UNIVERSIDADE DO SUL DE SANTA CATARINA

LUCAS COSTA TEIXEIRA

VINICIUS SCHVAMBACH DIEL

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO: ANÁLISE FOCADA NOS PROFISSIONAIS DE UMA EMPRESA DE TECNOLOGIA

Florianópolis

2020

LUCAS COSTA TEIXEIRA
VINICIUS SCHVAMBACH DIEL

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO: ANÁLISE FOCADA NOS PROFISSIONAIS DE UMA EMPRESA DE TECNOLOGIA

Trabalho de Conclusão de Curso apresentado ao Curso de Sistemas de Informação da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel.

Orientador: Maria Inés Castiñeira, Dra

Florianópolis
2020

LUCAS COSTA TEIXEIRA
VINICIUS SCHVAMBACH DIEL

ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO: ANÁLISE FOCADA NOS PROFISSIONAIS DE UMA EMPRESA DE TECNOLOGIA

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel e aprovado em sua forma final pelo Curso de Sistemas de Informação da Universidade do Sul de Santa Catarina.

Florianópolis, 16 de julho de 2020.

_____
Professor e orientador Maria Inés Castiñeira, Dra.
Universidade do Sul de Santa Catarina

_____
Prof. Fabio Eduardo Vieira Angelo, Msc
Universidade do Sul de Santa Catarina

_____
Prof. Mauricio Botelho, Meng.

Dedicamos este trabalho, a todas as pessoas que buscam desenvolver seus conhecimentos referente a segurança de informação. Dedicamos também a todos os professores, mestres e doutores, especialmente a nossos familiares e amigos que nos apoiaram durante esta fase.

AGRADECIMENTOS

Lucas Costa Teixeira agradece a:

Este é um momento muito importante, onde chego ao fim de um ciclo longo de vários altos e baixos. Nada disso teria sido possível se não fosse por Deus, que iluminou meu caminho ao longo desta jornada.

Agradeço meu amigo e sócio Vinícius Schvambach Diel, com quem tive o prazer de concluir mais um grande trabalho de muitos já realizados.

Agradeço à minha família, que quase não tenho palavras para descrever sua importância em minha vida, e que me permitiu chegar até este ponto.

Aos meus amigos, um muito obrigado por todas as vezes que estiveram ao meu lado. E a todos que participaram direta ou indiretamente da minha vida acadêmica, minha eterna gratidão!

Quero agradecer a nossa orientadora Dra. Maria Inés Castiñeira, pelo empenho dedicado neste trabalho.

Agradeço ao Meng Mauricio Botelho, por todo apoio durante o início deste trabalho, e por ter aceitado o convite para participar da nossa banca.

Agradeço aos demais professores do curso de Sistemas de Informação da Unisul, por compartilharem seu tempo e experiências conosco.

Vinícius Schvambach Diel agradece a:

É chegado um momento muito aguardado. O fim de uma jornada tão sonhada, com momentos inesquecíveis, novos conhecimentos e várias novas experiencias, que me apoiaram para os próximos desafios.

Antes de tudo, agradeço a Deus, pelas oportunidades e pela força que me deu para chegar até aqui.

Agradeço ao meu amigo Lucas Costa Teixeira, com quem tive o prazer de realizar este trabalho de conclusão de curso, sendo este um, dentre os vários projetos que já realizamos e ainda vamos realizar juntos.

Agradeço aos meus pais, Eugenio Diel e Nelsi Schvambach Diel, por todo apoio recebido, que me permitiu chegar até este ponto, e por me incentivarem a sempre continuar na busca dos meus sonhos.

Agradeço a todos os meus familiares e amigos, que de alguma forma, contribuíram para que eu chegasse onde estou.

Agradeço a nossa orientadora, Dra. Maria Inés Castiñeira, por todo apoio e pelas revisões deste trabalho. Obrigado por esclarecer tantas dúvidas e ser tão atenciosa.

Agradeço ao Meng Mauricio Botelho, por todo apoio durante o início deste trabalho, e por ter aceitado o convite para participar da nossa banca.

Agradeço também aos demais professores do curso de Sistemas de Informação da Unisul, por compartilharem seu tempo, conhecimento e experiências conosco.

“o único meio de ficar satisfeito é fazer o que você acredita ser um grande trabalho. E o único meio de se fazer um grande trabalho é amando o que você faz”. (JOBS, 2005).

RESUMO

A informação é entendida como um patrimônio para muitas empresas. Com o avanço das tecnologias, é necessário pensar em como proteger essas informações. A falsa sensação de segurança conduz as empresas a adiarem as providências necessárias para a redução dos riscos. Segurança da informação tornou-se crucial para sobrevivência das organizações. O fator humano é o elo mais fraco no que se refere a garantir segurança. Os engenheiros sociais utilizam da vulnerabilidade humana para obter informações sigilosas, sem que as vítimas percebam que estão sendo manipuladas. Este fato demonstra a importância de se conhecer os temas relacionados a engenharia social, pois o treinamento e conscientização são a melhor defesa contra estes tipos de ataque. É preciso conhecer os riscos para saber como minimizá-los. Com base neste contexto, o presente trabalho apresenta um estudo de caso, com enfoque nos funcionários de uma empresa de tecnologia, referente aos seus conhecimentos, práticas e expectativas sobre engenharia social. O objetivo principal foi a apresentação desse estudo de caso, realizado com um setor da empresa. Inicialmente foi realizado um levantamento bibliográfico sobre as áreas relacionadas. Na sequência, e com base na pesquisa bibliográfica, foi elaborado um questionário sobre o perfil socioeconômico e os conhecimentos e práticas na área de segurança da informação e engenharia social, para aplicar aos funcionários da empresa, participantes na pesquisa. As respostas desse questionário permitiram observar como muitos colaboradores ainda desconheciam a importância dos temas relacionados à segurança. A seguir foram implementadas diversas ações de conscientização como apresentação e envio de: folders, vídeos, e-mails, FAQ e seminários. Na sequência o mesmo questionário voltou a ser aplicado para os participantes da primeira pesquisa. Após o desenvolvimento das ações de conscientização, foi possível identificar um incremento de quase 80% em relação aos conhecimentos dos colaboradores em alguns dos tópicos abordados durante a pesquisa, comprovando a eficácia das ações de sensibilização na empresa pesquisada. Concluiu-se que a aplicação de ações de conscientização, são medidas simples e de baixo custo, porém muito eficazes no incremento das medidas de segurança e proteção dos ativos de informações das empresas.

Palavras-chave: Engenharia Social. Segurança da Informação. Políticas de Segurança.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE GRÁFICO

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A importância da tecnologia cresce de forma acelerada, tornando as empresas dependentes das facilidades que essas tecnologias trazem. Com essas facilidades, existe também o aumento do número de incidentes relacionados à segurança da informação. O grande problema para as empresas é se proteger dos riscos que ainda não se conhecem (NAKAMURA, 2007).

Sempre houve grande preocupação das empresas na segurança física, porém, mais recentemente os investimentos na proteção das informações tornaram-se uma prioridade nas empresas, inclusive nas de tecnologia (PRESTES, 2018). Mas, mesmo que a segurança física seja reforçada, há outras considerações a respeito da segurança das informações que ainda fragilizam as organizações e devem ser observadas, conforme observa Mitnick:

> Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialista, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Estes indivíduos ainda estarão completamente vulneráveis (MITNICK, 2003, p. 3).

As pesquisas ligadas a segurança da informação devem ser contínuas e evolutivas, isto porque as formas de ataque estão em constante evolução e a cada dia novas vulnerabilidades são identificadas. Ao mesmo tempo que surgem novas vulnerabilidades, são necessárias a criação de novas defesas, criando assim um ciclo que é contínuo (NAKAMURA, 2007).

Segundo Nakamura (2007), são vários tipos de riscos em que as organizações estão expostas, precisando se defender através de técnicas, tecnologias e conceitos. Uma destas ameaças é o fator humano, sendo este associado a práticas de engenharia social.

Raef Meeuwisse citado por Kevin Townsend (2019), propõe a engenharia social como: “[...] ato de construir relacionamentos, amizades ou outras interações humanas com o propósito de incitar o destinatário a realizar uma ação desaconselhável ou revelar informações secretas.”

> O fator humano tem sido considerado pelos especialistas a principal ameaça à segurança da informação. Os hackers ainda não encontraram uma maneira mais fácil de violar a proteção de uma empresa do que atacando um usuário

> e um PC específicos. Eles utilizam a engenharia social para obter informações confidenciais (PRESTES, 2018).

Muitas empresas estão sujeitas a vulnerabilidades que são provocadas, não somente por ameaças tecnológicas, mas também por aspectos humanos, pois ainda possuem uma deficiência na percepção dos problemas gerados pelo fator humano (SÊMOLA, 2014).

A segurança da informação é uma área muito abrangente e que exige o uso de diversas tecnologias e procedimentos, usados de forma complementar e que devem estar sempre sendo atualizados. As empresas que não estão preparadas para enfrentar tais procedimentos podem sofrer graves consequências. Neste trabalho, serão apresentados, através da sua metodologia, os conceitos referentes a segurança de informação e engenharia social, além das recomendações de boas práticas referentes a este tema. O trabalho tem enfoque nos funcionários de uma empresa de tecnologia que será usada como organização estudo de caso. Por questões de confidencialidade, o nome da organização não será divulgado.

1.1 OBJETIVOS

Com base no tema problema da pesquisa, apresentam-se na sequência, os objetivos do trabalho de conclusão de curso a serem alcançados.

1.1.1 Objetivo geral

Este trabalho tem como objetivo geral, através da pesquisa na área de segurança de informação e engenharia social, desenvolver um estudo para aplicação das técnicas de segurança e engenharia social em uma organização da área da tecnologia da informação e verificação da efetividade dessas ações.

1.1.2 Objetivos específicos

Para alcançar este objetivo, alguns dos objetivos específicos são:

- Pesquisar sobre a segurança da informação, com foco nos temas relacionados a engenharia social;

- Conceituar alguns dos principais tipos de ataques utilizados por “hackers” que utilizam táticas de engenharia social e os seus possíveis impactos.
- Realizar um levantamento com os funcionários da empresa estudada sobre os seus conhecimentos em Engenharia Social.
- Desenvolver uma ação na empresa estudada, disseminando o conhecimento sobre engenharia social e segurança da informação.
- Desenvolver uma nova pesquisa após as aplicações das ações sugeridas na empresa pesquisada neste trabalho.
- Validar através dos resultados das duas pesquisas, se as propostas de ações sugeridas tiveram o efeito esperado na empresa pesquisada neste trabalho.

1.2 JUSTIFICATIVA

Este trabalho visa colaborar com o conhecimento científico, trazendo informações atualizadas, focadas em um tema importante dentro da área de segurança da informação, que é a engenharia social.

Conforme Mitnick (2003, p. 3) “o fator humano é o elo mais fraco da segurança da informação”. É importante que as empresas em geral e não restrito somente as de tecnologia, conheçam os riscos pertinentes a área de engenharias social em que estão sujeitas, para que possam estar preparadas contra estas vulnerabilidades.

Um exemplo que reflete a importância de conhecer os temas abordados neste trabalho, aconteceu em uma empresa de tecnologia norte americana, chamada Ubiquiti Networks, que teve um prejuízo aproximado em 45 milhões de dólares, devido a um golpe onde foram utilizadas técnicas de engenharia social. Por este motivo o estudo das empresas sobre assuntos ligados a engenharia social, pode evitar novos casos, com prejuízos em valores inestimáveis (HAKETT, 2015, tradução nossa).

O trabalho irá apresentar sugestões práticas que devem ser adotadas por empresas de tecnologia que querem manter suas informações seguras. Essas sugestões práticas foram validadas a partir do macro conceitual que será apresentado na revisão bibliográfica.

1.3 ESTRUTURA DA MONOGRAFIA

Este trabalho será organizado como descrito a seguir.

No capítulo um, é abordado o tema e problemas, os objetivos gerais e específicos e a justificativa do trabalho.

No capítulo dois, é apresentada uma revisão da literatura sobre os conceitos gerais de segurança da informação.

No capítulo três, é apresentado uma revisão da literatura sobre engenharia social.

No capítulo quatro, é apresentado uma revisão da literatura sobre políticas de segurança, desenvolvimento de uma estrutura de segurança e orientações de treinamento e conscientização sobre segurança nas empresas.

No capítulo cinco, é apresentado a metodologia de pesquisa.

No capítulo seis, é apresentado uma pesquisa prática com funcionários da empresa de tecnologia, referente aos seus conhecimentos de engenharia social, junto com sugestões de ações para diminuir o risco de ataques dentro das empresas de tecnologia.

No capítulo sete, é apresentado as ações de conscientização aplicadas na empresa pesquisada, assim como a validação dos resultados após a aplicação destas ações, através da nova pesquisa realizada.

No capítulo oito, são apresentadas as conclusões e os trabalhos futuros desta monografia.

2 SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta a revisão da literatura a respeito do tema Segurança da Informação. É constituída da fundamentação teórica para o desenvolvimento da proposta a qual este trabalho tem por objetivo.

2.1 INFORMAÇÃO

Para entender a importância da segurança da informação para as organizações, primeiro vamos conhecer o que é um dado, e quando este mesmo dado se transforma em uma informação que requer investimentos para protegê-la. Afinal, segundo Ferreira (2003), a informação é um ativo importante que necessita ser protegido de forma adequada.

2.1.1 Dados

Os dados são fatos, eventos, atividades e transações que foram registradas, armazenadas e podem ter sido classificadas, porém não tiveram nenhum tipo de organização que gerasse algum tipo de significado (TURBAN; RAINER Jr; POTTER, 2003).

Segundo Côrtes (2008, p. 26) Dados são:

> Sucessões de fatos brutos, que não foram organizados, processados, relacionados, avaliados e interpretados, representando apenas partes isoladas dos eventos, situações ou ocorrências. Constituem as unidades básicas, a partir das quais informações poderão ser elaboradas ou obtidas.

Podemos concluir a definição de um dado como uma expressão que se encontra em estado bruto e não passou por nenhum tipo de interpretação de um fato (MAÑAS, 2005).

2.1.2 Informação

A informação pode ser definida como um conjunto de fatos organizados, de modo que faça sentido ao seu destinatário. As informações surgem sempre a partir

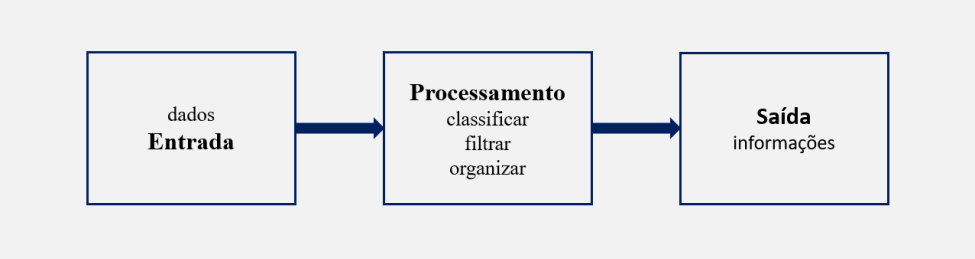
de dados que foram processados com o objetivo de agregar valor (TURBAN; RAINER Jr; POTTER, 2003).

Segundo Mañas (2005, p. 64), “Informação é um dado registrado, classificado, organizado ou interpretado dentro de um contexto, exprimindo um significado. É um acréscimo de conhecimento”.

Laudon e Laudon (2014), elucidam o conceito de informação de maneira simples, como dados que são apresentados em uma forma significativa e útil.

Côrtes (2008), ilustra através de um esquema básico o funcionamento de um sistema de processamento, onde dados são transformados em informação:

Figura 1 - Esquema básico de um processamento de dados.

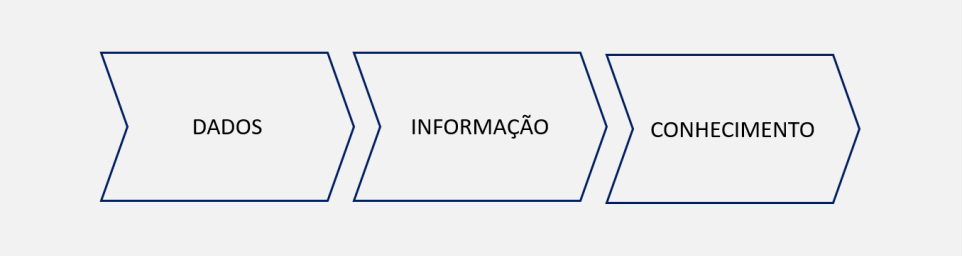


Fonte: Baseado em Côrtes (2008, p. 27).

As informações compõem recursos estratégicos para uma empresa, sendo um ativo fundamental para as empresas modernas, podendo inclusive trazer situações de vantagem diante da concorrência (MAÑAS, 2005).

Campos (2006) ilustra que a informação é a base para o conhecimento. Através dos dados conseguimos gerar informação e consequentemente conhecimento:

Figura 2 – Informação é a base para o conhecimento.



Fonte: Baseado em Campus (2006, p. 3).

É importante analisar e interpretar os dados coletados, para que em momentos oportunos, estes dados que se transformem em informação e possam apoiar nos

momentos de tomadas de decisões. Conforme citado por Mañas (2005, p. 51), “a informação vem acrescentar ganho de capital” dentro da organização.

Para as organizações, as informações são necessárias para mantê-las atualizadas, competentes e competitivas diante da sua concorrência, pois estas passaram-se a ser tratadas como o aspecto estratégico de maior relevância, aumentando as chances de sucesso na tomada de decisões (MAÑAS, 2005).

Na era da industrialização, as empresas protegiam seus ativos reais, em outras palavras, o seu patrimônio. Porém estamos hoje na era das informações, onde as empresas precisam proteger não somente seus ativos, mas também seu capital intelectual e suas informações. A informação é algo intangível, abstrato e que pode estar armazenado de diversas formas, o que dificulta a sua proteção (DAWEL, 2005).

2.1.3 Classificação das Informações

Para entender a importância que uma informação tem para a organização e poder garantir a segurança dos dados estratégicos, é preciso fazer a classificação das informações. Segundo Ferreira e Araújo (2006), a classificação atribui o grau de sigilo das informações, estejam elas armazenadas em meios digitais ou impressos.

De acordo com Ferreira e Araújo (2006, p. 51),” Para iniciar o processo de classificação das informações é necessário conhecer o negócio da organização, compreender os processos e atividades realizadas”.

A classificação das informações deve ser de fácil compreensão, com objetivo de garantir o entendimento entre todos os colaboradores da organização (FERREIRA, 2003).

Segundo Ferreira e Araújo (2006), a proteção das informações e segredos de negócio deve ser tratada com extrema importância, deve-se definir claramente quais dados são confidenciais e merecem tratamento especial. Somente três níveis já são suficientes para uma boa prática de classificação da informação:

- Informação Pública: São as informações que não necessitam de nenhum tipo de sigilo, podendo ter livre acesso a qualquer colaborador da organização, desta forma não é necessário investir em recursos de proteção para esses dados;

- Informação Interna: São informações que devem ser evitadas ao acesso externo, porém não existem graves consequências se esses dados se tornarem de conhecimento público;
- Informação Confidencial: São informações confidenciais dentro da organização e devem ser protegidas do acesso externo, pois o vazamento dessas informações pode comprometer as operações da organização.

A classificação das informações aumenta a confiabilidade dos dados e garante sua confidencialidade, integridade e disponibilidade. A classificação correta das informações reduz drasticamente os custos que seriam necessários para proteger as informações (FERREIRA, 2003).

Conforme Ferreira e Araújo (2006), após a classificação das informações, deve-se elaborar e implementar procedimentos para monitoramento contínuo. É necessário que seja revisado a classificação das informações para garantir que continuem adequadas aos critérios de segurança da organização.

2.2 SISTEMAS DE INFORMAÇÃO

Os sistemas de informação já são considerados partes integrantes das organizações. Segundo Laudon e Laudon (2014), para algumas empresas, sem a existência de sistemas de informação, não haveria negócio.

Segundo Laudon e Laudon (2014, p. 13),

> Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.

Sistemas de informação possuem componentes que coletam, manipulam e disseminam os dados em informações. Essas informações são utilizadas pelas organizações para a tomada de decisões (ALBERTÃO, 2005 apud CÔRTES, 2008).

As organizações entendem que os sistemas de informação são essenciais para sobrevivência e prosperidade das mesmas. Com as informações, em conjunto com esses sistemas, torna-se possível que as empresas estendam seu alcance, possam

oferecer novos produtos e serviços e possibilita a melhor estruturação dos seus processos (LAUDON; LAUDON, 2014).

Os sistemas de informação, são considerados atualmente, elemento indispensável para apoiar as operações e a tomada de decisões das empresas modernas (MAÑAS, 2005).

Embora esses sistemas proporcionam grandes vantagens e novas oportunidades para as organizações, também podem se tornar um problema desafiador aos administradores. Laudon e Laudon (2006), elege alguns pontos positivos e negativos desses sistemas de informação:

Quadro 1 - Impactos positivos e negativos dos sistemas de informação

Benefícios dos Sistemas de Informação	**Impacto Negativo**
Sistemas de informação podem processar cálculos ou papéis muito mais rapidamente do que as pessoas.	Automatizando atividades que anteriormente eram realizadas por pessoas, os sistemas de informação podem eliminar empregos.
Sistemas de informação podem ajudar as empresas a aprender mais sobre os modelos de compra e as preferências de seus clientes.	Sistemas de informação podem permitir que as organizações coletem dados pessoas sobre qualquer pessoa, violando sua privacidade.
Sistemas de informação proporcionam novas eficiências, por meio de serviços como caixas automáticos, sistemas telefônicos ou aviões e terminais aéreos controlados por computador.	Sistemas de informação são usados em tantos aspectos da vida diária que uma interrupção em seu funcionamento pode causar uma paralisação de uma empresa ou dos serviços de transportes, paralisando também as comunidades.
Sistemas de informação possibilitaram novos avanços na medicina nas áreas de cirurgia, radiologia e monitoração de pacientes.	Pessoas as que utilizam muito os sistemas de informação podem sofrer lesões por esforços repetitivos, tecnoestresse e outros problemas de saúde.
A internet distribui informação instantaneamente a milhões de pessoas no mundo inteiro.	A internet pode ser usada para distribuir cópias ilegais de softwares, livros, artigos e outras propriedades intelectuais.

Fonte: Baseado em Laudon; Laudon (2006, p. 29).

2.3 SEGURANÇA DA INFORMAÇÃO

Na nossa sociedade, ao mesmo tempo em que as informações são consideradas os principais patrimônios de uma organização, elas também estão em constante risco. Cada vez mais as informações das organizações são colocadas a prova por diversos tipos de ameaças (FERREIRA, 2003).

A falsa sensação de segurança conduz as empresas a adiarem as providências necessárias para redução dos riscos, o que as torna despreparadas para sobreviver e superar os ataques de invasores. Em contrapartida, algumas pesquisas demonstram que o orçamento investido para segurança da informação vem aumentando com o passar dos anos (DAWEL, 2005).

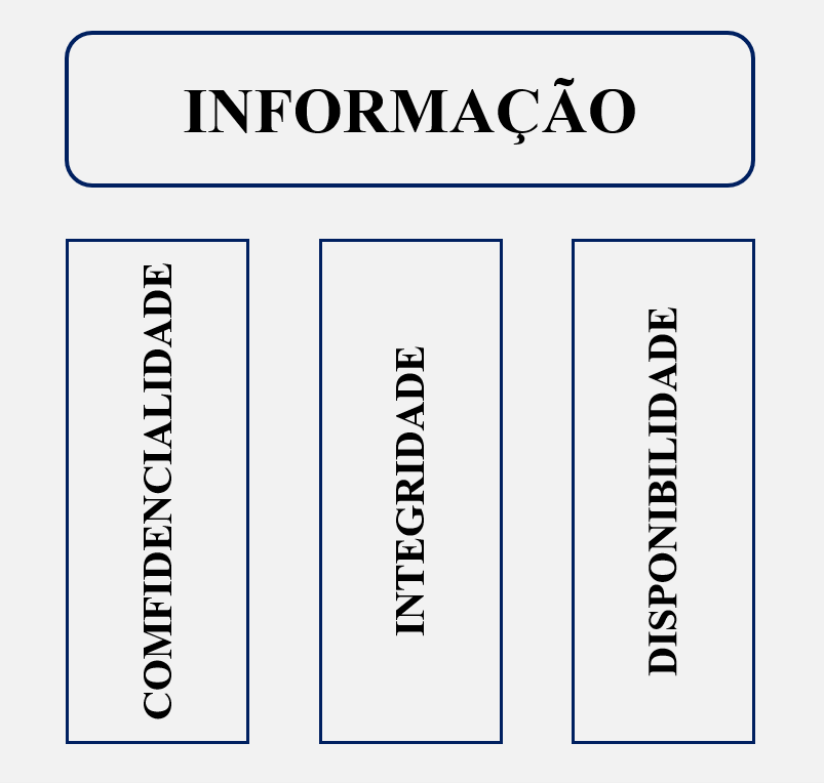
Segundo Turban, Rainer Jr e Potter (2003), em uma pesquisa da Dataquest, realizada no início do século 21, quase 80% de todas as corporações americanas enfrentaram ataques de computadores, o que demonstra o quão despreparadas as empresas estão no que se refere ao assunto de segurança.

É um consenso que o tema segurança da informação tornou-se ponto crucial para a sobrevivência das organizações (FERREIRA, 2003).

Os sistemas de informação possuem muitos componentes distribuídos de forma descentralizada, tornando-os vulneráveis a muitos riscos em potencial. Estas vulnerabilidades dos sistemas, aumentam à medida que nós direcionamos para um mundo de computação e rede (TURBAN; RAINER Jr; POTTER, 2003).

Segundo Campos (2006), um sistema de segurança de informação baseia-se nos princípios da confiabilidade, integridade e disponibilidade, conforme ilustrado na imagem:

Figura 3 – Características de segurança da informação.



Fonte: Baseado em Campos (2006, p. 5).

Segundo Laudon e Laudon (2006, p. 464), segurança da informação:

> Abarca as políticas, procedimentos e medidas técnicas usados para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Ela pode se dar por um conjunto de técnicas e ferramentas destinadas a salvaguardar hardwares, softwares, redes de computadores e dados.

Segundo Fontes (2014, p.11) a segurança da informação pode ser definida como “conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada”.

Segundo Ferreira (2003), a segurança da informação é caracterizada pela:

- Confidencialidade: Garante que a informação será acessada apenas por pessoas que tenham sido explicitamente autorizadas pelo proprietário daquela informação;
- Integridade: Garante a exatidão das informações, consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação;

- Disponibilidade: Garante que os usuários autorizados tenham acesso à informação sempre que necessário;
- Autenticidade: Garante a identificação correta de um usuário ou sistema. A autenticação deve garantir ao receptor que a mensagem realmente foi encaminhada pelo remetente autenticado.

A segurança da informação é a forma com que as empresas protegem suas informações, garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e oportunidades, pois as informações são consideradas recursos críticos nas tomadas de decisões gerenciais e também na efetivação de negócios (FERREIRA, 2003).

A segurança da informação minimiza os riscos do negócio em relação a dependência do uso de recursos de informação. Com uma informação incorreta ou sem o acesso à informação, o negócio pode ter perdas inestimáveis (FONTES, 2014).

À medida que cresce a utilização da internet, também aumentam as notícias sobre violação de segurança. Desta forma, é imprescindível que as empresas que desejam manter suas informações seguras invistam e conheçam os conceitos ligados a segurança da informação (LAUDON; LAUDON, 2014).

2.3.1 Principais tipos de ameaças

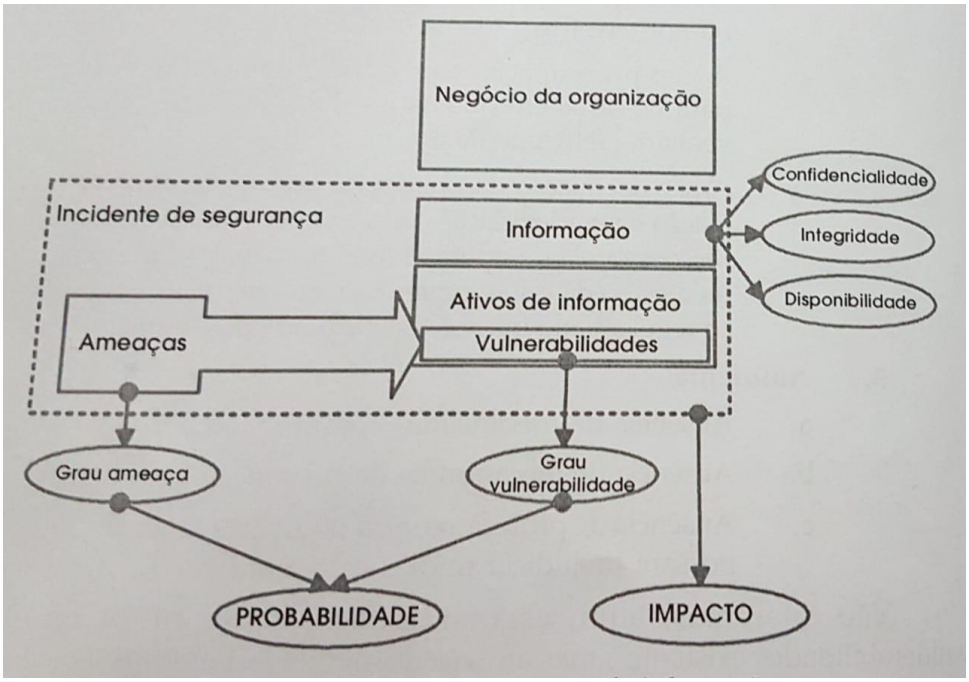
A cada dia surgem novos tipos de ameaças à segurança da informação. Segundo Ferreira (2003) grande parte dos ataques sofridos pelas organizações tem como causa a ausência de cuidado dos administradores, problemas de erros nos sistemas e configuração incorreta dos serviços.

As vulnerabilidades, são fraquezas que podem causar, intencionalmente ou não, a quebra dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade), estão presentes nos próprios ativos da organização das empresas. Uma ameaça surge quando um agente externo se aproveita destas vulnerabilidades (CAMPOS, 2014).

Os responsáveis por trás dessas ameaças são chamados de hackers. Estes podem ser definidos como “uma pessoa que consegue acesso não autorizado a uma rede de computadores, com o intuito de obter lucro, intervir criminosamente ou desfrutar de prazer pessoal” (LAUDON; LAUDON, 2006, p. 462).

Essas ameaças causam incidentes de segurança da informação, que podem causar interrupções nos processos de negócios, quebrando a confidencialidade, integridade ou disponibilidade da informação. Este incidente gera um impacto ou dano ao negócio, conforme ilustrado na imagem:

Figura 4 – Incidente de segurança da informação.



Fonte: Campos (2006, p. 14).

Algumas das principais ameaças que causam impacto para segurança da informação são:

2.3.1.1 Vírus

O vírus é um programa com a capacidade de anexar-se e infectar outros programas de computadores. O vírus tem a capacidade de se prevalecer sob um sistema infectado sem que o proprietário do programa o perceba. Quando o software é inicializado pelo mesmo, o vírus se espalha, provocando danos ao computador e obtendo informações sigilosas (TURBAN; RAINER Jr; POTTER, 2003).

Segundos Fontes (2014, p.66), “os vírus são programas que penetram no computador que utilizamos sem a nossa autorização e executam ações que não solicitamos. Normalmente, essas ações prejudicam o equipamento ou o seu desempenho”.

2.3.1.2 Malware

O malware, também conhecido como *malicious software,* é um tipo de ameaça que instala em seu computador programas que operam sem o seu consentimento, tendo permissões para executar tarefas sem seu conhecimento (MITNICK, 2003).

2.3.1.3 Trojan

Segundo a definição de Ferreira (2003) um trojan, também conhecido popularmente como “cavalo de troia”, é um programa disfarçado que se estabelece dentro do sistema e executa uma tarefa invasiva. Existem diversos trojans dedicados a roubar senhas e outros dados sigilosos.

Conforme Mitnick (2003, p. 48), um trojan é um programa que “contém um código malicioso ou prejudicial, criado para gerenciar os arquivos do computador da vítima ou para obter informações do computador ou da rede da vítima”. Este tipo de ameaça ocorre sem que a vítima perceba a presença da infecção.

2.3.1.4 Spyware

Um spyware é um software especializado em monitorar de forma oculta as atividades de um computador ou sistema. Esta ameaça captura as atividades do usuário, como sites acessados, teclas digitadas e senhas por exemplo (MITNICK, 2003).

Inicialmente um spyware era comercializado para que os pais conseguissem monitorar o acesso de seus filhos na internet, ou para que empresas conseguissem acompanhar o uso dos recursos por seus colaboradores. Posteriormente esse tipo de sistema começou a ser utilizado de forma irregular para espionagem industrial. Atualmente esses sistemas são muito utilizados para captura de informações sem as devidas autorizações do proprietário (MITNICK, 2003).

2.3.1.5 Ataque de força bruta

A força bruta é um ataque que através de um programa tenta todas as combinações de caracteres alfanuméricos e símbolos de forma sistemática, para

tentativa de descobrir uma senha. Estes sistemas normalmente têm alta velocidade, chegando a testar mais de 2,8 milhões de senhas por segundo (MITNICK, 2003).

2.3.1.6 Phishing

Phishing é um ataque utilizado para que a vítima revele informações pessoais como senhas, dados bancários ou dados pessoais. Nesta prática, são utilizados e-mail ou websites falsos, para induzir que a vítima informe dados pessoais sigilosos (PHISHING, 2019).

Segundo Mann (2018), este tipo de ataque trata-se de uma forma simples de explorar a falta de conhecimento referente a segurança das vítimas. O agressor envia um e-mail falso a vítima com informações convincentes, fazendo com que este acesse um link malicioso ou faça o download de um software infectado.

Em um exemplo apresentado por Mann (2018), mostra como esta técnica pode ser lucrativa para os atacantes, pois se forem encaminhados 1.000.000 de e-mails a destinatários aleatórios, onde 5% das pessoas visualizarem o mesmo, e somente 0,1% caíssem efetivamente no golpe. Se cada uma das vítimas possuísse R$1.000 reais em suas contas, o hacker teria ganhado R$50.000 reais neste único golpe.

2.3.1.7 Worms

Um “Worm de computador” é um programa que se auto replica e se espalha pelas redes de computadores. Devido essa infecção consumir muita memória do sistema, sobrecarrega-se o equipamento e consequentemente diminui-se o desempenho da máquina (WORMS, 2019).

2.3.1.8 Adware

O adware é um software mantido por propagandas, normalmente apresentadas como pop-up ou barra de ferramentas. No geral são ameaças que geram incômodo ao usuário, porém não causam danos. Alguns deles podem ser potencialmente perigosos, ao serem utilizados para coletar informações pessoais e rastrear sua navegação (ADWARE, 2019).

2.3.1.9 Ransomware

Um ransomware, também conhecido como *rogueware* ou *scareware*, é uma ameaça que restringe o acesso ao sistema. Posteriormente o atacante solicita que seja pago um resgate para liberar o acesso às informações (RANSOMWARE, 2019).

2.3.1.10 Ataque DDos

O DDos, também chamado de “ataque distribuído de negação de serviço”, é um tipo de ameaça que tenta derrubar sites ou sistemas, sobrecarregando o tráfego de acesso, utilizando milhares de computadores infectados chamados de botnets ou “máquinas zumbis”. Normalmente os alvos desses ataques são grandes organizações, bancos ou governos, porém os usuários comuns, que são usados como os botnets, sofrem os impactos devido a lentidão e travamentos do seu equipamento (DDOS, 2019).

2.3.1.11 Vulnerabilidade Zero-Day

Quando existe o lançamento de um novo sistema ou uma atualização de versões, os hackers procuram por possíveis vulnerabilidades para conseguirem acesso a informações sigilosas. A ameaça do tipo “dia zero” é considerada grave e utiliza-se de vulnerabilidades que são desconhecidas por desenvolvedores do sistema, fabricantes de antivírus ou do público em geral (DIA, 2019).

2.3.1.12 Cross-site scripting

O XSS, também conhecido como *cross-site scripting*, é uma ameaça pelo qual scripts maliciosos são inseridos em aplicativos ou páginas da internet que são considerados confiáveis. O principal objetivo do hacker é coletar dados pessoais, direcionar a navegação para sites fraudulentos ou danificar o computador da vítima (CROSS, 2019).

2.3.2 Principais defesas contra as ameaças aos sistemas

Os ataques contra rede de computadores aumentam consideravelmente a cada ano, tornando cada vez mais necessário o uso e mecanismos de defesa, a fim de minimizar a ação de invasores e pessoas mal-intencionadas". (FERREIRA, 2003).

> A mente humana é uma criação maravilhosa. É interessante notar como as pessoas podem ser criativas para desenvolver modos fraudulentos de conseguir o que querem ou de se livrar de uma situação difícil. Você tem de a usar a mesma criatividade e imaginação para salvaguardar as informações e os sistemas de computadores (MITNICK, 2003 p.175).

As ações que podem ser realizadas com objetivo de se defender contra as ameaças e vulnerabilidades, segundo Fontes (2014), podem ser classificadas como:

- Ações preventivas: seu objetivo é evitar que desastres aconteçam através de orientações básicas de prevenção contra as ameaças. São as mais conhecidas e mais baratas de se implementar;
- Ações detectivas: seu objetivo é identificar problemas que não foram impedidos através das prevenções. Quanto antes identificado uma situação-problema, maior é a chance para tomadas de ações corretivas efetivas;
- Ações corretivas: seu objetivo é minimizar um problema existente. São alternativas que corrigem uma situação-problema, retornando a normalidade do negócio.

Algumas das principais defesas contra ameaças e vulnerabilidades são:

2.3.2.1 Segurança física

Uma das formas mais tradicionais para defesa contra ameaças é a utilização da segurança física, através de barreiras perimetrais, que atuam como estruturas de impedimento para entradas ou saídas não autorizadas (PORTELLA, 2005).

Algumas instalações são altamente críticas ou vulneráveis, necessitando de múltiplas barreiras físicas no entorno dos perímetros de áreas restritas internas (PORTELLA, 2005).

2.3.2.2 Controles Biométricos

Segundo Turban, Rainer Jr e Potter (2003, p. 524), “o controle biométrico é um método automatizado de verificar a identidade de uma pessoa”.

Os sistemas biométricos podem ser considerados uma evolução dos sistemas manuais de reconhecimento. Com a evolução da tecnologia surgem novos sistemas cada vez mais sofisticados. Segundo Ferreira (2003), algumas das principais tecnologias e características dos sistemas biométricos são:

- Impressão digital: Essa tecnologia compara a impressão reconhecida com a base de dados. As digitais são características únicas e consistentes;
- Geometria da mão: Essa tecnologia compara os pontos da palma da mão com a base de dados. Porém este sistema pode não ser tão preciso, visto que com o aumento de peso ou idade pode haver alterações na característica da mão;
- Voz: Essa tecnologia é utilizada para controles de acesso, porém não é tão confiável devido a erros causados pelos ruídos no ambiente e problemas na garganta/cordas vocais do usuário;
- Análise de Íris e Retina: Essa tecnologia utilizada reconhece os pontos no olho do usuário e é considerada mais confiável que as impressões digitais, porém é menos popular devido aos seus custos de implementação serem mais elevado.

2.3.2.3 Autenticação e Autorização

A autenticação garante que somente pessoas previamente autorizadas, tenham acesso às informações. A identificação do usuário deve ser única e através de um código de acesso único, sendo alguns exemplos desses códigos a identificação por senha, cartão de acesso ou impressão digital. Essa unicidade de identificação permite o controle das ações praticadas pelos usuários (FERREIRA, 2003).

Através da identificação é possível se certificar qual usuário está acessando as informações. Dependendo das necessidades do negócio e da criticidade das informações pode-se utilizar uma combinação com mais de um tipo de autenticação, o que aumenta o nível de segurança (FONTES, 2014).

Este tipo de autenticação é chamado de autenticação de dois fatores, no qual é utilizado dois tipos diferentes de autenticação para verificação da identificação (MITNICK, 2003).

Conforme Fontes (2014), um dos recursos mais utilizados para identificação é através das senhas de acesso, em função do baixo custo de implementação e do alto nível de proteção que se pode alcançar. A grande dificuldade encontrada na utilização deste recurso é o uso de várias identificações e senhas para o mesmo usuário.

A autenticação é necessária sempre que for dar acesso a uma informação sigilosa. Cada organização defini quais os sistemas de autenticação são mais adequados ao seu negócio e ao seu ambiente (FONTES, 2014).

2.3.2.4 Firewall

Segundo Laudon e Laudon (2006, p. 473), um firewall “controla o acesso a redes internas da organização, agindo como um porteiro que examina as credenciais de cada usuário antes que ele possa acessar a rede”.

Os firewalls são utilizados para implementar políticas de acesso, seguindo diretrizes que permitem ou bloqueiam o tráfego dos dados. Para garantir uma segurança mais e para atender a necessidade da organização, podem existir diversos firewalls em um sistema de informação (TURBAN; RAINER Jr; POTTER, 2003).

Um firewall é definido por Turban, Rainer Jr e Potter (2003, p. 527) como:

> Um sistema, ou um grupo de sistemas, que reforça uma política de controle de acesso entre duas redes. Geralmente é utilizado como barreira entre a intranet corporativa segura, ou outras redes internas, e a internet, que se supõe serem seguras.

Um firewall pode ser comparado a muros que foram construídos ao redor de uma propriedade. Nesta analogia possuímos um muro virtual que possui algumas aberturas pela qual as informações fluem, existindo um filtro que determina quais informações podem entrar ou sair da rede (DAWEL, 2005).

Para se criar um bom firewall, é necessário escrever e manter as regras internas atualizadas, com objetivo de identificar pessoas, aplicações ou endereços permitidos / rejeitados na rede (LAUDON; LAUDON, 2014).

2.3.2.5 Antivírus

Laudon e Laudon (2006, p. 463) definem antivírus como" um software especial projetado para verificar sistemas de informações [...], a fim de detectar a presença de vários vírus de computador. Muitas vezes o software pode eliminar o vírus da área infectada".

Para reduzir as chances de infecção, as organizações podem utilizar softwares antivírus. Porém, a grande maioria desses sistemas somente é efetiva contra espécies de vírus já conhecidos. Para proteger seus sistemas de forma eficaz, deve-se atualizar constantemente seus antivírus (LAUDON; LAUDON, 2014).

2.3.2.6 Criptografia

A criptografia é uma tecnologia de segurança especialmente útil para proteger mensagens trafegadas na rede (LAUDON; LAUDON, 2014).

Laudon e Laudon (2006, p. 474) define a criptografia como:

> Codificação e a descaracterização de uma mensagem para impedir o acesso não autorizado ou a compressão dos dados transmitidos. Uma mensagem pode ser criptografada aplicando-se a ela um código numérico secreto, denominado chave de criptografia. Com isso, a mensagem será transmitida como um conjunto ininteligível de caracteres.

Segundo Turban, Rainer Jr e Potter (2003) a criptografia codifica um texto regular para transmissão através de um texto que não podem ser lidos. O texto criptografado é descriptografado (decodificado) no recebimento. A criptografia atende três propostos:

- Identificação: Ajuda a identificar os remetentes e destinatários legítimos;
- Controle: Evita alterações da mensagem original durante a sua transmissão;
- Privacidade: Impede o conhecimento da mensagem original por pessoas não autorizadas.

3 ENGENHARIA SOCIAL

Este capítulo apresenta a revisão da literatura a respeito da engenharia social. É constituída a fundamentação teórica para o desenvolvimento da proposta a qual este trabalho tem por objetivo.

3.1 CONCEITOS SOBRE ENGENHARIA SOCIAL

Para entendermos o conceito de engenharia social, é importante conhecermos o significado destas duas terminologias (MICHAELIS, 2019):

- Engenharia: “Arte de aplicar os conhecimentos científicos à invenção, aperfeiçoamento ou utilização da técnica industrial em todas as suas determinações”;
- Social: “Relativo à organização e ao comportamento do homem na sociedade ou comunidade”.

Uma definição direta sobre o que é engenharia social, conforme Mann (2018, p.20), é “manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação”.

Pode-se definir engenharia social como a arte de utilizar o comportamento humano para quebrar a segurança, sem que a vítima perceba que foi manipulada. As pessoas de forma ingênua, fornecem informações importantes, por serem prestativas, educadas ou por confiarem em outras pessoas. Pessoas mal-intencionadas podem se utilizar desta situação para conseguir informações preciosas (DAWEL, 2005).

A engenharia social é uma forma para obtenção de informações, é uma das mais perigosas e eficientes utilizada pelos invasores ao tentar obter alguma informação a qual não deveriam ter acesso (FERREIRA, 2003).

Segundo Côrtes (2008, p. 495), “uma das principais técnicas utilizadas pelos hackers é a engenharia social, por meio da qual é possível a uma pessoa obter senhas de acesso restrito sem grandes dificuldades “.

Nakamura (2007, p. 85) define a engenharia social como:

> Técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização. Essa técnica explora o fato de os usuários estarem sempre dispostos a ajudar e colaborar com serviços da organização.

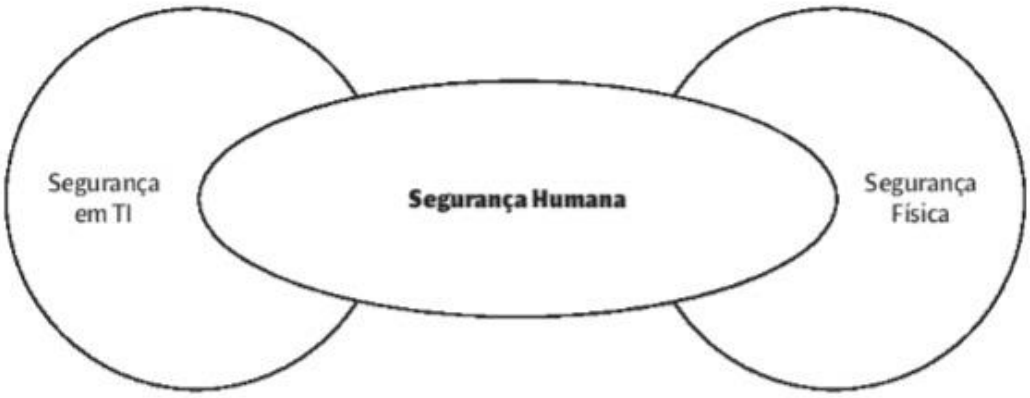
A engenharia social é um conjunto de procedimentos e ações utilizados para adquirir uma informação, sem o uso da força ou de qualquer tipo de brutalidade. “Quando alguém deseja invadir ou acessar dados de uma organização, o caminho mais fácil é através da engenharia social” (FONTES, 2014).

São desenvolvidas diversas soluções de segurança para minimizar riscos ligados ao uso de computadores, porém essas medidas deixam de fora a vulnerabilidade mais significativa, que é o fator humano. Este continua sendo a ameaça mais séria a segurança de informação (MITNICK, 2003).

> Ninguém está imune contra ser enganado por um bom engenheiro social. Devido ao ritmo da vida normal, nem sempre pensamos com cuidado antes de tomarmos as decisões, mesmo em questões que são importantes para nós. As situações complicadas, a falta de tempo, o estado emocional ou a fadiga mental, podem facilmente nos distrair. Assim sendo, tomamos um atalho mental e resolvemos sem analisar cuidadosamente as informações, um processo mental conhecido como resposta automática (MITNICK, 2003 p. 99).

Segundo Mann (2018), existe ampla variedade de ataques envolvendo a engenharia social, sendo a segurança humana uma parte central no que se refere a garantir a segurança das organizações.

Figura 5 – A segurança humana como foco



Fonte: Mann (2018, p.10).

A pessoa que faz a utilização das técnicas de engenharia social, é chamada de engenheiro social. É uma pessoa normalmente simpática, carismática, criativa, persuasiva e que consegue ganhar a confiança das pessoas de forma simples e metodológica (NASCIMENTO, 2018).

3.2 TENDÊNCIAS DA NATUREZA HUMANA

Existem tendências humanas que são utilizadas durante os ataques de engenharia social, tanto de forma consciente, como de forma inconsciente. É importante entender o motivo pelos quais o ser humano é tão vulnerável a este tipo de ataque, permitindo a sua manipulação por engenheiros sociais (MITNICK, 2003).

Segundo Mitnick (2003) existem seis tendências utilizadas pelos engenheiros sociais:

- Autoridade: O ser humano tende a aceitar uma solicitação realizada por uma pessoa com maior autoridade.
- Afabilidade: O ser humano tende a aceitar uma solicitação realizada por alguém que considere agradável ou que possua interesses semelhantes.
- Reciprocidade: O ser humano tende a aceitar uma solicitação quando acredita que vai receber algo em troca.
- Consistência: O ser humano tende a aceitar uma solicitação após adotar uma causa ou fazer um comprometimento.
- Validação social: O ser humano tende a aceitar uma solicitação quando esta parece estar de acordo com o que outras pessoas estão fazendo.
- Escassez: O ser humano tende a cooperar quando acredita que um determinado objeto está em falta ou estará disponível por um período de tempo curto.

3.3 PERFIL DO ENGENHEIRO SOCIAL

Segundo Mitnick (2003), o perfil do engenheiro social na maioria das vezes é amistoso, desembaraçado e prestativo, fazendo com que a vítima se sinta feliz e segura com sua presença.

Os engenheiros sociais têm uma grande habilidade em lidar com as pessoas, possuindo os traços sociais necessários para estabelecer confiança e afinidade durante a sua manipulação, sendo charmosos, educados e bem articulados. Segundo Mitnick (2003, p. 7), “o engenheiro social experiente pode ter acesso a praticamente qualquer informação-alvo usando as estratégias e táticas da sua habilidade”.

> Os engenheiros sociais também são habilidosos para distrair os processos de pensamento das pessoas para que elas cooperem. Pensar que determinadas pessoas não é vulnerável a esta manipulação é subestimar a habilidade e o instinto mortal de um engenheiro social. Um bom engenheiro social, por sua vez, nunca subestime seu adversário (MITNICK, 2003 p.126).

De acordo com Fontes (2014), as principais técnicas utilizadas pelos engenheiros sociais são:

- Falar com propriedade e conhecimento sobre o assunto.
- Adquirir a confiança do interlocutor, estabelecendo uma relação de vínculo entre o engenheiro social e a vítima.
- Prestando favores, oferecendo ao interlocutor ajuda para gerar confiança.

O risco enfrentado pelos engenheiros sociais diminuiu consideravelmente com a chegada da internet e diversas tecnologias de comunicação, permitindo ao agressor distância e anonimato (MANN, 2018).

Grande parte das informações que não aparentam ter grande valor dentro da empresa, é cobiçada pelo engenheiro social, pois com a soma das informações é possível criar credibilidade. Desta forma cabe as organizações a responsabilidade em manter as informações “não públicas” em segurança, pois o simples conhecimento de um termo interno faz com que o engenheiro social tenha autoridade e confiabilidade (MITNICK, 2003).

O objetivo primário do engenheiro social é desenvolver a confiança para que possa executar um ataque. Para podermos nos proteger destes ataques é importante entendermos os limites da confiança, pois confiar, em algumas situações, pode ser muito algo arriscado (MANN, 2018).

Conforme Mitnick (2003), é algo natural do ser humano confiar no próximo, principalmente quando um pedido parece ser aceitável. Os engenheiros sociais

utilizam destes conhecimentos para, através da exploração das vítimas, atingir seus objetivos e conseguir as informações que desejam.

O engenheiro social ganha a confiança facilmente quando a vítima não percebe um motivo para suspeitar. Em muitas vezes basta simplesmente pedir as informações de forma direta e simples, sem a necessidade de mentiras elaboradas e complexas (MITNICK, 2003).

Embora a maioria dos engenheiros sociais utilizem de técnicas por telefone, e-mail ou via internet, existem atacantes mais audaciosos, por realizar os ataques presencialmente. Neste caso são utilizadas técnicas de engenharia social para conseguir ultrapassar as barreiras físicas e ter acesso ao local do ataque (MITNICK, 2003).

O atacante coleta o máximo possível de informações sobre seu alvo, utilizando estas informações para ganhar confiança da vítima e em seguida iniciar o ataque (MITNICK, 2003).

3.4 PRINCIPAIS TÁTICAS UTILIZADAS

A sensação de segurança é enganosa. Incidentes ligados a este termo são sempre prejudiciais e acontecem todos os dias. Estes incidentes podem fazer uma empresa perder dinheiro ou até mesmo planos sobre novos produtos. Mitnick (2003), complementa afirmando que “se isso ainda não aconteceu na sua empresa, o problema não é se isso acontecera, mais sim quando acontecera”.

Um ditado popular diz que “um computador seguro é aquele que está desligado”. Esta afirmação em sua grande maioria é verdadeira, porém se levarmos em consideração que um engenheiro social conseguiria convencer alguém a ligar o computador, podemos perceber que tudo se trata de uma questão de tempo, paciência, personalidade e persistência (MITNICK, 2003).

Segundo Dawel (2005), as táticas de engenharia social podem ser divididas em duas categorias de atuação:

- Física: Pode ser categorizada por diversos tipos de ações, como a procura por informações em papéis em cima da mesa ou no lixo, escutar conversas telefônicas ou observar trabalhos de outras pessoas para conseguir informações privilegiadas.

- Psicológica: Pode ser categorizada por diversos tipos de ações relacionadas ao comportamento humano e sua tendência de ser educado, prestativo e de confiar nas pessoas.

Segundo Nascimento (2018), o engenheiro social pode utilizar diversos métodos para conseguir chegar em seu objetivo, sendo alguns deles:

- Pessoalmente: com advento da internet esta abordagem se tornou pouco comum, pois requer muita atuação para se passar por alguém e ultrapassar as barreiras de segurança física.
- Telefone: prática muito difundida entre os engenheiros sociais, pois através do telefone é possível contactar seu alvo. É muito utilizado para levantar as primeiras informações.
- Lixo: pode-se encontrar muitas informações relevantes no lixo que é descartado pelas organizações.
- Internet: existem vários métodos associados ao uso da internet como e-mail, redes sociais, mensageiros online, que podem atingir grande número de vítimas.
- Engenharia social reversa: Cria-se uma situação problema onde a vítima necessita da ajuda do engenheiro social. Após apoiar sua vítima, o mesmo consegue várias informações valiosas.
- Ouvidos atentos: através da conversa entre duas pessoas sobre algum assunto confidencial em local público, o engenheiro social escuta informações valiosas.

Segundo a Symantec (2019), algumas das táticas utilizadas para interação e manipulação humana são:

- *Baiting*: o engenheiro social deixa uma isca em local público, como por exemplo um pen drive infectado, para instigar a vítima, pois sabe que o ser humano tem a característica de curiosidade.
- *Farming*: é uma tática mais elaborada utilizada pelos engenheiros sociais, que procuram estabelecer um relacionamento com a vítima, com base nas informações obtidas em sua pesquisa e na análise do perfil da vítima.

- *Vishing*: este método consiste no atacante enganar a vítima se passando por outra pessoa.
- *Phishing*: pode ser entendido como “pescar informações”, sendo um dos truques mais utilizados pelos engenheiros sociais ao tentar coletar informações de suas vítimas. Normalmente utiliza-se e-mails ou páginas da internet fraudulentas.
- *Hacking* de e-mail e envio de spams: está tática consiste em invadir uma conta de e-mail e encaminhar mensagens aos contatos da vítima.
- *Quid Pro Quo*: também conhecido como “tomar uma coisa por outra”, é oferecido para vítima algum prêmio ou benefício em troca de suas informações pessoais.

Algumas formas mais utilizadas pelos engenheiros sociais para conseguir o acesso à informação são descritas na sequência:

3.4.1 Ataques a pessoas com pouco conhecimento sobre segurança

Segundo Mitnick (2003), os novos colaboradores das organizações são os alvos preferidos dos atacantes, pois estes desconhecem os procedimentos de segurança e as diretrizes daquilo que devem ou não devem fazer dentro da empresa. Muitas vezes estão ansiosos e tentando ser prestativos, para causar uma boa impressão, o que acaba tornando-os mais vulneráveis.

Muitos colaboradores desconhecem as ameaças e vulnerabilidades associados a engenharia social.

> Eles têm acesso às informações, mais não tem o conhecimento detalhado daquilo que pode ser uma ameaça a segurança. O engenheiro social visa um empregado que tem pouca compreensão de como são valiosas as informações que ele pode dar e, assim, fornecê-los a um estranho” (MITNICK, 2003 p. 102).

Um dos truques utilizados pelo engenheiro social, segundo Mitnick (2003), é a “virada da mesa”, na qual consiste em criar uma situação problema, e em seguida, auxiliar a vítima em resolver de forma rápida, enganando a vítima ao criar um vínculo de confiança, para futuramente conseguir dados sigilosos.

3.4.2 Sites falsos e anexos perigosos

Um golpe muito utilizado pelos engenheiros sociais, continua sendo oferecer algo de graça, pois sabem que no geral as pessoas gostam de ganhar algum benefício e neste momento não pensam com clareza nas possíveis consequências da promessa que está sendo feita (MITNICK, 2003).

Segundo Mitnick (2003, p.75), é importante tomar cuidado com anexos recebidos através dos e-mails e com software supostamente grátis. “O atacante experiente usa quase que qualquer meio para invadir a rede corporativa, incluindo o apelo para nosso desejo natural de receber um presente grátis”.

Recebemos diariamente inúmeras mensagens através do nosso e-mail, que oferecem diversos benefícios e promoções. Alguns destes podem conter links maliciosos ou oferecer o download de softwares suspeitos. O envio destas informações maliciosas é apenas uma pequena parte inicial do ataque, pois o atacante ainda precisa convencê-lo a seguir com o que foi solicitado no e-mail para que o ataque seja bem-sucedido e a vítima fique vulnerável (MITNICK, 2003).

3.4.3 Tratamento incorreto do lixo empresarial

Segundo Mann (2018 p.24), “muitas organizações subestimam o risco associado a terceiros que podem ter acesso às informações” e um local que pode conter informações valiosas é no lixo empresarial.

Buscar informações que foram descartadas como lixo por uma empresa, como se não possuíssem valor, é um meio de ataque de engenharia social, pois estas informações normalmente estão vulneráveis (MITNICK, 2003).

Segundo Mitnick (2003), existem oito formas de tratar corretamente o lixo empresarial:

1. Classificar as informações de acordo com seu grau de confidencialidade;
2. Estabelecer procedimentos de descarte das informações confidenciais;

3. Manter um nível de controle para selecionar as pessoas que farão parte da equipe de limpeza;

4. Conscientizar periodicamente os colaboradores sobre a natureza do material que estão jogando no lixo;
5. Todas as informações físicas que serão descartadas, devem passar por um triturador;
6. Inutilizar ou apagar completamente mídias de computador;
7. Usar “containers de lixo” separados para os materiais que possuem informações confidenciais e utilizar empresas especializadas no manuseio e descarte das informações;
8. Manter os containers de lixo trancados.

É importante que os colaboradores das organizações tenham a consciência de que podem existir pessoas vasculhando no lixo para obter informações sigilosas, sendo necessário possuir um descarte que garanta que as informações confidenciais estão sendo destruídas ou apagadas adequadamente, pois conforme citado por Mitnick (2003 p.128) “o seu lixo pode ser o tesouro do seu inimigo”.

3.4.4 Ataques a colaboradores com acessos externos

Segundo Mann (2018), pessoas que trabalham em casa ou que possuem acesso a informações confidenciais fora da instituição, são alvos interessantes para a engenharia social, pois estes possuem mais vulnerabilidades e estão cercados por menos medidas defensivas, principalmente no que se refere a segurança física.

A distância física do local de trabalho também pode ser explorada como forma de enganar os colaboradores que estão fisicamente na empresa, pois conforme citado por Mann (2018), os engenheiros sociais assumem a identidade de um colaborador com acesso externo.

3.5 CONSEQUÊNCIAS DOS ATAQUES

Os sistemas de informação concentram grande quantidade de informações que podem ser acessados por pessoas e grupos externos à organização, inclusive por hackers, tornando os dados suscetíveis a destruição, fraude, erro e uso indevido (LAUDON; LAUDON, 2014).

Uma pesquisa realizada pela Computer Security Institute, revelou que 85% das organizações entrevistadas detectaram quebras na segurança de informação nos últimos 12 meses. Além disso, esta pesquisa também identificou que 64% das organizações tiveram prejuízos financeiros devido aos ataques a sua infraestrutura de segurança em um ano (MITNICK, 2003).

Segundo Dawel (2005), em uma pesquisa divulgada pela Insight Magazine, aponta que 43% das pequenas e médias empresas nunca reabrem após sofrer um ataque, e 29% fecham em dois anos. Este é um dado alarmante pois somados totalizam 72% das empresas que não conseguem sobreviver ou superar um evento deste tipo.

3.6 ENGENHARIA SOCIAL NAS EMPRESAS DE TECNOLOGIA

Muitas organizações desenvolvem seus sistemas de gerenciamento de segurança da informação seguindo a norma internacional ISO 27001, que abrange áreas como segurança de TI, recursos humanos, segurança física e continuidade de negócios. Porém uma fraqueza desta normativa é sua abrangência em relação aos conhecimentos de engenharia social (MANN, 2018).

Em uma pesquisa realizada por analistas do mercado de segurança, revelou que 84% dos incidentes de segurança vem de dentro da empresa. Este dado confere com uma pesquisa realizada pelo FBI, que aponta 80% dos incidentes como internos à organização. Existem algumas explicações plausíveis que justificam o resultado da pesquisa: O desconhecimento do perigo, negligência em tratar as ameaças e a imperícia em lidar com assuntos ligados a segurança (DAWEL, 2005).

Essas pesquisas reforçam a necessidade da conscientização dos colaboradores das organizações, incluindo também os ligados à área de tecnologia, pois conforme enfatizado por Ferreira (2003, p. 81), “a melhor defesa contra este ataque é o treinamento e conscientização em segurança da informação dos funcionários e usuários de redes e computadores”.

Os problemas ligados a engenharia social geralmente requerem soluções completas, que não são muito atraentes para as organizações que estão focadas apenas no lucro. A maioria das soluções de segurança norteiam questões ligados a

segurança técnica, embora evidências demonstrem a necessidade de investir em segurança ligada ao elemento humano (MANN, 2018).

A prioridade para as organizações ligadas a área de tecnologia, é que seus colaboradores atuem no trabalho em que foram encarregados de realizar. Diante da pressão cotidiana, as práticas de segurança da informação em geral são ignoradas, ficando em segundo plano. Os engenheiros sociais utilizam desta negligência para praticarem seus ataques (MITNICK, 2003).

As empresas de tecnologia precisam estar preparadas para os ataques de engenharia social vindo de seus próprios colaboradores ou ex-funcionários. Mesmo que na maioria das vezes seja difícil detectar, é importante verificação de histórico para detectar candidatos a vagas de emprego de pessoas que tenham tendência a comportamentos duvidosos (MITNICK, 2003).

Após a contratação de novos colaboradores é importante acompanhar possíveis motivos de descontentamento que possam levar a execução de atividades perigosas a segurança interna da empresa. Também é importante realizar auditoria constante dos processos, para antecipar possíveis situações que estejam em desacordo com as políticas de segurança da empresa (MITNICK, 2003).

Segundo Mann (2018), infelizmente, não é tão fácil proteger o ser humano, como é proteger uma rede de computadores e sistemas. Os humanos são “programados” de maneiras infinitamente complexas e reagem de diversas maneiras aos ataques. Porém, existem aspectos humanos que podem ser moldados para prever comportamentos referentes ataques de engenharia social dentro das organizações.

4 POLÍTICAS E DESENVOLVIMENTO DE ESTRUTURA DE SEGURANÇA

Este capítulo apresenta a revisão da literatura a respeito das políticas de segurança, treinamento e conscientização sobre segurança da informação.

4.1 POLÍTICAS DE SEGURANÇA

Segundo Ferreira e Araújo (2006, p. 9), “Política de segurança define o conjunto de normas, métodos de procedimentos utilizados para manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem o uso dos ativos de informação”.

Conforme Campos (2014), uma política de segurança pode ser definida como conjunto de normas e procedimentos que de algum modo regulam o comportamento dos colaboradores.

Para proteger as informações da organização de forma eficaz, são necessárias várias ações que permitiram alcançar este objetivo. A política de segurança da informação é a base que sustenta as necessidades de segurança das empresas (FERREIRA, 2003).

De acordo com Fontes (2014, p.73), “quando a organização defini uma política de segurança, seu objetivo é explicitar aos usuários que acessam e utilizam a informação qual é a filosofia e quais são as regras sobre este recurso. A organização busca garantir que a informação esteja protegida contra possíveis perdas, danos, destruição e/ou mau uso”.

Segundo Ferreira e Araújo (2006), as políticas, normas e procedimentos de segurança da informação devem ser: simples, compreensíveis, flexíveis, testadas e alinhadas com a alta administração, estando de acordo com as estratégias de negócio da empresa, para garantir à proteção dos ativos de informação.

As políticas devem ser criadas antes de ocorrerem problemas associados a segurança, ou depois, para evitar reincidência de novos casos. Esta é uma ferramenta para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade (FERREIRA; ARAÚJO, 2006).

No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) lançou a norma NBR ISO/IEC27001, tendo como base a norma internacional ISO/IEC27001, que especifica requisitos básicos para a implantação, operação, monitoração e análise de

sistemas de segurança da informação, para possibilitar a adoção de controles de segurança. Essas duas normas constituem a base para o desenvolvimento de qualquer política de segurança de informação nas organizações (CÔRTES, 2008).

Conforme Ferreira e Araújo (2006), deve-se utilizar uma visão metódica, criteriosa e técnica no desenvolvimento e elaboração das políticas de segurança, alinhadas aos anseios dos proprietários das organizações, do perfil da empresa e dos negócios que ela pratica, possibilitando sugestões de alteração na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades.

As políticas de segurança devem obrigar os administradores do sistema a implantar as diretivas de segurança, com objetivo de depender o mínimo possível das pessoas, pois muitos colaboradores ignoram as políticas para sua conveniência e maior produtividade, criando desta forma vulnerabilidades (MITNICK, 2003).

Depois da implementação de uma política de segurança na organização, são realizados testes para identificar possíveis problemas e consequentemente ações para resolvê-los. Esta análise de riscos gera recomendações para a melhoria na política de segurança (CAMPOS, 2014).

É de extrema importância que os funcionários e parceiros de uma organização sigam as normas e políticas de segurança, padrões éticos e mantenham sigilo das informações a qual terão acesso. A formalização destes procedimentos deve estar documentada e assinada através de um termo de compromisso (FONTES, 2014).

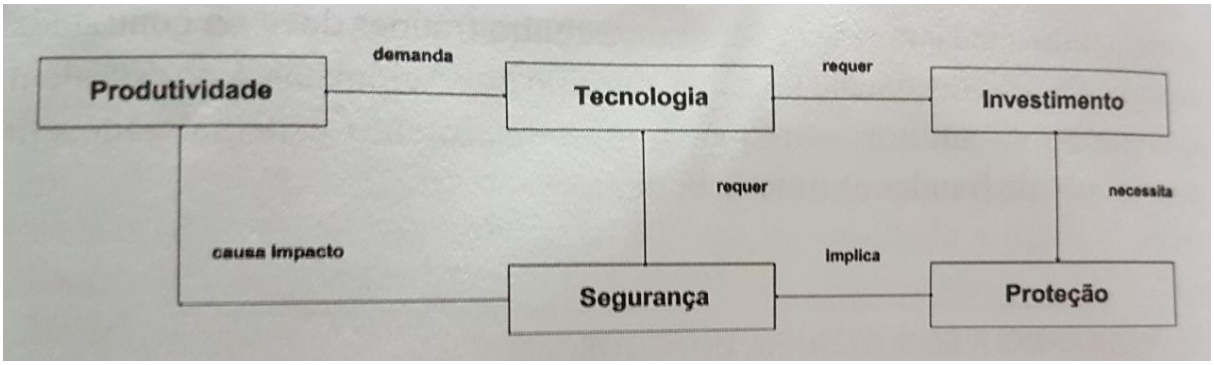
4.2 DESENVOLVIMENTO DE UMA ESTRUTURA DE SEGURANÇA

O grande desafio para desenvolver uma estrutura de segurança na prática, é prever todas as possibilidades de fraudes e ataques. Desta forma muitas empresas estabelecem controles indiscriminados, sem o devido conhecimento especializado em segurança, onde os resultados muitas vezes são questionáveis e possui um custo elevado (DAWEL, 2005).

Os esforços necessários para implantar controles de segurança da informação são acompanhados da necessidade de investimentos. É necessário demonstrar aos organizadores da administração as vantagens desta implementação (CAMPOS, 2014).

Segundo Dawel (2005), o grande desafio de um administrador de segurança é encontrar soluções adequadas às necessidades do seu negócio. As empresas buscam aumentar a sua produtividade, o que demanda investimentos e tecnologia, em contraponto estes desenvolvimentos demandam maior proteção gerando um ciclo contínuo:

Figura 6 - Diagrama das empresas na era da informação

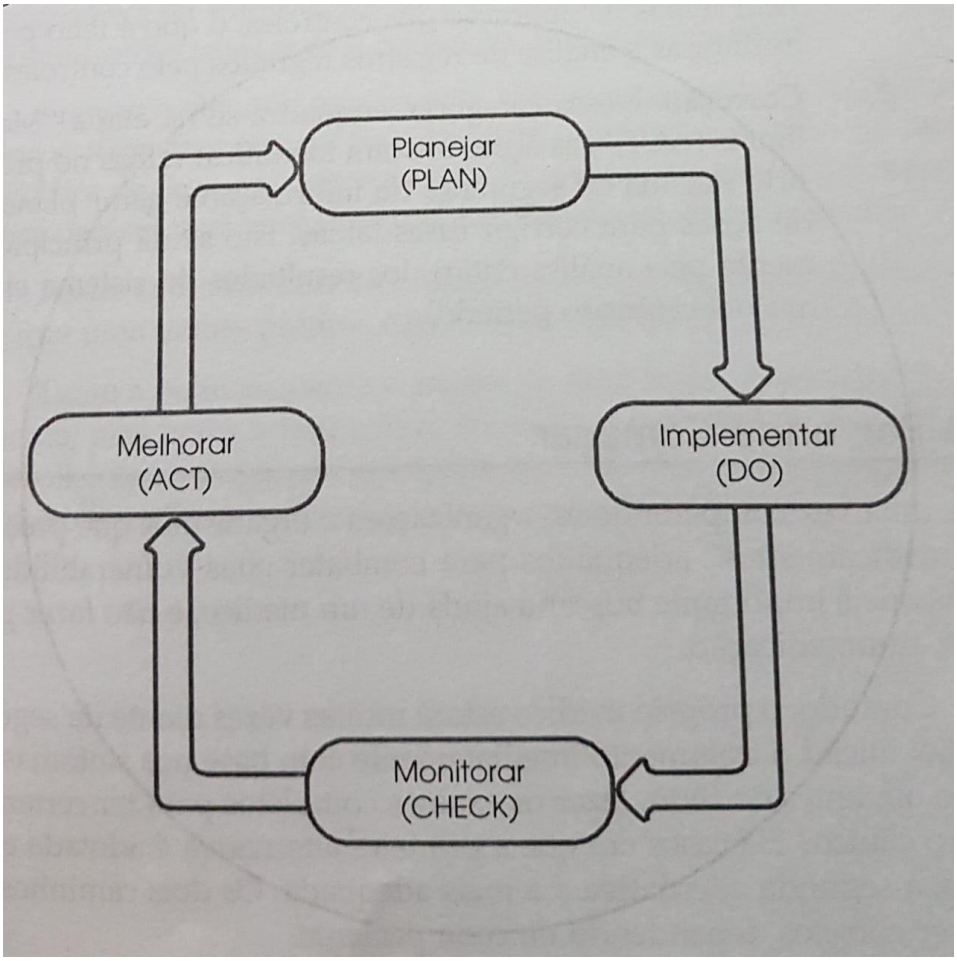


Fonte: Dawel (2005, p. 68).

Muitas organizações possuem recursos limitados para investimento em segurança, ficando imobilizados diante da decisão sobre quais tecnologias utilizar. A escolha mais assertiva destes produtos poderá garantir bons resultados ou prejudicar seriamente os processos da organização. É necessário analisar os resultados continuamente para estabelecer um conjunto de ações que garantam a segurança da informação (CAMPOS, 2014).

O desenvolvimento de um sistema de segurança da informação precisa ser planejado, implementado, monitorado e melhorado continuamente. Nestas etapas que visam diminuir as chances de incidentes, é necessário planejar o tratamento do risco, implementação dos controles de segurança, identificar falhas nas aplicações e corrigir essas falhas (CAMPOS, 2006).

Figura 7 – Ciclo contínuo do sistema de segurança da informação



Fonte: Campos (2006, p. 27).

O grande número de ameaças aos sistemas de informação, resultou em variadas estratégias e ferramentas de defesa. Atualmente defender um sistema de informação não é uma tarefa simples nem barata (TURBAN; RAINER Jr; POTTER, 2003).

Conforme Rainer, Synder e Carr (1991) citado por Laudon e Laudon (2006, p. 477), “Em algumas situações é possível que as organizações não conheçam a probabilidade exata das ameaças aos seus sistemas de informação, tampouco tem uma capacidade de quantificar o impacto de tais eventos”.

Desenvolver mecanismos de segurança pode ser tão caro e sua utilização tão complicada que torna o sistema economicamente e operacionalmente inviável, necessitando uma análise de custo/benefício para determinar quais mecanismos de controle oferecem as defesas mais eficientes sem sacrificar a eficiência operacional ou de custo (LAUDON; LAUDON, 2014).

Segundo Turban, Rainer Jr e Potter (2003, p. 523) o desenvolvimento de uma estrutura para proteção de segurança em TI somente é conseguido ao se inserir “mecanismos de defesa projetados para proteger todos os componentes de um sistema de informação, especificamente dados, software, hardware e redes. Sua implementação exige uma estratégia de defesa”.

4.3 TREINAMENTO E CONSCIENTIZAÇÃO SOBRE SEGURANÇA

Uma das formas mais efetivas para prevenção de ataques ligados a segurança, é o treinamento e conscientização de todos os que fazem parte da organização. Para evitar ataques relacionado a engenharia social, deve-se estabelecer uma rotina de treinamentos periódicos. Os colaboradores precisam conhecer os procedimentos conhecido pela empresa e estarem sempre atentos para se defenderem dos ataques (DAWEL, 2005).

Segundo Nascimento (2018), “conscientização é um processo contínuo. Não basta apenas treinar uma pessoa nos conceitos. É necessário garantir que a pessoa tenha a noção exata do impacto que é compartilhar uma informação sigilosa com alguém que não é de sua total confiança”.

Um problema recorrente é que diversas organizações não possuem uma política de segurança bem definida. O resultado dessa situação é a dificuldade de transmitir aos funcionários uma diretriz básica que deverá ser seguida para determinar comportamentos e definir aquilo que pode e o que não pode ser feito (CÔRTES, 2008).

As organizações devem se esforçar para orientar todos os seus colaboradores para que conheçam e sigam as políticas de segurança, pois o risco não diminui apenas definindo as regras por escrito, Pois segundo Mitnick (2003, p.198), “a ignorância sempre será a melhor desculpa do empregado, e é exatamente esta vulnerabilidade que os engenheiros sociais vão explorar”.

Segundo Mitnick (2003), antes que os novos colaboradores tenham acesso aos sistemas da organização, devem ser treinados para seguir as boas práticas de segurança.

Conforme citado por Côrtes (2008, p. 495) “Não adianta recriminar os funcionários se eles não forem adequadamente instruídos sobre questões de segurança”.

Segundo a norma NBR ISO/IEC 17799, o treinamento dos usuários deve garantir que eles estejam cientes das ameaças e das preocupações da segurança da informação, além de estarem equipados de forma a apoiar as políticas de segurança da informação durante a execução do seu trabalho (FERREIRA, 2003).

O treinamento de segurança da informação não deve apenas impor regras. É importante conhecer como se defender dos ataques, porém este não servirá em nada caso o treinamento não se concentrar na motivação dos colaboradores, para que usem este conhecimento (MITNICK, 2003).

Conforme Mitnick (2003), um treinamento e conscientização sobre segurança da informação, focando nos aspectos do comportamento humano, deve incluir:

- Descrição de como os atacantes podem usar suas habilidades para enganar as pessoas.
- Métodos utilizados pelos invasores para atingir seus objetivos.
- Como reconhecer um provável ataque.
- Procedimento ao receber uma solicitação suspeita.
- Pessoas ou setores responsáveis para relatar ataques.
- Importância de questionar quando receber uma solicitação suspeita.
- O fato que os funcionários não devem confiar em outras pessoas sem uma verificação adequada.
- Importância de validar a identidade ou autoridade da pessoa que fez uma solicitação.
- Procedimentos para proteger informações confidenciais.
- Localização das políticas e procedimentos de segurança.
- Resumo das principais políticas de segurança e uma explicação do seu significado.
- A obrigação de cada colaborador atender as políticas e as consequências do seu não-atendimento destas políticas.

Um programa de conscientização voltado para engenharia social envolve o conhecimento das interações e comunicações humanas, desta forma é importante também abordar alguns itens mais específicos durante o treinamento, conforme complementa Mitnick (2003):

- Políticas de segurança relacionadas a senhas.
- Procedimento de classificação e divulgação, para proteção das informações ou materiais confidenciais.
- Políticas e melhores práticas para o uso correto do e-mail, incluindo medidas para evitar ataques maliciosos.
- Requisitos de segurança física.
- A responsabilidade de questionar pessoas que estão nas instalações sem uma identificação visível.
- Eliminação adequada de documentos ou mídias com informações confidenciais.

A organização pode testar o domínio do conhecimento de seus colaboradores referentes às informações apresentadas no treinamento. Como recompensa e motivação é interessante que a empresa forneça um certificado comprovando a participação no treinamento de segurança. É recomendado que os colaboradores assinem um termo se comprometendo a seguir as políticas de segurança da informação (MITNICK, 2003).

Devido à importância de manter os colaboradores atualizados sobre os assuntos ligados a segurança da informação, é importante a existência de um programa constante de aprendizado e conscientização sobre o tema. Este programa deve ser criativo, utilizando canais tradicionais ou não tradicionais para evitar que sejam ignoradas. Segundo Mitnick (2003), algumas possibilidades de programa de conscientização contínuo e progressivo são:

- Fornecimento de livros sobre o assunto de segurança da informação a todos os colaboradores.
- Inclusão de itens informativos nas circulares da empresa.
- Pôsteres fixados em áreas comuns dos colaboradores.
- Notas publicadas na intranet e/ou quadros de aviso físicos.
- Envio de lembrete sobre o tema via e-mail.
- Uso de proteção de proteção de tela sobre o assunto.
- Inclusão da conscientização sobre segurança como item nos relatórios de desempenho anuais.
- Distribuição de folhetos sobre temas relacionados a segurança.

Algumas orientações básicas e práticas no que se refere ao treinamento e conscientização sobre segurança da informação são:

4.3.1 Criação de uma senha segura

As senhas atualmente são o recurso mais utilizado no que se refere a segurança da informação, devido a sua facilidade de implementação, baixo custo envolvido e bom nível de proteção. Porém o uso de senhas fracas, fragiliza a segurança das informações (FONTES, 2014).

Segundo Fontes (2014), deve-se seguir algumas orientações durante a escolha de uma senha:

- Utilizar senha com letras maiúsculas e minúsculas, números e caracteres especiais.
- Utilizar tamanho mínimo de sete posições.
- Não utilizar sequência de caracteres.
- Não utilizar datas comemorativas, nomes de pessoas, nomes de time ou outras informações que estejam ligadas a você ou a organização.
- Utilizar senhas fáceis de serem lembradas por você, porém difíceis de ser adivinhada por terceiros.
- Não utilize senhas pessoais no ambiente de trabalho.
- Deve-se atualizar a senha de forma periódica. Nunca repita uma senha já utilizada anteriormente.
- Sempre que receber uma senha automática e padrão do sistema, deve-se modificá-la imediatamente.

A senha é uma informação sigilosa e nunca deve ser fornecida a outras pessoas. Qualquer situação atípica em que seja identificado o vazamento ou compartilhamento da senha a terceiros, deve ser comunicado imediatamente o setor de segurança da informação (FONTES, 2014).

É extremamente importante para proteção da organização, o uso de senhas difíceis de serem descobertas combinadas com uma política rígida de segurança (MITNICK, 2003).

4.3.2 Cuidados com a estação de trabalho

Segundo Fontes (2014), boas práticas para manter sua estação de trabalho seguro são:

- Suspender sua seção de trabalho, toda vez que necessitar se ausentar do local onde se encontra o computador ou terminal.
- Programar o equipamento para entrar em estado de proteção de tela, com exigência de senha, sempre que não estiver utilizando durante um certo tempo.

Esses cuidados devem ser tomados pois, caso você se ausente do local da sua estação de trabalho, outras pessoas podem efetuar ações neste computador com o seu usuário e seus acessos a informação (FONTES, 2014).

4.3.3 Produtos homologados

As organizações definem um conjunto de ferramentas e padrão de produtos que serão autorizados para utilização por todos os usuários. Esses produtos são selecionados considerando vários fatores como: manutenção, conhecimento coletivo, possibilidade de suporte e negociações comerciais de licenciamento (FONTES, 2014).

Não se deve utilizar ferramentas não autorizadas pela intuição. Caso seja identificado produtos ou sistemas com características positivas ou melhores do que as já homologadas pela instituição, deve-se entrar em contato com a área de tecnologia e apresentar uma sugestão (FONTES, 2014).

4.3.4 Recebimento de e-mail externo

O uso do e-mail facilitou muito a comunicação entre as pessoas que possuem acesso a este recurso. Sua utilização deve seguir as políticas de segurança, e apenas para atividades profissionais (FONTES, 2014).

Conforme citado por Fontes (2014), ao receber um e-mail, deve-se verificar a confiabilidade do remetente, se as situações descritas são verdadeiras e ter um cuidado com os anexos recepcionados, para evitar golpes.

5 MÉTODO

Neste capítulo, será abordado o tipo de pesquisa realizado, as etapas metodológicas, o planejamento de atividades, a população, a proposta de solução e suas delimitações.

5.1 METODOLOGIA DA PESQUISA

Segundo Silva e Menezes (2001, p. 20) “pesquisa é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos. A pesquisa é realizada quando se tem um problema e não se têm informações para solucioná-lo”.

Para os autores, pesquisas devem ser classificadas de acordo com sua natureza, como pesquisa básica ou pesquisa aplicada. Uma pesquisa básica, tem como objetivo gerar conhecimentos novos que possam ser úteis para o avanço da ciência sem uma aplicação prática, já uma pesquisa aplicada tem o papel de fornecer conhecimentos para aplicações práticas, focadas na solução de problemas específicos (SILVA; MENEZES, 2005).

Este trabalho utiliza o método de pesquisa aplicada, pois será desenvolvido uma pesquisa, aplicando os conhecimentos relacionados a engenharia social na prática dentro da empresa de tecnologia estuda neste trabalho de conclusão de curso.

Segundo Silva e Menezes (2005, p. 20), a abordagem do problema durante a pesquisa pode ser classificada de duas formas:

> **Pesquisa Qualitativa:** considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicos no processo de pesquisa qualitativa. Não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave. É descritiva. Os pesquisadores tendem a analisar seus dados indutivamente. O processo e seu significado são os focos principais de abordagem.
>
> **Pesquisa Quantitativa:** considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las. Requer o uso de recursos e de técnicas estatísticas (percentagem, média, moda, mediana, desvio-padrão, coeficiente de correlação, análise de regressão, etc.).

Campos (2006) demonstra a diferença entre o método de pesquisa quantitativo e qualitativo através de um quadro:

Quadro 2 – Diferenças entre pesquisa quantitativa e qualitativa

Quantitativa	Qualitativa
Resultados baseados em valores objetivos	Resultados baseados em valores subjetivos
Cálculos complexos	Cálculos simples

Fonte: Baseado em Campos (2006, p. 45).

As pesquisas realizadas neste trabalho, podem ser classificadas no ponto de vista dessa abordagem como pesquisa quantitativa e qualitativa, pois irá descrever o assunto analisado, através de dados obtidos com as referências bibliográficas e através de pesquisa com especialista da área de segurança, além de trazer uma análise de dados mensuráveis, obtidos através dos questionários.

Segundo Silva e Menezes (2001), do ponto de vista do objetivo, a pesquisa pode ser definida como exploratória, descritiva e explicativa. Está primeira, proporciona maior familiaridade com problema e constroem hipóteses. A Pesquisa descritiva, descreve características de determinada população ou fenômeno, através de coleta de dados. Já a pesquisa explicativa, identifica os fatores que determinam a ocorrência de fenômenos, tentando explicar o “porque” das coisas.

Na visão dos objetivos da pesquisa deste trabalho, é aplicada a pesquisa exploratória, visto que sua intenção é promover maior familiaridade com o problema e com o objetivo, tentando construir uma hipótese sobre o mesmo (SILVA E MENEZES, 2005).

Do ponto de vista dos procedimentos técnicos, a pesquisa pode ser classificada das seguintes formas: Bibliográfica (elaborada a partir de materiais já publicados), Documental (elaborada a partir de materiais não analisados), Experimental (elaborada a partir de um objeto determinado de estudo), Levantamento (pesquisa direta a pessoas), Estudo de caso (estudo profundo de determinado assunto), Expost-facto (realiza experimentação depois da análise dos fatos), Pesquisa-ação (envolve uma ação para solução de um problema coletivo) e Pesquisa participante (desenvolvida a partir de interação entre pesquisadores) (SILVA E MENEZES, 2005).

Este trabalho utiliza como procedimento técnico o levantamento bibliográfico. Segundo Silva e Menezes (2005), neste tipo de pesquisa é elaborado referenciando

materiais já publicados, constituídos principalmente de livros, artigos e materiais disponibilizado na internet.

5.2 METODOLOGIA DO TRABALHO

O desenvolvimento da pesquisa se dá pela realização das etapas a seguir. Essas atividades foram elencadas temporalmente no cronograma da pesquisa, disponível no apêndice A:

a) Realização de uma pesquisa bibliográfica para entender os aspectos técnicos relacionados aos assuntos do tema.
b) Elaboração de um questionário com base nos conhecimentos abordados na pesquisa bibliográfica.
c) Aplicação de questionário junto a população definida no escopo da pesquisa (universo da pesquisa).
d) Análise dos resultados quantitativos e qualitativos da pesquisa realizada.
e) Desenvolvimento de ações com base nos resultados da pesquisa realizada com o objetivo de conscientizar a população da pesquisa.
f) Aplicação de novo questionário, para verificar a evolução da população referente ao tema.
g) Conclusão da pesquisa.

5.3 POPULAÇÃO

Segundo Silva e Mendes (2005, p.32) a população, também chamada de universo da pesquisa, “é a totalidade de indivíduos que possuem as mesmas características definidas para um determinado estudo”.

A população da pesquisa realizada contará com funcionários da empresa de tecnologia pesquisada neste trabalho, sendo um total de 57,5% dos 33 colaboradores que atuam no setor pesquisado, que trabalha realizando atendimento ao público interno e externo em suas atribuições.

5.4 DELIMITAÇÕES

Os conhecimentos ligados à área de engenharia social e segurança da informação são complexos e estão em constantes atualização. Devido ao tamanho e complexidade que a pesquisa pode abordar, segue abaixo as delimitações deste trabalho:

a) O questionário para validação dos conhecimentos ligados a engenharia social, será aplicado apenas aos funcionários que realizam atendimento interno ou externo dentro da empresa pesquisada.
b) A análise dos resultados obtidos será embasada apenas nos resultados do questionário aplicado.

6 DESENVOLVIMENTO DA PESQUISA

Este trabalho acadêmico, apresenta uma pesquisa desenvolvida, abordando os temas de Engenharia Social e Segurança da Informação entre os colaboradores de uma empresa de tecnologia. Este capítulo descreve a organização objeto do estudo, o desenvolvimento do questionário –baseado na teoria apresentada-, a aplicação do questionário e os resultados obtidos.

6.1 ORGANIZAÇÃO OBJETO DE ESTUDO

A pesquisa foi realizada em uma organização, situada no estado de Santa Catarina, voltada para o setor de tecnologia, com aproximadamente 200 funcionários e que segundo as definições do IBGE, pode ser definida como uma empresa de grande porte, pois está inserida no setor de serviços e possui mais de 100 funcionários (CUNHA, 2018).

Dentre aproximadamente os 200 funcionários que trabalham atualmente na empresa, foi aplicado o estudo com uma amostragem de 33 funcionários, que atuam diretamente em atendimentos ao público, interno e externo, sendo estes a população na qual se embasa esta pesquisa.

Definida a população da pesquisa, foi produzido e aplicado um questionário para conhecer os profissionais que atuam na área e seus conhecimentos sobre o tema desta pesquisa. Após identificar e entender os problemas ligados a Engenharia Social e Segurança da Informação, vivenciados pelos colaboradores da empresa de tecnologia, foram aplicadas algumas ações de conscientização sobre o tema.

Para análise dos resultados das ações aplicadas, e validação do seu resultado, foi aplicado um novo questionário, a fim de medir o desempenho dos colaboradores a respeito do referido tema.

6.2 DESEMVOLVIMENTO DO QUESTIONARIO

Com o objetivo de validar os conhecimentos sobre os temas de “engenharia social” e “segurança da informação” entre a população desta pesquisa, que são os colaboradores de uma empresa de tecnologia, foi desenvolvido um questionário, com

perguntas que proporcionaram descobrir os conhecimentos destes funcionários referente ao tema atualmente entre o público pesquisado.

O formulário da pesquisa é constituído por 4 categorias:

A. A primeira parte do questionário é relativa ao próprio profissional, para identificarmos as características da população. Foram solicitados dados sócios demográficos para identificação do perfil dos respondentes, entre eles idade, sexo e nível de escolaridade.
B. A segunda parte do questionário é focado em identificar as práticas que são realizadas atualmente pelos colaboradores referente a segurança da informação e engenharia social, relacionadas a teoria apresentada nos capítulos 2, 3 e 4.
C. A terceira parte do questionário é focada em avaliar os conhecimentos relacionados a teoria sobre informação, segurança e engenharia social, apresentada nos capítulos 2 e 3.
D. A quarta parte do questionário é sobre práticas de segurança da informação adotadas, como políticas, treinamentos e estruturas da empresa pesquisada, relacionadas a teoria apresentada nos capítulos 3 e 4.

Segue descrição das questões relacionadas a cada uma dessas partes do questionário.

a) Perfil da população

Na parte do questionário referente às características da população, foram realizadas sete perguntas referentes a dados sócios demográficos e tempo de trabalho na área de tecnologia. Nesta parte do questionário, foram incluídas outras duas perguntas cuja resposta não era obrigatória, para verificar se a população forneceria dados não relacionados ao tema da pesquisa, algo que pode ser relacionado a uma técnica utilizada na engenharia social chamada de *phishing*.

b) Práticas da população

Na parte do questionário focado nas práticas atuais dos colaboradores da empresa pesquisada, em seus 9 questionamentos, foram relacionadas as ações praticadas pelos colaboradores da empresa pesquisada durante sua rotina de trabalho com a teoria:

Foram realizadas quatro perguntas referentes ao tema senhas, sendo estas referente a sua criação e compartilhamento. Conforme Fontes (2014), as senhas são o meio mais utilizado no que se refere a garantir a segurança da informação.

Foi realizado uma pergunta referente aos cuidados com o bloqueio da estação de trabalho, pois segundo Fontes (2014), é importante suspender a sessão de trabalho sempre que estiver ausente para evitar o acesso de pessoas não autorizadas ao sistema.

Foi realizado uma pergunta referente a utilização de programas no ambiente de trabalho, pois conforme Fontes (2014), devemos apenas utilizar as ferramentas e produtos previamente autorizados pela organização.

Foi realizado uma pergunta referente aos cuidados ao receber e-mails, pois segundo Fontes (2014), é importante verificar a confiabilidade das informações recebidas de forma eletrônica para evitar problemas relacionados à segurança.

Foi realizado uma pergunta referente o descarte do lixo empresarial, pois conforme informado por Mitnick (2003), é importante ter a consciência que um descarte incorreto pode comprometer as informações da organização.

c) Conhecimento da população

Na parte do questionário focado nos conhecimentos referentes a informação, segurança e engenharia social, em seus 7 questionamentos, foram relacionados os conhecimentos da população pesquisada com a teoria:

Foi realizado uma pergunta referente os conhecimentos sobre informação. Segundo Laudon e Laudon (2014), as informações são dados apresentados de forma significativa. Turban, Rainer Jr, Potter (2003), complementam esta definição definindo que estes dados necessitam fazer sentido ao destinatário.

Foi realizado uma pergunta referente a classificação das informações. Conforme apresentado na teoria por Ferreira e Araújo (2006), que informa que

informações confidenciais são aquelas que devem ser protegidas do acesso externo, pois o vazamento dessas informações pode comprometer as operações da organização.

Foi realizado quatro perguntas referente a engenharia social, questionando a quem respondeu a pesquisa, sobre o significado do termo e suas próprias experiências referente ao mesmo. Segundo Mann (2018), a engenharia social é a técnica de manipulação de pessoas, para que forneçam informações ou executem ações. Dawel (2005), complementa esta definição como a arte de utilizar o comportamento humano para quebrar a segurança, sem que a vítima perceba que foi manipulada.

Ainda sobre engenharia social, foi questionado sobre os alvos preferidos sobre os engenheiros sociais. Segundo Mitnick (2003), os novos colaboradores das organizações são os alvos preferidos dos atacantes, pois estes desconhecem os procedimentos de segurança.

Foi realizado uma pergunta sobre um dos principais tipos de ataque a segurança de informação que é o *phishing*. Segundo Phishing (2019), este tipo de ameaça é utilizado para induzir que uma vítima informe dados pessoais sigilosos.

d) Perfil de segurança da informação da população

Na parte do questionário referente as práticas de segurança da informação, em seus 8 questionamentos, foram relacionados os conhecimentos e as ações praticadas pela população em seu ambiente de trabalho, e suas opiniões sobre a segurança na empresa em que trabalham.

Antes de sua aplicação no público alvo, o instrumento foi submetido a um processo de validação, com o intuito de "garantir a qualidade dos resultados da investigação no sentido de podermos aceitá-los como fatos indiscutíveis" (Coutinho, 2011, p. 110).

Realizou-se uma validação semântica que teve como propósito:

a- Evitar que um enunciado ou assertiva pudesse ter mais de uma interpretação;
b- Eliminar inconsistências relacionadas a linguagem utilizada no instrumento.

Este processo de validação, foi realizado com cinco pessoas que estão dentro do grupo da população desta pesquisa.

O formulário completo, com as perguntas apresentadas, pode ser visualizado no apêndice B.

6.3 COLETA DE DADOS

A coleta de dados foi realizada através da ferramenta de formulário Google Forms. O formulário ficou disponível através de um link encaminhado por e-mail à população da pesquisa. O e-mail pode ser localizado no apêndice C.

A amostra constituiu em um número de 33 colaboradores que trabalham na empresa de tecnologia pesquisada, atuando em um dos setores com atendimento ao público interno e externo. Destes 33 funcionários 57,5%, ou seja, 19 colaboradores responderam o formulário encaminhado via e-mail interno da organização.

A pesquisa foi realizada entre março e abril de 2020, durante a pandemia do COVID-19, quando a empresa já estava funcionando remotamente (home-office). Esse fato incidiu no total de respondentes ser menor do que o esperado devido a falta do contato presencial com os colaboradores, para estimular o preenchimento do questionário, assim como também a sobrecarga de trabalho destes trabalhadores neste novo regime de trabalho.

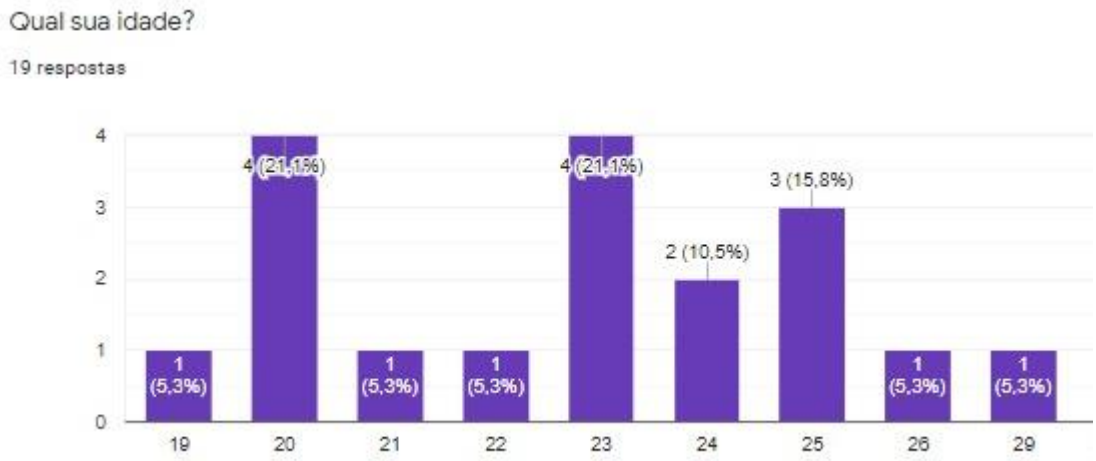
6.4 PESQUISA E ANÁLISE DE DADOS

Após aplicação do questionário, podemos verificar os conhecimentos da população referente a segurança de informação e engenharia social, além de suas práticas no que se refere a estes temas.

As primeiras perguntas, da primeira parte dos questionários, nos permitem conhecer melhor o perfil da população pesquisada.

No gráfico 1, pode-se observar que a maioria da população é composta por pessoas jovens, com idades entre 20 e 25 anos.

Gráfico 1: Idade

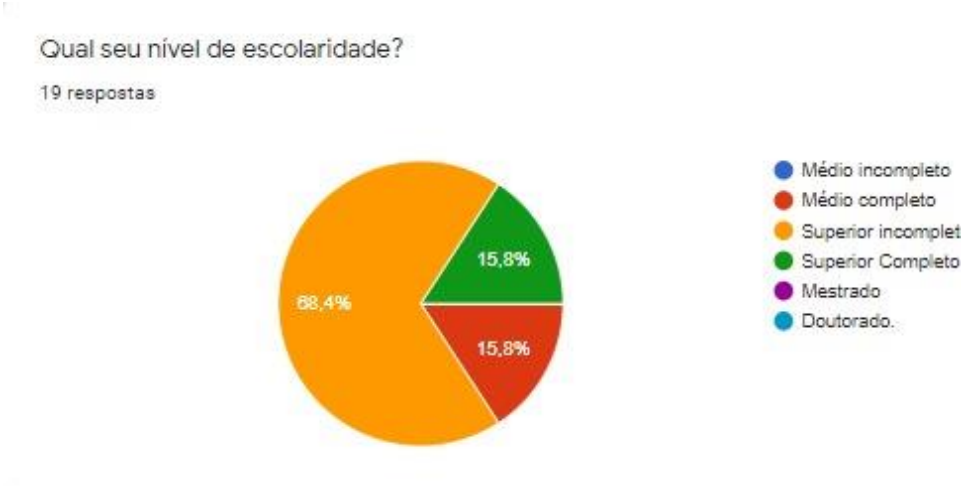


Fonte: dados da pesquisa.

Através da questão 2, foi realizado uma pergunta para identificar o gênero da população pesquisada, os 19 respondentes (100%) informaram ser do sexo masculino.

No gráfico 3, pode-se observar que a maioria da população (84,2%) possui nível de escolaridade superior, completo ou incompleto.

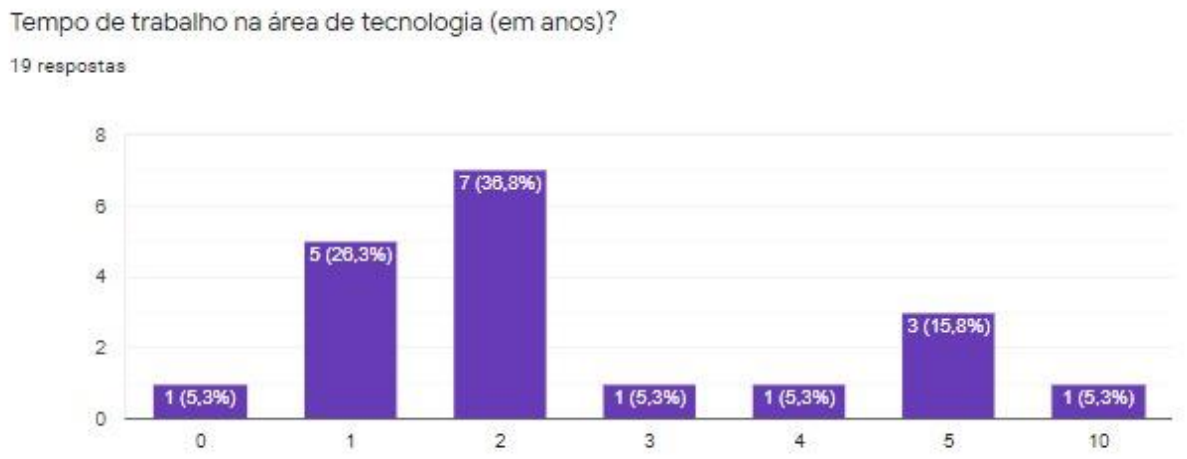
Gráfico 3: Escolaridade



Fonte: dados da pesquisa.

No gráfico 4, pode-se observar que a maioria da população trabalha na área de tecnologia a menos de dois anos, 13 do total de 19 respondentes.

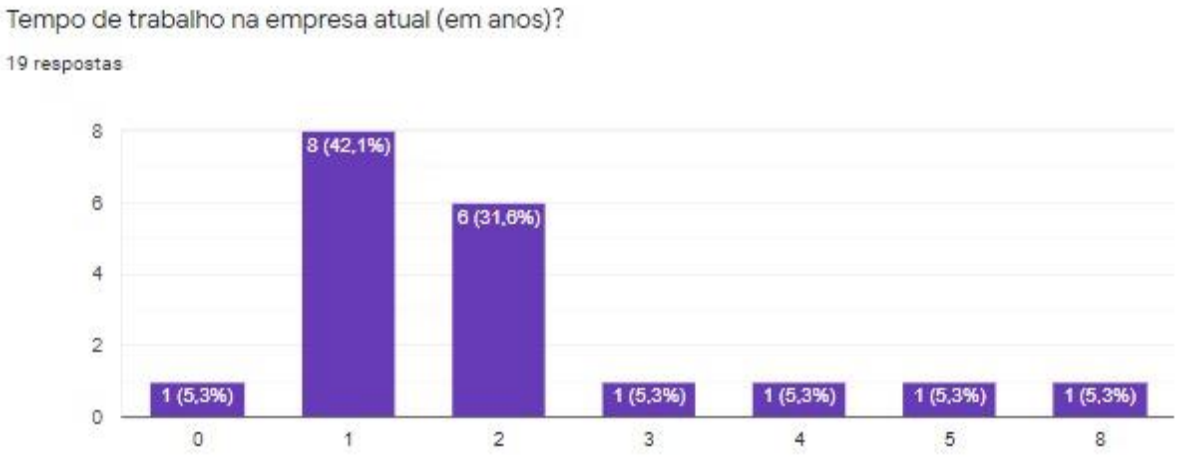
Gráfico 4: Tempo de trabalho na área de tecnologia



Fonte: dados da pesquisa.

No gráfico 5, pode-se observar que a maioria da população trabalha na empresa pesquisada no máximo a dois anos, 15 dos 19 colaboradores. Somente quatro deles têm mais anos na casa.

Gráfico 5: Tempo de trabalhado na empresa pesquisada



Fonte: dados da pesquisa.

No gráfico 6, pode-se observar que a maioria da população (78,9%) não tinha trabalhado em outras empresas de tecnologia, antes de trabalhar na empresa pesquisada.

Gráfico 6: Outras empresas de tecnologia

Fonte: dados da pesquisa.

No gráfico 7, pode-se observar que a maioria da população (73,7%) já havia trabalhado em outras empresas que não eram ligadas a tecnologia, antes de trabalhar na empresa pesquisada.

Gráfico 7: Empresas não ligadas a tecnologia

Fonte: dados da pesquisa.

Através das questões 8 e 9, foi realizada uma simulação de ataque do tipo *phishing*, muito comum de ser utilizada por engenheiros sociais para conseguir dados pessoais de uma vítima. No formulário, foi incluído duas perguntas, com resposta opcional, sobre temas não ligados à pesquisa, para verificar se a população forneceria estes dados.

Uma das questões era sobre a prática de atividade físicas e a outra indagava se o participante possuía filhos. As duas questões foram respondidas por 18 dos 19 entrevistados (94,7%), sendo que estas informações não agregam ao tema de engenharia social.

O segundo bloco de perguntas do formulário, é focado nas práticas da população referentes a segurança da informação e engenharia social.

No gráfico 10, pode-se observar que 68,4% da população, já utilizou usuário e senha compartilhados.

Gráfico 10: Senha compartilhada I

Fonte: dados da pesquisa.

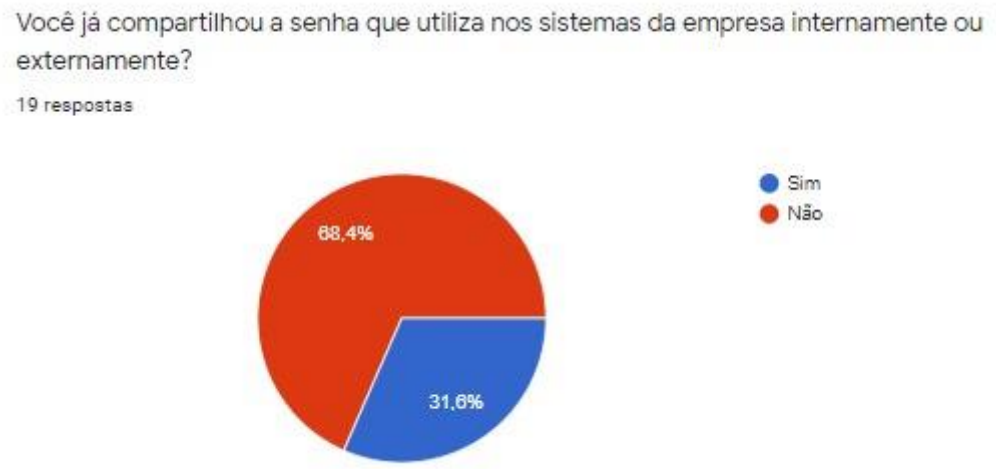
No gráfico 11, pode-se observar que 68,4% da população, já anotou sua senha em um local que outras pessoas poderiam ter acesso.

Gráfico 11: Anotação de senha I

Fonte: dados da pesquisa.

No gráfico 12, pode-se observar que 68,4% da população, já utilizou senhas compartilhadas pela equipe, ou compartilhou sua senha pessoal com outras pessoas, sendo estes colaboradores da empresa ou não.

Gráfico 12: Compartilhamento de senha I



Fonte: dados da pesquisa.

No gráfico 13, pode-se observar que 57,9% da população, utiliza senhas no ambiente corporativo que são similares as senhas que utiliza em contas ou serviços de uso pessoal.

Gráfico 13: Similaridade de Senha I

Fonte: dados da pesquisa.

No gráfico 14, pode-se observar que somente 31,6% da população segue todas as recomendações de segurança, durante a criação de uma senha. Também é possível identificar que 52,6% da população cria uma senha segura, somente se for obrigado pelo sistema.

Além destes números, observamos que 5,3% da população não sabe se está criando uma senha segura.

Gráfico 14: Recomendações de Senha I

Fonte: dados da pesquisa.

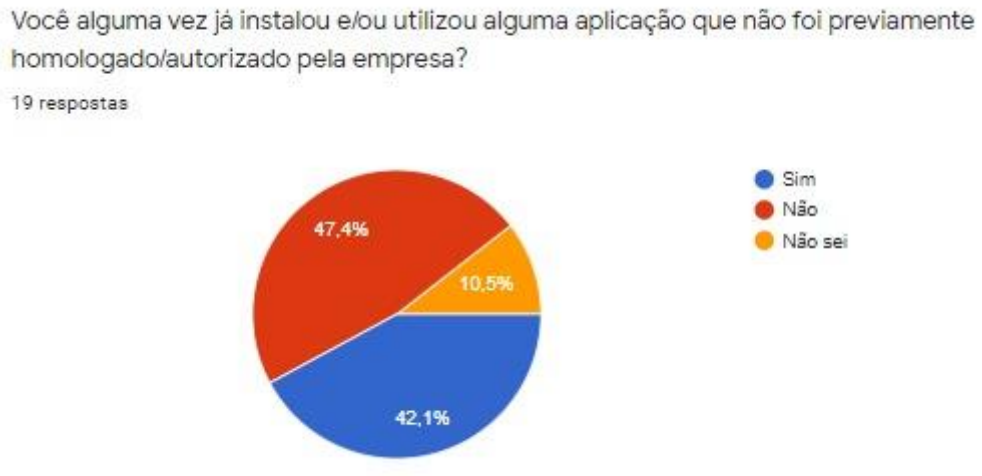
No gráfico 15, pode-se observar que a maioria da população não costuma realizar, com a frequência recomendada, o bloqueio do seu computador ao sair da sua estação de trabalho.

Gráfico 15: Estação de Trabalho I

Fonte: dados da pesquisa.

No gráfico 16, pode-se observar que menos da metade da população, informa que nunca utilizou uma aplicação que foi previamente homologada pela organização.

Gráfico 16: Homologação de Aplicação I



Fonte: dados da pesquisa.

No gráfico 17, pode-se observar a maioria da população tem o costume de verificar o remetente e o conteúdo do e-mail antes de realizar qualquer tipo de interação.

Gráfico 17: Remetente do E-mail I

Fonte: dados da pesquisa.

No gráfico 18, pode-se observar que apenas 15,8% da população, segue a recomendação presente na teoria apresentada por Mitnick (2003), onde é informado que devemos triturar todas as informações físicas, que serão descartadas e posteriormente utilizar “containers de lixo” exclusivos para o descarte dos documentos confidenciais.

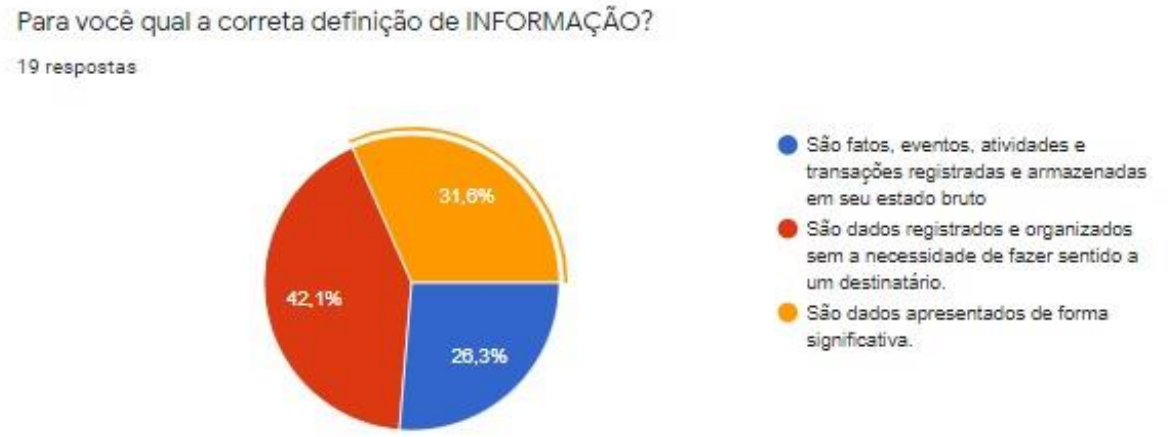
Gráfico 18: Descarte de Documentos I

Fonte: dados da pesquisa.

O terceiro bloco de perguntas do formulário, é focado em avaliar os conhecimentos relacionados com a teoria sobre informação, segurança e engenharia social.

No gráfico 19, pode-se observar que a maioria da população (68,4%), não conhece a correta definição de informação. A definição correta é “dados apresentados de forma significativa”.

Gráfico 19: Informação I



Fonte: dados da pesquisa.

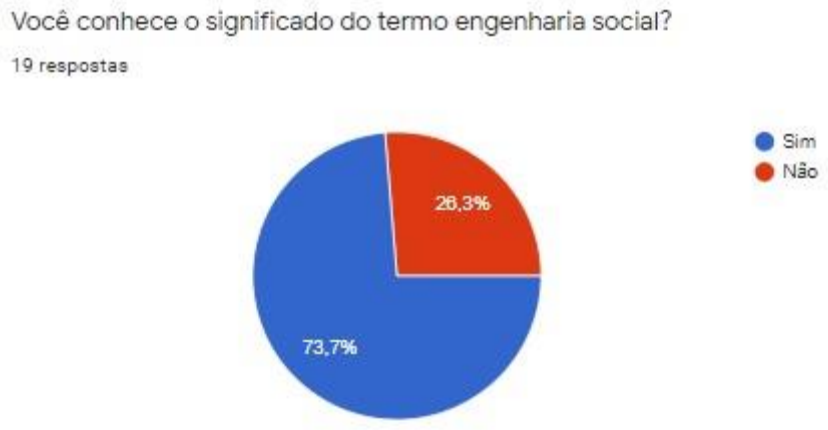
No gráfico 20, pode-se observar que 94,7% da população, não conhece a correta classificação das informações. Embora seja importante proteger as informações, somente o vazamento de “informações confidenciais” comprometem as operações da organização.

Gráfico 20: Classificação das Informações I

Fonte: dados da pesquisa.

No gráfico 21, pode-se observar que 73,7% da população, acredita conhecer o significado do termo engenharia social.

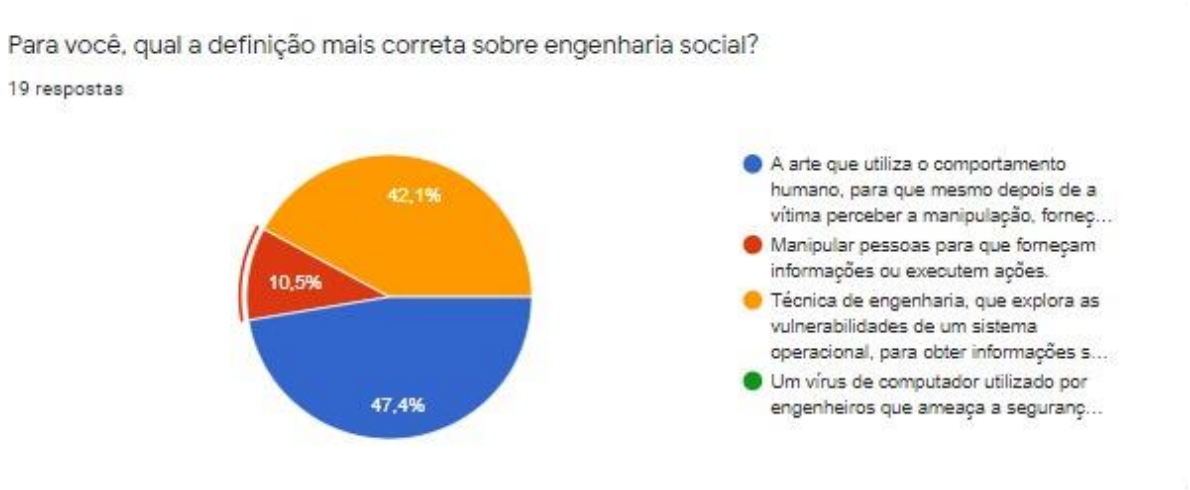
Gráfico 21: Significado Engenharia Social



Fonte: dados da pesquisa.

No gráfico 22, pode-se observar que apenas 2 de 19 pessoas respondentes conhece o significado do termo, que defini engenharia social como “Manipular pessoas para que forneçam informações ou executem ações”. No gráfico 21, podemos observar que 73,7% da população afirmou conhecer o termo, mas somente 10,5% da população realmente demonstrou conhecer o significado de engenharia social.

Gráfico 22: Definição Engenharia Social I



Fonte: dados da pesquisa.

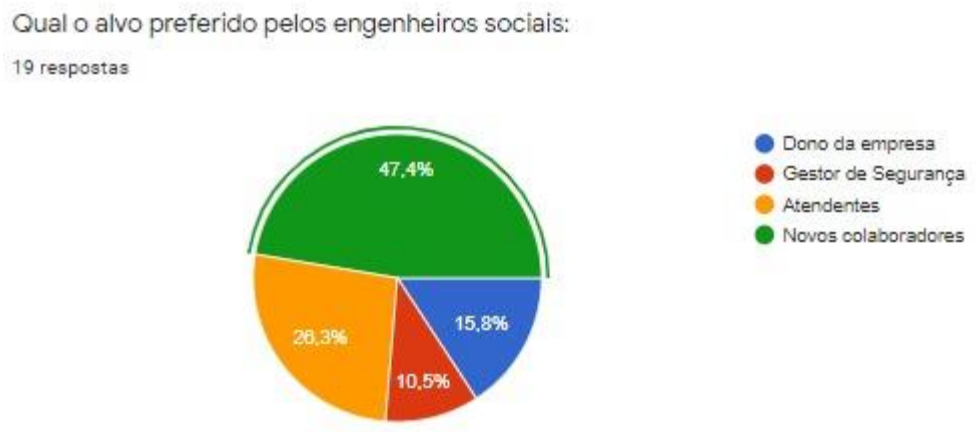
No gráfico 23, pode-se observar que apenas 26,3% da população acredita que nunca tenha sofrido ataque relacionamento a engenharia social. Este dado, demonstra a importância de compartilhar o conhecimento sobre o tema, pois 73,7% dos respondentes, acredita ter sido alvo, ou não saber se já sofreu um ataque de engenharia social.

Gráfico 23: Ataque de Engenharia Social

Fonte: dados da pesquisa.

No gráfico 24, pode-se observar que 52,6% da população, desconhece qual o alvo preferido dos engenheiros sociais durante um ataque, que são os “Novos colaboradores”.

Gráfico 24: Alvo Engenharia Social I



Fonte: dados da pesquisa.

No gráfico 25, pode-se observar que 52,6% da população, conhece a definição relacionada a phishing, na qual é uma das técnicas utilizada pelos engenheiros sociais.

Gráfico 25: Phishing I

Fonte: dados da pesquisa.

O quarto bloco de perguntas do formulário, é focado nas práticas de segurança de informação, adotadas pela empresa pesquisada, como políticas treinamentos e estrutura.

No gráfico 26, pode-se observar que 89,5% da população, recebeu algum tipo de treinamento de segurança da informação.

Gráfico 26: Treinamento de Segurança

Fonte: dados da pesquisa.

No gráfico 27, pode-se observar que 63,2% da população, não teve, ou não sabe se teve, algum tipo de treinamento sobre engenharia social na empresa pesquisada.

Gráfico 27: Treinamento de Engenharia social

Fonte: dados da pesquisa.

No gráfico 28, pode-se observar que 57,9% da população, não teve, ou não sabe se teve, algum tipo de orientação sobre como realizar atendimento ao público externo, pensando na segurança da informação.

Gráfico 28: Orientação para Atendimento

Fonte: dados da pesquisa.

No gráfico 29, pode-se observar que apenas 2 de 19 pessoas respondentes conhecem todas as políticas de segurança de informação da empresa em que trabalham.

Gráfico 29: Políticas de Segurança I

Fonte: dados da pesquisa.

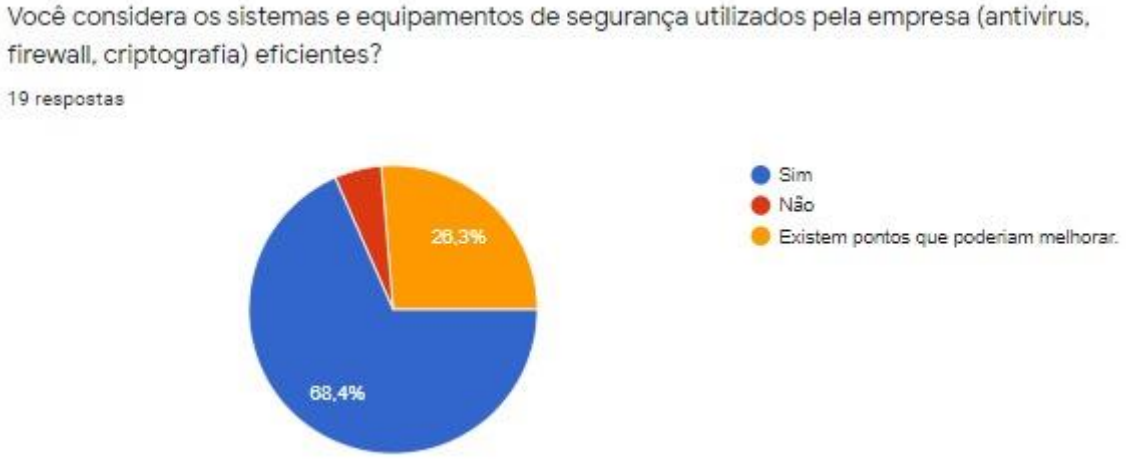
No gráfico 30, pode-se observar que 78,9% definem como bons ou excelentes os cuidados da empresa em que trabalham referente a segurança e engenharia social.

Gráfico 30: Cuidados de Segurança I

Fonte: dados da pesquisa.

No gráfico 31, pode-se observar que 68,4% da população consideram os equipamentos de segurança da empresa em que trabalham eficientes.

Gráfico 31: Equipamentos de Segurança I



Fonte: dados da pesquisa.

No gráfico 32, pode-se observar que 52,6% da população não consideram a segurança física eficiente ou acredita que existem pontos a melhorar.

Gráfico 32: Segurança física I

Fonte: dados da pesquisa.

No gráfico 33, pode-se observar que 89,5% da população gostaria de receber mais informação sobre o tema engenharia social da empresa em que está trabalhando.

Gráfico 33: Atualizações sobre Segurança I

Fonte: dados da pesquisa.

Após apresentação das respostas, seguem considerações gerais sobre os resultados obtidos.

6.5 CONCLUSÕES SOBRE A PESQUISA

Com os dados obtidos através da pesquisa, foi possível identificar os conhecimentos da população referente aos temas de engenharia social e segurança da informação, além de conhecer suas práticas relacionadas à segurança durante a rotina de trabalho na empresa pesquisada. Estes dados servirão como base no desenvolvimento das ações de conscientização.

7 AÇÕES DE CONSCIENTIZAÇÃO E VALIDAÇÃO DAS AÇÕES

Este capítulo apresenta as ações de conscientização para diminuir os riscos de ataques referentes a segurança de informação e engenharia social, baseado nos resultados do questionário 1, e posteriormente, a validação das ações sugeridas por meio de um novo questionário, aplicado dentro da mesma população, comprovando se estas ações tiveram o efeito esperado.

7.1 AÇÕES DE CONSCIENTIZAÇÃO

Foram realizadas, ações para conscientizar os colaboradores da empresa pesquisada, referente aos temas de engenharia social e segurança da informação.

Estas ações foram estruturadas com base nos resultados do questionário aplicado, que apontou as principais deficiências dos colaboradores referentes ao tema.

As ações foram diversificadas para alcançar o melhor resultado referente ao compartilhamento das informações, sendo elas:

7.1.1 E-mails de conscientização

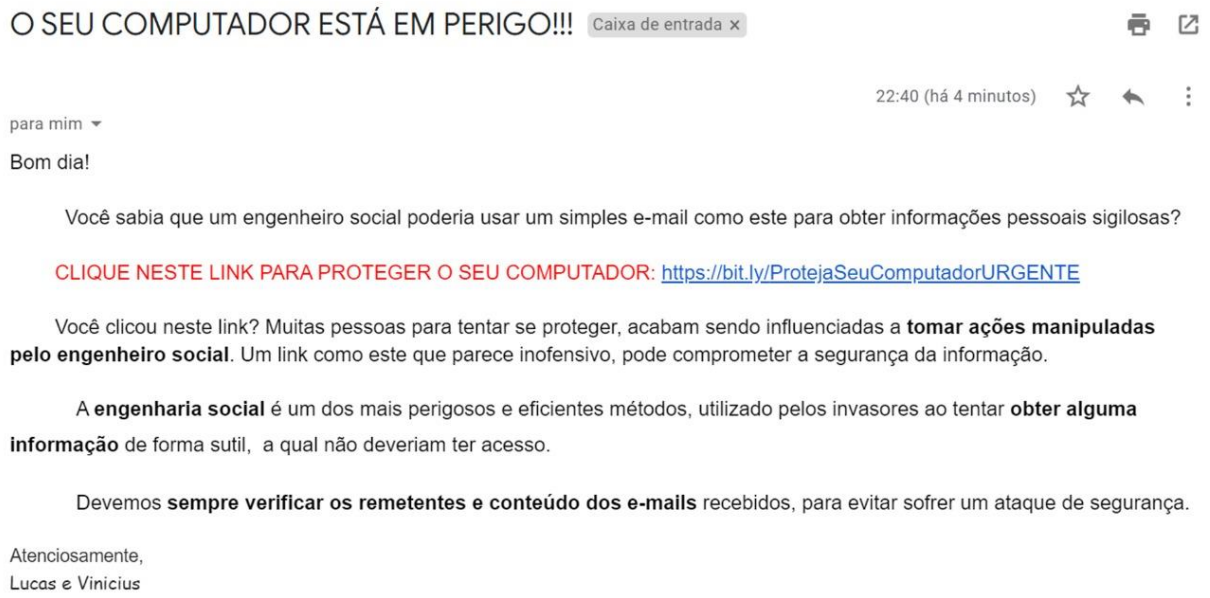
O e-mail é uma ferramenta que permite transmitir mensagens de forma instantânea através da rede, tornando-se uma ferramenta versátil, que possibilita o compartilhamento de informações de qualquer tamanho e com custo muito baixo (OGDEN, 2002).

Desta forma, o e-mail torna-se uma opção interessante para realizar o compartilhamento das informações referente a segurança da informação, encaminhando o conteúdo para o e-mail corporativo pessoal que todos os colaboradores possuem acesso.

As mensagens encaminhadas via e-mail, possuem informações detalhadas referentes ao tema, com uma linguagem de fácil interpretação, possibilitando uma rápida leitura e colaborando para o entendimento.

Modelo de e-mail encaminhado a população da pesquisa:

Figura 8 – Modelo de E-mail Informativo



Fonte: Elaborada pelos autores.

7.1.2 Seminário sobre Segurança da Informação

O seminário foi pensado como uma das principais formas de disseminar o conteúdo sobre segurança da informação e engenharia social, de forma presencial junto a população pesquisada, pois permite uma interação em tempo real para esclarecer todas as dúvidas sobre o tema e disseminar boas práticas de segurança.

Devido a pandemia pelo surto de uma doença causada pelo novo coronavírus (COVID-19) em 2020, constitui-se uma situação de emergência na saúde pública de importância internacional, com medidas de proteção sugeridas como o distanciamento social, recomendada pelas organizações de saúde (OPAS, 2020).

Devido a esse cenário não foi possível realizar esta interação de forma presencial pois a empresa, seguindo as medidas de saúde, orientou os funcionários a trabalhar em home office.

7.1.3 Folder informativo

O folder é muito utilizado como material de apoio para consultas rápidas. Com o objetivo de entregar de forma física a informação, foi elaborado um folder sobre engenharia social e segurança da informação, trazendo os principais conceitos sobre os temas de segurança e engenharia social, de formas resumidas e ilustrativas.

Figura 9 – Modelo de Folder Informativo

Fonte: Elaborada pelos autores.

Conforme mencionado na ação anterior (7.1.2 – Seminário sobre segurança de informação), devido às regras de distanciamento social decorrentes da pandemia relacionado a COVID-19, não foi possível entregar o folder de forma impressa como foi planejado. Devido esta situação, foi necessário encaminhar este folder por meio digital.

7.1.4 Publicações informativas na intranet

A intranet é uma plataforma acessada através da rede interna, sendo uma das principais formas de disseminação de conteúdo entre o público interno da empresa pesquisada, sendo da cultura da organização que os colaboradores o acessem regularmente no seu âmbito de trabalho, sendo uma forma muito interessante de divulgação das informações.

As publicações nesta plataforma, foram realizadas semanalmente, com informações rápidas e diretas, com um objetivo de disseminar os temas de segurança da informação e engenharia social.

O conteúdo das publicações apresentou os principais conceitos referente a esses temas, dicas de boas práticas para serem aplicadas no ambiente de trabalho e algumas das principais políticas de segurança da informação na organização.

Figura 10 – Publicação Intranet sobre Orientação de Segurança

Fonte: Elaborada pelos autores.

Figura 11 – Publicação Intranet sobre Engenharia Social

Fonte: Elaborada pelos autores.

7.1.5 Vídeo informativo

Com objetivo de disseminar a informação de uma forma mais intuitiva e de uma maneira muito mais confortável para o destinatário obter a informação. Segundo Coffee (2019), “60% dos internautas sempre vai preferir ver o vídeo de um conteúdo do que ler um texto, se tiver a oportunidade para isso”.

O vídeo aborda temas mais introdutórios sobre o mundo globalizado em que vivemos, suas vantagens e seus perigos, como ataques de engenharia social.

O vídeo desenvolvido, pode ser visualizado através do link:

https://bit.ly/TccEngenhariaSocial

7.1.6 FAQ – Perguntas Frequentes

Percebemos que existem muitas dúvidas frequentes no que se relacionamento a engenharia social e segurança da informação, muitos questionamentos são encontrados no dia-a-dia, e por diversas pessoas.

Para sanar estas dúvidas que são mais rotineiras, foi desenvolvido um FAQ, respondendo a esses questionamentos mais comuns, sendo alguns deles “O que é

engenharia Social?”, “Quais os principais tipos de ameaça a Segurança?” e “Como criar uma senha segura?”

O FAQ foi estruturado, com o intuito de possibilitar ser incluído nas documentações da empresa pesquisada, para ser disponibilizada aos novos colaboradores, que são as pessoas que têm menos conhecimento sobre segurança e são os principais alvos dos engenheiros sociais.

O FAQ desenvolvido, com suas perguntas e respostas completas, pode ser visualizado no apêndice D.

7.2 VALIDAÇÃO DOS RESULTADOS APÓS AÇÕES DE CONSCIENTIZAÇÃO

Após aplicação do primeiro questionário, podemos verificar os conhecimentos da população referente a segurança de informação e engenharia social, além de suas práticas no que se refere a estes temas. Após análise dos dados coletados do questionário 1, foram desenvolvidas ações de conscientização para disseminar os conhecimentos sobre o tema.

Após a execução dessas ações apresentadas no tópico “7.1 – Ações de conscientização”, foi aplicado um novo questionário seguindo o modelo de pesquisa apresentado nas seções “6.1 – Organização objeto de estudo” e “6.2 – Desenvolvimento do Formulário”, ou seja, foi aplicado na mesma população e seguindo as mesmas validações já apresentadas.

Por já possuirmos as informações referente à população, este novo questionário de pesquisa é constituído por 3 categorias, pois não foi reaplicado as perguntas relacionadas às características sócio demográficas da população:

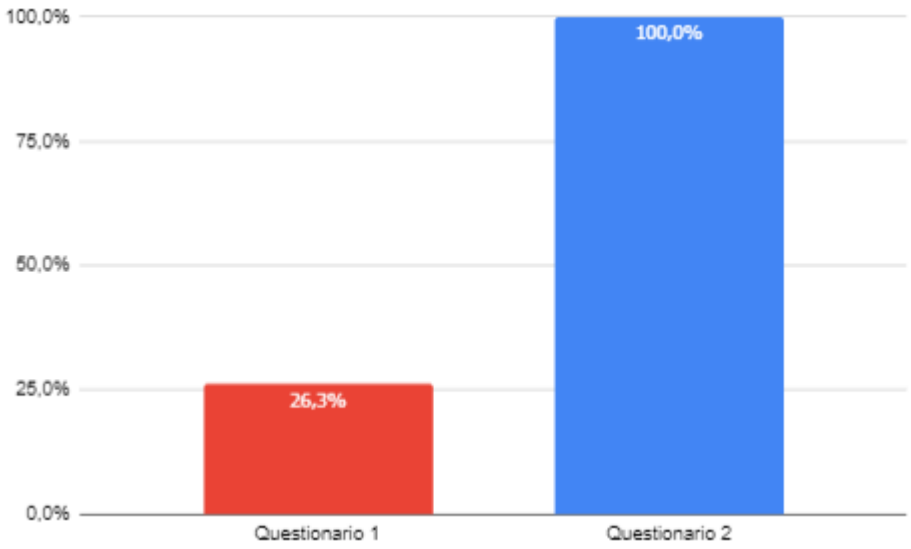
A. A primeira parte do questionário é focado em identificar as práticas que são realizadas posteriormente às ações de conscientização, pelos colaboradores, referente a segurança da informação e engenharia social, relacionadas a teoria apresentada nos capítulos 2, 3 e 4.
B. A segunda parte do questionário é focada em avaliar os novos conhecimentos relacionados a teoria sobre informação, segurança e engenharia social, apresentada nos capítulos 2 e 3.

C. A terceira parte do questionário é sobre práticas de segurança da informação adotadas, como políticas, treinamentos e estruturas da empresa pesquisada, relacionadas a teoria apresentada nos capítulos 3 e 4, após as ações de conscientização.

O formulário completo, com as perguntas apresentadas, pode ser visualizado no apêndice E.

No gráfico 34, pode-se observar que após as ações realizadas, 100% da população não acha seguro utilizar usuário e senha compartilhados, diferente do resultado no primeiro questionário (Gráfico 10) onde apenas 26,3% da população não utilizavam senhas compartilhadas.

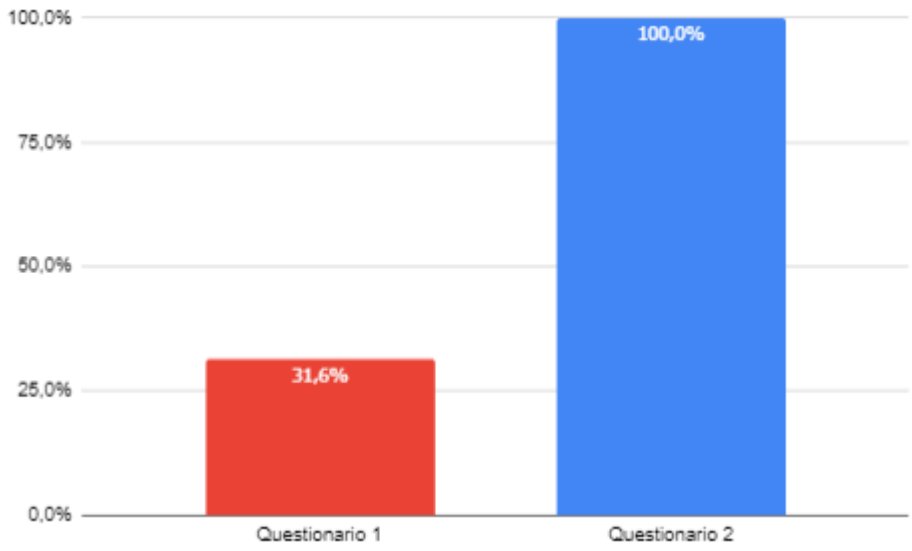
Gráfico 34: Senha Compartilhada II



Fonte: Dados da pesquisa.

No gráfico 35, pode-se observar que após as ações realizadas, 100% da população não anotaria sua senha em um local de fácil acesso, diferente do primeiro questionário (Gráfico 11) onde 31,6% da população nunca realizou esta ação.

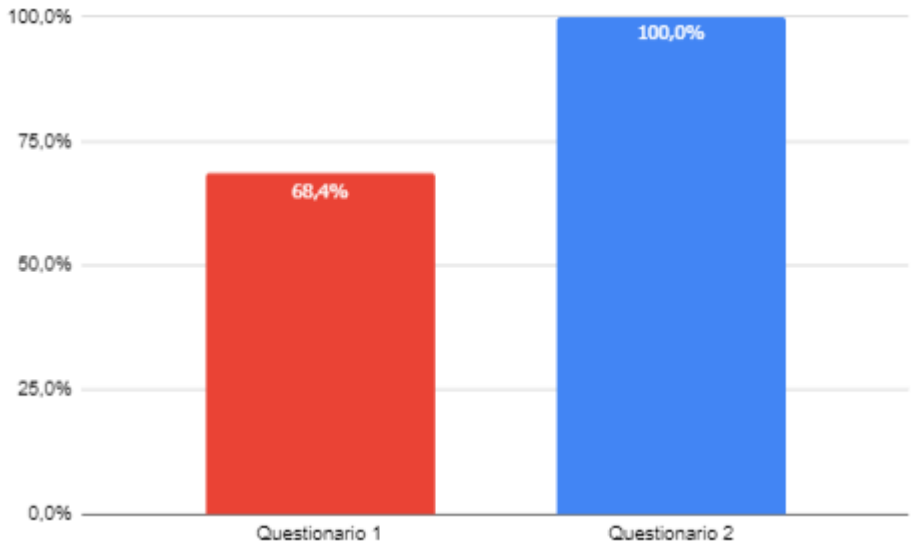
Gráfico 35: Anotação de Senha II



Fonte: Dados da pesquisa.

No gráfico 36, pode-se observar que após as ações realizadas, 100% da população não compartilharia uma senha de um sistema corporativo, diferente do primeiro questionário (Gráfico 12) onde 68,4% da população nunca compartilhou sua senha com algum colega de trabalho.

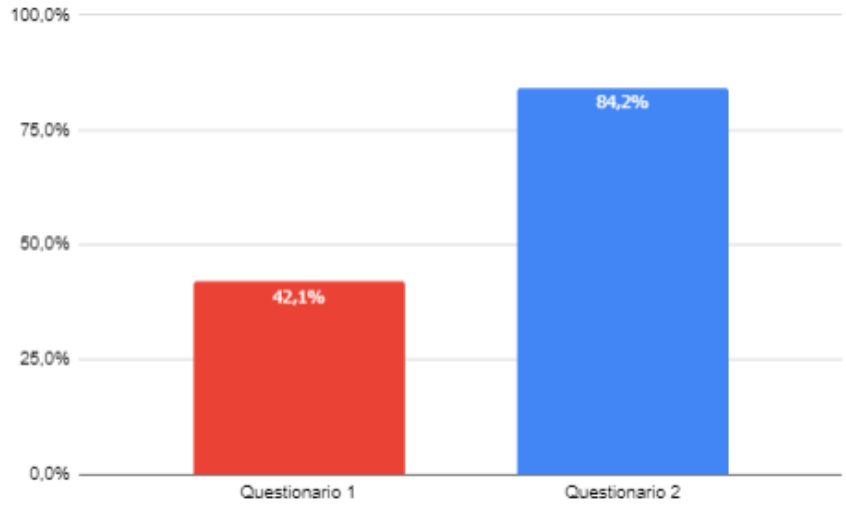
Gráfico 36: Compartilhamento de Senha II



Fonte: Dados da pesquisa.

No gráfico 37, pode-se observar que após as ações realizadas, 84,2% da população não criaria uma nova senha corporativa, similar a sua senha pessoal, diferente do primeiro questionário (Gráfico 13) onde este número era de 42,1% da população.

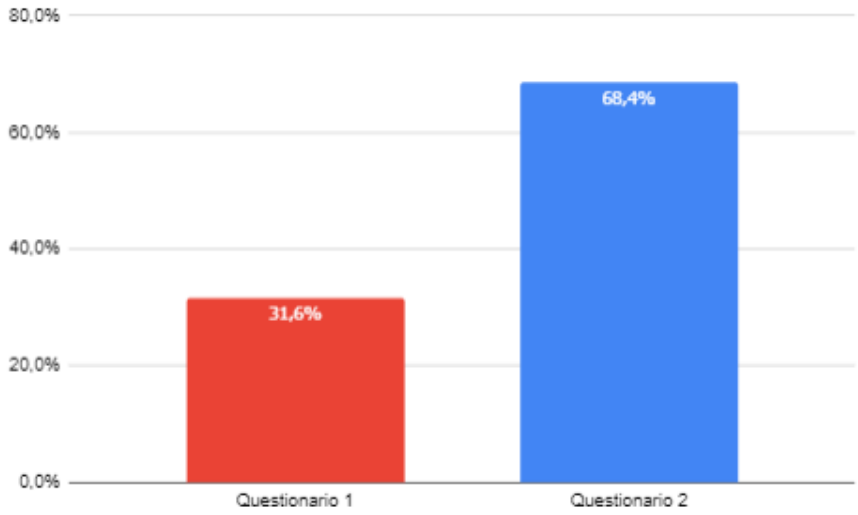
Gráfico 37: Similaridade de Senha II



Fonte: Dados da pesquisa.

No gráfico 38, pode-se observar que após as ações realizadas, 68,4% da população segue todas as recomendações ao criar uma nova senha, diferente do primeiro questionário (Gráfico 14) onde 31,6% da população informou seguir todas as recomendações anteriormente.

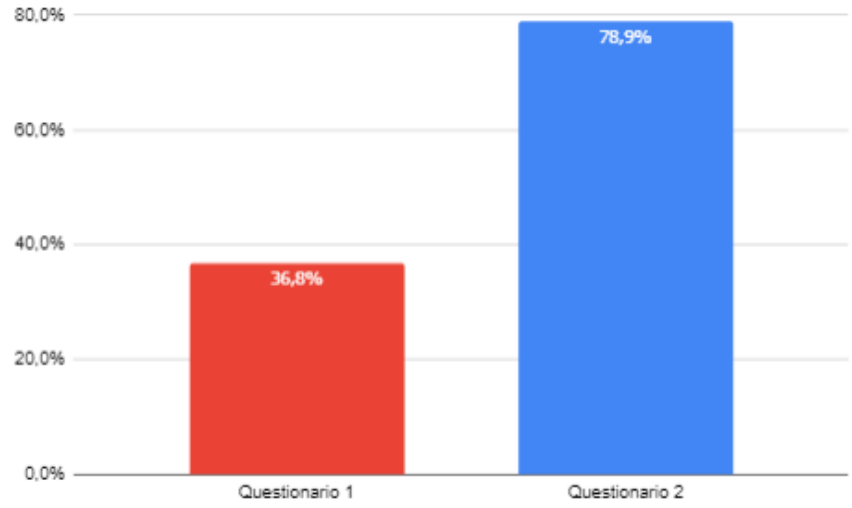
Gráfico 38: Recomendações de Senha II



Fonte: Dados da pesquisa.

No gráfico 39, pode-se observar que após as ações realizadas, 78,9% da população segue a recomendação de nunca deixar o computador desbloqueado ao deixar a estação de trabalho, diferente do primeiro questionário (Gráfico 15) onde este número era de apenas 36,8%.

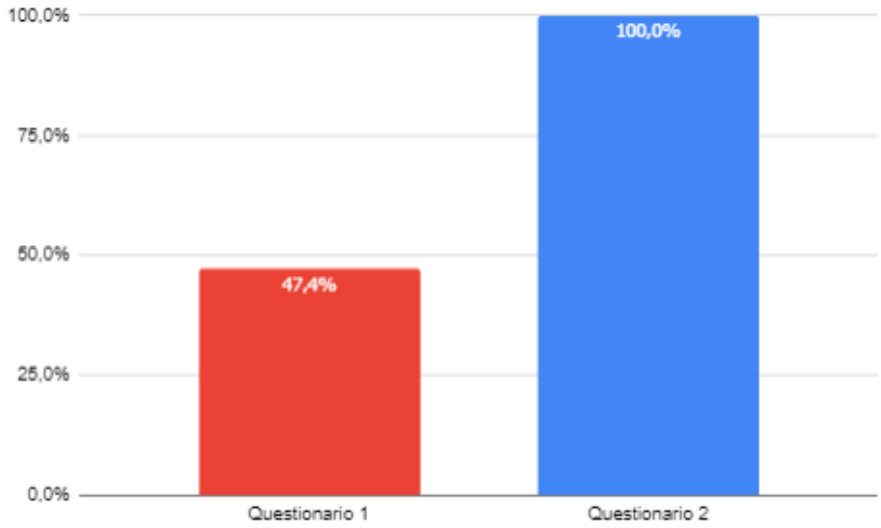
Gráfico 39: Estação de Trabalho II



Fonte: Dados da pesquisa.

No gráfico 40, pode-se observar que após as ações realizadas, toda a população (100%), não usaria uma aplicação não autorizada previamente e homologada pela empresa, diferente do primeiro questionário (Gráfico 16) onde 47,4% da população informou não utilizar algum aplicativo sem autorização da empresa.

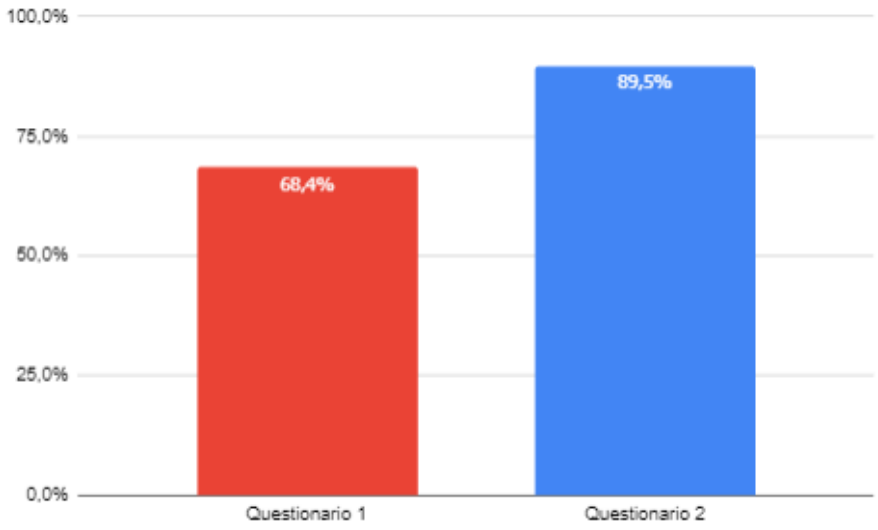
Gráfico 40: Homologação de Aplicação II



Fonte: Dados da pesquisa.

No gráfico 41, pode-se observar que após as ações realizadas, 89,5% da população sempre verificar o remetente e conteúdo de e-mail antes de realizar qualquer ação, diferente do primeiro questionário (Gráfico 17) onde apenas 68,4% da população realizava esta verificação nos e-mails recebidos.

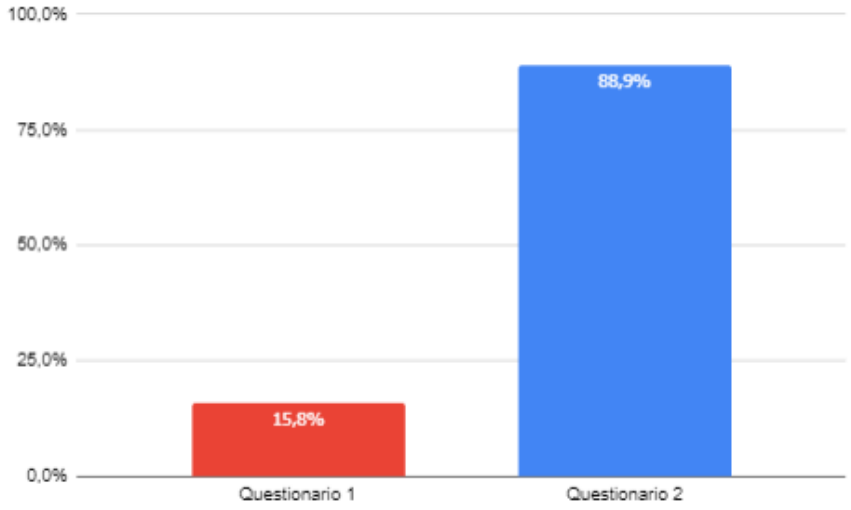
Gráfico 41: Remetente do E-mail II



Fonte: Dados da pesquisa.

No gráfico 42, pode-se observar que após as ações realizadas, 88,9% da população sabe que a forma correta para o descarte de documentos confidenciais é utilizando um triturador de lixo, diferente do primeiro questionário (Gráfico 18) onde apenas 15,8% da população informou que realizava o descarte do lixo desta forma.

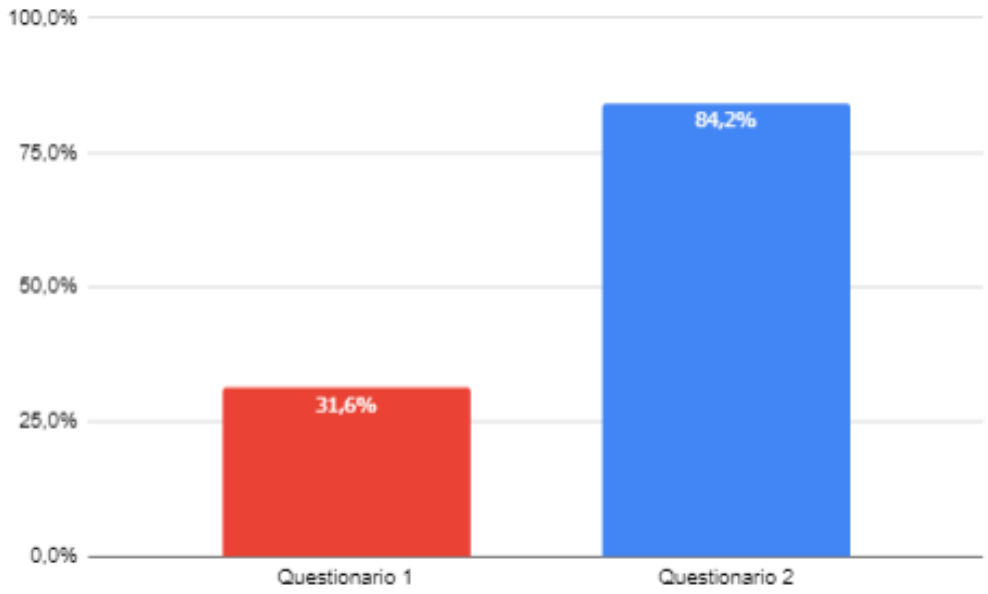
Gráfico 42: Descarte de Documentos II



Fonte: Dados da pesquisa.

No gráfico 43, pode-se observar que após as ações realizadas, 84,2% da população conhecem a correta definição de “Informação”, diferente do primeiro questionário onde (Gráfico 19) apenas 31,6% da população conhecia esta definição.

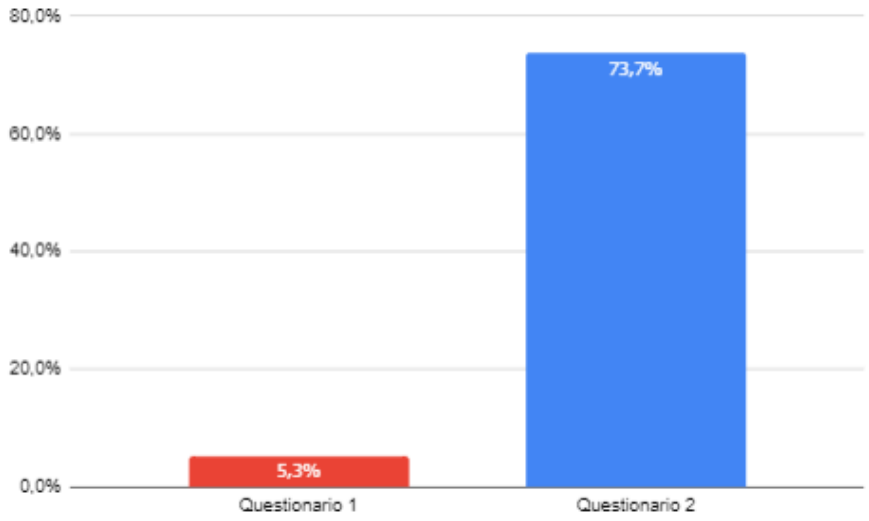
Gráfico 43: Informação II



Fonte: Dados da pesquisa.

No gráfico 44, pode-se observar que após as ações realizadas, 73,7% da população conhece a correta classificação das informações, diferente do primeiro questionário (Gráfico 20) onde apenas 5,3% da população conhecia esta classificação.

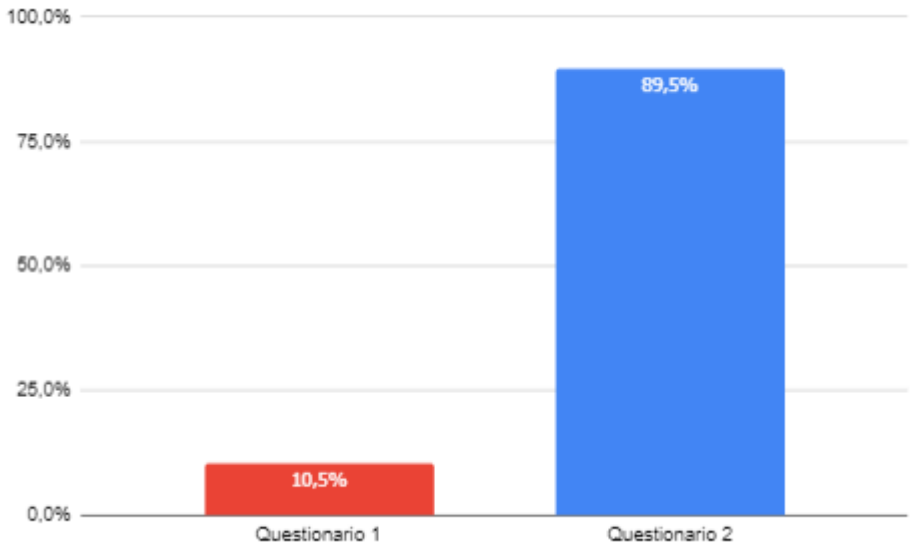
Gráfico 44: Classificação das Informações II



Fonte: Dados da pesquisa.

No gráfico 45, pode-se observar que após as ações realizadas, 89,5% da população conhece a definição de engenharia social, diferente do primeiro questionário (Gráfico 22) onde apenas 10,5% da população conhecia este termo.

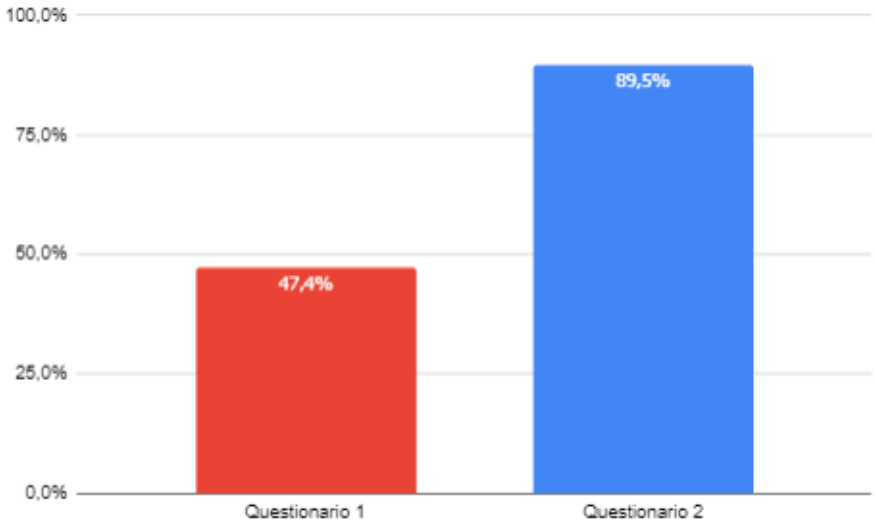
Gráfico 45: Classificação das Informações II



Fonte: Dados da pesquisa.

No gráfico 46, pode-se observar que após as ações realizadas, 89,5% da população conhece o alvo preferido dos engenheiros sociais, diferente do primeiro questionário (Gráfico 24) onde apenas 47,4% da população conhecia esta definição.

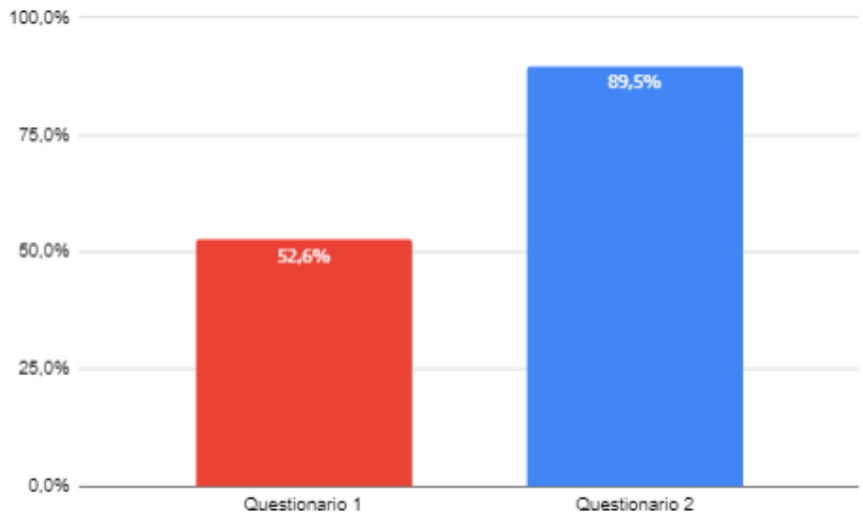
Gráfico 46: Alvo Engenharia Social II



Fonte: Dados da pesquisa.

No gráfico 47, pode-se observar que após as ações realizadas, 89,5% da população conhece a correta definição de phishing, que é um tipo de ameaça à segurança utilizada pelos engenheiros sociais, diferente do primeiro questionário (Gráfico 25) onde apenas 52,6% da população conhecia este tipo de ataque.

Gráfico 47: Phishing II



Fonte: Dados da pesquisa.

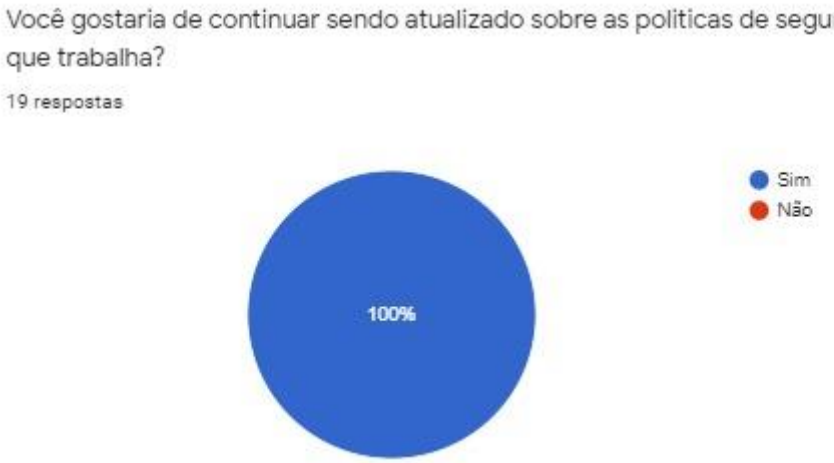
No gráfico 48, pode-se observar que após as ações realizadas, 94,7% da população considera extremamente importante ações de conscientização sobre engenharia social e segurança da informação.

Gráfico 48: Importância das Ações de Conscientização

Fonte: Dados da pesquisa.

No gráfico 49, pode-se observar que após as ações realizadas, 100% da população gostaria de continuar sendo atualizado sobre as políticas de segurança da empresa em que trabalham.

Gráfico 49: Atualizações sobre políticas de Segurança



Fonte: Dados da pesquisa.

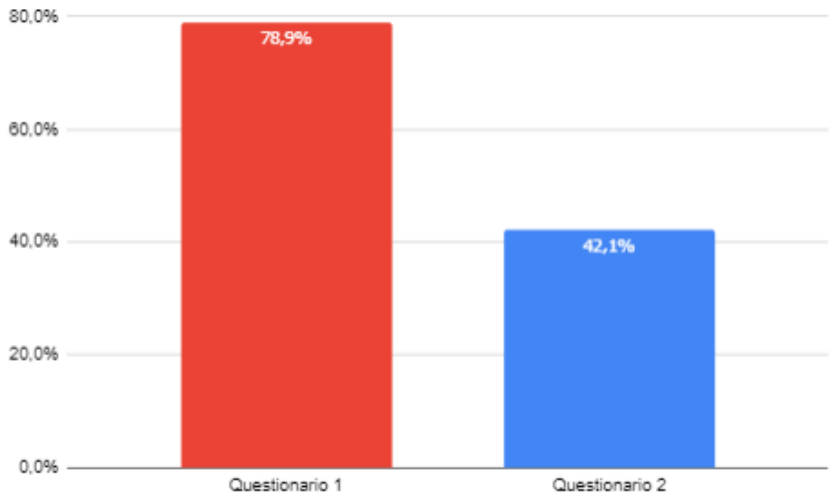
No gráfico 50, pode-se observar que após as ações realizadas, apenas 42,1% da população considera os cuidados da empresa referente a engenharia social e segurança da informação como bom ou excelente.

Gráfico 50: Cuidados de Segurança II

Fonte: Dados da pesquisa.

Diferente do primeiro questionário (Gráfico 30) onde este número era de 78,9%, o que demonstra que depois das pessoas conheceram mais sobre o tema, concluíram que as ações da empresa referente aos cuidados de segurança poderiam melhorar.

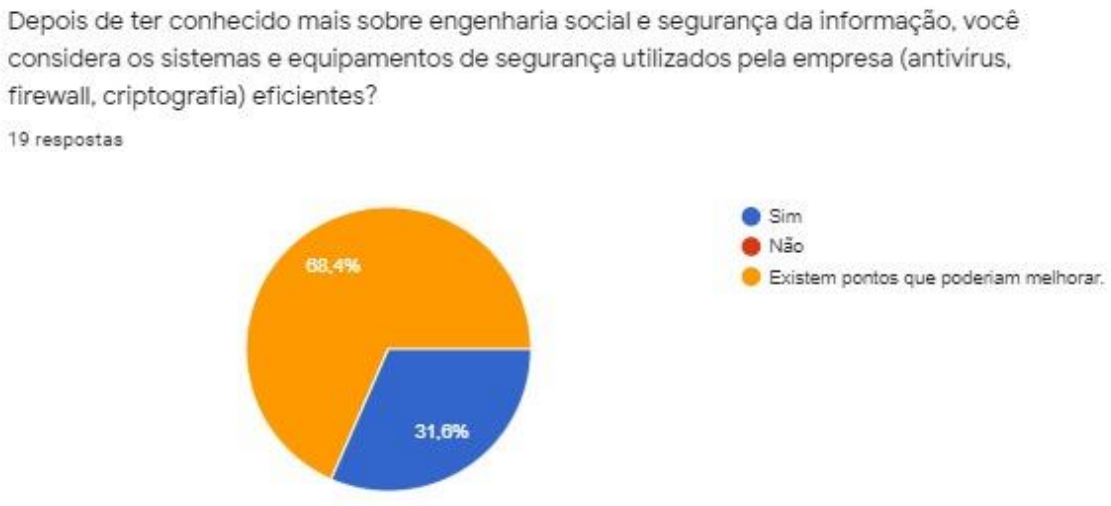
Gráfico 51: Cuidados de Segurança III



Fonte: Dados da pesquisa.

No gráfico 52, pode-se observar que após as ações realizadas, apenas 31,6% da população considera o sistema e equipamentos de segurança eficientes e outros 68,4% da população acreditam que existem pontos que precisam melhorar.

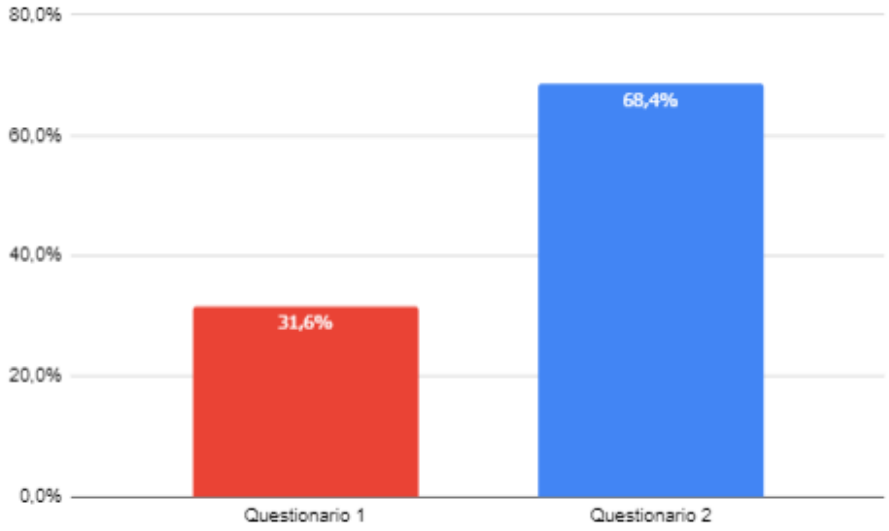
Gráfico 52: Equipamentos de Segurança II



Fonte: Dados da pesquisa.

Diferente do primeiro questionário (Gráfico 31) onde 68,4% da população acreditavam ser eficientes, o que demonstra que depois das pessoas conheceram mais sobre o tema, concluíram que o sistema e equipamentos de segurança poderiam melhorar.

Gráfico 53: Equipamentos de Segurança III



Fonte: Dados da pesquisa.

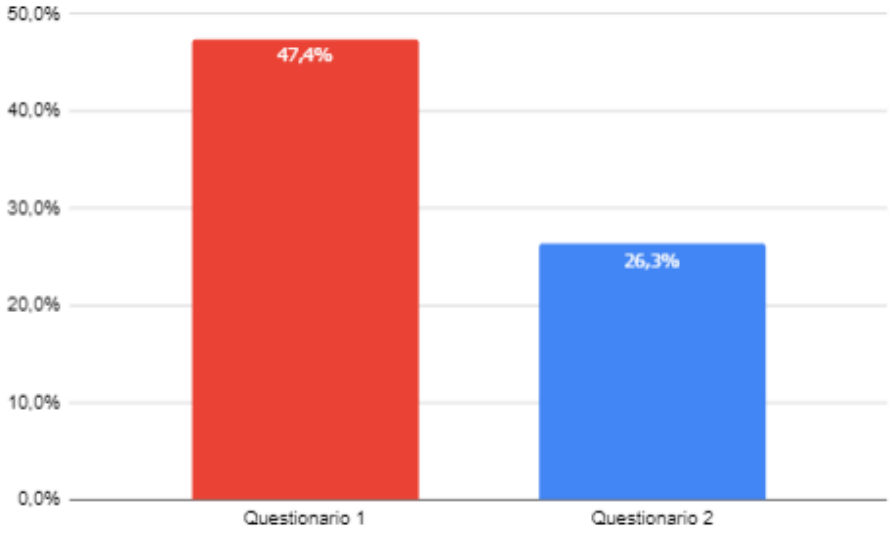
No gráfico 54, pode-se observar que após as ações realizadas, apenas 26,3% da população considera as barreiras de segurança física eficientes e outros 31,6% da população acreditam que existem pontos que precisam melhorar.

Gráfico 54: Segurança Física II

Fonte: Dados da pesquisa.

Diferente do primeiro questionário (Gráfico 32) onde 47,4% da população acreditavam ser eficientes, o que demonstra que depois das pessoas conheceram mais sobre o tema, concluíram que as barreiras de segurança física poderiam melhorar.

Gráfico 55: Segurança Física III



Fonte: Dados da pesquisa.

No gráfico 56, pode-se observar que as ações de conscientização que foram colocadas em prática na empresa pesquisa, antes da realização deste segundo questionário, foram consideradas boas ou excelentes por 94,7% pela população.

Gráfico 56: Avaliação das Ações

Fonte: Dados da pesquisa.

No gráfico 57, pode-se observar que após as ações realizadas, 94,7% da população gostaria de continuar sendo atualizado e participar de novas ações referente aos temas de engenharia social e segurança da informação.

Gráfico 57: Atualizações sobre Segurança II

Fonte: Dados da pesquisa.

Finalizando, pode se apresentar as diferenças dos valores e um gráfico resumindo as respostas da primeira e da 2ª aplicação da pesquisa.

O quadro a seguir apresenta esses valores, sendo que a 1ª Coluna “Questão”, indica qual é a pergunta considerada. A coluna “Antes” apresenta o valor da resposta em porcentagem, para a primeira pesquisa e a coluna “Depois” apresenta esse valor para a segunda aplicação considerando a questão indicada.

É importante destacar que quanto maior for o valor da porcentagem em cada resposta maiores serão as condições de segurança na empresa. Isso devido ao conhecimento sobre os conceitos e a aplicação adequadas das práticas de segurança da informação pelos funcionários da empresa. Dessa forma a coluna “Incremento” considera a diferença entre os valores da 2ª e da 1ª resposta (Depois-Antes) considerando essa diferença como um incremento nas condições de segurança.

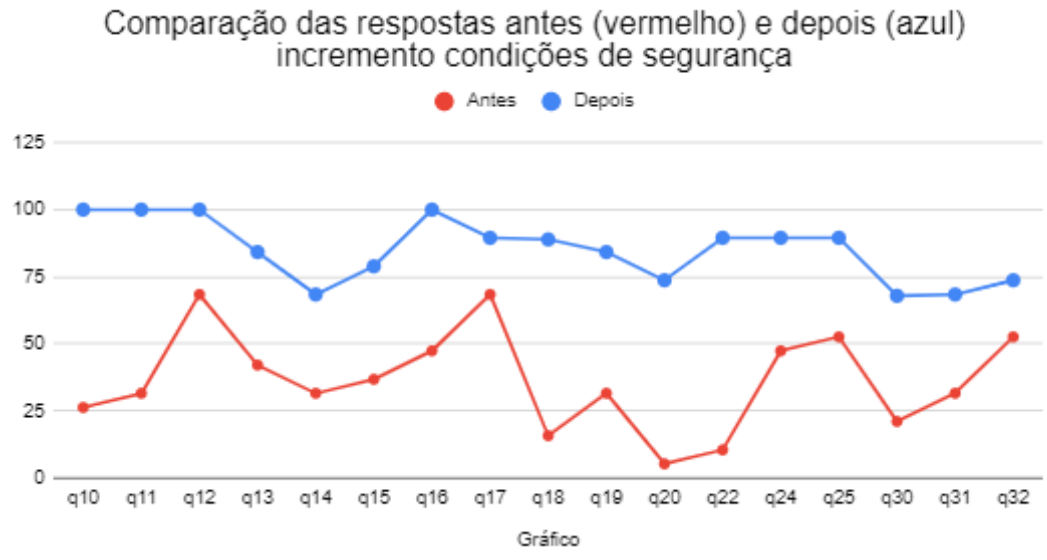
Quadro 3 - Comparativo nas respostas entre a 1ª e 2ª aplicação do questionário.

Questão	Antes %	Depois %	Incremento
q10	26,3	100	73,7
q11	31,6	100	68,4
q12	68,4	100	31,6
q13	42,1	84,2	42,1
q14	31,6	68,4	36,8
q15	36,8	78,9	42,1
q16	47,4	100	52,6
q17	68,4	89,5	21,1
q18	15,8	88,9	73,1
q19	31,6	84,2	52,6
q20	5,3	73,7	68,4
q22	10,5	89,5	79
q24	47,4	89,5	42,1
q25	52,6	89,5	36,9
q30	21,1	67,9	46,8
q31	31,6	68,4	36,8
q32	52,6	73,7	21,1

Fonte: Elaborada pelos autores.

O Gráfico a seguir apresenta esses números na forma de gráfico:

Gráfico 58 - Diferença entre as respostas para cada questão



Fonte: Elaborada pelos autores.

Ao analisar o gráfico é importante destacar que todas as respostas tiveram um incremento nos resultados apresentados na segunda aplicação do questionário. Em alguns casos chegando ao valor de 100%, isto é, quando na segunda pesquisa todos os entrevistados deram a resposta correta considerando as boas práticas de segurança.

O gráfico a seguir apresenta o valor do incremento em cada questão que pode se relacionar diretamente ao incremento nas condições de segurança, considerando cada questão. Esses valores, sempre positivos, variam de 20 a quase 80%.

Gráfico 59 - Incremento nos requisitos de segurança para cada questão

Fonte: Elaborada pelos autores.

Dessa forma pode se concluir que as ações de divulgação e conscientização aplicadas com o público alvo tiveram resultados altamente positivos.

Pela análise do perfil o público alvo pode ser descrito como sendo todos do sexo masculino, a maioria jovens, com poucos anos trabalhando na empresa pesquisada e para muitos sendo o primeiro emprego na área de tecnologia da informação. Por esse motivo recomenda-se a empresa, a continuidade das ações de prevenção e conscientização sobre a segurança da informação e engenharia social

com seus funcionários, em especial com todos os novos funcionários e com aqueles trabalhando com atendimento ao público interno e externo.

Pelos resultados apresentados percebe-se que medidas simples e de baixo custo, como as campanhas aqui demonstradas, pode ser muito eficazes no incremento das medidas de segurança e proteção dos ativos da informação da empresa.

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este capítulo apresenta as considerações finais baseadas na pesquisa realizada sobre engenharia social e a segurança da informação. Além disso, algumas sugestões para trabalhos futuros serão elencadas.

8.1 CONSIDERAÇÕES FINAIS

Neste trabalho, foram apresentados problemas relacionados à engenharia social e a segurança da informação. Esses temas são bastante amplos, o que pode ocasionar graves problemas para empresas que não estão preparadas para enfrentá-los.

O objetivo da pesquisa foi realizar um estudo na área de engenharia social em uma organização da área de tecnologia da informação.

Para isso, inicialmente foi realizado um levantamento bibliográfico da área. Nesta etapa foram encontradas dificuldades durante o período de busca por materiais científicos atualizados sobre segurança da informação, tema que está em constante atualização. Esse foi um desafio vencido mediante as pesquisas em referências bibliográficas confiáveis.

Nessa fase da pesquisa foram apresentados os principais tipos de ameaça e ataques utilizados por “hackers” que utilizam táticas de engenharia social e seus possíveis impactos em qualquer organização.

A falsa sensação de segurança conduz as empresas a adiarem as providências necessárias para redução dos riscos, o que as torna despreparadas para superar os ataques de invasores.

A segurança da informação é a forma com que as empresas protegem suas informações, garantindo a continuidade dos negócios, minimizando os danos e maximizando os resultados dos investimentos.

Surgem diariamente novos tipos de ameaças à segurança da informação. Para garantir esta segurança nas empresas, é preciso pensar tanto na segurança digital, protegendo os dados armazenado nos sistemas, assim como as barreiras de

segurança física, esta que muitas vezes é colocada em segundo plano, mas igualmente importante para garantir a segurança.

A engenharia social é uma forma para se obter informações confidenciais, sendo uma das mais perigosas e eficientes ao tentar obter essas informações. Existem vários ataques envolvendo a engenharia social, sendo importante entender por que o ser humano é tão vulnerável a ataques deste tipo.

O trabalho fez um levantamento com os funcionários de um setor da empresa sobre os seus conhecimentos, práticas e expectativas sobre Engenharia Social, através da aplicação de um questionário. Este documento foi elaborado a partir da teoria previamente estudada.

Após análise dos resultados deste questionário, diversas ações de conscientização sobre segurança da informação e Engenharia Social, foram realizadas dentro da empresa.

Outra dificuldade encontrada durante o desenvolvimento deste trabalho foi o desenvolvimento das ações junto a empresa pesquisada, pois devido a pandemia do COVID-19, a empresa estava em regime de home-office, o que impossibilitou a execução de algumas das ações que estavam planejadas. O home-office que precisou ser implantado na empresa, é um terreno fértil para a fragilidade da segurança da informação, o que torna ainda mais importante a disseminação do conhecimento sobre os temas de segurança da informação e engenharia social.

Após a aplicação das ações de conscientização foi novamente aplicado o questionário com o mesmo público alvo. Para todas as questões as respostas na segunda aplicação do questionário apresentaram um incremento dos resultados, considerando a primeira aplicação do questionário. Os valores do incremento em cada resposta, foram de 20 a quase 80%. Esse valor do incremento em cada questão pode se relacionar diretamente ao incremento nas condições de segurança.

Na segunda aplicação do questionário para algumas das perguntas todos os entrevistados deram a resposta correta considerando as boas práticas de segurança. Assim pode se afirmar que a proposta de ações sugeridas teve o efeito esperado na empresa pesquisada neste trabalho.

A prioridade para as organizações, é que seus colaboradores atuem no trabalho que foram encarregados de realizar. Diante da pressão cotidiana, as práticas de segurança da informação em geral são ignoradas. Os engenheiros sociais utilizam desta negligência para praticarem seus ataques.

Diversas pesquisas comprovam a necessidade da conscientização dos colaboradores das organizações, pois a melhor defesa contra os ataques de engenharia social é o treinamento e conscientização de todos que trabalham na empresa. Neste sentido, pode se afirmar que este trabalho comprovou a eficácia de ações simples de sensibilização e conscientização no incremento do conhecimento dos funcionários na empresa estudada.

É preciso conhecer os riscos e saber como minimizá-los, para garantir a segurança das informações da organização.

8.2 TRABALHOS FUTUROS

Apesar deste trabalho ter atingido os objetivos estabelecidos, trazendo os principais conceitos sobre engenharia social e segurança da informação, aplicando estes conhecimentos na realização de uma pesquisa, algumas ações poderiam agregar, acrescentando no resultado da pesquisa aplicada.

Ampliar a pesquisa e as ações de prevenção considerando também conceitos e práticas associadas à segregação de funções e política de privilégio mínimo. Sendo que, segundo Ferreira (2009), a "Política do menor privilégio: requer que não será dado a um usuário ou processo mais privilégios que o necessário para execução de seu trabalho", enquanto que, a Segregação de funções "visa garantir que nenhuma ação individual poderá comprometer a segurança de um sistema ou obter acesso não autorizado aos dados".

Após o retorno dos colaboradores da empresa, que estavam trabalhando em regime de home-office devido a pandemia do COVID-19, seria interessante a aplicação do seminário proposto como uma das ações de conscientização, pois permitirá uma interação para esclarecer todas as dúvidas sobre o tema e disseminar boas práticas de segurança presencialmente. Caso a empresa mantenha seu home-office por um longo período, recomenda-se a realização de webinars, seminários apresentados de forma digital.

Devido aos resultados positivos observados na conclusão da pesquisa, recomenda-se a aplicação das ações de conscientização sobre engenharia social e

segurança da informação para todos os colaboradores da empresa de tecnologia pesquisada neste trabalho.

Como citado anteriormente neste trabalho, os conhecimentos referentes a engenharia social e segurança da informação estão em constante atualização, por este motivo é importante continuar atualizando os conhecimentos das referências bibliográficas para que as empresas possam estar preparadas a se defender contra as novas ameaças.

Neste trabalho foram aplicadas uma série de ações de forma preventiva como seminário, FAQ, e-mail, intranet, vídeo, entre outros. Pode-se determinar um foco nessas ações, pesquisar sua eficiência, como ter a facilidade de aplicação e de divulgação, periodicidade adequada, para cada uma dessas ações, ou para a sua aplicação de forma conjunta.

Outra proposta de trabalhos futuros é a aplicação de pesquisas semelhantes a aquela desenvolvida neste trabalho em outras organizações.

REFERÊNCIAS

ADWARE. **Avast.** Disponível em: https://www.avast.com/pt-br/c-adware. Acesso em 17 nov 2019.

CAMPOS, André. **Sistemas de segurança da informação – controlando os riscos.** Santa Catarina: Editora Visual Books, 2006.

CAMPOS, André. **Sistemas de segurança da informação – controlando os riscos.** 3ª ed. Santa Catarina: Editora Visual Books, 2014.

CÔRTES, Pedro. **Administração de Sistemas de Informação.** São Paulo: Editora Saraiva, 2008.

COFFEE, Rafael. **Conteúdo em vídeo: entenda o poque desta febre e como aplicar em sua estratégia**. Disponível em https://rockcontent.com/blog/conteudo-em-video/. Acesso em 15 de mai 2020.

Confira frases marcantes de Steve Jobs, fundador da Apple. G1. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/10/confira-frases-marcantes-do-co-fundador-da-apple-steve-jobs.html. Acesso em 19 jun 2020.

COUTINHO, C. P.; LISBOA, E. Sociedade da Informação, Conhecimento e Aprendizagem Desafios para a Educação no Século XXI. **Revista de Educação**, Vol. XVIII, nº 1, 2011, pp. 5-22. Disponível em http://hdl.handle.net/1822/14854

CROSS-sit scripting (XSS). **Avast.** Disponível em https://www.avast.com/pt-br/c-xss. Acesso em 17 nov 2019.

CUNHA, Kaio. 2018. **Saiba como definir o porte da empresa e no que isso pode impactar o negócio.** Disponível em: https://conube.com.br/blog/como-definir-o-porte-da-empresa. Acesso em 04 dez 2019.

DAWEL, George. **A segurança da informação nas empresas - Ampliando horizontes além da tecnologia.** Rio de Janeiro: Editora Ciência moderna, 2005.

DDOS – ataque distribuído de negação de serviço. **Avast.** Disponível em: https://www.avast.com/pt-br/c-ddos. Acesso em 17 nov 2019.

DIA zero. **Avast.** Disponível em: https://www.avast.com/pt-br/c-zero-day. Acesso em 17 nov 2019.

FERREIRA, Fernando. **Segurança da Informação.** Rio de janeiro: Editora Ciência Moderna, 2003.

FERREIRA, Fernando; ARAÚJO, Márcio. **Políticas de Segurança da Informação - Guia prático para elaboração e implementação.** Rio de Janeiro: Editora Ciência Moderna, 2006.

FERREIRA, Harley Alves. **Auditoria de Segurança da Informação**. Tribunal de Contas. Secretaria de Fiscalização de Tecnologia da Informação. 2009. Disponível em https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14E01F8FC014E02CA0C3626DE. Acesso em 27 jul 2020.

FONTES, Edison. **Segurança da Informação – o usuário faz a diferença.** 1ª ed. – 6° tiragem São Paulo: Editora Saraiva, 2014.

HACKETT, Robert. 2015. **Fraudsters duped this company into handing over $40 million.** Disponível em: https://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million. Acesso em 04 Set. 2019.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais: administrando a empresa digital**. 5ª ed. São Paulo: Person Pretice Hall, 2006.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais: administrando a empresa digital**. 11ª ed. São Paulo: Person Pretice Hall, 2014.

MAÑAS, Antônio. **Administração de Sistemas de Informação - Como otimizar a empresa por meio dos sistemas de informação.** 6ª ed. São Paulo: Editora Érica, 2005.

MANN, Ian. **Engenharia social.** 1ª ed. São Paulo: Editora Blucher, 2018.

MICHAELIS, Dicionário online Michaelis. **Engenharia.** Disponível em https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/engenharia. Acesso em: 16 nov. 2019.

MICHAELIS, Dicionário online Michaelis. **Social.** Disponível em https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/social. Acesso em: 16 nov. 2019.

MITNICK, Kevin; SIMON, William. **A arte de enganar**. 1. ed. São Paulo: Makron Books, 2003.

NASCIMENTO, Felipe. Segurança da informação e engenharia social: a relevância do fator humano. **Sênior Blog**, 18 jul 2018. Disponível em: https://www.senior.com.br/blog/seguranca-da-informacao-e-engenharia-social-a-relevancia-do-fator-humano. Acesso em 17 nov 2019

NAKAMURA, Emilio; GEUS, Paulo. **Segurança de Redes em ambientes cooperativos**. 1. ed. São Paulo: Novatec Editora, 2007.
PHISHING. **Avast.** Disponível em https://www.avast.com/pt-br/c-phishing. Acesso em 17 nov 2019.

OGDEN, James. **Comunicação integrada de marketing – Modelo prático para um plano criativo e inovador**. 1 ª ed. São Paulo: Editora Pearson Education, 2002.

OPPAS. Organização Pan-Americana da Saúde. **Folha informativa – COVID-19 (doença causada pelo novo coronavírus).** Disponível em

https://www.paho.org/bra/index.php?option=com_content&view=article&id=6101:covid19&Itemid=875. Acesso em 15 mai 2020.

PORTELLA, Paulo. **Gestão de Segurança - História, Prevenção e Sistemas de proteção.** 2ª ed. Rio de Janeiro: Editora Rio Sociedade Cultural, 2005.

PRESTES, Vladimir. ARTIGO: Indústria e Segurança da Informação: as principais ameaças de 2018. **Revista Digital Security**, 11 out 2018. Disponível em: https://revistadigitalsecurity.com.br/artigo-industria-e-seguranca-da-informacao-as-principais-ameacas-de-2018. Acesso em 28 ago 2019.

RANSOMWARE. Avast. Disponível em https://www.avast.com/pt-br/c-ransomware. Acesso em 17 nov 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2ª edição. Rio de Janeiro: Elsevier, 2014

SILVA, Edna; MENEZES, Estera. **Metodologia da Pesquisa e elaboração de Dissertação**. 4ª ed. UFSC, Florianópolis, 2005.

SYSTEMATIC. **Ameaças emergentes – O que é engenharia social?.** Disponível em: https://br.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html. Acesso em 17 nov 2019.

TOWNSEND, Kevin. 2019. **Engenharia social: não se trata apenas de golpes de phishing.** Disponível em: https://blog.avast.com/pt-br/social-engineering-hacks Acesso em 26 ago 2019.

TURBAN, Efraim; RAINER JR, R. Kelly; POTTER, Richard. **Administração de tecnologia da informação - Teoria e Prática.** 3ª ed. Rio de Janeiro: Elsevier Editora, 2003.

WORMS de computador. **Avast.** Disponível em: https://www.avast.com/pt-br/c-computer-worm. Acesso em 17 nov 2019.

ZUCCHERATO, Gustavo. 2018. **ARTIGO: Indústria e Segurança da Informação: as principais ameaças de 2018.** Disponível em: https://revistadigitalsecurity.com.br/artigo-industria-e-seguranca-da-informacao-as-principais-ameacas-de-2018. Acesso em 20 ago 2019.

APÊNDICES

APÊNDICE A – CRONOGRAMA TCC

Cronograma TCC Engenharia social e segurança da informação – Alunos: Lucas Teixeira e Vinicius Diel – Orientador: Prof. Maria Inês.

ATIVIDADE	Outubro-				Novembro				Dezembro - Fevereiro				Março-				Abril-				Maio -				Junho-				Julho	
Semanas	1	2	3	4	1	2	3	4					1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
Leitura bibliografia	x	x	x	x																										
Redação Revisão bibliográgica	x	x	x																											
Entrega Cap2					x																									
Elaboração método				x	x	x	x																							
Entrega Cap3							x																							
Entrega Av Externo								x																						
Correções									x	x																				
Entrega Cap. 4																			x											
Elaboração questionário									x				x	x																
Revisão questionário															x	x														
Aplicação questionário																	x													
Analise resultado questionatio																		x												
Desenvolviemnto de ações																			x											
Elaboração Novo questionário																			x	x										
Aplicação novo questionário																				x	x									
Analise resultado questionário																					x	x								
Redação Cap 5																					x	x	x							
Entrega Cap. 5																								x						
Conclusões/ Resumo																							x	x						
Entrega Monog.																								x						
Apresentação																									x	x				
DEFESA																											x			
Correções																											x	x		
Entrega versão final																													x	

APÊNDICE B – QUESTIONARIO 1

Questionário - TCC sobre Engenharia social

Esta pesquisa faz parte do trabalho de conclusão de curso de Sistemas de informação da Unisul, desenvolvido por Lucas Costa Teixeira e Vinícius Schvambach Diel e orientado pela Dra. Maria Inés Castiñeira

Contamos com sua colaboração para o preenchimento deste questionário referente aos temas de Segurança da informação e Engenharia Social.

Sua identidade e suas informações serão preservadas e mantidas em sigilo.
Responda com sinceridade. *Obrigatório

Definição do perfil dos pesquisados

1. Qual sua idade? *

_____

2. Qual seu sexo? *

Marcar apenas uma oval.

- ◯ Masculino
- ◯ Feminino
- ◯ Prefiro não informar
- ◯ Outro:

_____

3. Você possui filhos(a)?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

4. Qual seu nível de escolaridade? * *Marcar apenas uma oval.*

- ◯ Médio incompleto
- ◯ Médio completo
- ◯ Superior incompleto
- ◯ Superior Completo
- ◯ Mestrado
- ◯ Doutorado.
- ◯ Outro: _____

5. Você pratica atividades físicas?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

6. Tempo de trabalho na área de tecnologia (em anos)? *

_____

7. Tempo de trabalho na empresa atual (em anos)? *

_____

8. Você já trabalhou em outras empresas de tecnologia antes da atual? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

9. Você já trabalhou em outras empresas que não eram ligadas a área de tecnologia? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

Avaliação sobre práticas de segurança

10. Você já utilizou usuário e senha compartilhadas? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei

11. Você já anotou sua senha em um lugar de fácil acesso? *

Marcar apenas uma oval.

- Sim
- Não

12. Você já compartilhou a senha que utiliza nos sistemas da empresa internamente ou externamente? * *Marcar apenas uma oval.*

- Sim
- Não

13. Sua senha profissional é igual ou similar a alguma senha que é utilizada no âmbito pessoal? *

Marcar apenas uma oval.

- Sim
- Não

14. Quando você cria uma senha, segue todas as recomendações de segurança *

Marcar apenas uma oval.

- Sim
- Não
- Somente quando obrigatório pelo sistema
- Não sei

15. Com qual frequência você costuma deixar seu computador desbloqueado ao deixar sua estação de trabalho? *

Marcar apenas uma oval.

	1	2	3	4	5	
Pouca						Muita

16. Você alguma vez já instalou e/ou utilizou alguma aplicação que não foi previamente homologado/autorizado pela empresa? * *Marcar apenas uma oval.*

- Sim
- Não
- Não sei

17. Você SEMPRE verifica o remetente e o conteúdo de um e-mail antes de clicar em um link ou fazer download de um anexo? * *Marcar apenas uma oval.*

- Sim
- Não

18. Como você realiza o descarte de documentos confidenciais? *

Marcar apenas uma oval.

- Utilizo um triturador de lixo para descartar todas as informações físicas
- Apenas descarto os documentos em lixeiras convencionais
- Outro: _____

Avaliação dos conhecimentos sobre informação, segurança e engenharia social

19. Para você qual a correta definição de INFORMAÇÃO? *

Marcar apenas uma oval.

- São fatos, eventos, atividades e transações registradas e armazenadas em seu estado bruto
- São dados registrados e organizados sem a necessidade de fazer sentido a um destinatário.
- São dados apresentados de forma significativa.

20. As informações podem ser classificadas como públicas, internas e confidenciais. “Informações que devem ser protegidas do acesso externo, pois um vazamento destas pode comprometer as operações da organização” é a definição de: * *Marcar apenas uma oval.*

- Informações internas e confidenciais.
- Somente informações internas.
- Somente informações confidenciais.
- Informações públicas.

21. Você conhece o significado do termo engenharia social? *

Marcar apenas uma oval.

- Sim
- Não

22. Para você, qual a definição mais correta sobre engenharia social? *

Marcar apenas uma oval.

- A arte que utiliza o comportamento humano, para que mesmo depois de a vítima perceber a manipulação, forneça informações importantes como senhas e dados sigilosos de uma organização.
- Manipular pessoas para que forneçam informações ou executem ações.
- Técnica de engenharia, que explora as vulnerabilidades de um sistema operacional, para obter informações sociais.
- Um vírus de computador utilizado por engenheiros que ameaça a segurança da sociedade.

23. Você acredita que já tenha sofrido um ataque de engenharia social? *

Marcar apenas uma oval.

- Sim
- Não
- Não sei

24. Qual o alvo preferido pelos engenheiros sociais: *

Marcar apenas uma oval.

- Dono da empresa
- Gestor de Segurança
- Atendentes
- Novos colaboradores

25. “Ataque utilizado para induzir que a vítima informe dados pessoais sigilosos”. É a definição para qual tipo de ameaça à segurança: *

Marcar apenas uma oval.

- Vírus
- Phishing
- Malware
- Spyware

Pesquisa sobre práticas da empresa pesquisada

26. Você recebeu algum tipo de treinamento de segurança da informação na sua empresa atual? *

Marcar apenas uma oval.

- Sim
- Não
- Não sei

27. Você recebeu algum tipo de treinamento especificamente sobre engenharia social da sua empresa atual? * *Marcar apenas uma oval.*

- Sim
- Não
- Não sei

28. Você recebeu orientações da empresa em que trabalha atualmente sobre realizar o atendimento externo? * *Marcar apenas uma oval.*

- Sim
- Não
- Não sei

29. Você conhece as políticas de segurança da informação da empresa na qual trabalha atualmente? * *Marcar apenas uma oval.*

- Conheço todas as politicas
- Não conheço todas as políticas
- Não conheço nenhuma política
- Não sei o que são politicas de segurança

30. Como você define os cuidados na empresa em que trabalha referente a segurança e engenharia social: * *Marcar apenas uma oval.*

1 2 3 4 5

Péssimos ◯ ◯ ◯ ◯ ◯ Exelentes

31. Você considera os sistemas e equipamentos de segurança utilizados pela empresa (antivírus, firewall, criptografia) eficientes? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Existem pontos que poderiam melhorar.

32. Você considera a segurança física (barreiras que impedem entradas e saídas não autorizadas) da sua empresa eficiente? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Existem pontos que poderiam melhorar.

33. Você teria interesse em receber mais informações sobre Segurança da informação e Engenharia Social por parte da sua empresa? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não

APÊNDICE C – E-MAIL QUESTIONARIO

Bom dia/Boa Tarde/Boa noite

Estamos lhe encaminhando um questionário, referente a pesquisa de trabalho de conclusão do curso de Sistemas de Informação da Unisul.

O tema abordado neste trabalho é Engenharia Social e a Segurança da Informação, onde serão apresentadas perguntas sobre o tema de Segurança e suas experiências na empresa de tecnologia que trabalha atualmente.

Solicitamos que respondam com sinceridade, pois sua identidade e respostas serão mantidas em sigilo e serão de extrema importância sua participação para o sucesso de nossa pesquisa.

Segue o Link para que possam responder a este formulário:
https://forms.gle/VFb52L5ZrFXYJGu97

Contamos com a sua colaboração.

Atenciosamente,
Vinicius Diel e Lucas Teixeira

APÊNDICE D – FAQ

FAQ - Principais dúvidas sobre segurança da informação

Você sabe o que é informação?

A informação pode ser definida como um conjunto de fatos organizados, de modo que faça sentido ao seu destinatário.

Pode-se entender de forma resumida que as informações **são dados apresentados de forma significativa,** e precisam fazer sentido a um destinatário

Você sabe a diferença entre informação pública, privada e confidencial?

- Informação Pública: São as informações que não necessitam de nenhum tipo de sigilo, podendo ter livre acesso a qualquer pessoa;
- Informação Interna: São informações que devem ser evitadas ao acesso externo, porém não existem graves consequências se esses se tornarem público;
- Informação Confidencial: São informações que devem ser protegidas do acesso externo, pois o vazamento delas pode comprometer as operações da organização.

Você sabe o que é segurança da informação?

A segurança da informação é a forma com que as empresas protegem suas informações, garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e oportunidades.

É imprescindível que as empresas que desejam manter suas informações seguras invistam e conheçam os conceitos ligados a segurança da informação

Manter sua senha segura, não utilizar senhas compartilhadas, assegurar que sua estação de trabalho esteja protegida, não utilizar aplicações não homologadas (como Spotify, Discord, Extensão do Chrome, entre outros recursos não aprovados previamente pela empresa) e verificar com atenção os e-mails antes de respondê los, são atitudes simples que ajudam a manter a segurança da informação.

Você sabe o que é engenharia social?

Engenharia social é a arte de utilizar o comportamento humano para quebrar a segurança, **manipulando pessoas para que forneçam informações ou executem ações** sem que a vítima perceba que foi manipulada.

Os **novos colaboradores das empresas são os alvos preferidos dos engenheiros sociais**, pois estes desconhecem os procedimentos de segurança e o que devem ou não devem fazer dentro da empresa.

Você sabe quais os principais tipos de ameaças à segurança?

- Vírus: É um programa com a capacidade de anexar-se e infectar outros programas de computadores. O vírus se espalha, provocando danos ao computador e obtendo informações sigilosas

- Phishing: É um ataque utilizado para que a vítima revele informações pessoais como senhas, dados bancários ou dados pessoais. Trata-se de uma forma simples de explorar a falta de conhecimento referente a segurança das vítimas.

- Malware: É um tipo de ameaça que instala programas e executa tarefas sem o seu consentimento

- Spyware: É um software especializado em monitorar de forma oculta as atividades de um computador ou sistema. Esta ameaça captura as atividades do usuário, como sites acessados, teclas digitadas e senhas por exemplo.

Como criar uma senha segura?

As senhas são o recurso mais utilizado no que se refere a segurança da informação. Porém o uso de senhas fracas, fragiliza a segurança das informações. A senha é uma informação sigilosa e nunca deve ser fornecida a outras pessoas.

Devemos seguir algumas orientações durante a escolha de uma senha:

- Utilizar senha com letras maiúsculas e minúsculas, números e caracteres especiais.
- Não deve ser utilizado senhas curtas
- Não utilizar sequência de caracteres.
- Não utilizar datas comemorativas, nomes de pessoas, nomes de time ou outras informações que estejam ligadas a você ou a organização.
- Utilizar senhas fáceis de serem lembradas por você, porém difíceis de ser adivinhada por terceiros.
- Não utilize senhas pessoais no ambiente de trabalho.
- Deve-se atualizar a senha de forma periódica.
- Sempre que receber uma senha automática e padrão do sistema, deve-se modificá-la imediatamente.

Identificado o vazamento ou compartilhamento da senha a terceiros, deve ser comunicado imediatamente o setor de segurança da informação.

APÊNDICE E – QUESTIONARIO 2

Questionário 2 - TCC sobre Engenharia social

Esta pesquisa faz parte do trabalho de conclusão de curso de Sistemas de informação da Unisul, desenvolvido por Lucas Costa Teixeira e Vinícius Schvambach Diel e orientado pela Dra. Maria Inés Castiñeira

Após as ações de conscientização que você participou sobre os temas, contamos com sua colaboração para o preenchimento deste segundo questionário referente aos temas de Segurança da informação e Engenharia Social, para validação das ações aplicadas.

Sua identidade e suas informações serão preservadas e mantidas em sigilo.
Responda com sinceridade.
*Obrigatório

Avaliação sobre práticas de segurança

1. Depois dos seu recentes conhecimentos sobre segurança da informação, você considera seguro continuar a utilizar usuário e senha compartilhadas? *

   Marcar apenas uma oval.

   - ◯ Sim
   - ◯ Não
   - ◯ Não sei

2. Depois dos seu recentes conhecimentos sobre segurança da informação, você anotaria a sua senha em um lugar de fácil acesso? * *Marcar apenas uma oval.*

   - Sim
   - Não

3.

   informação, você compartilharia a senha que utiliza nos sistemas da empresa? *

   Marcar apenas uma oval.

   - Sim
   - Não

4. Depois dos seu recentes conhecimentos sobre segurança da informação, você criaria uma senha para o ambiente profissional igual ou similar a alguma senha que é utilizada no âmbito pessoal? * *Marcar apenas uma oval.*

   - Sim
   - Não

5. Depois dos seu recentes conhecimentos sobre segurança da informação, você segue todas as recomendações parar criar uma nova senha segura? *

   Marcar apenas uma oval.

   - Sim
   - Não
   - Somente quando obrigatório pelo sistema

6.

informação, com qual frequência você costuma deixar seu computador desbloqueado ao deixar sua estação de trabalho? * *Marcar apenas uma oval.*

	1	2	3	4	5	
Pouca	◯	◯	◯	◯	◯	Muita

7. Depois dos seu recentes conhecimentos sobre segurança da informação, você instalaria e/ou utilizaria alguma aplicação que não foi previamente homologado/autorizado pela empresa? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Não sei

8. Depois dos seu recentes conhecimentos sobre segurança da informação, você verifica o remetente e o conteúdo de um e-mail antes de clicar em um link ou fazer download de um anexo? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não

9.

informação, como você considera a forma mais correta para o descarte de documentos confidenciais? * *Marcar apenas uma oval.*

- ◯ Utilizo um triturador de lixo para descartar todas as informações físicas
- ◯ Apenas descartando os documentos em lixeiras convencionais

Avaliação dos conhecimentos sobre informação, segurança e engenharia social

10. Para você qual a correta definição de INFORMAÇÃO? *

Marcar apenas uma oval.

- São fatos, eventos, atividades e transações registradas e armazenadas em seu estado bruto
- São dados registrados e organizados sem a necessidade de fazer sentido a um destinatário.
- São dados apresentados de forma significativa.

11. As informações podem ser classificadas como públicas, internas e confidenciais. “Informações que devem ser protegida do acesso externo, pois um vazamento destas pode comprometer as operações da organização” é a definição de: * *Marcar apenas uma oval.*

- Informações internas e confidenciais.
- Somente informações internas.
- Somente informações confidenciais.
- Informações públicas.

12. Para você, qual a definição mais correta sobre engenharia social? *

Marcar apenas uma oval.

- A arte que utiliza o comportamento humano, para que mesmo depois de a vítima perceber a manipulação, forneça informações importantes como senhas e dados sigilosos de uma organização.
- Manipular pessoas para que forneçam informações ou executem ações.

- [ ] Técnica de engenharia, que explora as vulnerabilidades de um sistema operacional, para obter informações sociais.
- [ ] Um vírus de computador utilizado por engenheiros que ameaça a segurança da sociedade.

13. Qual o alvo preferido pelos engenheiros sociais: *

Marcar apenas uma oval.

- [ ] Dono da empresa
- [ ] Gestor de Segurança
- [ ] Atendentes
- [ ] Novos colaboradores

14. “Ataque utilizado para induzir que a vítima informe dados pessoais sigilosos”. É a definição para qual tipo de ameaça à segurança: * *Marcar apenas uma oval.*

- [ ] Vírus
- [ ] Phishing
- [ ] Malware
- [ ] Spyware

Pesquisa sobre as ações de conscientização

15. Como avalia a importância de ações de conscientização sobre o tema de engenharia Social e segurança da informação?

Marcar apenas uma oval.

	1	2	3	4	5	
Pouco importante	◯	◯	◯	◯	◯	Extremamente importante

16. Você gostaria de continuar sendo atualizado sobre as politicas de segurança da empresa em que trabalha? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não

17. Depois de ter conhecido mais sobre engenharia social e segurança da informação, como você define os cuidados na empresa em que trabalha referentes a estes temas? * *Marcar apenas uma oval.*

	1	2	3	4	5	
Péssimos	◯	◯	◯	◯	◯	Excelentes

18. Depois de ter conhecido mais sobre engenharia social e segurança da informação, você considera os sistemas e equipamentos de segurança utilizados pela empresa (antivírus, firewall, criptografia) eficientes? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Existem pontos que poderiam melhorar.

19. Depois de ter conhecido mais cobre engenharia social e segurança da informação, você considera a segurança física (barreiras que impedem entradas e saídas não autorizadas) da sua empresa eficiente? * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Existem pontos que poderiam melhorar.

20. Como você avalia as ações (como folders, vídeos e e-mails) que foram colocadas em prática * *Marcar apenas uma oval.*

	1	2	3	4	5	
Insuficientes	◯	◯	◯	◯	◯	Excelentes

21. Você gostaria de continuar recebendo de forma constante novas informações sobre engenharia Social e segurança da informação no seu local de trabalho? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei