é infectado por um *software* malicioso, bloqueando a máquina. Apresenta mensagens que exigem pagamento de um determinado valor para permitir que o computador volte a funcionar. O *software* malicioso pode ser instalado na máquina através de *sites, links* falsos, fornecidos por *e-mails* e mensagens instantâneas. Este tipo de ataque pode bloquear a tela do computador ou criptografar (usando senha) arquivos considerados importantes (KARSPERSKY, 2020).

Os valores cobrados podem variar, mas, mesmo que sejam pagos, não há garantia de o bloqueio feito à máquina ser retirado.

Há diversas famílias de *Ransomware*, relacionadas a seguir:

- *Cerber:* o *software* malicioso é instalado na máquina através de *e-mails* de *spam*, exigindo pagamento de resgate em até uma semana. O método de ataque é através de infecção de arquivos e adição da extensão ". *cerber";*
- *Cryptolocker:* o *software* malicioso é instalado na máquina através de técnicas de engenharia social, convencendo a pessoa que sofre o ataque a realizar o *download* do *software* malicioso. Quando a pessoa atacada abrir o arquivo o *software* malicioso gera diversas chaves de criptografia;
- *Cryptowall:* após ser instalado na máquina, o *software* malicioso consegue 'enganar' o antivírus instalado no computador e criptografar arquivos;
- *Jigsaw:* após ser instalado na máquina, o *software* malicioso apaga arquivos de hora em hora. É uma estratégia usada para a pessoa atacada realizar o pagamento solicitado e não perder informações de sua máquina;

- *Locky:* o *software* malicioso é instalado na máquina através de *e-mails* de *spam e sites* comprometidos. Instala a extensão ". *locky"* aos arquivos criptografados;
- *Petya:* o *software* malicioso é instalado na máquina através de um *link* do *Dropbox.* Tem a capacidade de criptografar um disco rígido inteiro, em uma única ação. Esse tipo de ataque, geralmente, é direcionado aos colaboradores de recursos humanos de uma organização;
- *Wanna Cry:* o *software* malicioso é instalado na máquina através de um ataque do tipo *phishing,* usando *e-mail* contendo um *link* ou arquivo ".pdf" maliciosos. Se o ataque do tipo *phishing* for bem sucedido, o *software* malicioso tenta infectar a rede usando o protocolo *SMB (Server Message Block)*. Tenta atacar uma vulnerabilidade de sistemas *Windows* denominada *EternalBlue* (corrigida pela *Microsft* em 2017*)* (PROOF, 2018).

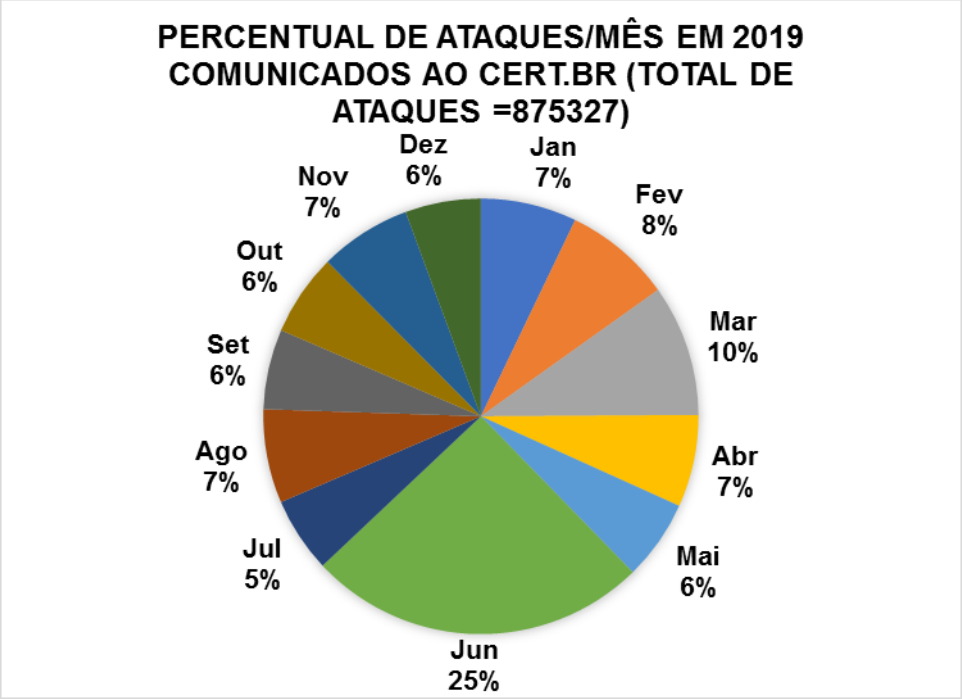
Sabe-se que pesquisas indicam crescimento exponencial de ataques do tipo *ransomware* durante a pandemia de 2020. Os atacantes usam este tipo de ataque com mais frequência, durante a pandemia, porque os colaboradores trabalham remotamente e nem sempre seguem todas as orientações de políticas de segurança da informação, vigentes nas organizações onde trabalham. Outro fator que facilita este tipo de ataque é o uso do recurso *Remote Desktop Protocol – RDP*, pois este recurso facilita a instalação de *software* malicioso (CIO, 2020).

A Lei Geral de Proteção de Dados – LGPD, determina que organizações de maneira geral precisam mostrar às autoridades do Brasil que possuem condições para garantir a manutenção de informações de forma segura, através de políticas de segurança da informação adequada (CIO, 2020).

1.3 Políticas de Segurança da Informação

Mitinick e Simon (2003), registraram o primeiro ataque no final da década de 1980 e desde então as organizações passaram a se preocupar com questões de segurança da informação. O Gráfico 2, a seguir, mostra os totais de ataques (por mês), às redes de organizações, comunicados ao CERT.br, em 2020.

Gráfico 2 – Total de ataques/mês - 2019 (comunicados ao CERT.br)



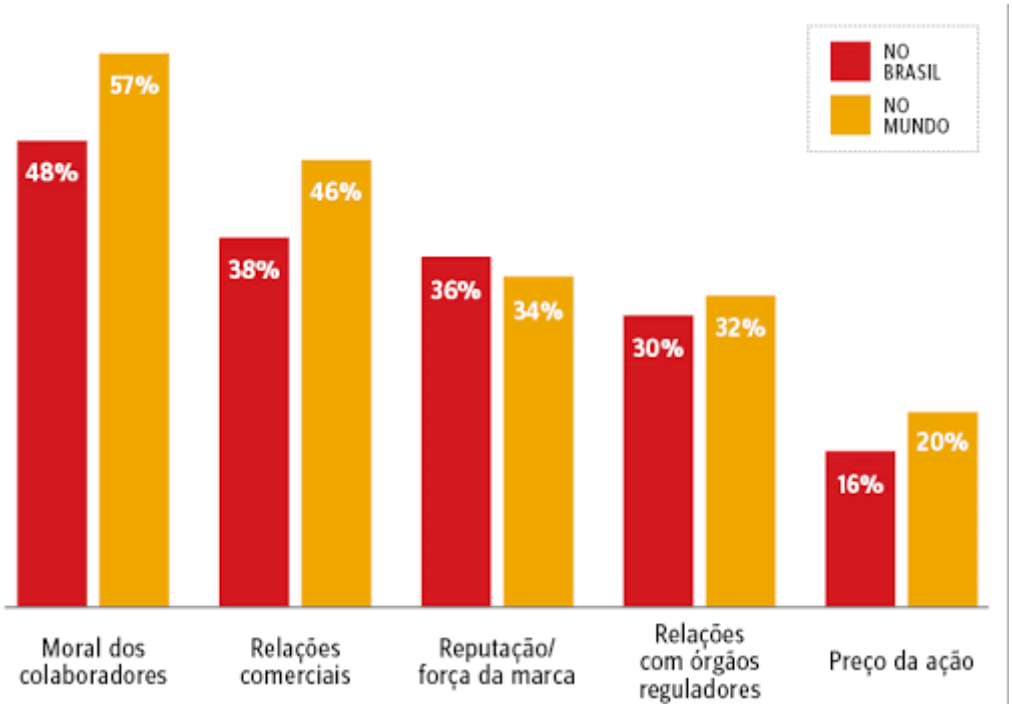
Fonte: CERT.br, 2020

Os percentuais apresentados no Gráfico 2 representam ataques de diversos tipos, tais como *worm,* invasão, *scan* e fraudes (entre outros) e indicam altos índices de valores. O crescimento persistente de ataques às redes de organizações mostraram a necessidade de maior eficiência na proteção e defesas contra essas investidas.

Maulais (2016), recomenda que proteções e defesas englobem desde aspectos físicos das instalações, ferramentas que auxiliam na mitigação de ataques que possam ocorrer, incluindo todos os colaboradores direta ou indiretamente envolvidos, sugerindo treinamentos e atualizações frequentes de todos os aspectos ligados à segurança da informação.

Questões relacionadas aos prejuízos e danos que ataques cibernéticos causam às organizações envolvem mais do que a parte financeira, como mostra o Gráfico 3, a seguir.

Gráfico 3 – Tipos de danos causados por ataques às organizações
2018



Fonte: GRUPO BETTENCOURT, 2018

Segundo Fontes (2001), o uso de políticas e regras para proteger a informação das organizações é tão importante quanto as políticas relacionadas aos recursos financeiros e materiais das instituições, pois se trata de um recurso importante e crítico para a continuidade dos negócios e preservação da missão de cada uma das organizações. No Brasil há organizações com manuais ou cartilhas relacionados às políticas de segurança da informação.

Tem-se conhecimento da cartilha de segurança para Internet da organização Cert.br, detalhando aspectos de segurança da informação, tipos de ataques e modos de proteção (CERT.br, 2012).

Outra instituição brasileira que possui cartilha sobre segurança da informação, tipos de ataques realizados por engenheiros sociais e orientações para reconhecer tentativas de ataques é a Federação Brasileira de Bancos – FEBRABAN (FEBRABAN, 2017).

Maulais (2016), argumenta que empresas são vulneráveis à medida que algum tipo de sistema ou ferramentas de proteção apresentem falhas ou fragilidade, deixando a informação disponível de forma inadequada. Isso pode incentivar ataques e provocar danos e prejuízos às organizações. Cita exemplos de vulnerabilidade tais

como aspectos relacionados aos colaboradores das organizações, falhas de *hardware* ou de *software,* formas inadequadas de organização e armazenamento da informação que interessa ao negócio das organizações.

Alexandria (2009), apresenta um conjunto de recomendações na área de gestão de SI para otimizar aspectos ligados à segurança em ambientes de pesquisa científica. Essas recomendações podem ser ampliadas para ambientes de organizações em geral.

A organização brasileira, PROOF, criada em 2008, publicou (em seu *blog*) recomendações sobre como criar e otimizar as Políticas de Segurança da Informação – PSI, nas organizações (PROOF, 2008) e (PROFF, 2017).

PSI é um documento que apresenta orientações e diretrizes de SI da organização, com o objetivo de proteger o ativo informação das instituições. Este documento deve englobar todas as áreas das organizações e estar alinhado à norma ABNT NBR ISO/IEC 27001:2005.

A organização recomenda que o conteúdo do documento PSI deve englobar responsabilidades dos colaboradores; responsabilidades da área de Tecnologia da Informação - TI; informações relacionadas à logistica ligada à implementação de TI nas organizações; tecnologias de defesa contra ataques; política de treinamento dos colaboradores. Apresenta, também, uma sequência de passos para uma campanha bem sucedida de divulgação e implementação da PSI e recomendações para que a política de SI funcione na prática (PROOF, 2017).

Bach (2001), recomenda mais atenção e cuidados às organizações de pequeno e médio porte, no que diz respeito à segurança da informação, pois algumas delas são alvos prediletos de *crackers,* visto que costumam ocorrer muitas brechas no quesito segurança dessas instituições.

Na literatura estudada, o ponto comum está sempre relacionado à existência de políticas de segurança da informação, qualquer que seja o porte da organização.

A literatura recomenda, também, uso de alguma metodologia de apoio ao plano de segurança da informação, sendo desenvolvida pela organização ou sendo alguma metodologia existente como, por exemplo, COBIT (*Control Objectives for Information and related Technology)*, certificação e alinhamento com a norma ABNT NBR ISO/IEC 27002 (ALEXANDRIA, 2009).

Fonseca (2017), recomenda que o plano de segurança de informação das organizações dê atenção à política de educação continuada a seus colaboradores,

fornecendo treinamento e informações de forma clara e objetiva. Sugere que a política de educação continuada tenha características tais como disciplinar e reforçar o aprendizado, além de fiscalizar sua aplicação e utilização.

1.3.1 Sobre as normas de ISO/IEC relacionadas à segurança da informação

A sigla ISO é uma sigla da organização *International Organization of Standardization* e a sigla IEC representa a organização *International Electrotechnical Commission* (I9 CONSULTORIA E CONTABILIDADE, 2019).

A ISO 27001 é uma das principais normas visando a garantia de implementação de políticas de segurança da informação, nas organizações de maneira geral.

A implementação da norma ISO 27001 requer certificação e possui 16 etapas, organizadas de forma semelhante à de um algoritmo. A primeira etapa é ter o apoio da direção da organização e a última etapa é a previsão de ações corretivas em etapas que deixaram algum(uns) item(ns) a desejar.

A organização certificada e que adota a ISO 27001, alinhada aos principais requisitos internacionais sobre SI, pode garantir contratos internacionais com outras organizações. Vale lembrar que a implementação e utilização correta desta norma garante alinhamento com a maioria das legislações de proteção de dados, inclusive com a Lei Geral de Proteção de Dados – LGPD (STRONGSECURITY, 2019).

A norma ABNT NBR ISO/IEC 27001:2005 especifica como colocar em prática um sistema de gestão de segurança da informação que tenha sido avaliado e certificado (ABNT, 2006).

Para padronizar a certificação relacionada às questões de proteção geral de dados foi publicada a norma ISO 27701, em agosto de 2019. Esta norma é considerada um marco para a gestão contínua de riscos que envolvem privacidade de informação, pois diz respeito ao estabelecimento de requisitos para um sistema de gerenciamento de privacidade de informações (JUSBRASIL, 2019).

Destaca-se que a norma ISO 27001 trata de questões relacionadas a sistema de gerenciamento de segurança da informação e a norma ISO 27002 relaciona-se a códigos de boas práticas de gestão de sistemas de segurança da informação (ABNT, 2013).

A norma ISO 27701 é uma extensão da norma ISO 27001. É considerada como um guia de orientação sobre como fazer para estar em conformidade com a LGPD e

com a *General Data Protection Regulation – GDPR.* Organizações certificadas nas normas ISO 27001 e ISO 27701, que seguem corretamente estas normas, dão um salto de qualidade nas questões de SI e proteção de dados considerados confidenciais e privados e podem ampliar suas atividades junto a outras organizações que requerem a certificação e adoção destas normas como padrão (JUSBRASIL, 2019).

2 SOBRE PERFIS DE ATACANTES, ENGENHEIRO SOCIAL E O ELO MAIS FRACO DA CADEIA DE SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta conceitos sobre perfis de atacantes, como surgiram esses atacantes, seus objetivos e denominações atribuídas a eles. Apresenta, também, o aparecimento de atacantes exercendo o papel de engenheiros sociais e o porquê desta denominação. Descreve os principais objetivos dos engenheiros sociais, focando no elo mais fraco da cadeia de segurança da informação, que é o ser humano. Destaca os tipos de abordagens realizadas pelos engenheiros sociais no planejamento de seus ataques e as consequências provocadas por esses ataques.

2.1 *Hackers, Crackers* e Engenheiros Sociais

Raymond (1999), indica que o termo *hacker* surgiu em 1961, em conhecida instituição de pesquisa e desenvolvimento, denominada *Massachussets Institute of Technology – MIT*, nomeando os estudantes daquela instituição que mais se dedicavam a conhecer as novas tecnologias de informática usadas por eles (além do que os estudos exigiam na época).

Bach (2001), define *hacker* como uma pessoa ligada à área de tecnologia de informática, com conhecimentos profundos na área de programação (dominando diversas linguagens e técnicas de programação) e de sistemas operacionais. *Hackers* são capazes de alterar e otimizar códigos, compartilhando seus conhecimentos com a comunidade de TI. Auxiliam pessoas a melhorar proteções em redes de computadores, procuram aprimorar seus conhecimentos e sentem-se atraídos por desafios.

Aguado e Canovas (2017), confirmam os conceitos apresentados por Bach (2001). Segundo eles os *hackers* possuem uma ética orientada a aprendizagem, colaboração, ampliando seus conhecimentos e contribuindo para melhorar o conhecimento de profissionais da área de TI. São dedicados, gostam do que fazem, consideram o que fazem uma verdadeira missão e prezam sua liberdade para continuar suas atividades.

Mitnick e Simon (2006), destacam que muitos *hackers*, em algum momento de suas vidas, mudaram de comportamento e passaram a usar seus conhecimentos para obtenção de benefícios que vão além do reconhecimento de seus trabalhos e contribuições.

É justamente esta mudança de comportamento que faz com que um *hacker* se torne um *cracker* (MITNICK; SIMON, 2006).

Bach (2001,) destaca alguns aspectos interessantes. Muitas pessoas usam os termos *hacker* e *cracker* como sinônimos, mas não são. Também na literatura esses termos são encontrados como sinônimos.

É justamente o comportamento de cada um deles que faz a diferença. Ambos possuem excelentes conhecimentos de tecnologia e usam esses conhecimentos na execução de suas atividades, porém o *cracker* faz uso de suas habilidades em benefício próprio, sem se preocupar com os danos causados. Essa postura é muito diferente da postura dos *hackers* e isso diferencia seus perfis (BACH, 2001).

Geralmente os *crackers* preferem ataques a organizações de pequeno e médio porte, pois as políticas de segurança dessas instituições possuem diversas brechas.

Mas há aqueles que aceitam atacar organizações de grande porte, geralmente para realizar algum tipo de espionagem, recebendo grandes recompensas por suas ações. Kevin Mitnick é citado como um dos *crackers* mais famosos mundialmente (BACH, 2001).

O termo engenharia social surgiu no final de 1980, com Kevin Mitnick (MITINICK, SIMON, 2003).

Gaspar (2015), comenta que o crescente uso de ferramentas, cada vez mais sofisticadas, para proteger os sistemas de informação, fez com que atacantes de SI mudassem as abordagens de ataques a esses sistemas. O foco passou a ser o lado humano relacionado à área de SI (direta ou indiretamente). Também comenta que a estratégia de exploração de fragilidades do ser humano trabalhando direta ou indiretamente com segurança e sistemas de informação fez surgir a engenharia social (GASPAR, 2015).

Mitnick e Simon (2003), consideram a engenharia social como a capacidade de iludir e persuadir os colaboradores de organizações a fornecer informações sigilosas da instituição, usando ou não a tecnologia.

Gaspar (2015), entende a engenharia social composta por um ou mais atos fraudulentos, por parte dos atacantes (engenheiros sociais), induzindo colaboradores de boa-fé a fornecerem as informações que os atacantes desejam.

Há duas formas de o engenheiro social realizar seus ataques, a forma direta e a forma indireta.

Os ataques diretos são bem planejados pelos engenheiros sociais. Estudam muito bem os alvos de seus ataques, usando diversos recursos, inclusive as redes sociais. Entram em contato com os colaboradores das organizações, pessoalmente ou por telefone, após conhecer melhor o alvo de ataque. Caso alguma coisa não dê certo, eles já possuem um plano preparado para não serem descobertos, pois são eficientes no planejamento de todas as etapas para realizar seus ataques (CARMO, 2017).

Os ataques indiretos usam *e-mail, sites* falsos ou outras maneiras de inserir códigos falsos ou maliciosos a colaboradores de organizações, visando a obtenção de dados confidenciais dessas instituições em proveito próprio.

A abordagem mais comum é o uso do método indireto, pois assim os engenheiros sociais ficam menos expostos (GASPAR, 2015).

Zager (2002), relaciona os principais motivos que incentivam um engenheiro social a realizar ataques. São eles:

- ganho financeiro: neste caso o engenheiro social realiza o ataque em proveito próprio. Geralmente, neste caso, o alvo do atacante é sempre prejudicado;
- interesse pessoal: o engenheiro social faz o ataque por diversão, curiosidade;
- ações sem intenções danosas, promovidas pelo engenheiro social: são ataques que podem provocar danos ao alvo que está atacando;
- desafio intelectual: o engenheiro social age por vaidade, mostrando que é possível atacar o alvo. Mesmo não tendo a intenção de prejudicar o alvo, pode causar sérios danos;
- vantagem competitiva: o engenheiro social realiza o ataque com finalidades de espionagem que podem trazer-lhe vantagens competitivas;
- pressão externa: o engenheiro social realiza o ataque sob pressão, para mostrar suas habilidades. Essa pressão pode vir dele próprio, por querer fazer parte de algum tipo de comunidade de engenheiros sociais, de algum grupo ao qual pertence, amigos e até mesmo familiares. As intenções do ataque podem variar, dependendo do motivo que o leva a realizar o ataque;
- ataque político: esse tipo de ataque recebe essa denominação, mas o motivo do ataque pode ser religioso, político, ambiental, entre outros e pode levar a sérias consequências, pois o atacante deseja tornar-se conhecido por seu feito;

- contenção de danos: neste tipo de ataque, o engenheiro social pretende minimizar os danos causados por um ataque anterior (realizado por ele ou não). Pode, ainda, querer auxiliar pessoas ou organizações para que melhorem ou corrijam as vulnerabilidades existentes em sistemas de informação.

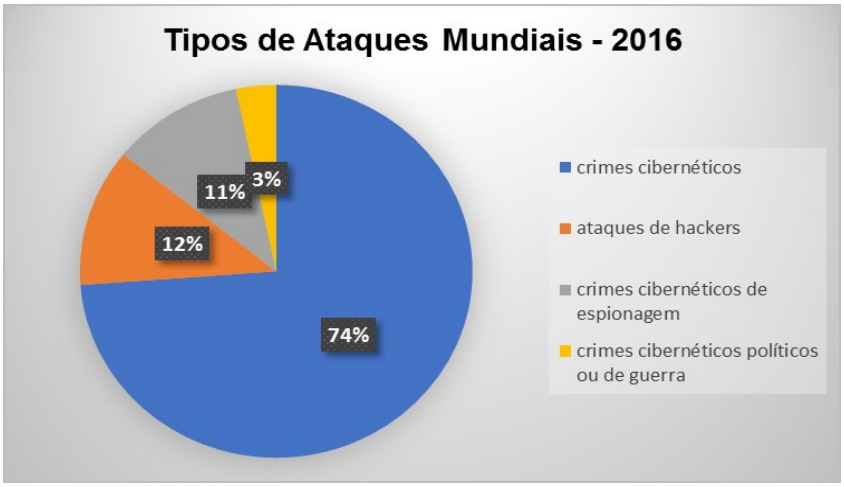
Qualquer que seja o motivo, percebe-se que o atacante denominado engenheiro social é vaidoso, organizado e tem forte capacidade de persuasão. Organiza seus ataques usando quatro etapas.

A primeira etapa é, após a escolha do alvo, organizar como será realizado o ataque. A segunda etapa engloba o início de manipulação do alvo. A terceira etapa é a exploração, de forma mais detalhada, de muitos aspectos que o alvo possui, usando sua capacidade de persuasão e conhecimento das características do alvo. A quarta e última etapa é a execução do plano organizado pelo engenheiro social (GASPAR, 2015).

Jaron Lanier lembra que a principal ferramenta usada pelo engenheiro social são as redes sociais. Os engenheiros sociais retiram a maior parte das informações sobre seus alvos nas redes sociais. Lanier apresenta justificativas do porquê as redes sociais são danosas para todos. Aconselha aqueles que participam de alguma rede social a cancelar suas participações. Considera altamente danosa a participação em redes sociais (HYPNESS, 2018).

O Gráfico 4, a seguir, reforça questões relacionadas aos cuidados tomados com as políticas de segurança da informação e melhor conhecimento do ser humano relacionado à tecnologia, conscientizando-se de suas vulnerabilidades.

Gráfico 4 – Ataques Mundiais ocorridos em 2016



Fonte: Crypto, 2019

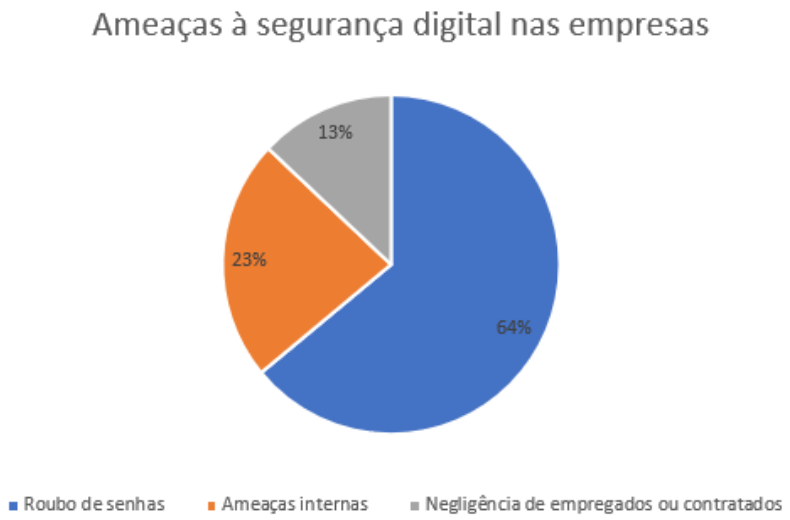
2.2 O elo mais fraco da cadeia de segurança da informação

Mitnick e Simon (2003), afirmam que o elo mais fraco da segurança da informação é o ser humano. Marciano (2009), faz a mesma afirmação, considerando que a corrente, formada por todas as ferramentas e políticas de segurança da informação de uma organização, vai até onde seu elo mais fraco permitir.

O engenheiro social faz uma verdadeira prospecção, objetivando as vulnerabilidades de pessoas e organizações, através do elo mais fraco (MITNICK; SIMON, 2003).

Marciano (2009), indica diversos segmentos ligados à Psicologia estudando, atualmente, os aspectos sociais do ser humano e suas influências na segurança da informação. O Gráfico 5, a seguir, apresenta percentuais de ameaças à segurança das organizações, mostrando a força de ponderação de seus colaboradores.

Gráfico 5 – Influências do elo mais fraco na segurança da informação



Fonte: ATECH, 2019

Negligência de colaboradores, roubos de senha e ameaças internas são algumas das possíveis falhas provocadas por colaboradores de organizações.

No Brasil há uma organização aérea denominada Empresa Brasileira de Aeronáutica – EMBRAER. Esta organização possui um grupo, criado em 1981, com a sigla ATECH – Sistema Avançado de Gerenciamento de Informações de Tráfego Aéreo e Relatório de Interesse Operacional (ATECH, 2017).

O grupo ATECH realizou um estudo, publicado em 2019, associado aos perfis dos colaboradores de organizações. Este estudo indicou as seguintes características de perfis:

- colaboradores que possuem sentimento de propriedade sobre as informações (principalmente informações sigilosas) que manipulam. Explica esse sentimento porque, de maneira geral, esses colaboradores auxiliaram na criação ou processamento de alguma aplicação. Acabam por confundir reponsabilidade sobre essas informações com direitos que possam ter por participarem de seus processos de criação;
- colaboradores com sentimento de vantagem competitiva, considerando que o controle exclusivo das informações e tecnologias que manipulam pode ser útil no futuro, pois são de um ativo de valor expressivo (é um tipo de oportunismo ou postura indicando ética duvidosa desses colaboradores);
- colaboradores que em algum momento de sua trajetória sentem-se injustiçados, utilizam as informações que manipulam como forma de reparar essas injustiças, ou até mesmo se vingar das organizações (vendendo essas informações, por exemplo) (ATECH, 2019).

Fonseca (2017), destaca características de perfis de colaboradores de organizações, explorados por engenheiros sociais, a saber:

- alguns seres humanos possuem necessidade de admiração ou reconhecimento por alguma coisa que tenham feito. Muitos colaboradores de organizações não fogem à regra. Alguns deles comentam com amigos, conhecidos e colegas de trabalho sobre ações realizadas por eles e sobre a imagem que outros têm desses colaboradores. Essa postura torna-os alvos fáceis dos engenheiros sociais;
- alguns seres humanos possuem curiosidades sobre novidades. Desejam adquirir novos conhecimentos e ampliar suas experiências. O que pode variar é o quanto cada um quer aprender, como utilizar conhecimento adquirido e até onde quer que chegue o alcance deste conhecimento. As curiosidades dos seres humanos chamam a atenção dos engenheiros sociais, facilitando, muitas vezes, sua abordagem junto aos colaboradores das organizações;
- alguns seres humanos possuem excesso de autoconfiança, acreditando ser capazes de cumprir uma tarefa sem auxílio de outras pessoas. Muitas vezes isso ocorre de fato. Mas, algumas vezes, as pessoas acreditam ter o domínio total de

determinados assuntos e fazem alarde sobre isso. Tornam-se, com isso, alvos fáceis dos engenheiros sociais;

- alguns seres humanos têm mais facilidade de serem convencidos, persuadidos do que outros. Essa qualidade facilita o trabalho do engenheiro social, no momento de persuadir seu alvo a realizar algum ato prejudicial à organização ou à pessoa que está sendo persuadida.

Silva *et al* (2013), acrescentam caraterísticas aos perfis de colaboradores de organizações e de muitos seres humanos, tais como:

- muitos seres humanos têm a necessidade de se mostrarem úteis, usam cortesia e atenção com pessoas que nem conhecem. Essa característica é facilitadora de ataques por parte de engenheiros sociais;
- seres humanos muitas vezes procuram novas amizades usando, inclusive, redes sociais e deixando disponíveis informações muitas vezes confidenciais. Essa postura facilita o trabalho de engenheiros sociais.

Silva *et al* (2013), reforçam que engenheiros sociais coletam, atualmente, a maior parte das informações sobre seus alvos através das redes sociais. Consideram que as redes sociais potencializam as vulnerabilidades dos alvos dos engenheiros sociais.

3 ESTUDO DE CASO REALIZADO E RESULTADOS OBTIDOS

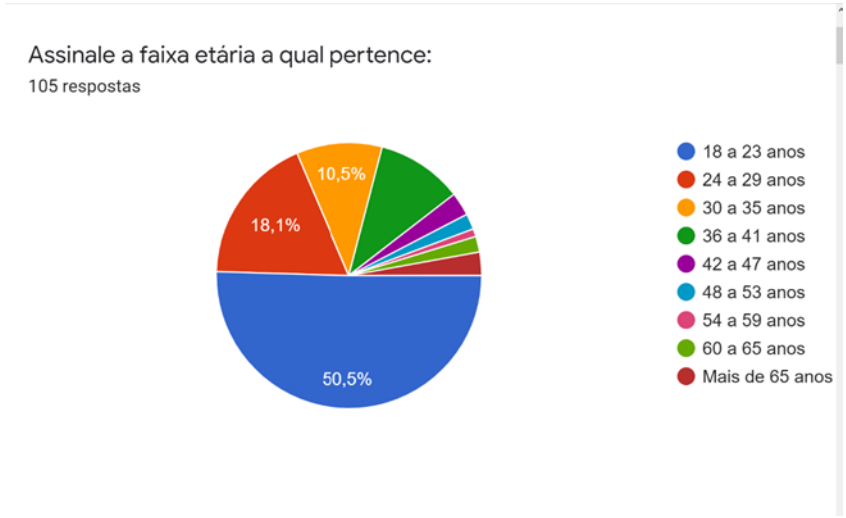
Este capítulo descreve o estudo de caso realizado pelo autor deste trabalho, usando um questionário com perguntas de caráter quantitativo. O objetivo desta pesquisa foi mapear as principais ocorrências de ataques sofridos por organizações ou pessoas físicas e ter informações sobre seus conhecimentos e formas de prevenção, relacionados à segurança da informação, engenharia social e ataques provocados por engenheiros sociais.

3.1 Descrição da pesquisa realizada

O autor deste trabalho realizou uma pesquisa quantitativa composta de nove questões (Apêndice A). Usou o aplicativo *Google Forms* deixando a pesquisa disponível entre 30 de setembro de 2020 a 16 de outubro de 2020. Quando o formulário foi fechado havia 105 respostas. O autor trabalhou com este universo.

Uma das questões pede ao respondente para assinalar a faixa etária à qual pertence. O Gráfico 6, obtido com as respostas é apresentado a seguir:

Gráfico 6 – Faixas etárias obtidas nas respostas



Fonte: Autoria própria, 2020

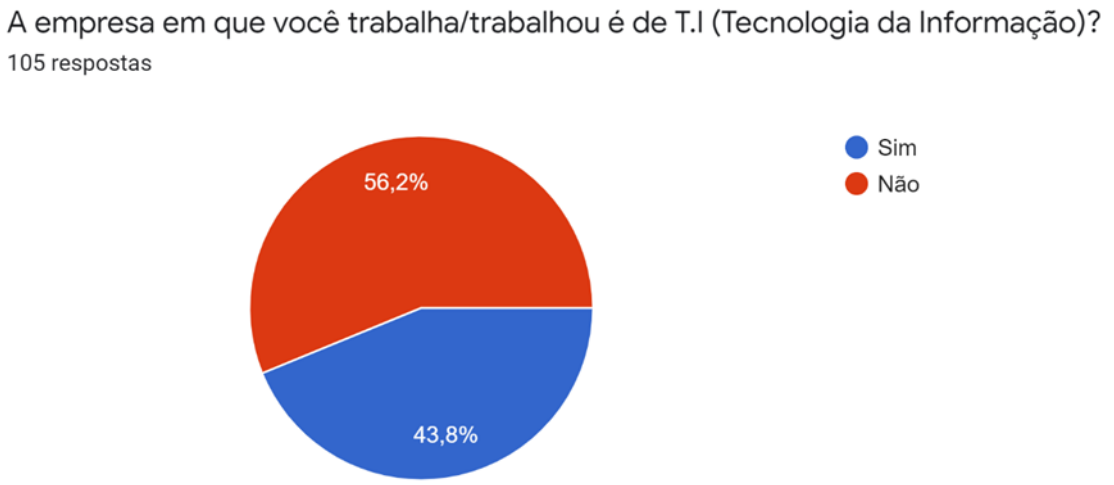
O Gráfico 6 mostra que a maior parte dos respondentes está em uma das três primeiras faixas etárias (têm, no mínimo, 18 anos e, no máximo, 41 anos). Os resultados mostram que mais de 80% dos respondentes têm até 41 anos.

As pessoas que pertencem às quatro primeiras faixas nasceram a partir de 1979. Resultados de pesquisas feitas pelo autor deste trabalho mostram que os

primeiros microcomputadores surgiram no início da década de 1980, no Brasil. A seguir a Internet ficou disponível a usuários de maneira geral. Portanto, a maioria dos respondentes nasceram em uma época em que a informática e a Internet começaram a ser usadas no Brasil e cujo uso cresceu rapidamente (TECHTUDO, 2019).

Outra pergunta cujas respostas podem interessar para o resultado deste trabalho é sobre o local de trabalho dos respondentes (se trabalham em uma organização de TI ou não). O Gráfico 7, a seguir, mostra os percentuais de respostas obtidas:

Gráfico 7 – Local de trabalho dos respondentes



Fonte: Autoria própria, 2020

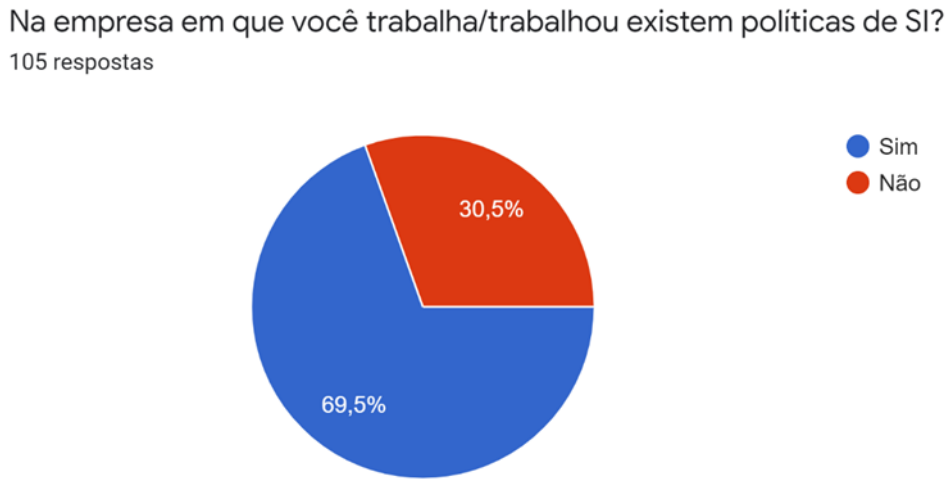
O fato de 56,2% responderem que não trabalham em uma organização de TI não invalida a questão e nem o resultado, pois instituições de ensino, por exemplo, não são organizações de TI (apesar de possuírem um grupo de colaboradores responsáveis pela área de TI). E há outros exemplos que podem ilustrar esta questão.

O aspecto importante desta questão é que mesmo que a organização não seja da área de TI, muitos colaboradores podem trabalhar em locais que requerem segurança da informação, portanto existe a probabilidade de trabalharem com algum dispositivo de informática. Os resultados apresentados nos dois gráficos a seguir reforçam esta questão.

Gráfico 8 – respondentes que já ouviram falar em SI

Fonte: Autoria própria, 2020

Gráfico 9 – Existência de políticas de SI nas organizações de trabalho dos respondentes



Fonte: Autoria própria, 2020

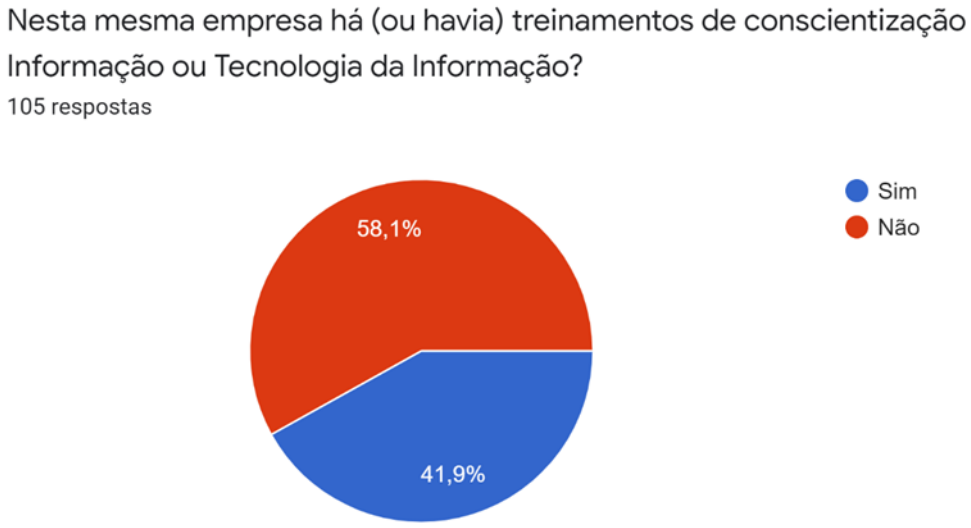
Mais de 95% dos respondentes ouviram falar de TI, como mostra o Gráfico 8, mas 69,5% das organizações de trabalho dos respondentes possuem políticas de SI.

Os incidentes reportados ao CERT.br em 2019, apresentados na Tabela 3, seção 1.2 deste trabalho, reforçam a necessidade de políticas de SI serem exercitadas nas organizações que possuem algum segmento dedicado à área de TI. Portanto, considerando-se este aspecto, o percentual de 69,5% das organizações, referenciadas no questionário, pode ser considerado insatisfatório.

Vale lembrar que mesmo o fato de 56,2% das organizações de trabalho dos respondentes não pertencerem à área de TI, não implica, necessariamente, que não tenham um grupo responsável pela parte de TI.

O Gráfico 10, a seguir, mostra resultados de como as organizações tratam a conscientização das políticas de Segurança da Informação:

Gráfico 10 – Tratamento dado às políticas de SI nas organizações de trabalho dos respondentes

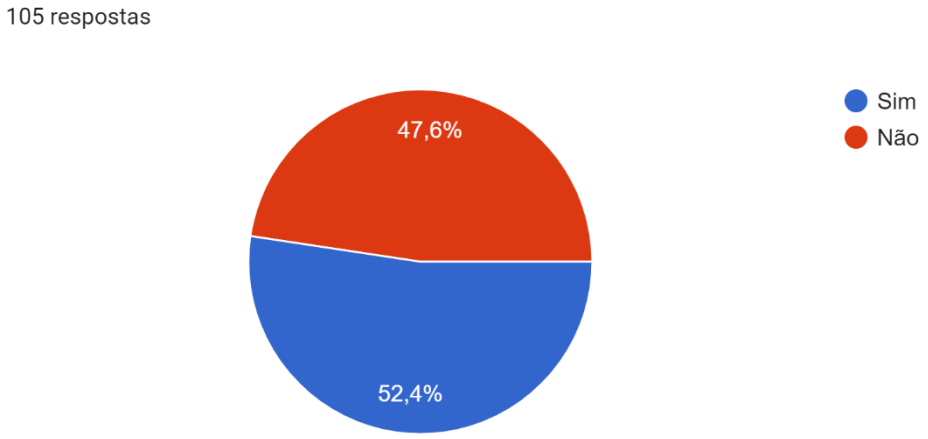


Fonte: Autoria própria, 2020

Os resultados mostram que mais de 50% das organizações não tratam adequadamente as políticas de SI. Este fato pode aumentar as brechas de segurança, expondo dados confidenciais. Além disso, a falta de conscientização, por parte das organizações, pode deixar seus colaboradores mais vulneráveis a ataques de engenheiros sociais.

Uma das questões sobre ataques sofridos pelos respondentes foi “Você já sofreu algum tipo de: ataque/roubo/vazamento de informações, sejam pessoais e/ou corporativas”. Os percentuais coletados confirmam a tendência de aumento de ataques bem como as vulnerabilidades de pessoas que utilizam dispositivos de TI. Os resultados são apresentados no Gráfico 11, a seguir:

Gráfico 11 - Percentual de respondentes que já sofreram algum tipo de ataque (pessoas ou corporativo)

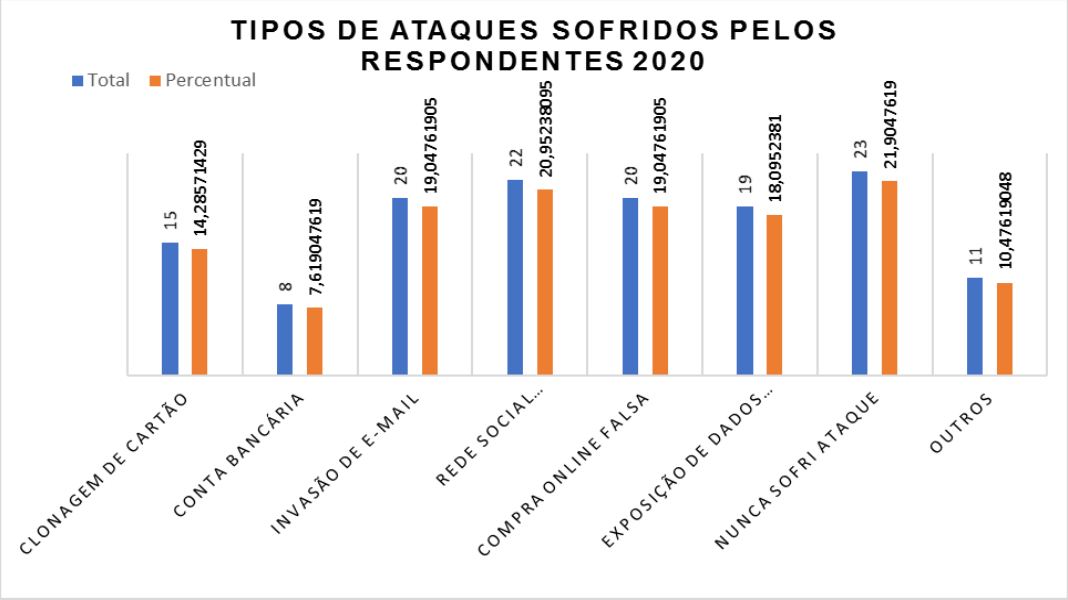


Fonte: Autoria própria, 2020

Os resultados obtidos nesta resposta mostram as vulnerabilidades do ser humano no que diz respeito à Segurança da Informação. Este aspecto é reforçado pelas respostas obtidas na próxima pergunta, que qualifica alguns dos ataques que podem ser realizados por engenheiros sociais.

O Gráfico 12, a seguir, mostra que a maioria dos respondentes já sofreu algum tipo de ataque (indicando vulnerabilidades nas áreas pesquisadas). Esta questão admitiu mais de uma alternativa assinalada, portanto os valores de totais ultrapassam 105 respostas e os valores dos percentuais somados ultrapassam 100%.

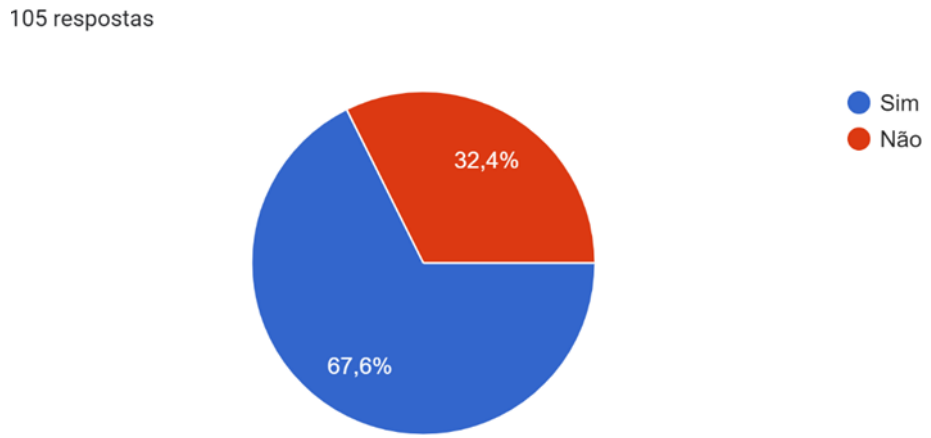
Gráfico 12 – Tipos de ataques sofridos pelos respondentes



Fonte: Autoria própria, 2020

O Gráfico 13, a seguir, está relacionado à questão “Você sabe identificar quando alguém está tentando atacar/obter informação pessoal sua pelas redes sociais/Internet?”. Os resultados mostram os percentuais de respostas obtidas indicando que quase 70% dos respondentes conseguem perceber a tentativa de ataque. Mesmo assim muitos respondentes já tiveram dados roubados em redes sociais/Internet, como mostra o Gráfico 12.

Gráfico 13 – Sobre conhecimento de possíveis ataques

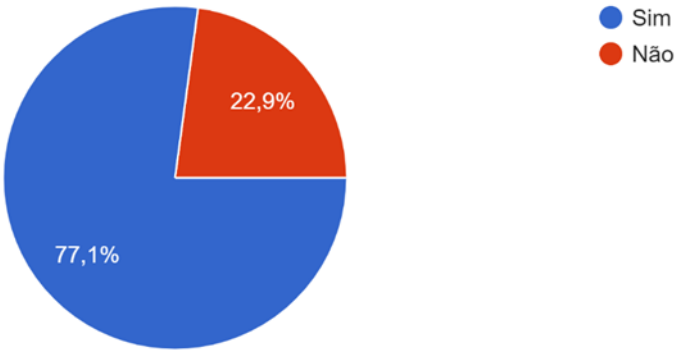


Fonte: Autoria própria, 2020

O Gráfico 14, a seguir, é relativo à pergunta “Você saberia identificar um ataque de *Phishing* (que é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito) caso algum

link/*site* que enviam/mandaram para você é realmente oficial/verdadeiro? *" (o asterisco indica que a resposta e obrigatória).

Gráfico 14 – Reconhecimento de um ataque do tipo *Phishing* por parte dos respondentes



Fonte: Autoria própria, 2020

Os Gráficos 13 e 14 mostram coerência nas respostas fornecidas. Também mostram que se houver um processo eficaz e contínuo de conscientização sobre ataques cibernéticos, a probabilidade de mitigação dos ataques é maior.

Os resultados de todas as questões do questionário estão no Apêndice B deste trabalho.

4 SUGESTÕES PARA MITIGAR ATAQUES À SEGURANÇA DA INFORMAÇÃO

Este capítulo utiliza os resultados obtidos na pesquisa descrita no capítulo anterior, para acrescentar sugestões de associadas às políticas de SI, apresentadas no Capítulo 1 deste trabalho. Apresenta uma análise de resultados obtidos em estudo de caso realizado por um pesquisador, reforçando a questão da vulnerabilidade do ser humano.

Utiliza informações obtidas no referencial teórico estudado, sobre segurança da informação, engenharia social e o elo mais fraco da cadeia de segurança da informação, para completar as sugestões a serem feitas.

4.1 Análise dos resultados da pesquisa feita

O questionário (com questões quantitativas), elaborado pelo autor deste trabalho. permaneceu na plataforma *Google Forms* no período de 30 de setembro de 2020 a 16 de setembro de 2020.

Quando foi encerrado, o autor trabalhou com um universo de 105 respondentes. A análise dos resultados obtidos através das respostas dadas mostrou dois aspectos distintos:

- características relacionadas aos respondentes;
- características relacionadas às políticas de segurança da informação.

Abordando as questões relacionadas às características dos respondentes, é possível fazer algumas considerações.

O Gráfico 6 mostrou que mais de 80% dos respondentes pertencem à faixa etária de 18 anos a 41 anos. Portanto, nasceram a partir de 1979. Pesquisas realizadas pelo autor deste trabalho indicaram alguns resultados relacionados à questão de faixas etárias, que dizem respeito ao ensino de Informática no Brasil.

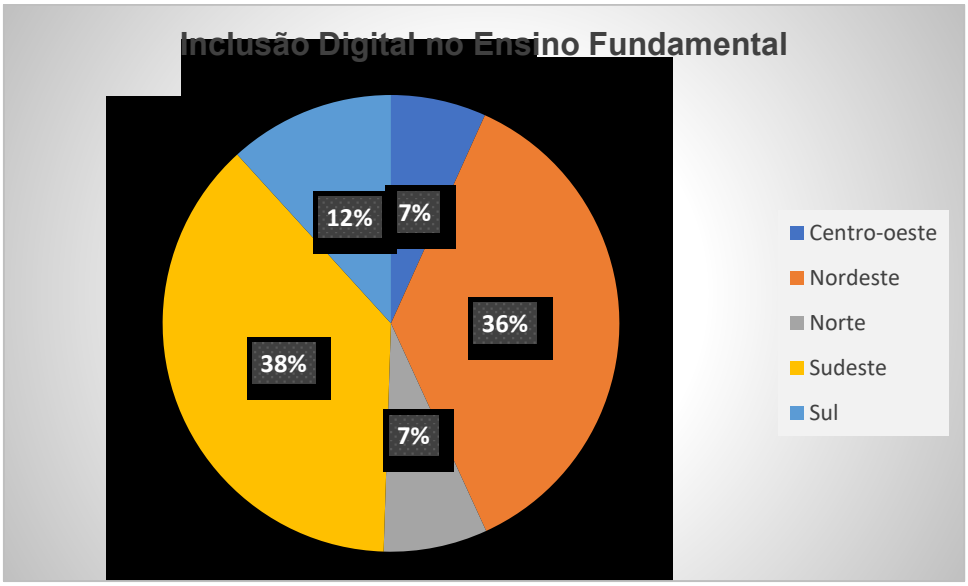
O primeiro curso na área de computação no Brasil, foi o curso de Ciência da Computação da UNICAMP, 1969. No mesmo ano foi criado o curso de Processamento de Dados, na Universidade Federal da Bahia. A criação de cursos na área de Informática continuou a crescer desde então, no nível de terceiro grau (JONATHAN, 2012).

A inclusão digital e os recursos denominados TICs (Tecnologias da Informação e Comunicação) passaram a ser oferecidos às escolas brasileiras, ainda que de forma opcional, a partir da década de 1990 (DURAN, 2008).

Vale lembrar que as TICs foram introduzidas, inicialmente, nas instituições de ensino privado, especificamente, no Ensino Médio, a partir de 1990. As instituições públicas de ensino incluíram conhecimentos de informática em diferentes datas e após o ano 2000. Atualmente os indivíduos que estudaram em instituições que usam as técnicas de inclusão digital desde a década de 1990, podem ter melhor conhecimento em informática, inclusive no quesito Engenharia Social (CAPOBIANCO; CURY, 2011).

Mattos (2010), lembra que a inclusão digital nas instituições públicas de Ensino Fundamental foi feita, em todo o Brasil, de maneira não uniforme, e indica o percentual dessa inclusão, apresentado no Gráfico 15, a seguir:

Gráfico 15 - Inclusão Digital nas Escolas de Ensino Fundamental



Fonte: Mattos, 2010

As considerações feitas mostram que os respondentes do questionário deste trabalho, que pertencem à faixa etária de 18 anos a 41 anos (portanto, nascidos a partir de 1979), têm grande chance de pertencerem ao grupo que recebeu educação na área de Informática. Mas fica a pergunta sobre o tipo de conteúdo sobre informática, apresentado às pessoas que frequentaram escolas nesse período.

Uma sugestão importante, do autor deste trabalho, é sobre a contínua atualização de conteúdos programáticos sobre informática, oferecidos pelas

instituições de ensino de maneira geral. Dessa forma a probabilidade de estudantes conhecerem informações sobre tipos de vírus, tipos de ataques, perfis de atacantes, ferramentas a serem utilizadas e maneiras de se precaver, reduzindo suas vulnerabilidades e mitigando, tanto quanto possível, os ataques que possam ocorrer.

O Gráfico 11, apresentado no Capítulo 4 deste trabalho, mostra o percentual de respondentes que já sofreram algum tipo de ataque (52,4%) e o Gráfico 12, apresentado no Capítulo 4 deste trabalho, apresenta os tipos de ataques sofridos com maior frequência.

Os resultados apresentados por estes Gráficos reforçam a sugestão dada pelo autor deste trabalho, pois a atualização contínua de conteúdos programáticos em disciplinas da área de Informática, oferecidas por instituições de ensino teriam uma contribuição efetiva para melhor manipular dispositivos de *hardware* e *software*, disponíveis nas organizações e no mercado. Pois, atualmente, parece ocorrer uma defasagem entre a utilização dos mais variados aplicativos e o conhecimento sobre os riscos que usuários de dispositivos de *hardware* quando usam esses recursos.

Além dos resultados apresentados, as pesquisas bibliográficas realizadas pelo autor deste trabalho mostraram resultados que podem ser considerados importantes para este trabalho (GASPAR, 2015).

Gaspar (2015), realizou um experimento envolvendo dois cenários, para analisar dois aspectos. O primeiro deles relaciona-se à coleta de informações, por parte dos engenheiros sociais, usando redes sociais. O outro aspecto diz respeito ao comportamento social de colaboradores de diversas organizações, em diversos países.

Foram enviadas solicitações aos responsáveis pela área de recursos humanos de diversas empresas, em vários países. A condição, para participar da pesquisa, era conhecer e comunicar-se usando a língua portuguesa. O objetivo da pesquisa relacionou-se à vulnerabilidade dos participantes, no que diz respeito ao comportamento social junto às redes sociais.

Os elementos do primeiro cenário foram os seguintes:

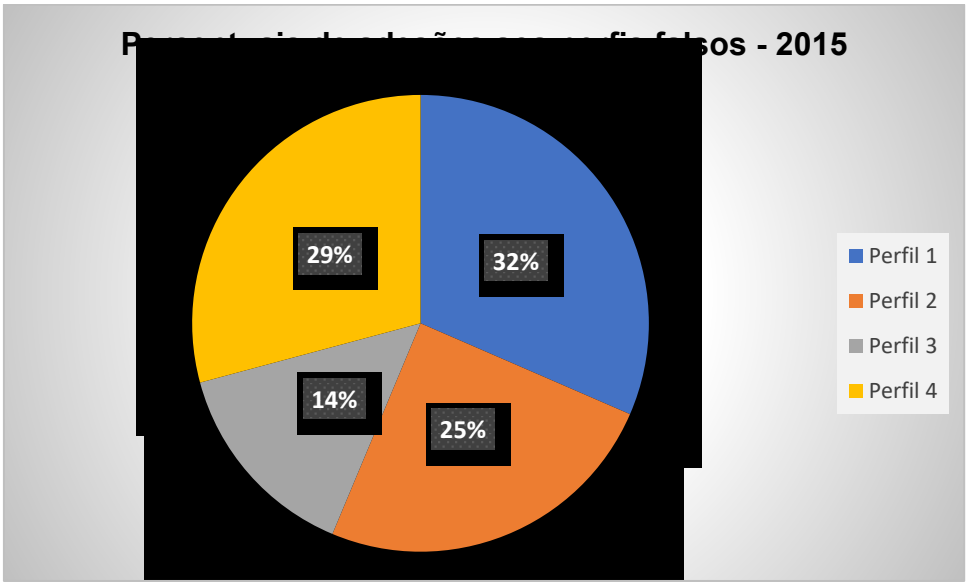
- Criação de 4 perfis diferentes usando o *Facebook*. Dois perfis de pessoas do sexo feminino de faixas etárias diferentes (20 anos e 50 anos). Dois perfis de pessoas do sexo masculino (27 anos e 45 anos). Cada um dos perfis recebeu alimentação de informações gerais, não possuindo dados ou fotos que os identificassem.
- Identificação dos perfis feita da seguinte forma:

- Perfil 1, pessoa do sexo feminino, idade 20 anos;
- Perfil 2, pessoa do sexo masculino, idade 27 anos;
- Perfil 3, pessoa do sexo masculino, idade 40 anos;
- Perfil 4, pessoa do sexo feminino, idade 50 anos.

- Permanência dos perfis no *Facebook* foi de 45 dias;
- A adesão de colaboradores das diversas organizações participantes da pesquisa foi de 3211 pessoas. Portanto a pesquisa trabalhou com este universo;
- Objetivo da pesquisa, relativo ao primeiro cenário, foi fornecer, ao engenheiro social, dados dos colaboradores que aderiram aos perfis falsos.

O número de adesões para cada perfil é apresentado pelo Gráfico 16, a seguir:

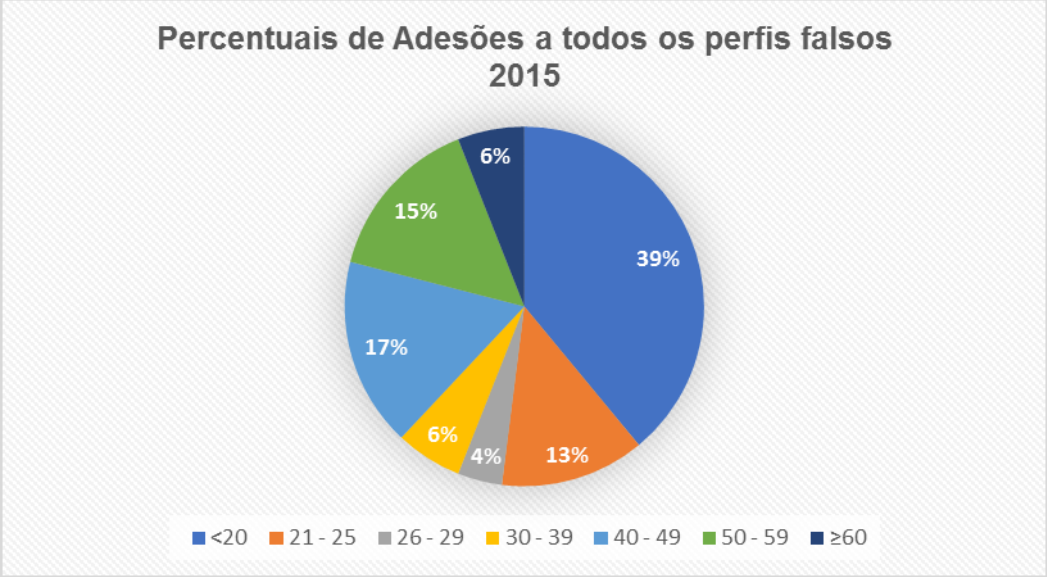
Gráfico 16 – Adesões a perfis falsos no *Facebook*



Fonte: Gaspar. 2015

Gaspar (2015) fez, também, uma análise de adesões a todos os perfis e separando-as por faixas etárias, para melhor visualizar as vulnerabilidades das faixas etárias, apresentadas no Gráfico 17, a seguir.

Gráfico 17 - Vulnerabilidades por faixas etárias



Fonte: Gaspar, 2015

Sem considerar a faixa etária de 40 anos ou mais e somando os percentuais das faixas etárias anteriores a 40 anos, tem-se o percentual de 62% de adesões aos perfis falsos, mostrando possíveis vulnerabilidades a ataques de maneira geral e, portanto, a ataques de engenheiros sociais.

Considerando a pergunta sobre as faixas etárias dos respondentes, apresentada no Capítulo 3, Gráfico 6, tem-se o resultado de 80% de respondentes com idades até 41 anos. Reunindo as informações do Gráfico 17 e as informações do Gráfico 6, é possível concluir que a maior parte dos respondentes pertence a faixas etárias potencialmente vulneráveis. Portanto, fazem parte do conjunto que representa o elo mais fraco da corrente em SI, reforçando a afirmação sobre o elo mais fraco de SI.

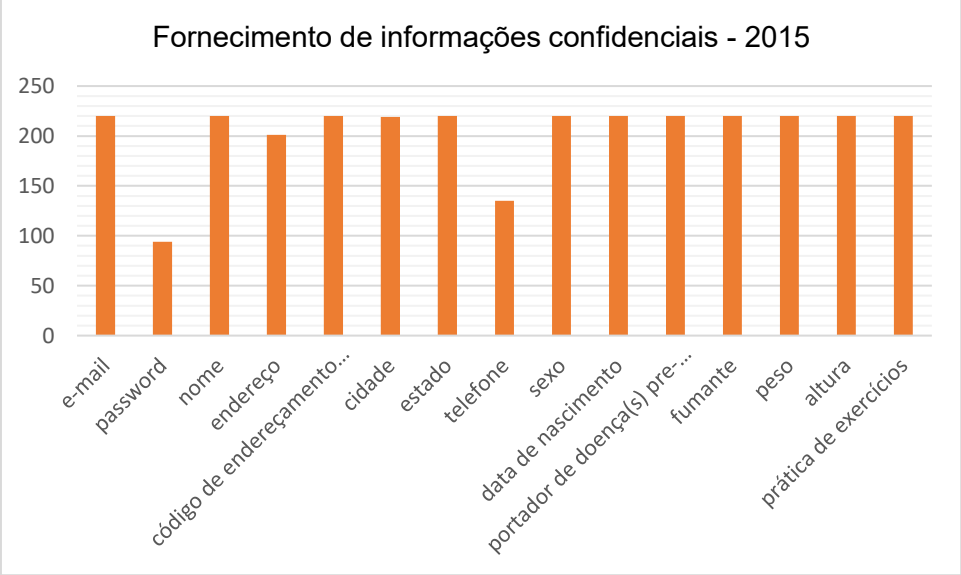
Gaspar (2015) elaborou o segundo cenário composto dos seguintes elementos:

- Criação de um *site* de notícias relacionadas à saúde e bem estar, com sugestões relacionadas a estes temas;
- Opção para receber de notícias semanais sobre saúde ou bem estar;
- Preenchimento de um formulário com informações, caso os participantes aceitassem fazer a adesão às notícias semanais;
- Existência de dezesseis campos a serem preenchidos, sendo quatro campos obrigatórios e os outros opcionais;

- Campos obrigatórios foram sexo, data de nascimento, código de endereçamento postal e aceitação dos termos e condições de utilização;
- Campos opcionais foram *e-mail, password,* nome completo, telefone, endereço, cidade, estado, peso, altura, ser fumante ou não, ser portador de doença(s) pré-existente(s) e adotar práticas de exercícios.
- Utilização do mesmo universo do cenário 1 (3211 participantes), porém a adesão a este segundo cenário foi de 220 participantes, portanto o cenário 2 trabalhou com um universo de 220 participantes da pesquisa.

Os resultados obtidos confirmam e reforçam a questão das vulnerabilidades de colaboradores de organizações de maneira geral, conforme mostram os dois gráficos a seguir.

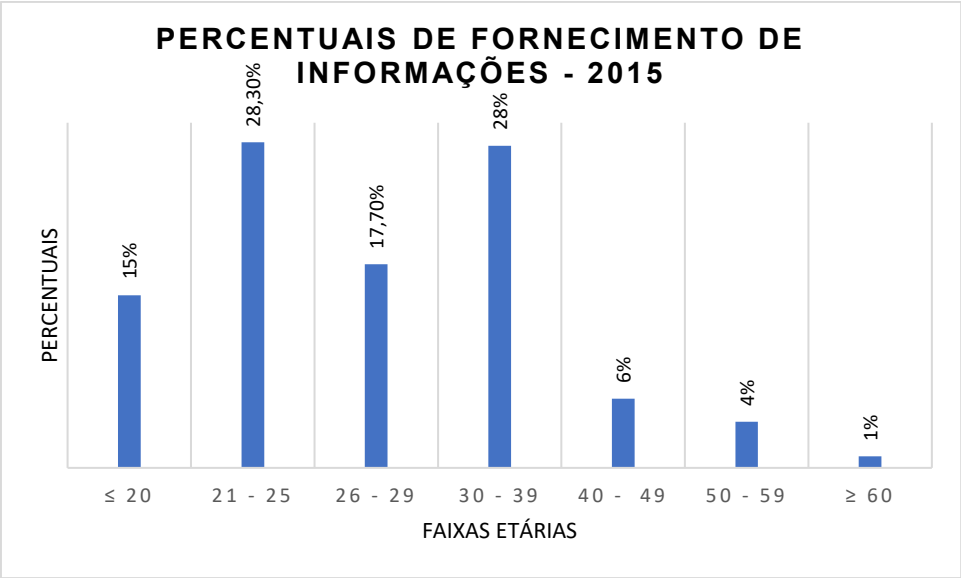
Gráfico 18 – Vulnerabilidades ao fornecer informações



Fonte: Gaspar, 2015

Vale lembrar que o preenchimento era obrigatório apenas para os campos sexo, data de nascimento, código de endereçamento postal e aceitação dos termos e condições de utilização. Analisando o gráfico 18, percebe-se a vulnerabilidade dos participantes da pesquisa, pois a maioria forneceu informações não obrigatórias (e algumas delas confidenciais).

Gráfico 19 – Vulnerabilidades por Faixas Etárias



Fonte: Gaspar, 2015

Analisando o Gráfico 19, percebe-se que 89% dos participantes da pesquisa têm até 39 anos. O Gráfico 6, apresentado no Capítulo 3 deste trabalho, apresenta os percentuais das faixas etárias dos respondentes da pesquisa feita pelo autor deste trabalho, lembrando que mais de 80% destes respondentes têm até 41 anos. Os percentuais dos Gráficos 6 e 19 estão muito próximos. Isto destaca a vulnerabilidade dos participantes da pesquisa feita pelo autor deste trabalho.

O Gráfico 13, apresentado Capítulo 3 deste trabalho, mostra o percentual (67,6%) de respondentes que conseguem distinguir possíveis ataques. A forma de elaboração das questões não permitiu distinguir se este percentual surgiu após respondentes terem sofrido algum tipo de ataque ou se os respondentes já possuíam esta percepção antes dos ataques que sofreram.

O autor deste trabalho reconhece que esta dúvida pode estar associada a alguma falha na elaboração das questões, pois a diferença entre aqueles que já sofreram ataques (52,4%) e os que percebem tentativas de ataques (67,6%) é de 15,2% (é um valor com algum destaque).

Quanto às características relacionadas às políticas de segurança da informação, também há aspectos a serem considerados.

O Gráfico 7, apresentado no Capítulo 3 deste trabalho, mostra os percentuais de respondentes que trabalham (ou trabalharam) em organizações da área de TI. As respostas indicam que 43,8% dos respondentes trabalham ou trabalharam em

organizações na área de TI e que 56,2% não trabalham ou não trabalharam em organizações da área de TI. Esses percentuais devem ser considerados, mas vale lembrar que o fato de uma organização não pertencer à área de TI não implica, necessariamente, que não tenha uma área responsável por TI, como instituições de ensino, por exemplo. Existe a probabilidade de os respondentes trabalharem com dispositivos de *hardware* e *software* e isso deve ser considerado também.

O Gráfico 8, apresentado no Capítulo 3 deste trabalho, reforça a afirmação feita, visto que 96,2% dos respondentes ouviram falar em segurança da informação, ou seja, possuem algum conhecimento sobre a necessidade de se proteger a informação manipulada nas organizações.

O Gráfico 9, apresentado no Capítulo 3 deste trabalho, mostra percentuais sobre a existência de políticas de segurança da informação no local de trabalho dos respondentes. Cerca de 69,5% responderam que havia políticas de segurança da informação em seu local de trabalho e 30,5% responderam que não havia. O percentual de 69,5% de respostas é expressivo e importante, e o Gráfico 10 justifica tal afirmação.

No Gráfico 10, apresentado no Capítulo 3 deste trabalho, 41,9% dos respondentes indicam que havia tratamento dado à política de segurança da informação em seus locais de trabalho e 58,1% dos respondentes disseram que não havia tratamento dado à política de segurança da informação. A diferença de 27,4% entre as respostas dos Gráficos 9 e 10 é expressiva, pois mostra que organizações nem sempre trabalham com políticas de SI de forma adequada.

Além disso, as respostas merecem reflexões sobre a existência e melhorias contínuas nas políticas de segurança da informação, nas organizações. O uso cada vez maior de aplicações na *web* 2.0, a complexidade dessas aplicações e o aumento de ataques de diferentes características são fatores de peso no quesito segurança da informação das organizações. (ALEXANDRIA, 2009).

Para completar a questão sobre vulnerabilidades do ser humano e fornecimento de dados pessoais e confidenciais, há um vídeo que trata de uma pesquisa em uma organização farmacêutica, coletando dados pessoais de clientes tais como: CPF, RG, nome dos pais, realizando biometria digital, tirando fotos de frente e de perfil dos clientes. No final do vídeo são apresentados questionamentos sobre a não resistência dos clientes ao fornecer as informações, sobre a falta de

questionamento sobre porque os dados e as imagens são coletados. Antes do encerramento do vídeo aparece a mensagem “Resista” (INTERNETLAB, 2018).

A norma ABNT NBR/ISO/27002:2013 (ABNT, 2013) estabelece, em uma de suas seções, sobre segurança da informação, que colaboradores, fornecedores e terceiros (se for o caso) devem receber treinamento adequado em conscientização e atualizações periódicas sobre práticas e procedimento organizações, relacionados aos cargos e funções que exercem, bem como a adequada manutenção dessas políticas de segurança da informação (ALEXANDRIA, 2009).

Alexandria (2009), recomenda que as organizações tenham um documento sobre as políticas organizacionais relacionadas à segurança da informação, destacando o esforço a ser feito, por parte das organizações, para que seus colaboradores, fornecedores e terceiros (quando for o caso) sejam conscientizados sobre a importância de conhecer e seguir as normas de políticas de segurança da informação estabelecidas pelas organizações e as incorporem ao seu cotidiano.

Treinamentos e atualizações contínuas sobre as políticas de segurança da informação, bem como o comprometimento de todas as instâncias das organizações e a adoção de alguma metodologia relacionada à SI também são fatores de peso nessa questão de SI (ALEXANDRIA, 2009).

4.2 Proposta de medidas adicionais sobre política de SI para melhorar a mitigação dos ataques

O Gráfico 3, apresentado no Capítulo 1 deste trabalho, sobre tipos de danos causados por ataques às organizações em 2018, mostra que diversos aspectos relacionados aos negócios das organizações são atingidos em casos de ataques, a saber:

- Moral dos colaboradores das organizações;
- Relações comerciais das organizações com parceiros/fornecedores e outros;
- Reputação/força da marca de cada uma das organizações envolvidas;
- Relações com órgãos reguladores;
- Preço de ações (GRUPO BETTENCOURT, 2018).

Vale lembrar que Mitnick e Simon (2003), consideram importante o treinamento dos colaboradores de organizações, esclarecendo a importância da informação para

a continuidade do negócio da instituição e a importância de o comportamento do colaborador estar alinhado às políticas de segurança da informação da organização.

Bach (2001), destaca a preferência de atacantes (*crackers* e engenheiros sociais) por parte de organizações de pequeno e médio porte, pois nem sempre adotam políticas de segurança da informação adequadas devido ao alto custo de adoção, atualização e manutenção dessas políticas.

A adoção de políticas de segurança da informação, apresentada na seção anterior engloba um número expressivo de ações a serem realizadas pelas organizações. Algumas questões podem ser acrescentadas à adoção dessas medidas, tais como:

- Gerenciamento adequado no que diz respeito sobre esclarecimento aos colaboradores da importância da informação para a continuidade de negócios da organização;
- Gerenciamento adequado no que diz respeito ao treinamento de colaboradores, em todas as instâncias, sobre tipos de vulnerabilidades, ataques e suas consequências danosas às organizações;
- Gerenciamento adequado das atualizações de tipos de ataques com maior incidência aos colaboradores das organizações, bem como ao ativo tecnológico dessas instituições;
- Revisão e gerenciamento adequados dos controles feitos sobre treinamentos dos colaboradores e sobre a adequação da tecnologia adotada pelas organizações visando a mitigação de ataques;
- Gerenciamento adequado da área de Recursos Humanos sobre a compatibilidade das qualificações de seus colaboradores com os cargos que ocupa;
- Existência de políticas de gestão de colaboradores por parte da área de Recursos Humanos;
- Estabelecimento de um ambiente adequado de trabalho para os colaboradores, evitando, tanto quanto possível, ambiente organizacional hostil (SÊMOLA, 2003).
- Conscientização, nos diversos níveis de organizações, sobre não ser suficiente investir em *hardware* e *software*, na melhoria da segurança da informação. Recomenda-se a realização de planejamento e investimentos contra a Engenharia Social (GASPAR, 2015).

Nas pesquisas bibliográficas para a elaboração deste trabalho, verificou-se que mesmo adotando procedimentos em políticas de SI, com a certificação e utilização das normas ISO/IEC 27001:2013 (regulamentação para o uso de políticas de SI) e ISO/IEC 27002:2005 (implementação, manutenção e melhorias nas práticas de utilização de políticas de SI), metodologias e regulamentos adicionais utilizados pelas organizações, os ataques às instituições crescem quase que no mesmo nível de crescimento da TI.

Tendo em vista esta questão, organizações e pesquisadores da área de SI perceberam a necessidade de análise de colaboradores de organizações e usuários de maneira geral (GARTNER, 2016).

Tecnologias mais sofisticadas têm sido utilizadas no combate às ameaças e ataques à área de SI. Um exemplo é o uso de inteligência artificial e aprendizagem de máquina para análise do comportamento de colaboradores, usuários e organizações. Este conceito é denominado *User and Entity Behavior Analytics – UEBA*. Esta técnica pode auxiliar na identificação de ações consideradas padrões ou ações consideradas suspeitas, por parte de colaboradores, usuários e organizações (OLHAR DIGITAL, 2020).

Recomenda-se uma análise de custo/benefício na utilização de ferramentas com a abordagem de inteligência artificial e aprendizagem de máquina. Porém, o crescimento de utilização de ferramentas usando Inteligência artificial e aprendizagem de máquina cresceu 270% desde 2016 até 2019. Em 2015, cerca de 10% de participantes de uma pesquisa realizada pela Gartner, utilizavam ferramentas baseadas em inteligência artificial. Em 2019 foi realizada a mesma pesquisa, indicando que a adesão a essas ferramentas subiu para 37% (GARTNER, 2019).

Finalmente, recomenda-se a certificação adoção das normas ISO 27001 e sua extensão ISO 27701, bem como a certificação e adoção da norma ISO 27002, para se adequar às questões de segurança da informação, como exercitar a gestão da segurança dos sistemas de informação e a adequação à LGPD e *GDPR.* As organizações que procederem dessa forma estarão alinhadas às normas vigentes e à Lei Geral de Proteção de Dados, bem como à *GDPR* (regulamentada em diversos países)

5 CONSIDERAÇÕES FINAIS

A problematização proposta neste trabalho foi verificar se é possível melhorar a mitigação dos ataques realizados por engenheiros sociais às organizações através de seus colaboradores, que são considerados o elo mais fraco da cadeia de segurança da informação.

Para responder esta questão o autor deste trabalho cumpriu o objetivo geral proposto, de analisar as principais técnicas de ataques relatadas na literatura, principalmente por engenheiros sociais. Para executar esta atividade, o autor executou todos os passos previstos nos objetivos específicos deste trabalho, apresentando os resultados de seus estudos nos Capítulos 1 e 2 deste trabalho.

Realizou a pesquisa quantitativa prevista, sobre segurança da informação, em organizações de maneira geral e sobre ataques sofridos por seus colaboradores, com um universo de 105 respondentes, apresentando a descrição da pesquisa realizada no Capítulo 3 deste trabalho. Vale ressaltar que a questão número 7 do questionário possuía uma resposta aberta (outros tipos de ataques), acabando por pulverizar respostas de tipos de ataques sofridos, não sendo possível quantificá-los, pois os percentuais foram não significativos em relação ao universo de respondentes.

Fez uma análise dos resultados obtidos na pesquisa realizada, contrapondo-os a resultados obtidos na literatura estudada, no Capítulo 4 deste trabalho. Os resultados mostraram que, no universo pesquisado, há um percentual considerável de organizações que deveriam adotar medidas de segurança e de gestão de seus sistemas de informação e não o fazem.

Usando os resultados obtidos no estudo da literatura sobre este tema, foram relacionadas medidas fortemente recomendadas por pesquisadores da área de segurança da informação.

As recomendações apresentadas pelos pesquisadores possuem diversos pontos em comum, tais como: certificação e adoção das normas ISO/IEC 27001 e sua extensão ISO/IEC 27701 e ISO/IEC 27002 para a gestão da segurança da informação e orientação de como conduzir as práticas de gestão. Vale ressaltar que com a certificação e adoção da norma ISO/IEC 27701 as organizações alinham-se à LGPD e à *General Data Protection Regulation – GDPR*. Esta última trata-se de um novo conjunto de regras de privacidade, em vigor na União Europeia – UE, desde 2018.

Organizações que não se certificarem na ISO/IEC 27001 e ISSO/IEC 27701 podem ser afetadas em seus negócios, pois organizações da UE dão preferência

àquelas organizações alinhadas às mesmas normas adotadas pelos países que pertencem a UE.

Outro aspecto importante é que mesmo com o desenvolvimento e otimização de ferramentas para mitigar ataques às organizações, os ataques cresceram na mesma proporção, conforme pesquisa realizada pela *Gartner*, como visto no Capítulo 4 deste trabalho.

Foi visto que, atualmente, a adesão das organizações na utilização de ferramentas baseadas em inteligência artificial e aprendizagem de máquina, tem crescido desde 2015, de acordo com pesquisa realizada pela *Gartne*r. Essa adesão atende recomendações feitas por pesquisadores, no sentido de estudar o comportamento de seus colaboradores, conforme visto no Capítulo 4 deste trabalho.

Finalmente, foi apresentado um estudo sobre a aprendizagem de TICs no Brasil, no Capítulo 4 deste trabalho. Os resultados apresentados mostram que instituições privadas adotaram as TICs no início da década de 1990. Nas instituições públicas as TICs foram adotadas, de forma opcional e não uniforme nas cinco regiões do Brasil, a partir da década de 2000.

Não há estudos realizados sobre o conteúdo programático das TICs, praticados nessas instituições. Também não há estudos realizados sobre o alinhamento desses conteúdos programáticos com a realidade atual, principalmente no que diz respeito à questão vulnerabilidade.

Trabalhos futuros sobre as questões apresentadas poderão contribuir para a melhoria do conhecimento de usuários de tecnologia da informação, principalmente em uma época que dispositivos de *hardware* e *software* estão cada vez mais disponíveis. Esta recomendação reforça o estudo que apresenta o aumento de índice de ataques no mundo inteiro, durante a pandemia (que não se sabe quanto tempo vai durar). Trabalhos *home-office,* aulas virtuais, compras pela Internet, entre outras atividades, contribuem fortemente para o aumento desses ataques.

Governos, em todas as instâncias, organizações e instituições de ensino poderiam unir-se no sentido de criar programas educacionais, oferecidos de maneira contínua, para evidenciar os males provocados por ataques, de maneira geral, bem como para orientar e conscientizar usuários sobre aspectos comportamentais a serem adotados e a importância do não fornecimento de informações confidenciais, em situações consideradas vulneráveis.

REFERÊNCIAS

ABNT. Tecnologia da Informação- Técnicas de Segurança – Código de Prática para Controles de Segurança: ABNT NBR ISO/IEC 27002:2013. 1ª ed. Rio de Janeiro, 2013.

ABNT: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos: NBR ISO/IEC 27001, 2006. Disponível: https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf. Acesso em: 10 nov. 2020

AGUADO, Alexandre Garcia; CANOVAS, Isabel Álvarez. **EDUCAÇÃO *HACKER* E EMPODERAMENTO: partilhando caminhos e experiências**. *In:* Actas del II Congreso Internacional Move.net. sobre Movimientos Sociales y TIC. 25 – 27 de octubre 2017. Universidad de Sevilha. COMPOLITICAS. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revistateias/article/view/43375 Acesso em: 28 set. 2020.

ALEXANDRIA, João Carlos Soares de. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO: Uma proposta para potencialização a efetividade da segurança da informação em um ambiente de pesquisa científica.** Tese (Doutorado em Tecnologia Nuclear). IPEN. São Paulo, SP, 2009.
Disponível em: https://www.teses.usp.br/teses/disponiveis/85/85131/tde-22092011-095831/pt-br.php Acesso em: 27 set. 2020.

ALLEASY. Ataques Cibernéticos: Qual é a posição do Brasil? *In:* **Alleasy,** São Paulo, 2020.
Disponível em: https://www.alleasy.com.br/2020/01/20/ataques-ciberneticos-brasil-ranking-mundial/. Acesso em: 26 ago. 2020.

ATECH. Inovação e Tecnologia. *In:* **ATECH,** São Paulo, 2017. Disponível em: https://www.atech.com.br/nossa-trajetoria/. Acesso em: 19 out. 2020.

ATECH. Segurança x UX: Qual a relação do usuário com a segurança do sistema? *In:* **ATECH.** São Paulo, 2019. Disponível em: https://www.atech.com.br/blog/tag/seguranca-digital/. Acesso em: 19 out. 2020.

BACH Sirlei Lourdes. **CONTRIBUIÇÃO DO HACKER PARA O DESENVOLVIMENTO TECNOLÓGICO DA INFORMÁTICA.** Dissertação (Mestrado em Ciência da Computação). Universidade Federal de Santa Catarina. Florianópolis, SC, 2001. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/82176/184565.pdf?sequence=1&isAllowed=y Acesso em: 03 out. 2020.

CANALTECH. Isolamento e home-office levaram a aumento em ataques de *ransomware* no Brasil. Escrito e publicado por Felipe Demartini, *In:* **Canaltech,** 26 março 2020. Disponível em: https://canaltech.com.br/hacker/isolamento-e-home-office-levaram-a-aumento-em-ataques-de-ransomware-no-brasil-162463/. Acesso em: 07 nov. 2020.

CAPOBIANCO, Lígia; CURY, Lucilene. **Princípios da História das Tecnologias da Informação e Comunicação Grandes Invenções.** *In*: VIII Encontro Nacional da Mídia Brasileira, Unicentro, Guarapuava, PR, abril 2011. Disponível em: http://www3.eca.usp.br/sites/default/files/form/cpedagogica/Capobianco-Princpios_da_Histria_das_Tecnologias_da_Informao_e_Comunicao__Grandes_Histrias_Principles_of_ICT_History.pdf. Acesso em: 01 nov. 2020.

CARMO, Francisco. A. S. **A eficiência das principais práticas nos ataques de Engenharia Social.** INATEL – Instituto Nacional de Telecomunicações. Santa Rita do Sapucaí, MG, 2017. Disponível em: https://www.researchgate.net/publication/322488951_A_EFICIENCIA_DAS_PRINCIPAIS_PRATICAS_NOS_ATAQUES_DE_ENGENHARIA_SOCIAL. Acesso em: 29 ago. 2020.

Cert.br. Incidentes reportados ao Cert.br – Janeiro a dezembro 2019, 2019. Disponível em: https://www.cert.br/stats/incidentes/2019-jan-dec/total.html Acesso em: 29 ago. 2020.

CERT.br. Estatísticas dos Incidentes reportados ao Cert.br, 2020. Disponível em https://www.cert.br/stats/incidentes/. Acesso em: 29 ago. 2020.

CERT.br Cartilha de Segurança para Internet. Versão 4.0. São Paulo. 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf Acesso em: 25 set. 2020.

CHIAVENATO, Idalberto. **Comportamento Organizacional: a dinâmica do sucesso das organizações.** 2ª ed. Rio de Janeiro: Elsevier, 2005.

CIO, Ataques de *ransomware* se multiplicam durante a pandemia. Como fica a LGPD? Escrito e publicado por Denis Brach. *In:* **CIO from IDG,** 26 outubro 2020. Disponivel em: https://cio.com.br/tendencias/ataques-de-ransomware-se-multiplicam-durante-a-pandemia-como-fica-a-lgpd/. Acesso em: 08 nov. 2020.

COMPUGRAF. Guerra Cibernética e os conflitos na era da Informação. Escrito e publicado por Luisa Varella *In:* **Compugraf: Segurança da informação,** Julho 2020. Disponível em: https://www.compugraf.com.br/guerra-cibernetica/. Acesso em: 18 set. 2020.

CRYPTO. Como as empresas podem elevar a segurança contra novas ameaças e ransomware? ESCRITO E PUBLICADO POR Fernando Cardoso. *In:* **CRYPTO ID**, Setembro, 2019. Disponível: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/emailseguro/. Acesso em: 24 out. 2020.

DURAN, Débora. **Alfabetismo Digital e Desenvolvimento:** das afirmações às interrogações. Tese (Doutorado em Educação). USP, São Paulo, 2008. Disponível em: https://www.teses.usp.br/teses/disponiveis/48/48134/tde-07052013-162230/publico/debora.pdf. Acesso em: 01 nov. 2020.

FEBRABAN.ENGENHARIA SOCIAL: Saiba como identificar possíveis armadilhas e se proteger de golpes, São Paulo. 2017. Disponível em:

https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/cartilha_eng_social_final.pdf. Acesso em: 25 set. 2020.

FONSECA, Marcelo. **ENGENHARIA SOCIAL: Conscientizando o elo mais fraco da segurança da informação.** Monografia (Curso de Especialização em Inteligência da Segurança Pública). Universidade do Sul, Santa Catarina, SC, 2017. Disponível em: https://riuni.unisul.br/handle/12345/2402. Acesso em: 30 ago. 2020.

FONTES, Eison. **Segurança da Informação.** 1ª ed. São Paulo: Saraiva. 2001.

GARTNER. 10 Principais tecnologias em segurança da informação para se atentar. *In:* **AlgarTech Blog,** 2016. Disponível em: https://algartech.com/pt/blog/gartner-10-principais-tecnologias-em-seguranca-da-informacao-para-se-atentar/. Acesso em: 09 nov. 2020.

GARTNER. Software de Inteligência Artificial: Conheça mais de 30 ferramentas para adotar em sua gestão. *In:* **Runrun.it Blog,** 2019. Disponível em: https://blog.runrun.it/software-de-inteligencia-artificial/. Acesso em: 09 nov. 2020.

GASPAR, Jana Eça Hohlenwerger Muniz. **Análise Comportamental sobre ataques de engenharia social.** Dissertação (Mestrado em Engenharia Informática). Escola Superior de Tecnologia e Gestão, ESTG. Politécnico do Porto, Portugal, 2015. Disponível em: https://recipp.ipp.pt/bitstream/10400.22/11096/1/DM_JanaGaspar_MEI_2015.pdf Acesso em: 10 out. 2020.

GUISSO, Leonardo. **Segurança Digital: Avaliação do nível de conhecimento da população sobre os riscos de segurança atrelados ao uso da internet na região de Bento Gonçalves.** Trabalho de Conclusão de Curso (Curso de Sistemas de Informação). Universidade de Caxias do Sul. Bento Gonçalves, RS, 2017. Disponível em: https://repositorio.ucs.br/handle/11338/3081. Acesso em: 27 set. 2020.

GOCACHE. Veja os 10 países do mundo com o maior número de hackers e crimes cibernéticos**.** *In:* **GOCACHE,** 2017. Disponível em: https://www.gocache.com.br/seguranca/dez-paises-com-mais-ataques-de-hackers/ Acesso em: 25 ago. 2020.

GRUPO BETTENCOURT. Metade das empresas brasileiras foi vítima de crimes econômicos. *In:* **JusBrasil,** 2018. Disponível em: https://bettencourt.jusbrasil.com.br/noticias/560143923/metade-das-empresas-brasileiras-foi-vitima-de-crimes-economicos. Acesso em: 24 de out. 2020.

HENRIQUES, Francisco de Assis Fialho. **A influência da Engenharia Social no fator humano das Organizações.** Dissertação (Mestrado em Ciência da Computação). Universidade Federal de Pernambuco, Recife, PE, 2016. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/25353/1/DISSERTA%c3%87%c3%83O%20Francisco%20de%20Assis%20Fialho%20Henriques.pdf Acesso em: 12 set. 2020.

HYPNESS. Aqui vai um breve resumo do livro 10 argumentos para você deletar agora suas redes sociais. Escrito e publicado por Jaron Larnier. *In:* **Portal Hypness**. Brasil. 2018. Disponível em: https://www.hypeness.com.br/2018/12/aqui-vai-um-breve-resumo-do-livro-10-argumentos-para-voce-deletar-agora-suas-redes-sociais/. Acesso em: 11 out. 2020.

I9 CONSULTORIA E CONTABILIDADE. Conheça a certificação ISO/IEC 27001- Sistema de Gestão de Segurança da Informação. *In:* **I9 Consultoria e Treinamento**. São Paulo, SP, 2019. Disponível em: https://www.i9ce.com.br/iso-27001/. Acesso em: 10 nov. 2020

INTERNETLAB. #PerguntePorQue. 19 julho 2018 (2m4s). *In:* **Pesquisa em direito e tecnologia,** 19 julho 2018. Disponível em: https://www.youtube.com/watch?v=uHZs3ADb6RQ&feature=emb_logo. Acesso em: 07 nov. 2020.

JONATHAN, Miguel. **Um breve histórico em computação no Brasil.** HCTE – Universidade Federal do Rio de Janeiro – UFRJ, Rio de Janeiro, RJ, 2012. Disponível em: http://www.hcte.ufrj.br/downloads/sh/sh6/SHVI/trabalhos%20orais%20completos/trabalho_118.pdf .Acesso em: 01 nov. 2020.

JUSBRASIL. ISO 277001: Como a norma se harmoniza com a LGPD e como adequar e certificar sua empresa? Escrito e publicado por José Milagre. *In:* **jusBrasil,** 2019. Disponível em: https://josemilagre.jusbrasil.com.br/artigos/783012120/iso-27701-como-a-norma-se-harmoniza-com-a-lgpd-e-como-adequar-e-certificar-sua-empresa. Acesso em: 10 nov. 2020.

KASPERSKY. O que é *ransomware*? *In:* **KASPERSKY,** 2020. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware. Acesso em: 07 nov. 2020.

MAGALHÃES, Leandro. Engenharia Social: 4 formas que os golpes são aplicados**.** *In:* **Brasil Cloud Nuvem Corporativa**. Uberlândia, MG, 2020. Disponível em: https://blog.brasilcloud.com.br/4-formas-que-os-golpes-da-engenharia-social-sao-aplicados/. Acesso em: 25 set. 2020.

MARCIANO, João Luiz Pereira. **Segurança da Informação: Uma abordagem Social.** Tese (Doutorado em Ciência da Informação). UNB, Brasília, DF, 2009. Disponível em: https://repositorio.unb.br/handle/10482/1943
Acesso em: 13 out. 2020.

MATTOS, Cristiane Millan. **A escola como espaço de inclusão digital:** Facetas da inclusão digital caracterizando-se em sua maioria em uma pesquisa de campo. Trabalho de Conclusão de Curso (Curso de Matemática) Universidade de Passo Fundo, Rio Grande do Sul, RS, 2010. Disponível em:

https://monografias.brasilescola.uol.com.br/matematica/a-escola-como-espaco-inclusao-digital.htm. Acesso em: 01 nov. 2020.

MAULAIS, Cláudio Nunes dos Santos. **ENGENHARIA SOCIAL: Técnicas e estratégias de defesa em ambientes virtuais vulneráveis.** Projeto de Pesquisa (Mestrado em Sistemas de Informação). Universidade FUMEC. Belo Horizonte, MG, 2016. Disponível em: http://www.fumec.br/revistas/sigc/article/view/3733 Acesso em: 29 ago. 2020.

MICHAELIS. **Moderno Dicionário da Língua Portuguesa,** 2016. Disponível em: http//michaelis.uol.com.br. Acesso: 17 set. 2020.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. São Paulo: Makron (Pearson Education), 2003.

MITNICK, Kevin. D.; SIMON, William L. **A arte de invadir**. São Paulo: Makron (Pearson Education), 2006.

OLHAR DIGITAL. O que a análise de comportamento do usuário revela para a segurança. Escrito e publicado por Waldo Gomes. *In:* **OLHAR DIGITAL,** 24 agosto 2020. Disponível em: https://olhardigital.com.br/pro/noticia/o-que-a-analise-de-comportamento-do-usuario-revela-para-a-seguranca/105762?fbclid=IwAR2zzLhU1IwOH2QAjmAPEsGjKhUz-VK6GeSH0WT08X__1Idz-j_CYmp-VNs. Acesso em: 09 nov. 2020.

POSITIVO TECNOLOGIA. Seis golpes de Engenharia Social para ficar de olho. *In:* **PANORAMA POSITIVO.** São Paulo, 2018. Disponível em: https://www.meupositivo.com.br/panoramapositivo/golpes-de-engenharia-social/ Acesso em: 26 set. 2020.

PROOF. **Somos PROOF.** *In:* **PROOF – SEGURANÇA DA INFORMAÇÃO,** Rio de Janeiro, 2008. Disponível em: https://www.proof.com.br/somos-proof/. Acesso em: 6 set. 2020.

PROOF. Política de Segurança da Informação: Como criar uma política de segurança da informação em sua empresa**.** *In:* **PROOF – SEGURANÇA DA INFORMAÇÃO,** Rio de Janeiro, 2017. Disponível em: https://www.proof.com.br/blog/politica-de-seguranca-da-informacao/. Acesso em: 27 set. 2020.

PROOF. *Ransomware*, o que você sabe sobre essa ameaça? *In:* **PROOF-SEGURANÇA DA INFORMAÇÃO,** Rio de Janeiro, 2018. Disponível em: https://www.proof.com.br/blog/ransomware/. Acesso em 08 nov. 2020.

RAYMOND, Eric Steven. **A Brief History of Hackerdom.** 1999. Disponível em: http://catb.org/~esr/writings/cathedral-bazaar/hacker-history/ar01s02.html Acesso em: 04 out. 2020.

SÊMOLA, Marcos. **Gestão da Segurança da informação: uma visão executiva.** Rio de Janeiro: Campus Elsevier, 2003.

SILVA, Narjara Bárbara Xavier *et al*. **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.** *In:* RICI: R.Ibero-Amer. Ci. Inf**.,** ISSN 1983-5213, Brasília, DF, v. 6, n. 2, p. 37-55, ago./dez. 2013. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782/1573 Acesso em: 13 out. 2020.

SILVA, Thaise de Oliveira; SILVA, Lebiam Tamar Gomes. **Os impactos sociais, cognitivos e afetivos sobre a geração de adolescentes conectados às tecnologias digitais.** *In*: Revista PsicoPedagogia, Vol. 34, N^0 103, ISSN 0103-8486. São Paulo, SP, 2017.
Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S0103-84862017000100009. Acesso em:12 set. 2020.

SIPAHI, Guilherme Matos. **A (r)evolução da informática.** *In*: Notícias, IFSC, Instituto de Física, USP- São Carlos. São Carlos, SP, 2012.
Disponível em: https://www2.ifsc.usp.br/portal-ifsc/a-revolucao-da-informatica/ Acesso em: 12 set. 2020.

STRONGSECURITY. Conheça a ISO 27001 e sua influência na segurança da informação. *In:* **STRONGSECURITY.** São Bernardo do Campo. SP, 20 setembro 2019.Disponível em: https://www.strongsecurity.com.br/blog/conheca-a-iso-27001-e-sua-influencia-na-seguranca-da-informacao/. Acesso em: 10 nov.2020.

TECHTUDO. Dia da Informática: veja a evolução dos PCs ao longo das décadas. Escrito e publicado por Filipe Garret.**TechTudo,** 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/08/dia-da-informatica-veja-a-evolucao-dos-pcs-ao-longo-das-decadas.ghtml. Acesso em: 21 out. 2020.

TOREZANI, Nathália. O crescimento do e-commerce no Brasil**.** *In:* **EcommerceBrasil Muito mais que Ecommerce**. São Paulo, SP, Agosto 2008. Disponível em:https://www.ecommercebrasil.com.br/artigos/o-crescimento-do-e-commerce-no-brasil/. Acesso em: 30 ago. 2020.

ZAGER, Masha. **Who are the Hackers?** *In:* InfoSecNew, 17 setembro 2002. Disponível em: http://lists.jammed.com/ISN/2002/09/0076.html. Acesso em: 10 out. 2020.

APÊNDICE A

Questionário TCC - Engenharia Social

Questionário TCC - Engenharia Social - Paulo Henrique Romualdo

Por favor, poderia participar de uma análise, respondendo as questões a seguir para uma pesquisa quantitativa que é parte do meu Trabalho de Conclusão de Curso, com finalidades apenas acadêmicas.
*Obrigatório

1)Assinale a faixa etária a qual pertence: *

18 a 23 anos

24 a 29 anos

30 a 35 anos

36 a 41 anos

42 a 47 anos

48 a 53 anos

54 a 59 anos

60 a 65 anos

Mais de 65 anos

Outro:

2) Sexo: *

Masculino

Feminino

Outro:

*Obrigatório

3)A empresa em que você trabalha/trabalhou é de T.I (Tecnologia da Informação)? *

Sim

Não

*Obrigatório

4) Já ouviu falar de Segurança de Informação? *

Segurança da Informação é o conjunto de medidas necessárias para garantir que a confidencialidade, integridade e disponibilidade das informações de uma

organização ou indivíduo de forma a preservar esta informação de acordo com necessidades específicas.

Sim
Não
*Obrigatório

5) Nesta mesma empresa há (ou havia) treinamentos de conscientização sobre Segurança da Informação ou Tecnologia da Informação? *

Sim
Não

6) Já sofreu algum tipo de: ataque/roubo/vazamento de informações seja pessoais e/ou corporativas? *

Sim
Não
*Obrigatório

7) Das áreas a seguir marque quais ataques já sofreu: *

Clonagem de cartão
Conta bancária
Invasão de e-mail
Rede social roubada/hackeada
Compra online falsa
Exposição de dados pessoais pela Internet
Outro:
*Obrigatório

8) Você sabe identificar quando alguém está tentando atacar/obter informação pessoal sua pelas redes sociais/internet? *

Sim
Não

9) Você saberia identificar um ataque de *Phishing* (que é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito) caso algum *link*/*site* que enviam/mandaram para você é realmente oficial/verdadeiro? *

Sim

Não

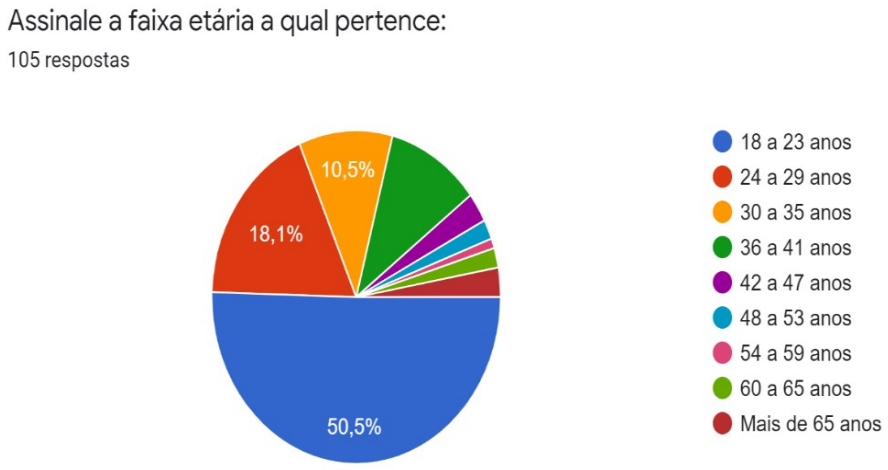
*Obrigatório

(https://docs.google.com/forms/d/e/1FAIpQLSeHobwrhaFEUrAjm0egz-ouu8E6mlpiH2RdcwOXmW5x29yiXw/viewform)

APÊNDICE B

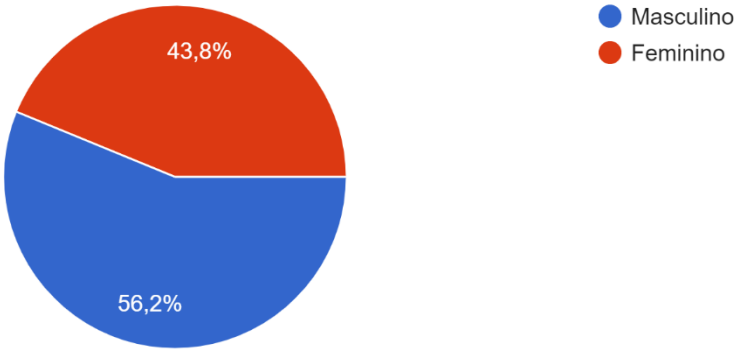
Gráficos o Questionário Sobre SI/Engenharia Social.

Gráficos do Questionário sobre Segurança da Informação/Engenharia Social.



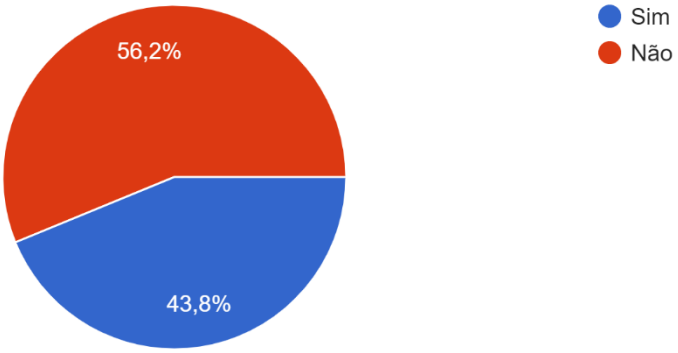
Sexo:

105 respostas



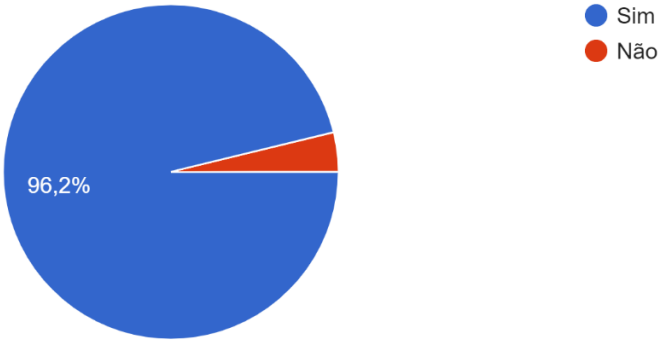
A empresa em que você trabalha/trabalhou é de T.I (Tecnologia da Informação)?

105 respostas



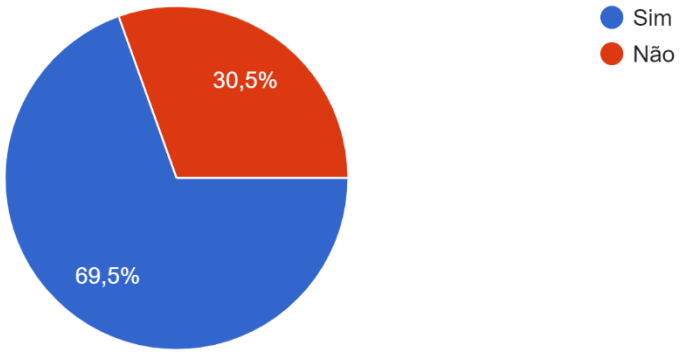
Já ouviu falar de Segurança de Informação?

105 respostas



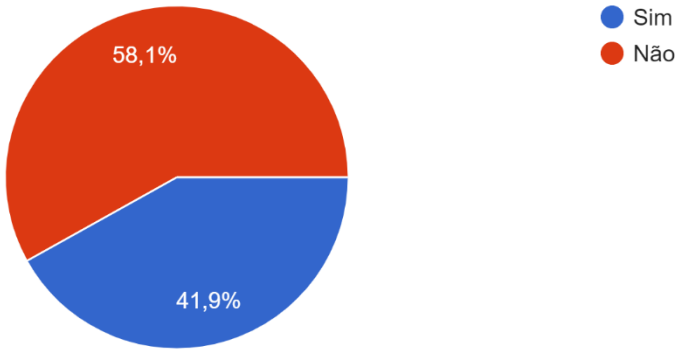
Na empresa em que você trabalha/trabalhou existem políticas de SI?

105 respostas



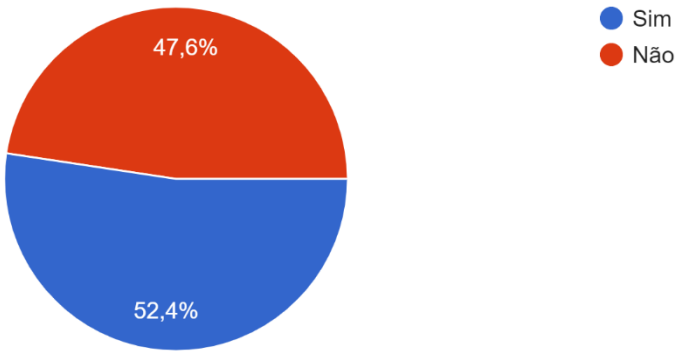
Nesta mesma empresa há (ou havia) treinamentos de conscientização Informação ou Tecnologia da Informação?

105 respostas



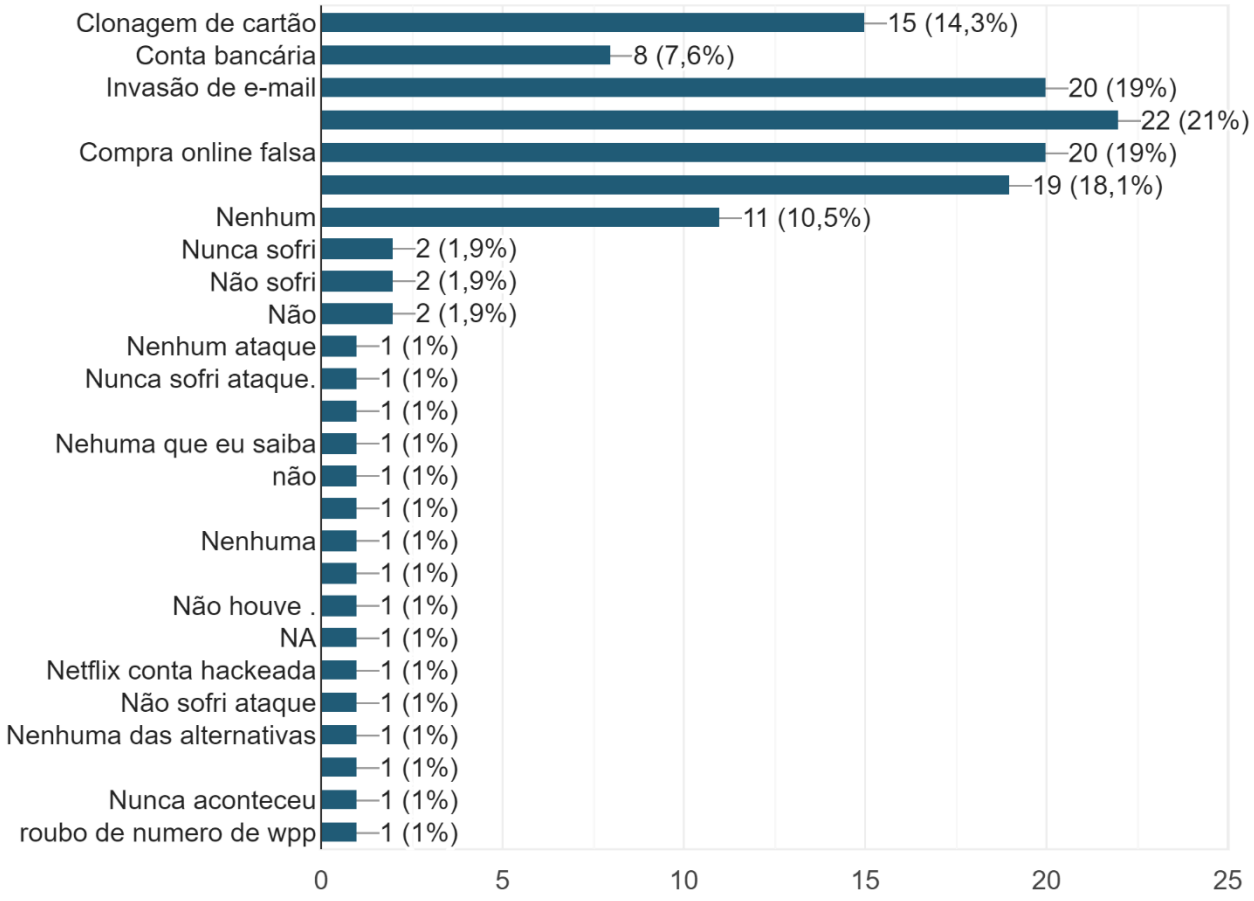
Já sofreu algum tipo de: ataque/roubo/vazamento de informações seja pessoais e/ou corporativas?

105 respostas



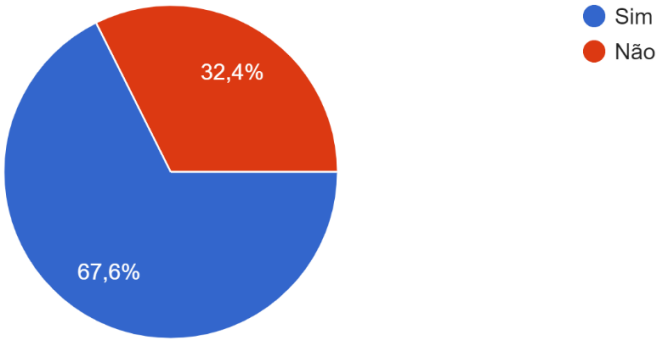
Das áreas a seguir marque quais ataques já sofreu:

105 respostas



Você sabe identificar quando alguém está tentando Atacar/obter Informação pessoal sua elas redes sociais/Internet?

105 respostas



Você saberia identificar um ataque de Phishing, que é o crime de enganar as pessoas para que compartilhem informações confidenciais como senh...ram para você é realmente oficial/verdadeiro?

105 respostas