UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Engenharia Social e Técnicas de Defesas: uma abordagem no nível de conhecimento e de conscientização de usuários de dispositivos de Internet das Coisas

Dissertação de Mestrado

Maiara de Castro Santos

São Cristóvão – Sergipe

2022

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Maiara de Castro Santos

Engenharia Social e Técnicas de Defesas: uma abordagem no nível de conhecimento e de conscientização de usuários de dispositivos de Internet das Coisas

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Sergipe como requisito parcial para a obtenção do título de mestre em Ciência da Computação.

Orientador(a): Dr. Admilson de Ribamar Lima Ribeiro
Coorientador(a): Dr. Gilton José Ferreira da Silva

São Cristóvão – Sergipe

2022

Resumo

Frente ao crescente uso de dispositivos de Internet das Coisas (IoT) e, em decorrência da contribuição destes para a sociedade, a questão da segurança tem uma grande repercussão atualmente, de maneira que o grande desafio é fazer uso das informações prezando pelos princípios da segurança e promovendo ambientes virtuais éticos úteis, e coesos com as demandas sociais. Desta forma, o objetivo macro desta pesquisa foi promover um espaço virtual onde os usuários de tecnologias como IoT, entre outras, possam conhecer melhores práticas de uso, de modo a sentirem mais seguros em rede. Para o alcance deste objetivo, busca-se por meio de uma coleta de dados, uma análise aprofundada acerca do nível de conhecimento de usuários de dispositivos tais como IoT, a fim de descrever riscos e vulnerabilidades aos quais estes possam estar expostos, bem como propor ações de mitigação de tais riscos. Para a validação do instrumento (portal CIS), direcionou-se um formulário aplicado a gestores de TI, que buscou captar a opinião do público-alvo acerca da eficiência do curso oferecido pelo Portal. Esta avaliação permite concluir que se trata de uma ferramenta relevante, cuja utilização contribui com a segurança em Redes de Internet das Coisas e tecnologias similares.

Palavras-chave: Internet das Coisas, Segurança da Informação, Engenharia Social; Usuários.

Abstract

Faced with the growing use of Internet of Things (IoT) devices and as a result of the contribution of these to society, the issue of security has a great repercussion currently, so that the great challenge is to make use of the information valuing the security principles and promoting useful ethical virtual environments, cohesive with the demands social. Thus, the macro objective of this research was to promote a virtual space where users of technologies such as IoT, among others, can get to know better usage practices, in order to feel more secure in the network. To achieve this objective, we sought to if through data collection, an in-depth analysis of the level of knowledge of users of devices such as IoT in order to describe risks and vulnerabilities to which they may be exposed, as well as proposing actions to mitigate such risks. For validation of the instrument (CIS portal), a form was applied to managers of TI, which sought to capture the opinion of the target audience about the efficiency of the course offered by the Portal. This evaluation allows us to conclude that it is a relevant tool, whose use contributes to security in Internet of Things Networks and similar technologies.

Keywords: Internet of Things, Information Security, Social Engineering; Users.

Agradecimentos

Primeiramente a Deus que permitiu que tudo isso acontecesse ao longo de minha vida, que me deu saúde e forças para superar todos os obstáculos nessa caminhada.

A minha mãe Maria Auxiliadora, pelo seu amor e dedicação em compartilhar meus sonhos, dividir meus medos, por todo apoio e dedicação.

Aos meus irmãos, Maiane, Maíza e Marxs, por sonharem sempre ao meu lado e não permitir que eu desanimasse diante das incertezas e dos obstáculos.

Aos demais familiares, especialmente aos meus tios Reginaldo e Eliane, e a minha vó Paulina pelo apoio e incentivo.

Aos meus amigos: Ricardo, Ilanna, Moisés, especialmente a Caio, Natália, Jadson e Mairon, que desde o início, me apoiaram sem medir esforços.

Agradeço ao meu orientador e coorientador Admilson e Gilton Ferreira, respectivamente, por ter sido meu orientador e ter desempenhado tal função com dedicação e amizade.

Enfim, a todos os funcionários do DCOMP/UFS especialmente a secretária Elaine por terem contribuído nesta conquista pessoal e profissional.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX
CE	Critérios de Exclusão
CI	Critérios de Inclusão
CIS	Checklist IoT Security
CMS	Content Management System
COVID-19	Doença do Coronavírus de 2019
DCOMP	Departamento de Computação
IPS	sistema de prevenção de intrusos
IDP	Sistema de detecção e prevenção
LGPD	Lei Geral de Proteção dos Dados Pessoais
MSL	Mapeamento Sistemático da Literatura
PII	Personally Identifiably Information
RFID	Identificação por Radiofrequência
QPP	Questão de Pesquisa Primária
QPS	Questões Pesquisa Secundárias
SUBA	Security User Behavior Analytics
SGSI	Sistemas de Gestão de Segurança da Informação
SSL	Secure Sockets Layer
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicação
TGS	Teoria Geral de Sistemas
UEBA	User and Entity Behavior Analytics
UBA	User behavior analytics

UFS	Universidade Federal de Sergipe
UFRGS	Universidade Federal dO Rio Grande do Sul
VPN	Virtual Private Network

Sumário

1 Introdução

Este capítulo faz uma breve contextualização acerca da Internet das Coisas, do inglês Internet of Things (IoT), enquanto objeto de pesquisa e aborda a motivação, a problemática, uma justificativa e a organização do documento.

1.1 Apresentação Geral

A IoT, Internet das Coisas, do inglês Internet of Things, responde a comandos através de impressões digitais, expressão facial e gestos corporais, denominadas informações biológicas. Rosner (2016) explicita sobre privacidade dos usuários de IoT, pontuando que tais meios de acesso, são reversíveis e, quando relacionados à privacidade dos usuários, deixam a desejar por ser necessário utilizar dados pessoais o tempo todo, cabendo questionar a respeito de um método seguro para a ocultação destas informações (DONG et al., 2018).

Cavalli (2016) para conceituar IoT, insere a Internet das Coisas em um conjunto de tecnologias e protocolos associados, ou seja, interconectados, capazes de permitir que objetos comuns do dia a dia, sejam agregados a uma rede de comunicações e sejam identificados e controlados através desta conexão de rede.

Alexandrov, Desnitsky e Chaly (2019), explicitam que o conceito de IoT está cada vez mais presente nas sociedades atuais. Essa nova configuração traz como obstáculo, a exposição do usuário em rede e, consequentemente, a vulnerabilidade. De modo que, para criar um módulo protegido de sistema de informação e telecomunicações que implemente o conceito Internet das Coisas, é importante levar em consideração todos os seus aspectos.

De acordo com Magrani (2018) presume-se que, com o aumento exponencial de utilização de dispositivos interconectados que já existem ou que entrarão em breve no mercado, devemos estar atentos aos riscos que isso pode acarretar para a privacidade e a segurança dos usuários, uma vez que, quanto maior a exposição em rede, maior o risco.

Dong et al. (2018) alertam que, enquanto esses dispositivos domésticos inteligentes crescem em popularidade frente à capacidade de tornar a vida cotidiana mais confortável e conveniente, esses também levantam preocupações com relação à segurança e à privacidade, além da baixa capacidade técnica.

Para os autores, frente às preocupações referentes à segurança e privacidade e, considerando a proposição de que um ataque de Engenharia Social é, por si, uma ação elaborada que se dá frente à boa vontade e colaboração de outrem, o invasor estará em uma posição privilegiada no fluxo da informação. Tal requisito torna-se elemento facilitador para o alcance dos objetivos do invasor. Tal premissa permite alcançar um agravante, haja vista, a Engenharia Social a partir do prisma da confiança estabelecida, bem como, pontuar que a confiança é construída por meio da comunicação.

De acordo com Qusa et al. (2019), a segurança empreendida em redes deve ser tão levada a sério, quanto a segurança física de uma organização comercial. Esta última trabalha com funcionários preparados com habilidades técnicas necessárias. Significa que a segurança em rede deve contar com um suporte tão eficiente quanto a física. Necessitando também de inibidores.

Mediante à amplitude que o uso de IoT tem alcançado nos cenários atuais, a busca por soluções relativas à Internet das Coisas no que tange à Engenharia Social, enfatiza uma dificuldade significativa no que diz respeito a se permanecer seguro em relação ao uso de IoT, essa tecnologia que permite uma conexão a tudo e a todos. Portanto, é evidente que a implementação de pesquisas neste âmbito se faz relevante.

1.2 Motivação

Frente ao crescente uso de IoT e, em decorrência da contribuição destes aparatos para com a sociedade, uma vez que proporcionam uma vida com mais comodidade e praticidade, promovendo um mundo conectado, cujo monitoramento e controle desses objetos são feitos de forma remota, faz-se crucial um olhar aprofundado acerca da segurança em rede.

Gartner (2014) já contava com tal crescimento afirmando que, dentre as tecnologias emergentes para os dias atuais, a IoT estaria no topo. A afirmação ganha consistência quando Magrani (2018) traz dados mais atualizados ao afirmar que pesquisas apontam que a quantidade de objetos conectados em 2020, ultrapassará 25 bilhões, podendo chegar a 50 bilhões.

Quanto maior o número de usuários de IoT conscientes, menor será o enfrentamento no que tange à vulnerabilidade. Portanto, propõe-se neste ínterim, a disseminação de um curso manual de instruções que aponte os principais ataques de engenharia social e oriente os usuários a buscar melhores práticas de uso das tecnologias.

Faz-se importante identificar as vulnerabilidades de alto risco em dispositivos IoT domésticos inteligentes, bem como listar as principais ameaças e vulnerabilidades que afetam os

dispositivos IoT domésticos inteligentes (COSTA; BARROS; TAVARES, 2019).

Quando se concentram mais na utilidade e conveniência dos dispositivos IoT sem a devida preocupação com as falhas de segurança inerentes a tais dispositivos, os consumidores se expõem a alguns riscos e danos como apontam (PLACHKINOVA; MENARD, 2019).

A IoT passou a ser cada vez mais atuante nos ambientes domiciliares, cujas casas Inteligentes trazem em si, um conjunto de sistemas de automação que entregam bem-estar, segurança material e conectividade. Todos esses elementos integrados e a medida em que a casa inteligente se torna cada vez mais comum, os dispositivos, da geladeira ao termostato, vão se conectando entre si, fazendo com que cresçam também as discussões acerca da segurança da informação neste contexto (JUNIOR; FARINELLI, 2018). O constante crescimento tecnológico, o qual traz benefícios, traz também uma preocupação para as pessoas, no que concerne à privacidade.

Tais questões de segurança têm uma grande repercussão hoje, dado o poder da Internet, de maneira que o grande desafio, atualmente, é fazer uso das informações prezando pelos princípios da segurança, promovendo ambientes virtuais éticos e úteis, coesos com as demandas sociais.

Ainda de acordo com os estudos de plachkinova2019examination mesmo quando os sistemas de automação trazem consigo mensagens de ganho e perda, essas mensagens se configuram enquanto comunicação persuasiva.

Uma representação de casa inteligente expressa na Figura 1, traz uma ideia aproximada de como os objetos se interconectam e do funcionamento de cada um destes objetos, que por sua vez, são controlados e monitorados através do aparelho celular ou similar (tablet, notebook, etc.). Tal conexão e monitoramento incidem sobre a exposição do seu usuário em rede.

A praticidade, mediante o uso de IoT, tem ampliado a adesão destes sistemas. Afinal, desligar luzes, regar o jardim, abrir ou fechar cortinas, são tarefas que podem ser feitas à distância, necessitando apenas um comando de voz ou um toque na tela do dispositivo eletrônico conectado.

Figura 1 – Esquematização de Casa Inteligente

Fonte: Google

1.3 Justificativa

Segundo revisões da literatura sobre a área, não há trabalhos que forneçam recursos significativos para os cenários presentes neste âmbito. Assim, a maioria dos estudos analisados descreve o funcionamento e aplicabilidade dos sistemas identificando ameaças reais e defesas.

1.4 Objetivos

Esta seção apresentará o Objetivo Geral deste trabalho, bem como os Objetivos Específicos.

1.4.1 Objetivo Geral

Desenvolver uma ferramenta informativa capaz de conscientizar usuários de IoT e de outros dispositivos inteligentes, acerca da importância de identificar e prevenir ataques em rede.

1.4.2 Objetivos Específicos

- Fazer levantamento e análise dos trabalhos relacionados a ataques de engenharia social a redes IoT;
- Descrever os desafios da Segurança da Informação da Internet das Coisas, analisando as vulnerabilidades da Segurança em IoT, com ênfase em engenharia social;
- Analisar as ações de mitigação utilizadas por usuários de dispositivos de Internet das Coisas;
- Analisar o conhecimento dos usuários de dispositivos inteligentes acerca de segurança da informação e ataques de engenharia social;

- Desenvolver material no qual o usuário possa adquirir conhecimento capaz de estimular o uso de bons hábitos em rede.

1.5 Estrutura do Documento

Para efeito de clareza e coesão, o trabalho será dividido em capítulos e seções, nas quais:

- Capítulo 1 - Introdução: aborda as definições preliminares das literaturas pertinentes, a questão problematizadora, as argumentações e objetivos;
- Capítulo 2 - Fundamentação teórica: que consiste na revisão de literatura pertinente a estudos que envolvem Engenharia Social, IoT e Smarthomes;
- Capítulo 3 - Metodologia, materiais e métodos utilizados na elaboração da pesquisa;
- Capítulo 4 - Desafios da Segurança no contexto de Internet das Coisas;
- Capítulo 5 - O fator humano e suas vulnerabilidades;
- Capítulo 6 - Conscientização sobre a importância da Segurança da Informação;
- Capítulo 7 - Desenvolvimento.
- Capítulo 8 - Considerações Finais

2

Fundamentação Teórica

Neste capítulo será apresentada a fundamentação teórica, com a seguinte organização: 2.1 - Internet das Coisas- Conceitos e Aplicações; 2.2 - Segurança da Informação, Habilidades e Competências para o Século XXI; 2.3 - Smart Homes; e 2.4 - Engenharia Social; 2.5- Ataques de Engenharia Social; 2.6 Internet of Things e Segurança da Informação; 2.7 LGPD.

2.1 Internet das Coisas

Frente aos novos desafios enfrentados pelas sociedades da atualidade, a revolução tecnológica envolvendo uma diversidade de dispositivos interconectados, a IoT (internet of things), ou Internet das Coisas, tem trazido consigo importantes inovações e possibilidades relacionadas a negócios, pesquisas, e nichos mercadológicos em geral (LEMOS; MARQUES, 2018).

Volkmann (2022) conceitua a Internet das Coisas enquanto um paradigma que tem alcançado um lugar de destaque no cenário moderno das telecomunicações *Wireless*, cuja ideia consiste em interconectar uma gama de objetos, como sensores, tags RFID, *smartphones*, computadores, etc.

O conceito de Internet das Coisas está cada vez mais presente nas sociedades atuais. Os avanços tecnológicos neste sentido, possibilitam a oportunidade para desenvolvimento de novos negócios. O recente avanço das tecnologias de Internetworking tem proporcionado a conectividade não só entre humanos, mas também entre as coisas (ALEXANDROV; DESNITSKY; CHALY, 2019).

2.1.1 Segurança da Informação em IoT

Para Alexandrov, Desnitsky e Chaly (2019), diante dos novos cenários na nova era tecnológica, o maior obstáculo enfrentado pela humanidade tem sido a exposição do usuário em

rede e, consequentemente a vulnerabilidade. Neste ínterim, para que se crie um módulo protegido de sistema de informação e telecomunicações que implemente o conceito Internet das Coisas, faz-se relevante considerar vários aspectos.

Qusa et al. (2019) afirmam que as novas configurações sociais oriundas da revolução em IoT responsáveis por mudanças de hábitos que incluem a necessidade de se ter uma casa inteligente, automatizada, proativa e sustentável, embora nem sempre o usuário esteja atento ao fato de que o novo layout, no entanto, requer uma alta dependência da Internet, o que por sua vez, denota a vulnerabilidade perante a segurança da informação.

Loureço e Duarte (2020) enfatizam neste contexto, métodos e processos, evidenciando a relevância de boas práticas que possam auxiliar em um ambiente menos vulnerável no que tange à Segurança da Informação.

A IoT amplia dessa forma, a possibilidade de ataques à segurança da informação e, sobretudo, permite que estes sejam cada vez mais avançados e complexos através da combinação de vetores diversos. Essa nova configuração traz como obstáculo a exposição do usuário em rede e, consequentemente a vulnerabilidade. Para criar um módulo protegido de sistemas de informação e telecomunicações que implemente o conceito Internet das Coisas, é importante levar em consideração todos os seus aspectos (ALEXANDROV; DESNITSKY; CHALY, 2019).

Ribeiro et al. (2018), explicitam que, devido à interconexão de dispositivos presentes em IoT, na qual vários objetos se encontram conectados, caso um deles venha a ter sua segurança comprometida, afetará todo o conjunto de dispositivos conectados, prejudicando a segurança e a resiliência da internet, perdendo-se dados importantes.

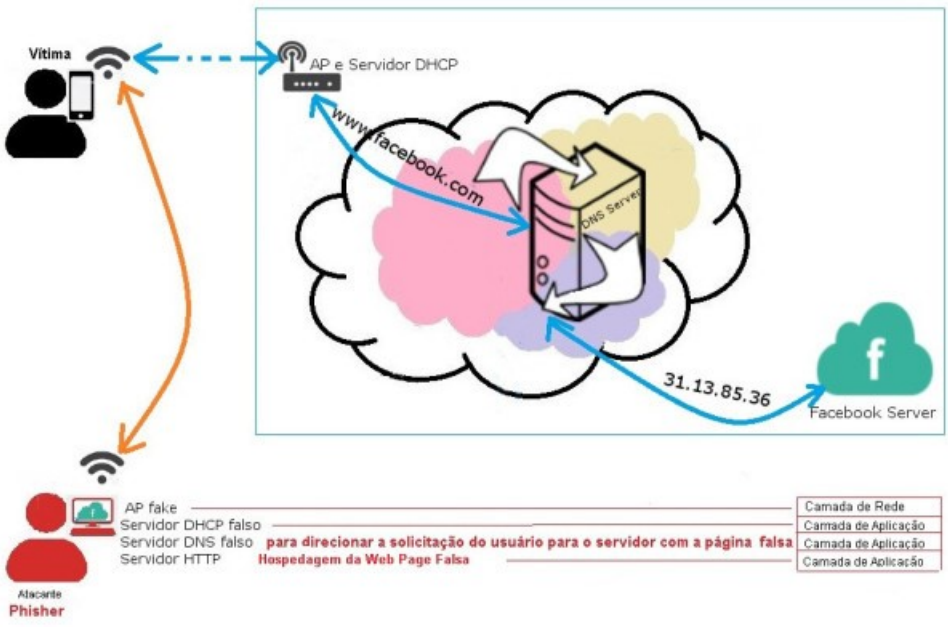
São vários os desafios induzidos pela complexidade e interoperabilidade de serviços e dispositivos massivamente interconectados, de modo que a comunicação, o ambiente de rede e as topologias se tornaram aspectos cada vez mais complexos, bem como se tornaram ainda mais complexos os problemas de segurança que envolvem a IoT (CAMPHOUSE; NGALAMOU, 2019).

Com relação às soluções de segurança que vêm sendo estudadas no contexto de IoT, surgem os dispositivos comportamentais. Neste sentido, cabe afirmar a proposta de processamento de métricas estatísticas geradas com o intuito de produzir os recursos apropriados para a construção de agrupamentos de dispositivos (SPANOS et al., 2019).

Notícias sobre invasões e ataques cibernéticos não são incomuns. Estas ações ocorrem a todo momento, deixando na maioria das vezes a vida particular de suas vítimas expostas.

A Figura 2, traz a simulação de uma rede falsa por meio da qual criminosos acessam informações das suas vítimas, utilizando-as em golpes cibenéticos. Uma rede aberta, seja em uma praça, aeroporto ou outro local público, se estiver sendo utilizada por um um invasor, poderá significar um dano grave.

Figura 2 – Simulação de rede falsa para roubar senhas



Fonte: Google, 2020

É válido considerar que grande parte dos “crimes” virtuais são resultados do modelo de vida adotado nos últimos anos, e que se torna agravante devido ao mau uso das aplicações que têm apenas o objetivo de tornar a vida do usuário mais rápida e facilitar a realização de atividades comuns no dia a dia (SPANOS et al., 2019).

Embora as tendências de mercado e o comportamento dos consumidores apontem um crescimento extraordinário para o uso de IoT, pouco se sabe sobre como as percepções de riscos de segurança influenciam nas decisões dos proprietários por adotarem dispositivos domésticos inteligentes (KLOBAS; MCGILL; WANG, 2019)

Costa, Barros e Tavares (2019) explicitam acerca de como permanecer seguro na camada de detecção comum de sistemas IoT baseados em nuvem, bem como ocultar informações biológicas, como impressões digitais, expressão facial e gestos corporais, que são reversíveis para manter a privacidade dos usuários.

A abordagem de (ARABO, 2015) foca na falha de avaliação de segurança de IoT, apontando que há uma preocupação em relação ao desenvolvimento de mecanismos de defesa de infraestruturas cooperativas e nacionais, quando na verdade a vulnerabilidade desses sistemas se encontra nos dispositivos usados em casas inteligentes conectadas.

Zhou et al. (2018) apresentam o conceito de recursos de IoT discutindo os efeitos de segurança e privacidade de oito destes, listando as ameaças, as soluções existentes para ameaças e os desafios de pesquisa ainda a serem resolvidos. Ressalta-se ainda que o trabalho de (ZHOU et al., 2018) ilustra a tendência no cenário pesquisado e revela como os recursos de IoT afetam a

pesquisa de segurança existente.

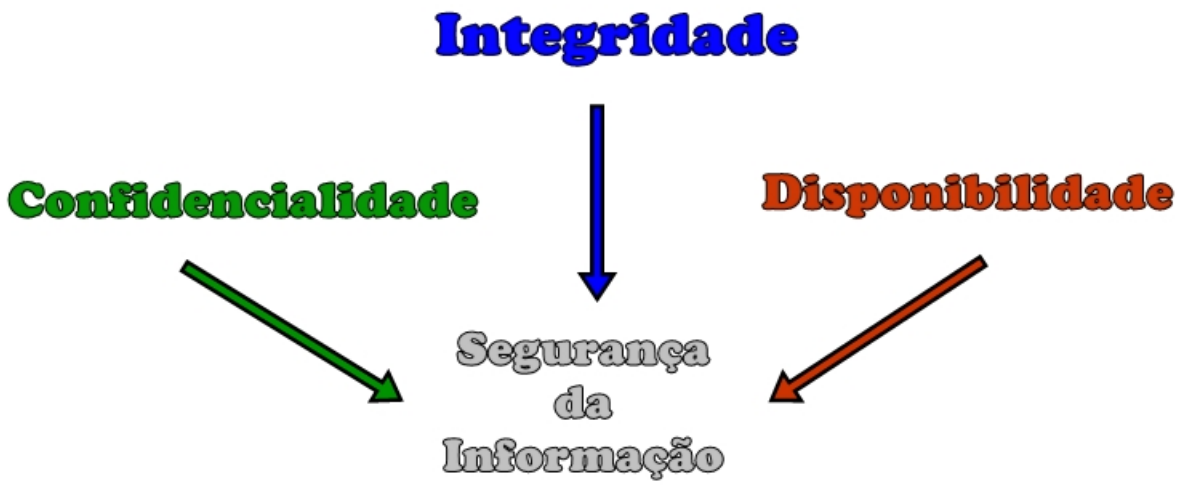
2.2 Segurança da Informação

De acordo com Lyra et al. (2008), o conceito de ameaça pode ser explicado enquanto um agente externo que se aproveita da vulnerabilidade, podendo quebrar um ou mais dos três princípios da segurança da informação. De acordo com (HAMDI et al., 2019), vulnerabilidade é uma característica inerente de qualquer elemento que necessite avaliação, pois praticamente todos os componentes do ambiente computacional possuem pontos vulneráveis.

Segundo Castilho (2012), a tecnologia sempre esteve associada à informação, embora nos últimos tempos estejamos vivendo uma nova era, a Era da Informação, pois esta nunca foi tão fácil e acessível. Este contexto, no entanto, traz uma controvérsia: lidar com informações requer princípios básicos ou pilares.

Alguns teóricos defendem três pilares essenciais: a integridade, a confidencialidade e a disponibilidade (SANTOS, 2019).

Figura 3 – Diagrama demonstrativo dos Principios da Segurança da Informação



Fonte: Autores, 2022

De acordo com a NBR ISO/IEC 2702 (ABNT, 2005):

- Confidencialidade: a confidencialidade, enquanto princípio da Segurança da Informação, diz respeito a um conjunto de ações desempenhadas para assegurar que informações restritas sejam resguardadas de ciberataques ou espionagem, entre outras práticas, que venham a expor de forma negativa a organização e seus colaboradores;

- Integridade: do ponto de vista da integridade, no que tange à Segurança da informação, este princípio impede que determinada informação fique exposta a manuseio por um usuário não autorizado, e que este venha a realizar operações as quais não foram aprovadas e não estão sob controle do administrador. Tal princípio prima pela informação sem ranhuras, onde dados sejam preservados na íntegra, mantendo-a clara, consistente, coesa e precisa enquanto processo ou durante o seu ciclo de vida. A integridade refere-se à garantia de que os dados circulem, cheguem ao seu destino e sejam armazenados mantendo a mesma estrutura do momento da sua criação, ou seja, que tais dados não sejam corrompidos, danificados ou comprometidos, seja por falha no dispositivo de armazenamento, ou outro fator coexistente;

- Disponibilidade: Ressalta-se ainda que as organizações devem assegurar aos seus dados e sistemas operacionais a disponibilidade. Este princípio imprime a capacidade de manter tais elementos acessíveis aos seus colaboradores, evitando assim a quebra da comunicação necessária ao bom funcionamento da organização.

Spanos et al. (2019) sugerem e desenvolvem dispositivos comportamentais tomando como referência um Cluster, (conjunto de computadores que operam em rede executando a mesma tarefa) no qual, durante um evento anormal, o dispositivo será movido para longe do centro do Cluster, consequentemente gerando um alerta que pode ser utilizado na formulação de ações mitigadoras.

Grammatikis, Sarigiannidis e Moscholios (2019) oferecem um modelo de avaliação de risco, por meio do qual se avalia qualitativa e quantitativamente cada ameaça possível por camada, além de examinar e identificar as contra-medidas apropriadas com atenção especial aos mecanismos de segurança e vulnerabilidades dos protocolos de comunicação.

Camphouse e Ngalamou (2019) indicam uma pesquisa recente na qual se chegou a dados reais que apontam as pessoas mais velhas e com maior escolaridade mais propensas em levar em consideração suas próprias avaliações de risco de segurança ao adotar dispositivos domésticos inteligentes.

De acordo com Mahaini, Li e Sağlam (2019), o tema segurança cibernética é altamente interdisciplinar e dinâmico, portanto, em constante evolução, de modo que não é incomum pesquisadores e profissionais da área buscarem construir e usar taxonomias e ontologias que melhor organizem o conhecimento em diferentes subtemas dentro da amplidão do assunto. Ainda (MAHAINI; LI; SAĞLAM, 2019), afirmam que taxonomias e ontologias abrangentes, neste sentido, são raras.

Yiğit et al. (2019) enfatizam a vulnerabilidade à qual smart homes estão expostas sinalizando o quanto esses objetos levam a violações e comprometimentos de segurança graves, dada a natureza interconectada e independente destes aparatos, além das capacidades restritas

em relação aos recursos computacionais, fatores que tornam impossível a aplicabilidade dos mecanismos convencionais de segurança.

Kettani e Cannistra (2018) desenvolvem um trabalho de conscientização com a finalidade de alertar a comunidade listando quinze ameaças cibernéticas usadas de maneira abrangente para aproveitar as vulnerabilidades e lançar operações cibernéticas usando vários ataques vetores. este trabalho enfatiza vetores de ataque específicos, técnicas de mitigação, cadeia de destruição e agentes de ameaça que abordam ambientes digitais inteligentes, incluindo IoT.

A pesquisa de Gunduz e Das (2020) tem foco nos tipos de ataques cibernéticos e fornece uma visão aprofundada do estado de segurança cibernética da rede inteligente. Apresenta também uma discussão acerca do exame das vulnerabilidades da rede, contra-medidas de ataque e requisitos de segurança com objetivo de fornecer uma compreensão profunda das vulnerabilidades e soluções de segurança cibernética, bem como um guia sobre futuras direções de pesquisa para segurança cibernética em aplicativos de rede inteligente.

Chang, Chang e Liao (2020) definem e classificam os fatores de risco críticos que influenciam a governança do controle interno da empresa em um ambiente de IoT e estuda sua importância em tal ambiente. O estudo usa o mapa de conhecimento Vee de Gowin como uma estratégia de pesquisa para mitigar as limitações da pesquisa qualitativa por meio de um conjunto de procedimentos rígidos de pesquisa.

O estudo de Mavropoulos et al. (2019) busca refinar a linguagem de modelagem do Apparatus Framework, propondo uma notação baseada em classes da linguagem de modelagem e uma abordagem estruturada para a transição entre diferentes modelos.

Apparatus é uma estrutura de segurança desenvolvida para facilitar a análise de segurança em sistemas IoT com este estudo de Mavropoulos et al. (2019) demonstra a aplicação da estrutura testando como modelo a segurança do sistema de transporte público inteligente. A análise de segurança e visualização do sistema são facilitadas por um aplicativo de software que foi desenvolvido como parte do aparato Framework.

A abordagem de Jinhong, Chul-Soo e ONIK (2019) propõe um fator de risco de Personally Identifiably Information (PII), trazendo modelagem de risco agregada a informações pessoais no ambiente IoT. A abordagem mostra que, intuitivamente, a maioria dos dispositivos IoT é produzida por fabricantes idênticos. (JINHONG; CHUL-SOO; ONIK, 2019), afirmam ainda que os dispositivos inteligentes normalmente reúnem fatos a partir de muitos dispositivos em que os proprietários das informações coletadams são mutuamente inclusivos.

Lee (2020) estende as teorias existentes de privacidade e vulnerabilidade para demonstrar a importância da privacidade física e proteções de vulnerabilidade do usuário em ambientes domésticos de IoT. Em Lee (2020), para validar seu modelo de pesquisa, foi realizada uma análise empírica em 265 amostras com uma técnica de modelagem de equações estruturais de mínimos quadrados parciais. As diferenças nos fatores de vulnerabilidade, junto com questões de

privacidade e resistência aos serviços domésticos de IoT, também foram comparadas por gênero, experiência e tipo de moradia.

A aplicação da segurança em ambientes de Internet das Coisas foi identificada no trabalho de Jacobsson, Boldt e Carlsson (2016) como uma das principais barreiras para concretizar a visão de inteligência, em casas e edifícios com eficiência energética. A abordagem de Jacobsson, Boldt e Carlsson (2016) parte de uma análise de risco aplicada em um sistema de automação residencial inteligente desenvolvido em um projeto de pesquisa envolvendo os principais atores industriais.

O estudo de Jacobsson, Boldt e Carlsson (2016) traz ainda uma análise de risco aponta para o necessidade de um modelo mais geral de segurança e privacidade incluído na fase de projeto de casas inteligentes, que deverá contribuir para reforçar a segurança do sistema e aumentar a privacidade do usuário em casas inteligentes, ajudando assim a perceber ainda mais o potencial em tais ambientes.

O estudo de Andrade e Yoo (2019) apresenta um modelo de segurança cognitiva que integra soluções tecnológicas como Big Data, Aprendizado de Máquina e Sistemas de Apoio à Decisão com os processos cognitivos de analistas de segurança usados para gerar conhecimento, compreensão e execução de ações de resposta de segurança. O modelo considera alternativas para estabelecer o processo de automação na execução de tarefas cognitivas definidas nos processos de operações cibernéticas.

2.3 Smart Homes

Spanos et al. (2019) apresentam um estudo acerca de smarthomes baseado na modelagem, onde agentes dentro da casa inteligente fazem observações e implementam o comportamento pretendido. Este modelo requer um engajamento mínimo do usuário e está focado na detecção de ameaças.

Rafferty et al. (2018) apresentam um estudo acerca de smart homes baseado na modelagem, no qual, agentes dentro da casa inteligente fazem observações e implementam o comportamento pretendido. Este modelo requer um engajamento mínimo do usuário e está focado na detecção de ameaças.

Para Spanos et al. (2019), a abordagem proposta por Rafferty et al. (2018), negligencia a detecção de dispositivos vulneráveis dentro da casa inteligente, além de inibir o processo de atuação, ou seja, o processo de decisão de quais ações realizar para atingir um objetivo.

Spanos et al. (2019) apresentam uma contrapatida mais intrusiva ao tema usuários de Smarthomes no contexto de segurança de rede, apontando a pesquisa desenvolvida por Habibi et al. (2017), a qual propõe uma técnica de detecção de intrusão baseada em whitelist específica para dispositivos IoT devices.

Um protótipo de casa inteligente é apresentado por Qusa et al. (2019), cuja abordagem traz a garantia de que o modelo promove a segurança física e cibernética dos sistemas da casa inteligente projetada. Neste protótipo, apoia-se o design de sistema aberto, onde o proprietário consegue selecionar vários fornecedores para implantar serviços e funções inteligentes em casa, garantindo segurança com o uso dos sistemas de monitoramento de incidentes e eventos do sistema.

2.4 Engenharia Social

Mitnick e Simon (2003), referem-se a Engenharia Social como sendo o uso da manipulação, engano e influência sobre um indivíduo pertencente a uma organização, para que este adira a um determinado pedido. Esse pedido poderá consistir na divulgação de determinada informação ou o desempenho de determinada tarefa que beneficia o atacante. Poderá ser tão simples quanto falar ao telefone, até algo tão complexo como fazer com que o alvo visite um determinado website que explore uma falha técnica e permita ao hacker tomar conta do computador.

A cada dia, a prática de engenharia social vem se ampliando, dado o uso massivo de dados. Magrani (2018), afirma que, para que se transforme um objeto analógico em objeto inteligente, se imprime ao mesmo, falhas inexistentes a priori, ao tempo em que gera-se riscos em relação à segurança e à privacidade, já que se trata de um extenso volume de dados (big data) processados, na escala de bilhões, possibilitando conhecer cada vez mais os indivíduos em seus hábitos, preferências, desejos e tentando, assim, adivinhar suas escolhas.

Comumente o invasor é um tipo de pessoa agradável, educada, simpática e carismática. Acima de tudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente (PEIXOTO, 2004). Até mesmo pessoas sem conhecimento antecipado desta denominação já cometeram algum ato de engenharia social involuntariamente.

Hadnagy (2010), aborda que a Engenharia Social, no contexto da segurança no uso de Tecnologias de Informação e Comunicação (TIC), refere-se às ações praticadas para obter e quebrar o valor da informação. Também para obter dados importantes e sigiloso de organizações e/ou sistemas computacionais, por meio da exploração da confiança das pessoas.

Coelho, Rasma e Morales (2013) conceituam Engenharia Social enquanto um conjunto de técnicas e artes dirigidas à manipulação das pessoas com a finalidade de conseguir que estas realizem atos que normalmente não fariam, em grande escala, ou divulguem voluntariamente informações pessoais ou da empresa na qual prestam serviço. Neste contexto, a IoT expõe seus usuários a esses ataques, uma vez que estabelece a necessidade de fornecimento de dados como e-mail, telefone e outros, oporunizando aos invasores induzir usuários a forneserem senhas por meio de confiança estabelecida.

Coelho, Rasma e Morales (2013) afirmam que, para minimizar as perdas referentes aos

ataques da engenharia social, em uma empresa, por exemplo, torna-se crucial programar políticas de segurança nas organizações e sua ampla divulgação, bem como promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social.

Segundo Eiras (2004), a Engenharia Social tem como objetivo enganar as pessoas fazendo com que elas forneçam informações pessoais, como senhas, dados bancários, podendo também engenheiros sociais segurarem o acesso para chantagear suas vítimas, ou ainda permitir acesso aos seus computadores para secretamente instalar um *software* malicioso.

Para Aramuni e Maia (2020) trata-se do estudo de técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma pessoa ou organização, através da própria pessoa, ou de funcionários e colaboradores de uma corporação ou de uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança.

Aramuni e Maia (2020), afirma ser necessário também, executar a implementação e monitoramento dos mecanismos de segurança e não manusear informações corporativas fora da empresa ou tampouco fornecer informações pessoais ou secretas. Neste sentido, buscar cuidados especiais com o relação ao lixo eletrônico, assim como em qualquer outro meio, através de regras claras de descarte.

De acordo com Souza e Fernandes (2016), estão cada vez mais avançados e complexos os ataques à segurança da informação que, por sua vez, se dão através de dados obtidos na Internet de modo que a engenharia social tem se tonado uma preocupação cada dia mais forte. Tais ataques persistentes e avançados, combinam diversos vetores na busca para o alcance dos seus objetivos.

Silva, Araújo e Azevedo (2013), afirmam ser a conscientização dos usuários e a execução de uma política de gestão de segurança da informação, elementos essenciais para as empresas. No que concerne ao pessoal, estratégias adequadas devem ser pensadas pelo indivíduo comum no uso de redes sociais online, a fim de evitar ataques de engenheiros sociais e suas consequências morais ou financeiras.

O estudo de heartfield, analisa uma defesa mais significativa contra ataques de engenharia social, diferentemente de outros trabalhos, tal proposta aponta que a responsabilidade pela segurança não pode ser colocada exclusivamente sobre os ombros dos desenvolvedores de sistema ou das organizações provedoras.

Lallie et al. (2021), analisa a pandemia COVID-19 sob o prisma do crime cibernético e destaca a variedade de vividos globalmente durante a pandemia. No referido estudo, ataques cibernéticos são analisados e considerados dentro do contexto dos principais eventos globais para revelar o modus operandi das campanhas. Os autores ainda apontam que os ciber criminosos aproveitaram eventos importantes e anúncios governamentais para criar e projetar campanhas de crimes cibernéticos com cuidado.

Waraga et al. (2020) conduz uma análise abrangente de estudos anteriores acerca de segurança de dispositivos IoT, com foco nas várias ferramentas usadas para testar tais dispositivos e as vulnerabilidades encontradas. O documento contém uma pesquisa na literatura de testes de segurança baseados em IoT, além de apresentar uma plataforma de código aberto para identificar pontos fracos em redes e comunicações neste âmbito. Essas análises permitem verificar do nível do impacto de ataques de engenharia social em redes IoT, bem como identificar técnicas utilizadas em ataques de engenharia social e técnicas de defesa.

2.5 Ataques de Engenharia Social

A seguir são apresentados alguns exemplos de ataques reais de Engenahria Social:

- *Shark Tank* (DANTAS, 2022):

  O Golpe Shark Tank Trata-se de um phising que gerou um prejuízo de aproximadamente USD 400.000, cuja vítima foi Barbara Corcoran, juíza do programa *Shark Tank*.

  Na ocasião, um cibercriminoso se passou por uma assistente da vítima, enviando um e-mail para o contador, no qual solicitava o pagamento de uma renovação relacionada a investimentos em imóveis.

  Para consolidar o golpe, o criminoso usou um e-mail similar ao endereço legítimo.

- Toyota (PASCHOAL; PEREIRA, 2019):

  No Japão, a Toyota Boshoku Corporation perdeu cerca de USD 37 milhões em um ataque de engenharia social . Neste, usando de persuasão, os invasores convenceram um executivo do departamento financeiro a alterar as informações da conta bancária e assim efetuar uma transferência eletrônica de fundos.

- Condado de Cabarrus (JÚNIOR, 2018):

  O Condado de Cabarrus, nos Estados Unidos, foi acometido por ataque de engenharia social cujo prejuízo culminou em USD 1,7 milhão. Hackers utilizaram e-mails maliciosos e se passaram por fornecedores do condado, solicitando que os pagamentos fossem feitos em uma nova conta bancária. Segundo consta em registros investigativos, nos e-mails, os golpistas apresentaram documentação aparentemente legítima.

- Ethereum Ethereum:

  O site da Ethereum Classic foi hackeado, em 2017. De maneira que várias pessoas ao mesmo tempo perderam milhares de dólares em criptomoedas. Usando de engenharia social, os hackers se passaram pelo proprietário da Classic Ether Wallet e, acessando o registro de domínio, o redirecionaram para um servidor próprio, roubando as criptomoedas Ethereum das vítimas através de um código adicionado ao site que permitia a visualização de chaves privadas.

- Partido Democrata (HONÓRIO, 2018):

  A eleição presidencial dos Estados Unidos, em 2016, tornou-se caso emblemático de engenharia social. Através de spear phishing, hackers criaram um e-mail falso no Gmail, do qual enviavam links convidando usuários a alterarem senhas. Desta prática, ocorreu o vazamento de e-mails e informações confidenciais do Partido Democrata, fato que, de acordo com especialistas, pode ter influenciado o resultado da eleição, dando a vitória a Donald Trump sobre Hillary Clinton.

- Ubiquiti Networks (PINZÓN et al., 2015):

  Em Hong Kong (China), a empresa Ubiquiti Networks sofreu um prejuízo de aproximadamente USD 40 milhões através de ataque de phishing, quando a conta de e-mail de um funcionário de alto escalão foi invadida fazendo com que os invasores solicitassem do departamento contábil da empresa pagamentos fraudulentos .

2.6 Técnicas de Defesas

Com o crescente número de ataques cibernéticos cresceu também o interesse de pesquisadores e empresas na busca por ferramentas capazes de desviar tais ataques ou, pelo menos, reduzir ou controlar tais problemas. Neste sentido, foram desenvolvidos diversos meios de proteção que permitam proteger a infraestrutura IoT. A seguir, apresenta-se uma lista das principais ferramentas de defesa.

- Firewall, o *Firewall* (na língua portuguesa, Parede de Fogo) é apenas uma camada da segurança, portanto é importante utilizá-lo adicionado a outra solução, conforme a necessidade do que deve ser protegido. O Firewall consiste no bloqueio de tráfego de dados indesejados e na liberação de acesso com base nas políticas de segurança, com base em hardware ou software, funciona a partir da análise do tráfego de rede, determinando a execução de transmissão sob regras pré-definidas (SOUZA, 2018).

- Sistema de Detecção de Intrusos (IDS), Trata-se de uma ferramenta extremamente importante, em um sistema de segurança, uma vez que é responsável por monitorar uma rede ou um componente de rede a fim de detectar comportamentos maliciosos. O IDS, se apresenta em dois modelos distintos, o sistema passivo, que detecta a anomalia, registra e envia um alerta ao administrador do sistema; e o sistema reativo, no qual o IDS bloqueia a ameaça tão logo ela seja visualizada (PINHEIRO, 2018).

- Antivírus, Trata-se de um programa que detecta, evita e atua na neutralização ou remoção de outros programas mal-intencionados, como vírus e worms. É um sistema de segurança ativo capaz de fornecer segurança em todas as camadas do sistema. Atua por meio de políticas e regras de tráfego de rede que permitem emitir alertas em caso de tráfego suspeito.

Também permite ao administrador, executar ações com base no alerta recebido (MOURA; NEVES, 2021).

- Rede Virtual Privada (VPN), A VPN se conceitua enquanto uma conexão para o acesso privado de dados por meio de uma rede pública pré - existente, cujo processo se faz de modo que a comunicação entre dois pontos ocorra através de um túnel capaz de ocultar os dados para elementos não autorizados (LIMA et al., 2013).

2.7 LGPD

A cada dia, em decorrência da Globalização e do uso crescente da Internet, amplia-se a busca por soluções no que concerne a segurança de dados pessoais. Tal demanda, ocasionou a criação da Lei nº 13.709, a Lei Geral de Proteção dos Dados Pessoais (LGPD) ou Marco Civil da Internet (BRASIL, 2018) enquanto medida preventiva e proativa frente a manutenção e proteção de dados (PINHEIRO, 2020).

Belli (2021), aponta o art. 9º do Marco Civil da Internet pelo capítulo II do Decreto no 8.771/2016, e novos desdobramentos estimulados pela IoT, no qual ressalta a importância de se desenvolver estratégias de segurança. Frente a essa perspectiva, ilustra a reflexão do que ocorreria se uma empresa desenvolvesse carros conectados e sinais conectados e decidisse priorizar o trânsito de dados emitidos e recebidos pelos próprios carros. Estratégias de cibersegurança podem garantir que o desenvolvimento da IoT não torne os usuários de objetos conectados vulneráveis aos ataques cibernéticos que, sem dúvida, são destinados a se multiplicar exponencialmente no setor.

Neste sentido, ampliou-se também as discussões acerca da temática, de modo que algumas literaturas relevantes se destacam no novo cenário. Visando mapear políticas de proteção dos dados pessoais nos programas de nota fiscal, Machado, Bioni et al. (2016) descreve uma pesquisa de campo em 12 Estados da Federação que resultou em um projeto intitulado Programa Nota Fiscal.

Moraes e Prado (2018), versam acerca do uso de dados individuais e opacidade sobre o faturamento dos gastos públicos em relação a tecnologia, segurança e privacidade e acesso aos dados o que impacta linearmente ao tema desse trabalho.

3
Metodologia

Este Capítulo, apresenta os materiais e os métodos utilizados na elaboração desta pesquisa.

3.1 Métodos

Para definir o tipo de pesquisa adotado neste trabalho, ressalta-se que se trata- de uma pesquisa básica e ao mesmo tempo aplicada. De acordo com Gil (2008), a pesquisa básica "busca gerar conhecimentos novos capazes de contribuir para avanços na ciência, embora sem aplicação prática. No trabalho ora desenvolvido, adotou-se a pesquisa básica para delimitação dos temas de estudos, tais como Segurança da Informação e Engenharia Social pontuados no escopo. Tais estudos buscam mitigar ataques cibernéticos por meio da conscientização dos usuários.

No que concerne à pesquisa aplicada, esta foi adotada no levantamento de dados sobre o nível de conhecimento dos usuários em IoT, que culminou no desenvolvimento de um portal enquanto ferramenta de apoio na aprendizagem de bons hábitos em rede. Ressalta-se que uma pesquisa aplicada busca gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos (SILVEIRA; CÓRDOVA, 2009). Esta abordagem define a natureza desta pesquisa, segundo Gil (2008), Boaventura (2004), é aquela na qual se busca pôr em prática os conhecimentos para a solução de problemas sociais. Gil (2008), afirma ainda que as pesquisas com esse tipo de natureza estão voltadas mais para a aplicação imediata de tais conhecimentos.

Quanto aos objetivos específicos e procedimentos, afirma-se esta, possuir caráter de pesquisa exploratória, uma vez que através de levantamentos bibliográficos, aplicação de questionários e análise de exemplos, buscou-se uma ampla familiaridade com o problema.

Como toda pesquisa científica deve possuir embasamento bibliográfico, utilizou-se o mapeamento sistemático para definir as temáticas e subsidiar a seleção, a revisão e a sintetização dos trabalhos que, de acordo com a relevância, embasaram a pesquisa. Para tanto, foram consultadas publicações entre os anos 2012-2020.

Petersen et al. (2008) ainda na fase de planejamento da pesquisa, o mapeamento sistemático consistiu em descrever os desafios da Segurança da Informação da Internet das Coisas em automação residencial, analisando as vulnerabilidades da Segurança em internet das coisas, além de estudar mecanismos de proteção demonstrando sua eficiência em infra estruturas que utilizam essa tecnologia, tal procedimento fomentou o caráter descritivo e exploratório da pesquisa.

Os capítulos 4, 5 e 6 apresentam respectivamente os resultados de Mapeamento Sistemático, Revisão Sistemática e Literatura Cinzenta ou *Snowball* . Na fase de Mapeamento Sistemático o desenvolvimento da pesquisa consistiu em descrever os desafios da Segurança no Contexto de Internet das Coisas através de uma discussão pontual no que diz respeito a dispositivos domésticos inteligentes e Internet das Coisas com ênfase em mecanismos de proteção através de demonstrativos de eficiência das infraestruturas que utilizam essa tecnologia. Já a Revisão Sistemática foi desenvolvida a partir de revisão de literatura e fez-se enquanto levantamento de episódios de falhas de segurança.

Nesta fase da pesquisa, os elementos pesquisados apontaram que a cada dia, cresce a preocupação com privacidade e a segurança da informação, o que torna a temática, uma questão de alto interesse social. Enfatiza-se que a Revisão Sistemática seguiu um protocolo detalhado proposto por Kitchenham (2004) e foi dividida em três etapas: execução da busca, primeira etapa de seleção e segunda etapa de seleção. Uma Revisão Sistemática da literatura de acordo com Kitchenham (2004) é o estudo que trata de identificar, avaliar e interpretar toda a pesquisa disponível e relevante para determinado tema ou questão de pesquisa específica.

Para elucidar a Segurança da Informação, no âmbito do comportamento de usuários de IoT e Engenharia Social, utilizou-se a metodologia Bola de Neve ou *Snowball*, que consiste em um tipo de amostra não probabilística, cujos resultados advêm de algum critério de inclusão preestabelecido e não atinge à toda população no que diz respeito a participação na amostragem como apontam (BICKMAN; ROG, 2008). Justifica-se esta estratégia de pesquisa dado o fato da insuficiência de resultados na fase de Mapeamento Sistemático na pesquisa empreendida, já que, o objetivo desta Revisão de Literatura é conscientizar os usuários em rede e explicitar sobre Engenharia Social.

Para desenvolvimento desse levantamento bibliográfico, utilizou-se as seguintes bases de dados SpringerLink, ACM Digital Library, IEEE Digital Library, ISI Web Of Science, Science Direct e Scopus. Os termos de busca utilizados foram: Internet Of Things, Iot, Information security, Engerning Social, smart homes.

Ressalta-se ainda, que, para uma visão mais ampla acerca da temática analisada, buscou-se a Literatura Cinzenta. De acordo com Gama (2022), quando um tema é ainda um campo de pesquisa pouco amplo, tornando as contribuições científicas pouco encontradas em materiais acadêmicos, faz-se necessário analisar textos e artefatos úteis através de um tipo de material chamado Grey Literature (GL). Isso inclui, relatórios técnicos, artigos, revistas, blogs e outros

recursos que são desenvolvidos e mantidos por práticos da área (WEN et al., 2020).

3.2 Materiais

O levantamento de dados utilizado para este estudo resultou da aplicação de três questionários online, com perguntas fechadas e abertas, por meio das quais se aferiu como este público- alvo se comporta em rede bem como o nível de conhecimento acerca de segurança em IoT.

Por meio desse raio-x, desenvolveu-se um curso com 5 módulos que está disponivel no site : <https://cis.blog.br/>.

O site foi criado utilizando o WordPress 6.0, que é um *Content Management System* (CMS), Sistema de Gerenciamento de Conteúdo. No site temos um blog que por padrão já vem no próprio WordPress. Todo o conteúdo está hospedado em um servidor da HostGator, o mesmo oferece suporte ssl gratuito para o site na plataforma.

Utilizou-se também o plugin elementos Pro para criação das telas e elementos do site, esse plugin é responsável pela renderização e customização de cada página. O servidor da HostGator além de dar ssl gratuito, ele conta com até 3 contas de e-mail gratuitas para serem usadas em nosso site. Usamos a versão mais recente do PHP 7.4 , que além de que utilizar o MySQL[1] para banco de dados, seu servidor possui uma bande de 4GB de processamento.

[1] O MySQL é um sistema gerenciador de banco de dados relacional de código aberto usado na maioria das aplicações gratuitas para gerir suas bases de dados.

4

Desafios da Segurança no Contexto de Internet das Coisas

O crescente uso de dispositivos IoT capazes de tornar a vida cotidiana mais confortável e conveniente, levanta preocupações com relação à segurança e privacidade. Esta nova configuração traz como obstáculo a exposição do usuário em rede, de modo que se faz pertinente discutir e analisar aspectos que vão desde a percepção de riscos, até o comportamento dos usuários.

Frente a tal configuração, cabe uma discussão pontual no que diz respeito a dispositivos domésticos inteligentes e Internet das Coisas com ênfase em conhecer mecanismos de proteção através de demonstrativos de eficiência das infraestruturas que utilizam essa tecnologia. As abordagens ora apresentadas neste capitulo buscam descrever os desafios da Segurança da Informação da Internet das Coisas em automação residencial, frente a uma análise de vulnerabilidade da Segurança em Internet das coisas, de maneira que se possa conhecer mecanismos de proteção através de demonstrativos de eficiência das infraestruturas que utilizam essa tecnologia.

4.0.1 Questões de pesquisa

Este capítulo responderá a seguinte Questão de Pesquisa Primária (QPP): Quais principais ameaças à Segurança da Informação em IoT em automação residencial?. Para a obtenção da resposta a esta questão, foram incluídas Questões de Pesquisa Secundárias (QPS). Ao se concluir a pesquisa procurou-se responder a maioria das questões norteadoras (primária e secundárias) bem como obter os dados propostos para esse mapeamento.

A seguir as questões de pesquisa:

1. São mencionadas ameaças à segurança da informação?
2. Qual o tipo de veículo de publicação da pesquisa?
3. Quais técnicas podem ser adotadas para reduzir riscos no contexto de Internet das Coisas?
4. Quais técnicas são mais eficazes?

5. Qual o ano de publicação do estudo?

4.0.2 Estratégia de busca

A pesquisa foi conduzida mediante bases internacionais sendo ACM Digital Library, IEEE Xplore Digital Library, Science@Direct, Scopus, e ISI Web of Science, totalizando 5 bases.

Foram utilizadas as seguintes bases de pesquisa:

- IEEE Xplore Digital Library <<http://ieeexplore.ieee.org>>;
- ISI Web of Science <<https://www.webofknowledge.com/>>;
- Science Direct <<http://www.sciencedirect.com>>;
- ACM Digital Library <<http://portal.acm.org>>;

Na Tabela 1 são apresentadas as Palavras-Chave utilizadas utilizadas para formar a *string* de busca.

Tabela 1 – Palavras-Chave utilizadas

Palavra-chave	**Sinônimo em Inglês**
Internet das Coisas,	IoT, Internet of Things
Segurança da Informação	Information security,
Automação Residencial	Smart Homes

Fonte: Autores, 2020

Na Tabela 2 é apresentada a *string* utilizada para as buscas nas bases:

Tabela 2 – *String* utilizada para realizar as buscas nas bases

((“internet das coisas*”) OR “internet of things” OR “iot"AND (“segurança da informação” OR “information security”) AND (“automação residencial”OR "Smart Homes"))

Fonte: Autores, 2020

Para filtrar os artigos relevantes foram estabelecidos Critérios de Inclusão (CI) e Exclusão (CE) indicados abaixo. Assim foram selecionados a partir somente da leitura do título e resumo de cada artigo resultando em 25 artigos oriundos de 482 artigos encontrados pela string. Após esta etapa vem o filtro por meio da leitura completa dos artigos resultantes da primeira seleção, analisando-os a partir de Questões de Qualidade.

A seguir os Critérios de Inclusão:

1. Acessível via web de maneira gratuita;

2. Artigos apenas com idioma inglês e português;
3. Somente estudos primários.

A seguir os Critérios de Exclusão:

1. Estudos Duplicados;
2. Falta de disponibilidade para download de maneira gratuita;
3. Trabalhos publicados como resumos ou resumo expandido ou prefácio de periódicos e eventos;
4. Trabalhos que não contemplam a temática.

O critério de inclusão e exclusão enquanto ferramenta de busca, possibilitou o acesso a estudos de diferentes regiões que apresentam os desafios da segurança da informação no contexto de Internet das Coisas em automação residencial. Inclui-se neste interim, pesquisas empreendidas através da publicação de artigos em conferências ou periódicos; selecionados mediante tal critério, apenas artigos em inglês e português. Também foram utilizados somente estudos publicados a partir de 2017.

No que concerne à exclusão, não houve ênfase em relação a estudos duplicados, estudos secundários e trabalhos publicados como resumos ou resumo expandido ou prefácio de periódicos e eventos. Também foram excluídas informações incompletas ou aquelas sem disponibilidade para download.

4.1 Respostas

Nas próximas subseções serão analisados os resultados das 4 Questões de Pesquisa Secundárias com o intuito de responder à Questão de Pesquisa Primária, serão apresentados os dados encontrados nos artigos e feita uma breve análise do mesmos. [1]

4.1.1 QPS 1 - São mencionadas ameaças à Segurança da Informação?

Foram apresentados 3 estudos com ameaças e 22 sem ameaças a Segurança da Informação.

O estudo de Alexandrov, Desnitsky e Chaly (2019) insere o conceito de Internet das Coisas enquanto abordagem cada vez mais presente na atualidade e trata os avanços tecnológicos como a oportunidade para desenvolvimento de novos negócios apontando que o avanço em internetworking tem proporcionado a conectividade não só entre humanos, mas também entre

[1] https://docs.google.com/spreadsheets/d/19n8CguFCYh7HCPSr5gsdAIRvv9ncxr_1B1-qU65vJVw/edit?usp=sharing

as coisas, de modo que esta nova configuração traz, como obstáculo, a exposição do usuário em rede e, consequentemente, a vulnerabilidade. Fica explícito que para determinar ameaças relevantes, é necessário usar a análise de risco detalhada de acordo com padrões preexistentes.

Dong et al. (2018) faz uma relevante abordagem acerca do crescente o uso de IoT (Internet of Things), e, afirma serem estes dispositivos domésticos inteligentes capazes de tornar a vida cotidiana mais confortável e conveniente, embora levantem preocupações com relação à segurança e privacidade além da baixa capacidade técnica.

No estudo de Costa, Barros e Tavares (2019) apresenta-se um método desenvolvido com o objetivo de identificar vulnerabilidades de alto risco em dispositivos IoT domésticos inteligentes. Além disso, também apresenta alguns tópicos relacionados às principais ameaças e vulnerabilidades que afetam os dispositivos IoT domésticos inteligentes.

Tabela 3 – Ameaças à Seguranca Da Informação

Ameaças à Segurança da Informação	**Quantidade de Estudos**
Sim	3
Não	22

Fonte: Autores, 2020

4.1.2 QPS 2- Qual o tipo de veículo de publicação da pesquisa?

A maior parte dos estudos aceitos para análise de dados origina-se de uma variação de três tipos de publicação, a saber: Conferência (6), Periódico (5), e, Workshop (1), destacando-se uma maior quantidade de estudos em Conferências, o principal veículo de publicação.

Para cada estudo selecionado, mediante a execução do processo de avaliação da qualidade dos estudos primários, foram extraídos os objetivos do artigo, a data de publicação, os tipos de soluções e as sugestões para trabalhos futuros. Os resultados foram analisados, organizados, agrupados e comparados.

Tabela 4 – Veículo de Publicações

Veículo de Publicações	**Quantidade de Estudos**
Conferência	6
Periódico	5
Workshop	1
Forúm	1

Fonte: Autores, 2020

4.1.3 QPS 3- Quais técnicas podem ser adotadas para reduzir riscos no contexto de Internet das Coisas?

Frente a abordagem de Qusa et al. (2019), deve haver uma sincronização entre a utilização de sistemas abertos de inteligência de segurança e o uso de algum controle de segurança cibernética no servidor. Este funciona como sistema de prevenção e detecção de intrusões (IDP / IPS); Qusa et al. (2019) faz alusão ao firewall de monitoramento do tráfego da rede, enquanto medida eficaz, junto a técnicas de criptografia. Considera-se que o papel da técnica criptográfica é o de tornar os dados ilegíveis sempre que não houve autenticação ou autorização para navegar através destes.

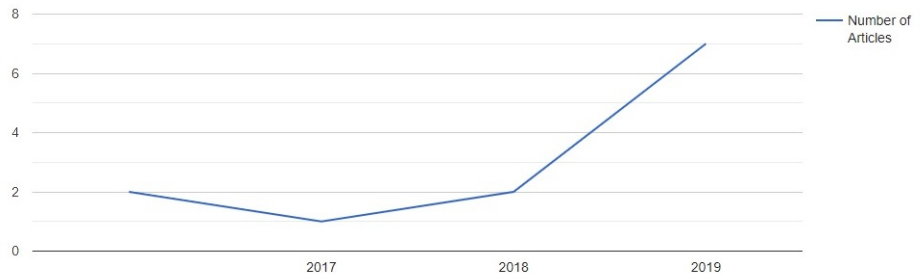
4.1.4 QPS 4- Quais técnicas mais eficazes?

Plachkinova e Menard (2019) faz uma breve análise acerca da metodologia de avaliação crítica de ameaças, ativos e vulnerabilidades (OCTAVE), e afirma que a operacionalidade crítica é o ponto chave para a segurança em IoT, para tanto, a conscientização do usuário torna-se elemento indispensável. A referida pesquisa recomenda programas de autenticação multifatorial, associados ao treinamento de redução de riscos.

4.1.5 QPS 5-Em qual ano foi publicado?

Foram encontrados estudos relevantes para este trabalho a partir do ano 2000 até o ano de 2020, havendo destaque para os anos mais recentes com uma crescente de artigos a partir do ano de 2015 com 8 artigos, chegando a 15 em 2020, apenas com uma queda no ano de 2018 com 6 artigos. Como pode ser apresentado no gráfico da Figura 4.

Figura 4 – Ano de Publicação



Fonte: Autores, 2020

4.2 Considerações do Capítulo

Os resultados encontrados nas pesquisas selecionadas para o presente trabalho, permitem responder as questões norteadoras que embasaram o mapeamento sistemático, o que vem a validar os caminhos percorridos na coleta de dados.

No contexto de Segurança da Informação, ao analisar a expansão que a IoT tem ganhado nas últimas décadas, leva-se em consideração que se faz pertinente um foco de discussão maior, no que tange às questões de segurança. A maioria dos estudos analisados apenas descrevem o funcionamento e a aplicabilidade dos sistemas identificado ameaças reais e recomendando para o combate às mesmas. Faz-se necessário neste item, parafrasear ações inibidoras das ameaças.

Ainda é desafiador repensar maneiras de permanecer seguro na camada de detecção comum de sistemas IoT baseados em nuvem com ênfase na ocultação de informações biológicas como impressões digitais, expressão facial e gestos corporais, que são reversíveis no que concerne à privacidade dos usuários.

O constante crescimento do mercado da IoT, necessita por parte dos seus pesquisadores, uma conjuntura que permita, influencie e oriente os consumidores a buscarem o conhecimento e as habilidades necessárias para o uso seguro destes dispositivos. Estudos apontam vieses para os profissionais de segurança da informação alcançarem tais resultados.

Um estudo promissor neste âmbito, parte do pressuposto de modelos calculados através da combinação de técnicas estatísticas e de aprendizado de máquina de acordo com o comportamento da rede, nestes termos, as métricas estatísticas geradas vão sendo processadas para produzir os recursos apropriados que são usados na construção de agrupamentos de dispositivo

Frente a elaboração deste mapeamento concluiu-se que há dificuldades significativas no que diz respeito a se permanecer seguro em automação residencial, portanto é evidente que a sua implantação é inevitável como também a procura do usuário por tecnologias e conhecimento quanto as técnicas de segurança.

Dessa forma foi definido como trabalho futuro, investigar as lacunas identificadas neste estudo de mapeamento e levantar dados que permitissem desenvolver métodos capazes de tornar os usuários de tecnologias de Internet das Coisas mais aptos a procura por técnicas de segurança.

5

O fator humano e suas vulnerabilidades

Na atualidade, dado o fácil acesso à informação, notifica-se, ameaças e ataques cibernéticos em casas inteligentes, enquanto problema recorrente. Para determinar a relevância dessas ameaças, utiliza-se uma análise detalhada de risco de acordo com padrões preexistentes. No entanto, ao adotar medidas preventivas, é necessário confiar nas ameaças previamente identificadas. O estudo empreendido neste capitulo, busca analisar e descrever as vulnerabilidades de segurança em IoT, com ênfase na engenharia social para que, a partir dessa análise, sejam desenvolvidos em em infraestruturas que utilizam essa tecnologia, bem como ambientes de automação residencial e afins, mecanismos e ações mitigatórias eficazes.

5.1 Estratégia de busca

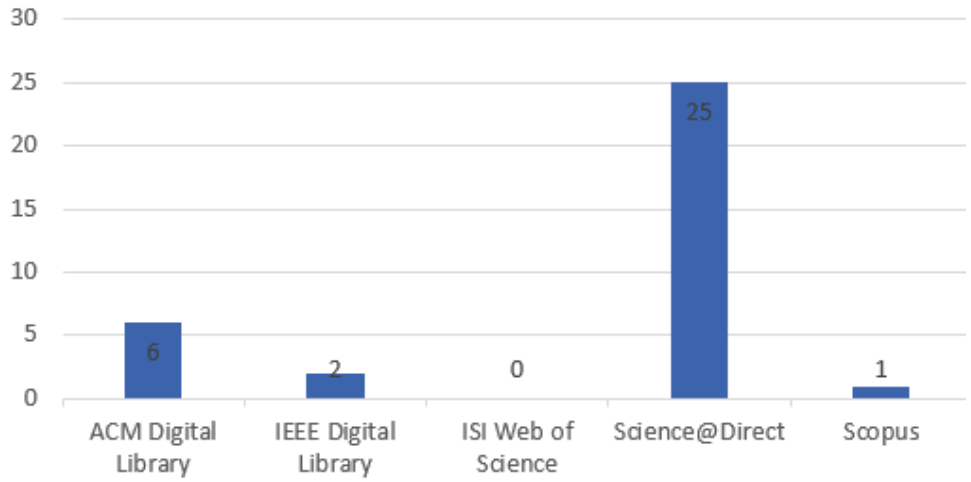
Para o desenvolvimento desse levantamento bibliográfico foram utilizadas as seguintes bases de dados: SpringerLink, ACM Digital Library, IEEE Digital Library, ISI Web Of Science, Science Direct e Scopus. Os termos de busca utilizados foram: Internet Of Things, Iot, Information security, Engerning Social, smart homes.

A Revisão Sistemática seguiu um protocolo detalhado proposto por Kitchenham (2004) e foi dividida em três etapas: execução da busca, primeira etapa de seleção e segunda etapa de seleção. Para a etapa de execução da busca, foi utilizada a seguinte string, ("Internet das Coisas"OR "Internet of Things "OR "IoT") AND ("segurança da informação"OR "information security") AND ("automação residencial"OR "smart homes") AND (“Engenharia Social “OR “Social engineering”).

Desta forma a string é utilizada nas fontes selecionadas e os resultados alcançados são armazenados na ferramenta online Parsifal 7. A coleta de dados foi realizada no mês outubro de 2020, não se definiu limite temporal, foram selecionados apenas artigos publicados em conferências ou periódicos. Assim, a pesquisa teve como resultados um total de 34 artigos, como

pode ser visto no Gráfico 1, sendo 6 artigos na base ACM Digital Library, 2 artigos na base IEEE Digital Library, 0 artigos na base ISI Web of Science 1 artigo na base Scopus.

Figura 5 – Artigos levantados



Fonte: Autores, 2020

Neste ínterim, detectar, mitigar e desenvolver técnicas de defesa, eleva os usuários de dispositivos IoT, a um maior nível de segurança. Assim é importante analisar o nível de conhecimento dos usuários de dispositivos inteligentes acerca de ataques de segurança da informação e engenharia social. Busca-se através deste estudo, desenvolver artefatos e técnicas de conscientização dos usuários, tais como: pesquisas, formulários, publicação e elaboração de informações que apontem ações mitigatórias referentes a ataques de engenharia social.

Com relação às soluções de segurança que vêm sendo estudadas no contexto de IoT, surge os dispositivos comportamentais. Neste sentido, cabe afirmar a proposta de processamento de métricas estatísticas geradas com o intuito de produzir os recursos apropriados, para a construção de agrupamentos de dispositivos.

O acesso a informações protegidas é concedido por meio da exploração humana. O que torna o ser humano o maior fator de vulnerabilidade em segurança da informação.

A elaboração deste trabalho, parte do pressuposto de que se faz mister uma revisão na qual se analise as vulnerabilidades da segurança em IoT, com ênfase em engenharia social que permita aplicar ações de mitigação utilizadas em ambientes de automação residencial, bem como conhecer mecanismos de proteção e sua eficiência em infraestruturas que utilizam essa tecnologia.

O artigo está estruturado em seis sessões,na seção 2, o conceito e a aplicabilidade de segurança em IoT; engenharia social no contexto de IoT e Smarthomes; na seção 3, uma revisão de literatura pertinente ás temáticas supracitadas; a seção 4 apresenta os desafios de pesquisa e; na seção 5, conclusão e trabalhos futuros.

5.2 Resultados

Grande parte dos trabalhos analisados, conforme a Tabela 5 , aponta a falta de informações claras e pontuais como sendo o maior fator de risco, embora nenhum trabalho se proponha a fazer uso de aparatos capazes de disseminar tais informações. Nesse contexto, toma-se como referência o trabalho de Kettani e Cannistra (2018), que busca alertar a comunidade fazendo uso de uma lista de quinze ameaças cibernéticas usadas por criminosos em engenharia social de maneira abrangente.

Cabe ressaltar que esta pesquisa se limitará a apresentar propostas de práticas de segurança em IoT, sem, no entanto, se comprometer em provar a eficácia destas medidas, ou seja, o trabalho ora empreendido não oferecerá garantia de maior segurança no campo aplicado.

Tabela 5 – comparação entre os estudos relacionados

ARTIGO	IOT	E.SOCIAL	DESAFIOS	AMEAÇAS	DETECÇÕES	VULNERABILIDADES	SOLUÇÕES	ATAQUES
(MAHAINI; LI; SAĞLAM, 2019)	X							
(YIĞIT et al., 2019)	X					X	X	
(ARABO, 2015)	X					X		
(KETTANI; CANNISTRA, 2018)	X	X		X			X	
(ZHOU et al., 2018)	X		X	X			X	
(HEARTFIELD; LOUKAS, 2018)	X	X						
(LALLIE et al., 2021)	X	X						
(GRAMMATIKIS; SARIGIANNIDIS; MOSCHOLIOS, 2019)					X	X	X	
(YANG; LEE; ZO, 2017)						X		
Este estudo	X	X	X	X	X	X	X	X

Fonte: Autores, 2020

5.3 Considerações do Capítulo

Os ataques a redes inteligentes se tornam a cada dia, problemas graves no que concerne à informação. A detecção, mitigação, proteção e técnicas de defesa que conscientizem os usuários de dispositivos IoT promovem um maior nível de segurança para os mesmos.

São poucos os trabalhos de pesquisa que apontam técnicas desenvolvidas diretamente com os usuários de IoT, cabendo uma discussão mais abrangente nesse sentido.

Portanto, para o alcance de uma discussão pertinente que atenda as necessidades detectadas, foi desenvolvido um questionário através do qual foi possível ser mensurado o nível de conhecimento dos usuários, bem como as vulnerabilidades relativas à Engenharia Social às quais estes estão expostos.

Neste sentido, a dissertação proposta para este trabalho, teve como principal foco a identificação dos principais ataques de engenharia social em IoT, além de um estudo acerca dos tipos e técnicas de defesa que deverão ser utilizadas para mitigar os ataques cibernéticos.

Para atingir o objetivo macro ora proposto, foi feito um levantamento e análise dos trabalhos relacionados a ataques de engenharia social a redes IoT que permitiu verificar do nível do impacto de ataques de engenharia social em redes IoT, bem como identificar técnicas utilizadas em ataques de engenharia social e técnicas de defesa.

Para tanto, foi necessário analisar o nível de conhecimento dos usuários de tecnologias de Internet das Coisas, acerca de segurança da informação e ataques de engenharia social. Este estudo resultou na elaboração de técnicas para conscientização dos usuários.

Considerando as demandas encontradas nas pesquisas que subsidiaram este trabalho, nota-se ser abrangente o campo de estudo na referida área, dado o alarmante número de ataques de engenharia social, bem como a vulnerabilidade à qual se expõem os usuários de smart homes e demais redes inteligentes. Neste sentido, pontua -se a relevância de conscientizar os usuários de IoT e tecnologias deste âmbito acerca da importância da Segurança da Informação.

6

Conscientização sobre a importância da Segurança da Informação

Neste capítulo serão apresentados os resultados da pesquisa sobre o comportamento de usuários de IoT e Engenahria Social.

6.1 *Snowball*: Estratégia

Uma pesquisa complementar se fez necessária para elucidar as informações empreendidas neste trabalho. Para tanto, utilizou-se a metodologia bola de neve, *Snowball*, que consiste em um tipo de amostra não probabilística. Seus resultados advêm de algum critério de inclusão preestabelecido e não atinge a toda população no que diz respeito à participação na amostragem como aponta (BICKMAN; ROG, 2008).

Na presente abordagem, a metodologia se aplica com base nos seguintes passos: a identificação de documentos ou informações-chaves, convencionadas enquanto sementes; As sementes indicarão outros colaboradores para a linha de pesquisa; os novos colaboradores indicam outros; a saturação (por repetição de temáticas), sem retornar novas indicações ou a quantidade satisfatória de amostras (VINUTO, 2016) .

Os novos colaboradores, mesmo indicados, são selecionados somente quando se enquadrarem nas características exigidas. Uma *snowball* é empregada para fins exploratórios que buscam: "[..] compreender um tema, testar a viabilidade de realização de um estudo mais amplo, e desenvolver os métodos a serem empregados em todos os estudos ou fases subsequentes"(VINUTO, 2016).

A insuficiência de resultados na fase de Mapeamento Sistemático na pesquisa empreendida, sugere a utilização desta metodologia, já que, o objetivo desta Revisão de Literatura é conscientizar os usuários em rede e explicitar sobre Engenharia Social.

Para a elaboração desta revisão, realizou-se uma busca no Google Scholar [1] durante o período de 02 a 20 de julho de 2022, com os seguintes termos de busca: Conscientização, Segurança da Informação, Usuários, Engenharia Social. A partir dos critérios de seleção, foram escolhidos cinco trabalhos como sementes. As sementes levaram algumas "indicações"e foram denominadas referências. Os trabalhos selecionados como semente passaram pelos seguintes critérios de seleção:

- Estar entre 10 primeiros resultados retornados do *Google Scholar* ;
- Estar disponível para leitura;
- Ser publicado entre os anos de 2012 a 2022, período em que a busca foi realizada, priorizando-se os mais recentes, por trazerem resultados e informações mais atualizadas. As referências das sementes seguiram os seguintes critérios para aceitação:
- Disponibilidade para leitura;
- Relação Usuários IoT e Engenharia Social;
- Não ser livro ou artigo de sites e blogs.

6.2 Resultados

A Tabela 6 descreve os trabalhos selecionados como sementes para a revisão snowball. Foram obtidos no total treze trabalhos para a revisão de literatura.

Tabela 6 – Sementes da Revisão Bola de Neve

ID	**Titulo**	**Referência**
S1	Tecnologias e ferramentas para prevenção de ataques em redes de computadores	(SILVA; MESQUITA; PAIVA, 2018)
S2	Conscientização sobre Segurança da Informação no uso de redes sociais aos alunos da aprendizagem industrial -Senai Itajaí/SC	(SILVA, 2020)
S3	Um objeto de aprendizagem sobre medidas de prevenção na internet: conscientização do usuário.	(SANTOS et al., 2014)
S4	A influência da Engenharia Social no fator humano das organizações.	(HENRIQUES, 2017)
S5	Análise das questões relacionadas ao uso de redes sociais online	(OLIVEIRA, 2019)

Fonte: Autores, 2022

S-1 ou primeira semente, contempla o artigo de SILVA, MESQUITA e Paiva (2018), foi a primeira semente selecionada. A imersão se fez por levantamento, classificação e análise dos sistemas de detecção de invasão (Intrusion Detection System – IDS), já a ideação consistiu em mostrar as vulnerabilidades presentes em redes sem fio.

[1] Ferramenta de pesquisa que permite localizar literatura acadêmica em periódicos científicos e fontes especificas.

A S-1 aborda uma análise na qual foram utilizados testes de intrusão em um ambiente controlado, demonstrando falhas presentes em redes de computadores sem a devida proteção. A síntese consiste no princípio de detecção de invasão e identificação dos aspectos operacionais do sistema para a prevenção da rede contra esses ataques. SILVA, MESQUITA e Paiva (2018), conclui que "à medida em que mais ferramentas de proteção são aplicadas pelo usuário, maior é a segurança que se consegue e, quanto mais atenção se emprega a essas técnicas, mais segura fica a utilização de uma rede de computadores." Esta semente não retornou outra semente.

A S-2, ou segunda semente, se refere ao artigo de Silva (2020), e busca prevenir que alunos acerca de vulnerabilidade às ameaças provocadas pela internet, identificando estas ameaças. O referido artigo explora uma metodologia eficaz para a conscientização dos alunos da Aprendizagem Industrial do SENAI Itajaí/SC sobre a Segurança da Informação, cuja abordagem advém de questionário formulado com a ferramenta Google Forms, aplicado para alunos da modalidade de Aprendizagem Industrial do SENAI da cidade de Itajaí(SC) no ano de 2020.

A análise se fez através de um Quizz online, demostrando possíveis ameaças e vulnerabilidades que podem acontecer quando se navega pela internet. Para a síntese, a cada pergunta feita no Quizz, e logo após a resposta, realizou-se uma intervenção com explicação de como podem prevenir-se. Esta semente retornou a outras duas sementes;

A terceira semente, S-3, Santos et al. (2014), desenvolve conteúdos educacionais para conscientização dos usuários sobre os riscos e ameaças existentes na Internet, apresentando medidas e dicas de segurança. A imersão parte do envolvimento e motivação dos alunos para com a temática. A ideação valida um experimento (OA) Objeto de Estudo, aplicado em uma turma de EJA no Colégio de Aplicação/UFRGS.

A análise adveio dos seus resultados, nos quais se observou que o uso de recursos de Tecnologias de Informação e Comunicação tem aumentando na educação. Enquanto síntese pode se afirmar que, não necessariamente temas como segurança e engenharia social são tratados como deviam, nestes ambientes. A terceira semente não retornou outra semente

A quarta semente S-4 Henriques (2017), tem como imersão a mitigação do conhecimento de um determinado grupo acerca de Engenharia Social. A ideação foi feita através da aplicação de um questionário. Enquanto análise, detectou-se como este grupo percebe a Engenharia Social e como é tratada a questão da Segurança da Informação. Sintetiza-se este trabalho apresentando técnicas de Engenharia Social no sentido de conhecimento e prevenção, bem como a sugestão de uma visão mais humana da Segurança da Informação.

Tabela 7 – Resultados da S4

ID	Título	Referência
S4A1	Tendências e ameaças técnicas	(VERISIGN, 2016)
S4A2	Social Engineering Threats and Awareness: A Survey	(KUMAR; CHAUDHARY; KUMAR, 2015)

Fonte: Autores, 2022

Verisign (2016), fornece uma visão geral das principais tendências de segurança cibernética do ano anterior e conhecimentos de como a Verisign acredita que essas tendências evoluirão nos próximos anos. O objetivo deste relatório é informar as equipes de segurança cibernética e operações de negócios sobre as ameaças e tendências cibernéticas mais importantes que afetam sua empresa.

Kumar, Chaudhary e Kumar (2015) definem engenharia social e explica como se pode usar a mente humana para capturar informações úteis sobre organizações ou indivíduos. Ele também fornece recomendações sobre como defender e proteger contratacantes que usam técnicas de engenharia social, enquanto método não técnico de intrusão hacker, que depende fortemente da interação humana e muitas vezes envolve enganar as pessoas para quebrar o normal procedimento de segurança.

Oliveira (2019), na quinta semente, S-5, desenvolveu uma pesquisa que com a finalidade de estudar a engenharia social, suas definições e práticas baseadas na obtenção de informações privadas através de apropriação indevida ou formas de enganação. Para isso verificou questões referentes ao comportamento dos usuários em redes sociais online relacionadas às possibilidades de ataques da Engenharia Social.

Oliveira (2019) teve como objetivo investigar a aplicação da engenharia social nas redes sociais online, buscando refletir sobre suas práticas e maneiras de minimizar os incidentes de segurança da informação e da conscientização do usuário, que é considerado o pilar mais frágil da segurança da informação. A semente 5 trouxe (01) apenas uma nova semente, na qual sugere, de uma visão mais humana da Segurança da Informação.

Tabela 8 – Resultados da S5

ID	Título	Referência
S5B1	Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos.	(CÔRTE, 2014)

Fonte: Autores, 2022

Côrte (2014), defende os pilares: tecnologia, pessoas e processos e,faz uma abordagem do ponto de vista epistemológico, ao se referir que ciência da informação possui, por objeto de estudo, a informação, E ASSIM SENDO, preocupa-se com a análise dos processos de construção, de comunicação e de uso da informação, bem como com a concepção dos produtos e dos sistemas que permitem sua organização, sua comunicação, seu armazenamento e seu uso. Esta semente não retornou outra semente.

Carneiro e Almeida (2013), investigam a inter-relação entre o elemento humano e a segurança da informação no contexto corporativo visando explorar como, por que e em quais circunstâncias ocorrem falhas de segurança que envolvem pessoas e entender como lidar com elas. O referido artigo faz-se enquanto estudo quali-quantitativo, no âmbito das Ciências Sociais Aplicadas, com a intenção de contribuir para esclarecer a interferência do elemento humano na

segurança da informação. Fatores como perfis dos usuários, e circunstâncias nas quais as falhas de segurança ocorrem, bem como a natureza dos incidentes de segurança informacional e suas razões, são relevantes discussões neste estudo.

6.2.1 Considerações do Capítulo

Os artigos selecionados indicam a necessidade de uma maior disseminação do tema, uma vez que surgem novas formas de ataque a cada dia, não existindo uma tecnologia definitiva no combate, assim, a prevenção contínua, possibilita minimizar essa questão. Esta prevenção contínua consiste em entender o comportamento dos atacantes e as principais ações tomadas por estes na tentativa de alcançar os objetivos desejados como afirma (HENRIQUES, 2017).

Com a facilidade de propagação e acesso às informações De acordo com Santos et al. (2014) e (OLIVEIRA, 2019), tendo o usuário como o pilar mais frágil da segurança da informação, quando maior for o conhecimento acerca desta fragilidade, mais fácil se torna minimizar os incidentes neste sentido.

Em suma, considerando as afirmações de Carneiro e Almeida (2013), acerca da inter relação entre o elemento humano e a segurança da informação, o princípio básico da segurança da informação exige do usuário um conhecimento capaz de distinguir as fontes seguras das maliciosas, a fim de evitar a obtenção de dados sigilosos e outras formas de ataques.

Diante destas abordagens, angariou-se subsídios para a criação do portal CIS. Para tanto, as informações desse e dos capítulos anteriores foram relevantes, bem como se fizeram relevantes na elaboração do próximo capítulo.

7

Desenvolvimento do Portal

Neste capítulo será descrito cada artefato desenvolvido durante a pesquisa, os resultados, a avaliação e validação das funcionalidades dos artefatos e a discussão dos resultados.

7.1 Projeto

Consiste em um curso composto por cinco módulos intercalados à aplicação de questionários, cujo foco principal é a identificação dos principais ataques de engenharia social em IoT além de um estudo acerca dos tipos e técnicas de defesa que deverão ser utilizadas para mitigar os ataques cibernéticos e visa propor mecanismos de controle que possam ser usados para inibir desvios de comportamentos e possíveis ataques a redes IoT.

Módulo I: Conceitos básicos sobre Segurança da Informação; Q1; Módulo II, (SGSI) Sistemas de Gestão de Segurança da Informação; Módulo III, O Fator Humano e Q2; Módulo IV, Vulnerabilidades e Módulo V Engenharia Social e Q3.

Este curso foi ministrado na Disciplina de Teoria Geral de Sistemas (TGS), uma disciplina obrigatória para Curso Bacharelado em Sistemas de Informação e optativa nos cursos de bacharelado em Engenharia e Ciência da Computação do Departamento de Computção (DCOMP) da Universidade Federal de Sergipe (UFS).

Para uma maior disseminação e armazenamento destes conteúdos foi desenvolvido um portal cujo título Checklist IoT Security (CIS), aponta uma analogia à lista de verificação de um passo a passo com dicas para se manter seguro em Rede, disponível em: <https://cis.blog.br/>.

7.2 Curso

O desenvolvimento do Módulo 1, cujo conteúdo: Conceitos básicos sobre Segurança da Informação, faz-se relevante já que neste segmento da área de Tecnologia da Informação (TI),

lida com a integridade física e lógica dessas informações, protegendo-as contra acessos não autorizados. A figura 6, apresenta o ícone do Módulo 1, no qual estão dispostos os conceitos de Segurança da Informação, um breve histórico da Segurança da Informação, os princípios básicos da Segurança da Informação e as principais referências.

Figura 6 – Módulo 01

Fonte: Autores, 2022

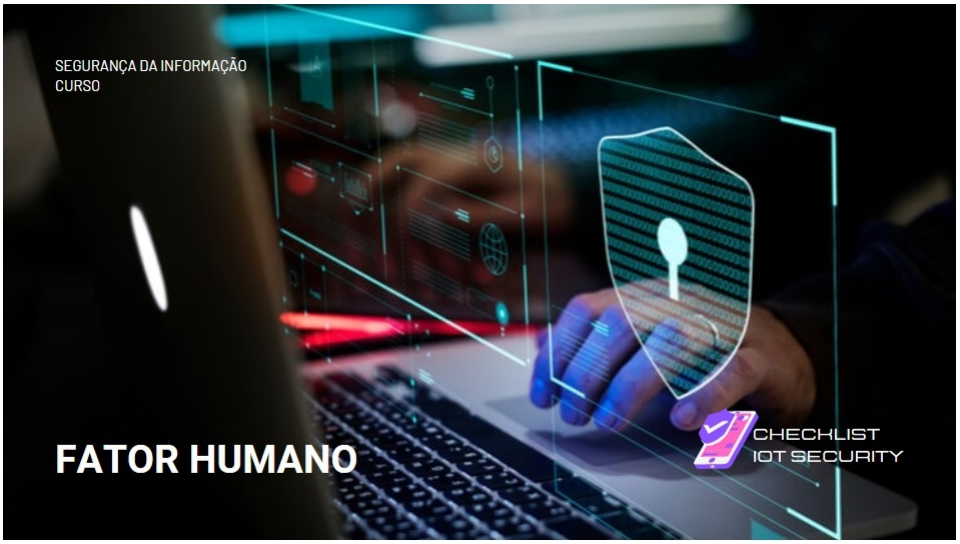
A Figura 7, apresenta o ícone do módulo 2, que traz uma abordagem do processo de gestão do SGSI (Sistema de Gestão de Segurança da Informação); a implementação do SGSI; auditorias, análise crítica e melhorias do SGSI. Este módulo dispõe também da Norma ISO IEC 27000 que especifica requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Figura 7 – Módulo 02

Fonte: Autores, 2022

O módulo 3, como abordado na Figura 8 faz uma abordagem pontual no que concerne à proteção de dados confidenciais nas empresas e se fundamenta no componente técnico e no fator humano. De acordo com as últimas tendências de desenvolvimento da segurança da informação, o foco passa a ser o indivíduo. Isto é evidenciado por tecnologias como UEBA (User and Entity Behavior Analytics), UBA (User behavior analytics), SUBA (Security User Behavior Analytics) e outras ferramentas de análise de comportamento de usuários que visam detectar ameaças presentes.

Figura 8 – Módulo 03



Fonte: Autores, 2022

O módulo 4, abordado na Figura 9 trata de Vulnerabilidade e traz um breve conceito de

acordo com a ISO 27000, que define princípios, nomenclaturas, vocabulários e guias práticos. O módulo também versa sobre os tipos de vulnerabilidade: física, natural, hardware, vulnerabilidade de código ou criptografia, comunicação e humana, escrevendo e ilustrando cada um dos tipos.

Figura 9 – Módulo 01

Fonte: Autores, 2022

O módulo 5, como abordado na Figura 10 conceitua Engenharia social, mencionando os tipos de ataque, define ataques diretos ou indiretos e dá exemplos de ataques mais comuns. Neste capítulo, traça-se um um perfil do Engenheiro Social e enfatiza-se o ataque do tipo Phishing que consiste em atrair ou fisgar as vítimas por meio de mensagens falsas, cujos danos vão desde prejuízos materiais a psicológicos.

Figura 10 – Módulo 05

Fonte: Autores, 2022

7.3 Resultados

Seguem alguns dados baseados nos resultados dos formulários aplicados no curso. Trata-se de 03 (três) formulários intercalados entre as aulas, com o objetivo de avaliar o nível de cohecimento do aluno/participante ao longo do curso. Não se aplicou Termo de Consentimento de Livre e Esclarecido (TCLE), dado o caráter avaliativo dos formulários. Apresenta-se neste ínterim, a pergunta e a estatística das respostas.

Os dados apresentados foram coletados a partir de respostas de 16 alunos. Ressalta-se que não se atingiu a todos os alunos do curso, uma vez que alguns optaram por não participar da pesquisa. As respostas foram de múltipla escolha e abertas e, as alternativas escalonadas, que permitiram que o respondente indicasse o seu posicionamento diante da pergunta, utilizando os seguintes padrões: pouco, muito ou razoável. A primeira e a segunda pergunta refere-se ao nome e e-mail do participante.

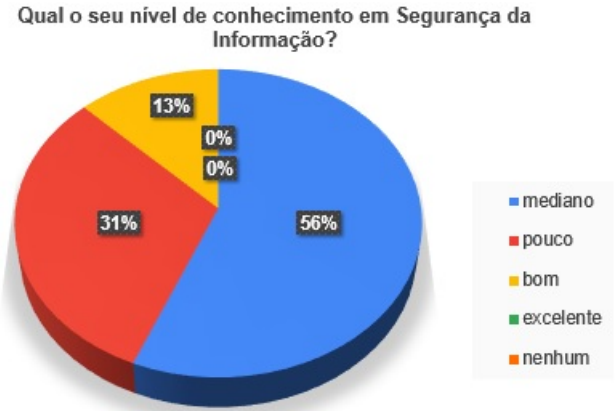
A terceira pergunta do formulário 01, disposto no seguinte endereço: <https://forms.gle/6BwhNKvUh2WQMJ866>, buscava conhecer um pouco mais sobre o aluno. Assim, foi perguntado qual a faixa etária, como apresentado na Figura 11. A maioria dos participantes tinham entre 18 a 25 anos. Propositalmente, se buscou atingir a faixa etária adulta para este público-alvo, por saber se tratar de um contigente de indivíduos capazes de responder pelos próprios atos, cientes das suas responsabilidades e escolhas. Tal critério isenta os pesquisadores de buscarem autorização junto aos pais e/ou responsáveis para a aplicação da pesquisa.Também se manteve o anonimato dos respondentes.

Figura 11 – Q3 Formulário 01

Fonte: Autores, 2022

A quarta pergunta, busca saber qual o nível de conhecimento sobre segurança da informação. Tal levantamento se faz relevante, uma vez que traça um panorama de como estes usuários lidam com tal fator. A partir das respostas, alcançou-se um percentual de 56% das pessoas pesquisadas que consideram seu nível de conhecimento mediano, 31% consideram pouco conhecimento, 13% afirma ser bom o seu nível de conhecimento. Não houve respostas para os termos, excelente e nenhum. Conforme está apresentado no gráfico da Figura 12.

Figura 12 – Q4 Formulário 01

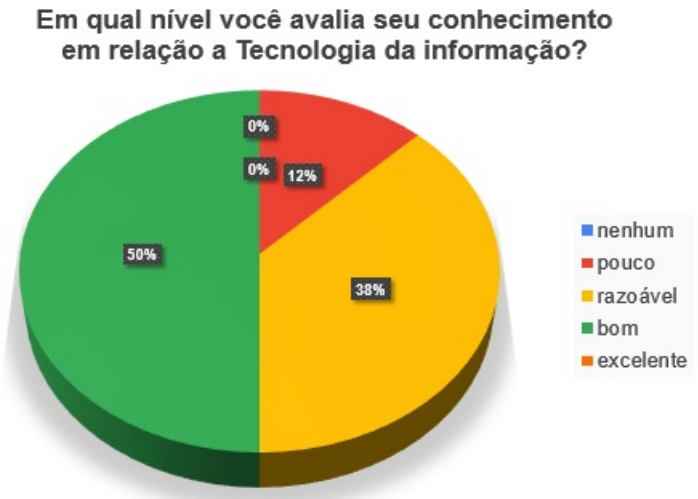


Fonte: Autores, 2022

A quinta pergunta do formulário se refere à auto-avaliação acerca do nível de conhecimento em relação à Tecnologia da Informação. Como resultado obteve-se: 50% dos respondentes apontaram ser bom, 38% razoável e 12% pouco. Como pode ser visualizado no gráfico da Figura

13.

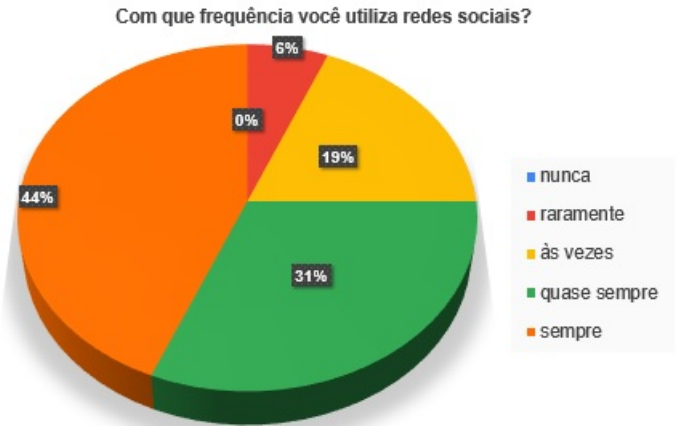
Figura 13 – Q5 Formulário 01



Fonte: Autores, 2022

A questão 6, como apresentado na Figura 14.aborda acerca da frequência de uso de redes sociais cujos resultados foram: 44% sempre; 31% quase sempre; 19% às vezes; e 6% raramente. Para o termo nunca não se obteve resposta. Tal resultado aponta um público-alvo conectado com a rede.

Figura 14 – Q6 Formulário 01



Fonte: Autores, 2022

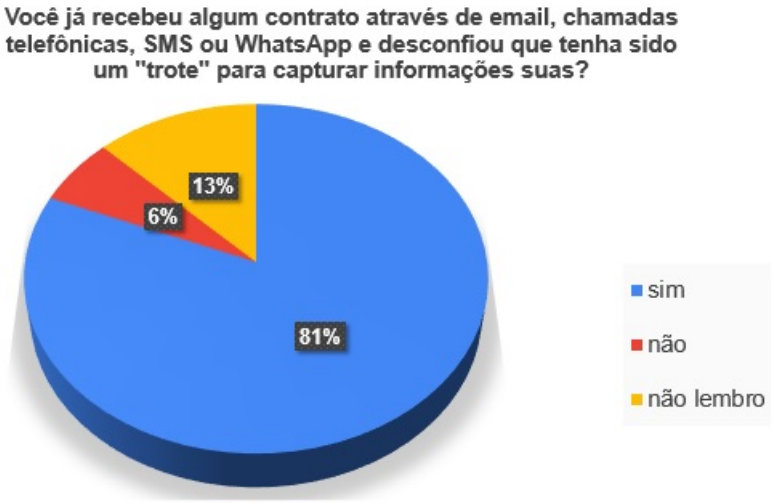
Acerca da frequência com que publica informações pessoais em rede, como demonstrado na Figura 15 obteve-se um percentual de 81% para raramente; 13% para às vezes; 6% para nunca. Os termos: quase sempre e sempre, não foram mencionados.

Figura 15 – Q7 Formulário 01

Fonte: Autores, 2022

Com relação a “trote” através de e-mail, chamadas telefônicas, SMS e WhatsApp, com alternativas: sim, não e não lembro, Obteve-se: 81 % para sim; 6% para não e 13%, para não lembro, como aponta o gráfico da Figura 16.

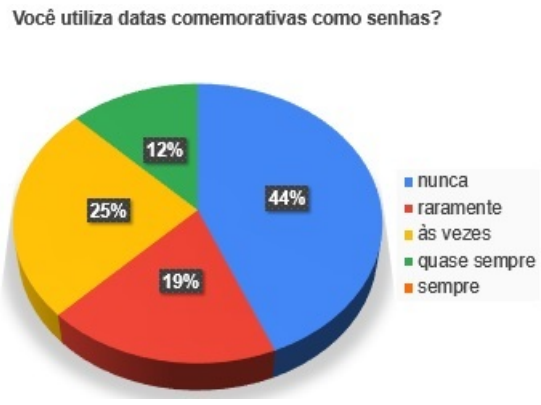
Figura 16 – Q8 Formulário 01



Fonte: Autores, 2022

A questão 9, versa sobre a utilização de datas comemorativas na fomulação de senhas. As alternativas foram compostas pelos seguintes termos: nunca, raramente,às vezes, quase sempre e sempre. O gráfico permite a leitura dos seguintes resultados: 44% nunca; 19% raramente; 25% às vezes; 12% quase sempre; e 0 % sempre, como abordado na Figura 17.

Figura 17 – Q9 Formulário 01



Fonte: Autores, 2022

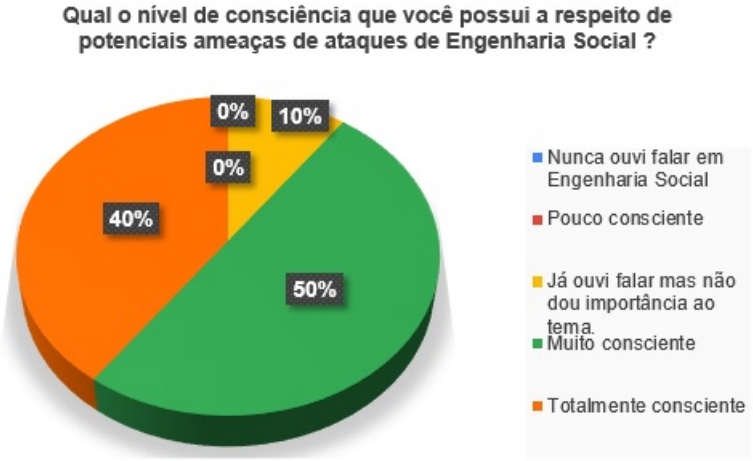
A informação apontada no gráfico da Figura 18 busca conhecer o nível de conhecimento do público alvo acerca de Engenharia Social. Para a coleta de dados, utilizou-se duas alternativas: sim e não. Nesta, obteve-se: 87% para sim e 13% para não.

Figura 18 – Q10 Formulário 01

Fonte: Autores, 2022

A questão 3 do segundo formulário, disposto no seguinte endereço: <https://forms.gle/2dd3Xz9cuthCzasv5> aborda acerca do nível de consciência do público alvo com relação a potencial ameaça de ataques de Engenharia Social. As alternativas contemplam os seguintes termos e expressões: nunca ouvi falar; pouco consciente; já ouvi falar mas, não dei importância ao tema; muito consciente; totalmente consciente. As respostas forneceram os seguintes percentuais: 56% para muito consciente; 25% para totalmente consciente; 13% para já ouvi falar mas, não dei importância ao tema; 6 % para nunca ouvi falar; e 0% para pouco consciente, como indicado no gráfico apontado na Figura 19

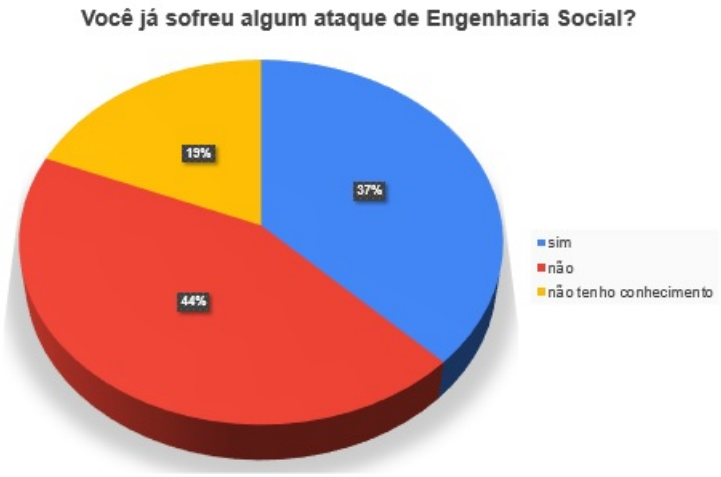
Figura 19 – Q3 Formulário 02



Fonte: Autores, 2022

O gráfico da Figura 20 permite conferir que, ao ser questionado se já sofreu algum ataque de Engenharia Social, o público-alvo que teve como alternativas: sim; não; e, não tenho conhecimento, reagiu da seguinte forma: 44% não; 37% sim; e, 19% não tenho conhecimento.

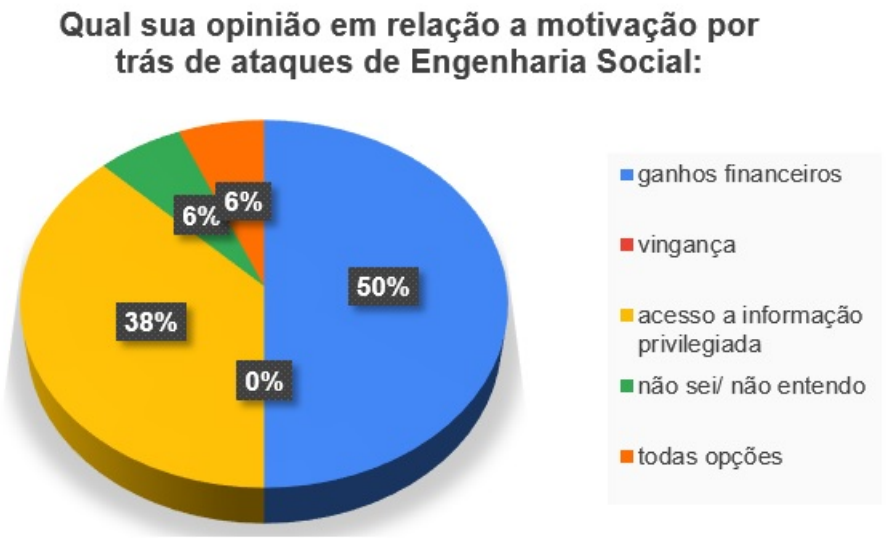
Figura 20 – Q4 Formulário 02



Fonte: Autores, 2022

Acerca da opinião em relação à motivação por trás de ataques de Engenharia social ; os termos e expressões alternativas foram: ganhos financeiros; vingança; acesso informação privilegiada; não sei/não entendo; e, todas as opções. Obteve-se os seguintes dados: 50% para ganhos financeiros; 38% para acesso informação privilegiada; 6% para não sei ou não entendo; 6% para vingança; e, 0 resposta para todas as opções, como abordado na Figura 21

Figura 21 – Q5 Formulário 02

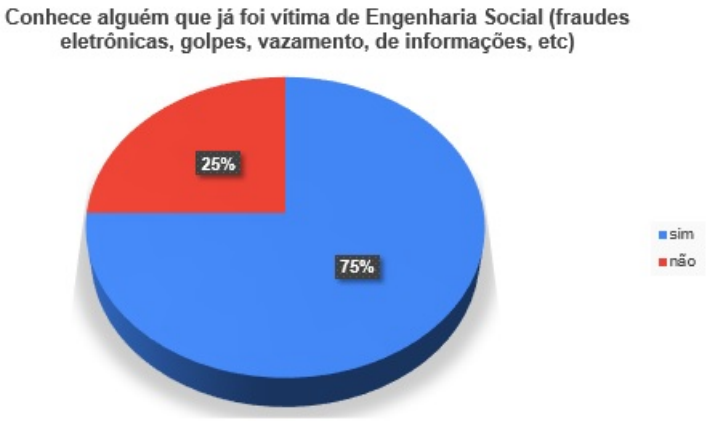


Fonte: Autores, 2022

A questão 6 apresenta a seguinte abordagem: Em sua opinião que tipo de pessoa é mais suscetível a ataques de engenharia social?

Questionados sobre conhecer alguém que já foi vítima de Engenharia Social (fraudes eletrônicas, golpes, vazamentos de informações , etc.), o público-alvo, mediante as alternativas: sim e não, reagiu com: 75% para sim e 25% para não, como abordado na Figura 22

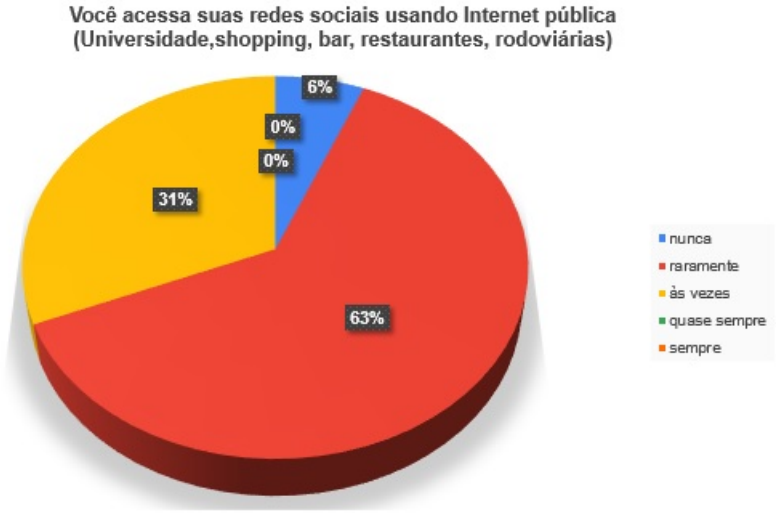
Figura 22 – Q7 Formulário 02



Fonte: Autores, 2022

O gráfico abordado na Figura 23, se refere a questão 8, que versa sobre o uso das redes sociais usando Internet pública (Proveniente de Universidades, Shoppings, bares, restaurantes e rodoviárias). As alternativas contemplam os seguintes termos: nunca; raramente; às vezes; quase sempre; e sempre. Os resultados contemplados foram: 63% para raramente; 31% para às vezes; 6% para nunca; 0% para quase sempre; e 0% sempre.

Figura 23 – Q8 Formulário 02



Fonte: Autores, 2022

Quando questionados se desconfiam de mensagens atrativas recebidas em mídias sociais, tendo como alternativas os termos: nunca; raamente; às vezes; muitas vezes; e sempre , 75% dos consultados respondeu sempre; 19% nunca; e 6% respondeu raramente. As demais alternativas não foram mencionadas, como aponta o gráfico da Figura 24.

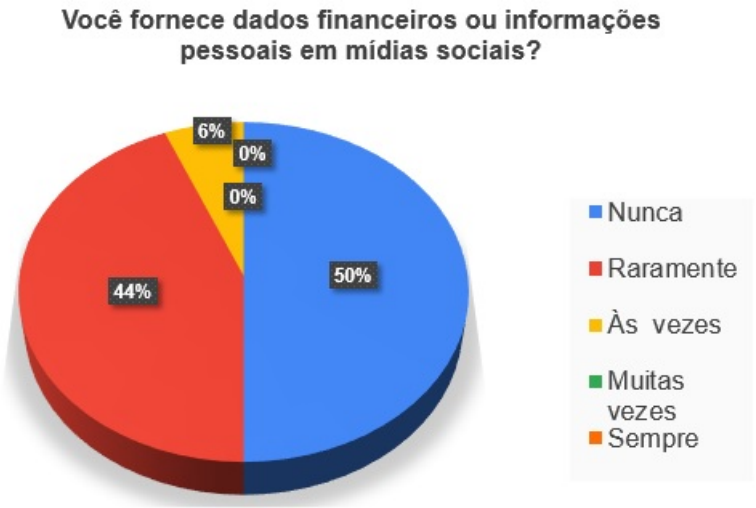
Figura 24 – Q9 Formulário 02

Fonte: Autores, 2022

A questão 03 do formulário 03, disposto no seguinte endereço: <https://forms.gle/2dd3Xz9cuthCzasv5>, abordou acerca do fornecimento de dados financeiros ou informações pessoais em mídias sociais tendo como alternativas os termos: nunca; raramente; às vezes; muitas

vezes; e sempre, 50% mencionaram nunca; 44% raramente; e 6% nunca. Os demais termos não foram mencionados como demonstrado no gráfico da Figura 25

Figura 25 – Q3 Formulário 03



Fonte: Autores, 2022

O gráfico da Figura 26 ilustra dados acerca da utilização de recursos de privacidade (marcação de pessoas, verificação em duas etapas), com as alternativas: nunca, raamente, às vezes, muitas vezes, e sempre. A partir das quais foram levantados os seguintes dados: 56% dos consultados respondeu muitas vezes; 31% sempre; 7% nunca; e as demais alternativas não foram mencionadas.

Figura 26 – Q4 Formulário 03

Fonte: Autores, 2022

Sobre alterar o nome de usuário e senha padrão dos dispositivos de Internet, frente aos termos: nunca; raramente; ás vezes; muitas vezes e sempre, obteve-se: 31% para às vezes; 19%, muitas vezes; 13% sempre; e 6% nunca, como informa o gráfico da Figura 27.

Figura 27 – Q5 Formulário 03

Fonte: Autores, 2022

O gráfico da Figura 28 aponta que, acerca de buscar infomações sobre o nível de proteção e segurança antes de comprar um dispositivo, tendo como alternativas nunca, raramente, às vezes, muitas vezes, e sempre. O público-alvo reagiu da seguiNte maneira: 50% para às vezes; 13% para muitas vezes; 13% ´para sempre ; 12% para nunca; e 12% para raramente.

Figura 28 – Q6 Formulário 03

Fonte: Autores, 2022

Quando questionados se protegem com senha todos os dispositivos (computadores, smartphones, etc.), tendo como alternativas, sim e não, os consultados reagiram com 94% sim e 6% não. Como apontado no gráfico da Figura 29

Figura 29 – Q7 Formulário 03

Fonte: Autores, 2022

O percentual apontado no gráfico da Figura 30, refere-se sobre saber que a troca de senhas a cada seis meses aumenta a segurança de forma significativa. Com as alternativas sim e não, obteve-se 75% de sim e 25% de não.

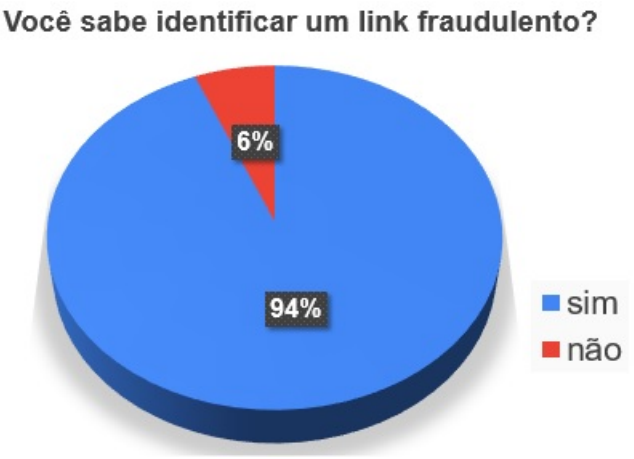
Figura 30 – Q8 Formulário 03

Fonte: Autores, 2022

O gráfico abordado na Figura 31, aponta que 94% dos consultados identifica um link

fraudulento, enquanto apenas 6% não consegue identificar. De acordo com os resultados obtidos percebe-se que o conteúdo apresentado no curso cumpriu com seu objetivo.

Figura 31 – Q9 Formulário 03



Fonte: Autores, 2022

Os seguinte dados foram coletados a partir de informações obtidas através de um formulário aplicado a 10 profissionais da área da Tecnologia. Disposto no seguinte endereço: <https://forms.gle/K188BNgTuNbHahacA>

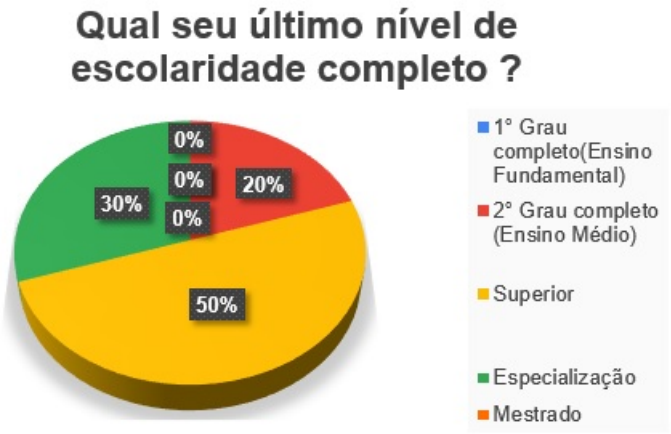
A segunda pergunta deste formulário se refere à faixa etária e busca identificar, traçar um perfil do público-alvo e assim, selecionar e agrupar. Os dados obtidos com esta pergunta permitiram os seguintes resultados: 40% dos consultados tem entre 26 e 32 anos; 30% entre 18 e 30 anos; e outros 30% entre 34 e 41 anos. Nenhum dos consultados tem mais de 40 anos, como abordado na Figura 32.

Figura 32 – Q2 Formulário 04

Fonte: Autores, 2022

A questão 3, acerca do nível de escolaridade completo, cujas opções: 1º grau completo (Ensino Fundamental), 2º grau completo(Ensino Médio), Superior, Especialização, Mestrado, Doutorado e Pós doutorado, apontou os seguintes resultados : 50% dos consultados possui Nível Superior; 30% possui Especialização; e 20%, 2º grau completo (Ensino Médio), como aborda a Figura 33.

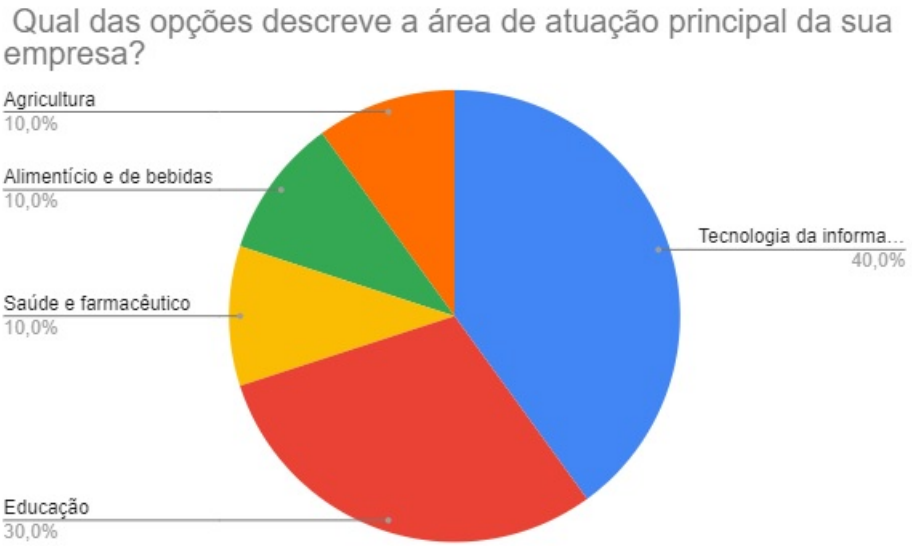
Figura 33 – Q3 Formulário 04



Fonte: Autores, 2022

Sobre a área de atuação principal da empresa na qual estão inseridos, referente a questão 7, listou-se vários segmentos e obtendo-se dados significativos para: tecnologia da informação, agricultura, saúde e farmacêutico, alimentício e bebidas, e Educação. Nestes termos, 40% dos consultados atua em Tecnologia da Informação, e 30% em Educação. No segmento Saúde e farmacêutico apontou-se 10%. Também obteve-se 10% para o segmento Alimentícios e bebidas e mais 10% para Agricultura, abordado na Figura 34.

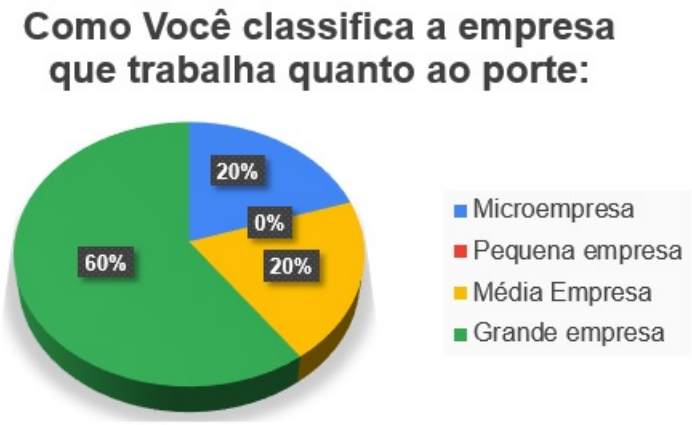
Figura 34 – Q7 Formulário 04



Fonte: Autores, 2022

A questão 8, cuja abordagem se refere à classificação da empresa em que trabalha quanto ao porte, forneceu os seguintes resultados: 60% das pessoas consultadas trabalham em uma grande empresa 20% em uma microempresa, e outros 20% em uma média empresa, como abordado na Figura 35.

Figura 35 – Q8 Formulário 04

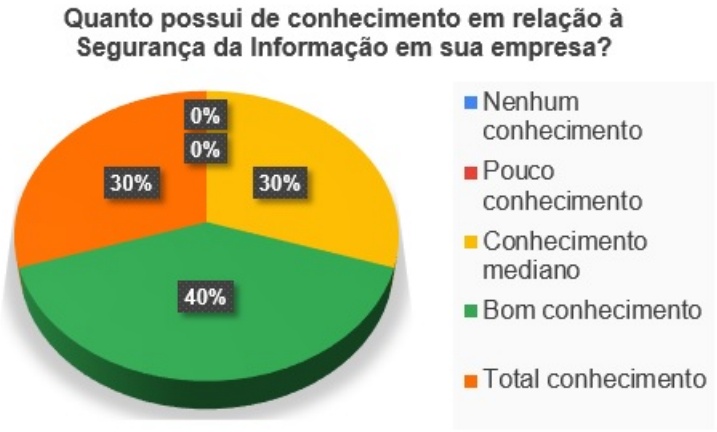


Fonte: Autores, 2022

A questão 9, que versa sobre o nível de conhecimento da empresa na qual atua em relação à Segurança da Informação, fez uso dos termos: Nenhum conhecimento, Pouco conhecimento, Conhecimento mediano, Bom conhecimento e Total conhecimento. Esta retornou 40% para

bom conhecimento, 30% para conhecimento mediano e mais 30% para total conhecimento, apresentado na Figura 36.

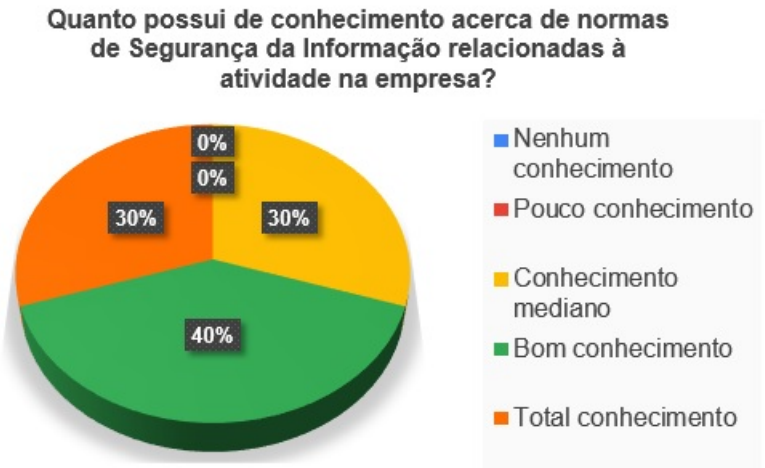
Figura 36 – Q9 Formulário 04



Fonte: Autores, 2022

Acerca do conhecimento das normas de Segurança da Informação relacionadas à atividade exercida pelo consultado na empresa, como dispõe a questão 8, obteve- se 30% para Conhecimento mediano, 30% para Bom conhecimento e 40% para Total conhecimento, como apresentado na Figura 37.

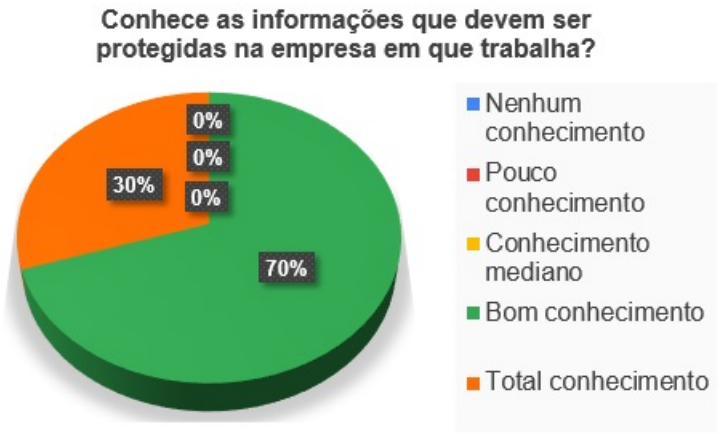
Figura 37 – Q10 Formulário 04



Fonte: Autores, 2022

Em relação a questão 11 do formulário 3, quando perguntado se conhece as informações que devem ser protegidas na empresa em que trabalha, sendo as alternativas: Nenhum conhecimento; Pouco conhecimento; Conhecimento mediano; e Bom conhecimento; obteve-se 70% para Bom conhecimento, 30% para Total conhecimento, como aborda a Figura 38 .

Figura 38 – Q11 Formulário 04



Fonte: Autores, 2022

Perguntados na questão 12, se a empresa na qual atuam realiza treinamento de conscientização em Segurança da Informação para os funcionários e parceiros de negócios, (cujas opções de respostas foram: Não existe política de treinamentos em Segurança da Informação; Existe um processo definido e totalmente aplicado de treinamentos em Segurança da Informação.) Diante das alternativas, o gráfico aponta um retorno de 20% para existe um projeto para realizar treinamentos em Segurança da Informação; 40% para não existe política de treinamentos em Segurança da Informação e os outros 40% para existe um processo definido e totalmente aplicado de treinamentos em Segurança da Informação, abordado na Figura 39.

Figura 39 – Q12 Formulário 04

Fonte: Autores, 2022

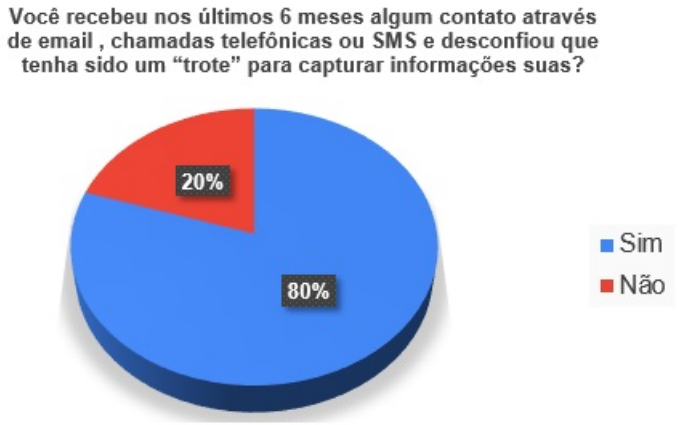
A questão 13 versa sobre a percepção do consultado enquanto colaborador/ gestor acerca da “Segurança da Informação” enquanto debate estratégico na empresa, disponibilizou-se as seguintes alternativas: Sim. É tratado com importância total; Não. Mas a empresa já possui planos para tratar o assunto; Desconheço; Sim. O assunto é debatido mas não sai do papel; Não. Mas a empresa já possui planos para tratar o assunto. Nesta, 60consultados responderam que sim, o assunto é tratado com importância total; 20% apontaram que não, embora a empresa já possua planos para tratar o assunto; 10% desconhecem; e, outros 10% sinalizam que a empresa não dá a importância devida como abordado na Figura 40 .

Figura 40 – Q13 Formulário 04

Fonte: Autores, 2022

A questão 14, acerca do recebimento de mensagem suspeita ou denotando “trote” para captura de dados através de e-mail, chamadas telefônicas ou SMS nos últimos 6 meses, (cujas alternativas: sim e não), retornou 80% para sim e 20% para não como apresentado na Figura 41 .

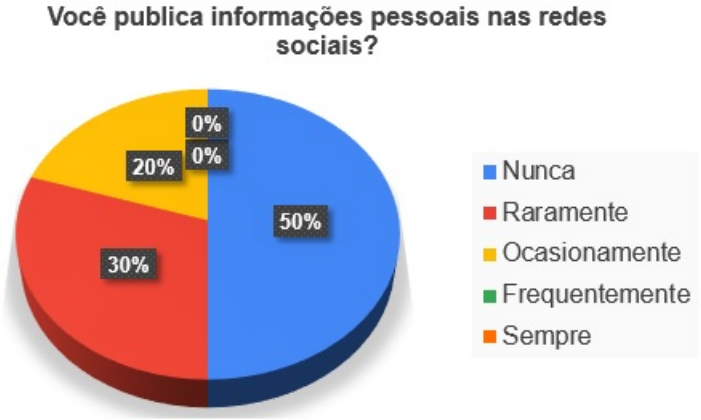
Figura 41 – Q14 Formulário 04



Fonte: Autores, 2022

Perguntados na questão 15, se publicam informações pessoais nas redes sociais, tendo como opção de respostas: nunca, raramente, ocasionalmente, frequentemente e sempre, obteve um retorno de 50% para nunca; 30% para raramente; e, 20% para ocasionalmente como apresentado na Figura 42.

Figura 42 – Q15 Formulário 04



Fonte: Autores, 2022

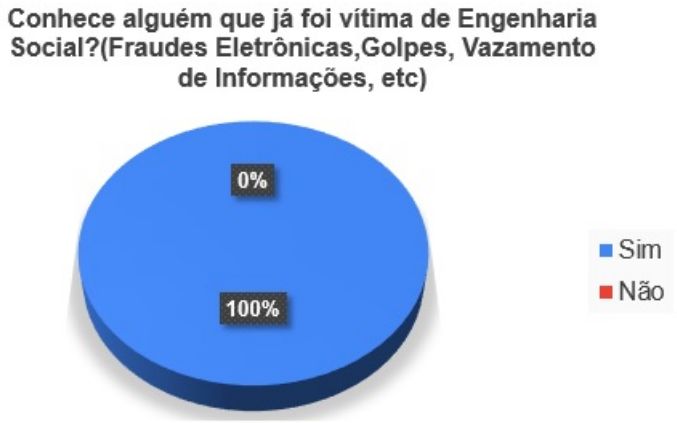
Na abordagem da questão 16, quando perguntados se já tinham ouvido falar no termo “Engenharia Social”, disponibilizadas as opções: sim; não; e, não tenho certeza, obteve-se uma totalidade de 100% para sim. Este feedback fornece a compreensão que se trata de um assunto muito comentado na atualidade como abordado na Figura 43.

Figura 43 – Q16 Formulário 04

Fonte: Autores, 2022

A questão 17, refere-se a conhecer alguém que já foi vítima de Engenharia Social(Fraudes Eletrônicas, Golpes, Vazamento de Informações, etc). Com as opções, sim e não, retornou 100% sim. O que reforça a ideia de que não se trata apenas de um assunto muito comentado, e sim, vivenciado, como abordado na Figura 44.

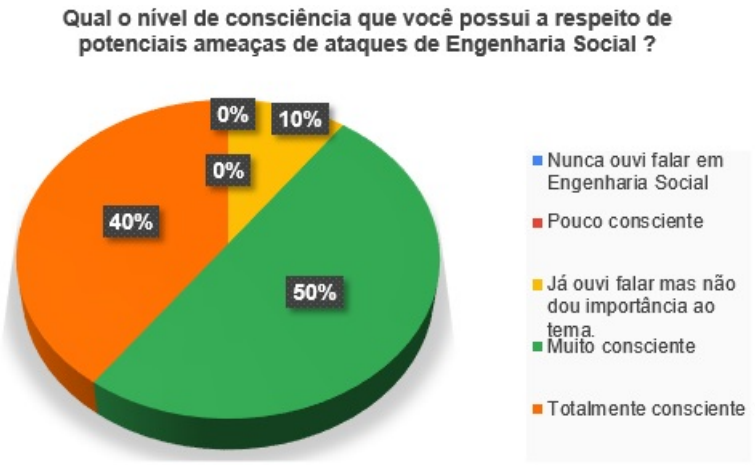
Figura 44 – Q17 Formulário 04



Fonte: Autores, 2022

Quando perguntados na questão 18, sobre o nível de consciência que possuem a respeito da potencial ameaça de ataques de Engenharia Social, (disponibilizados os termos: nunca ouvi falar em Engenharia Social; pouco consciente; já ouvi falar mas não dou importância ao tema; muito consciente; e totalmente consciente), obteve-se: 50% para muito consciente; 40% para totalmente consciente e apenas 10% para já ouvi falar mas não dou importância ao tema, apresentado na Figura 45.

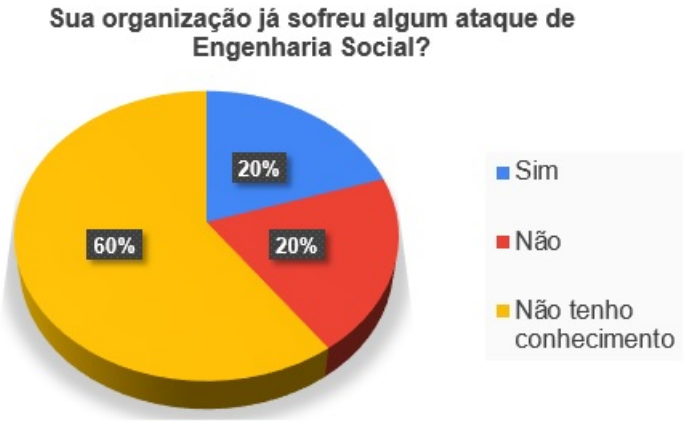
Figura 45 – Q18 Formulário 04



Fonte: Autores, 2022

A abordagem presente na pergunta 18, se sua organização já sofreu algum ataque de Engenharia Social, cujas opções: sim, não, e não tenho conhecimento, obteve enquanto retorno: 60% para não tenho conhecimento; 20% para sim e, outros 20%, para não, como mostrado na Figura 46.

Figura 46 – Q19 Formulário 04



Fonte: Autores, 2022

Acerca da motivação por trás de ataques de Engenharia Social abordada na pergunta 20, tendo como opções: Ganhos financeiros; Acesso a informações privilegiadas; Vantagem competitiva; e Vingança Pessoal, houve um retorno de 60% para ganhos financeiros e 40% para acesso a informações privilegiadas. Os demais itens não foram mencionados, abordado na Figura 47.

Figura 47 – Q19 Formulário 04

Fonte: Autores, 2022

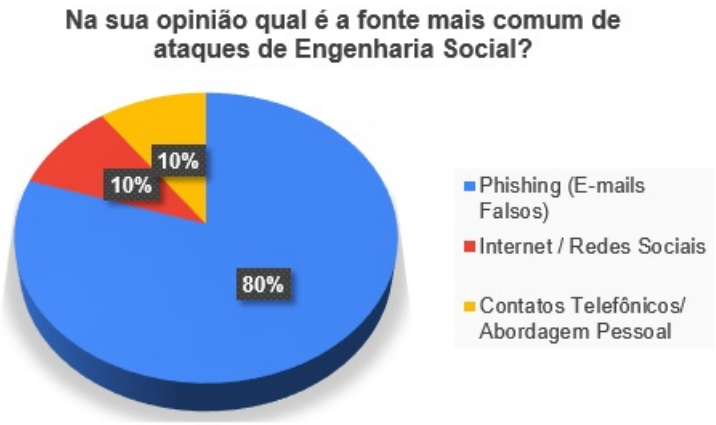
Sobre o tipo de pessoal mais suscetível a ataques de Engenharia Social, abordagem presente na questão 18, apresentadas as opções: novos empregados; terceirizados; assistentes executivos; pessoal de TI; alta diretoria), na opinião de 50% dos consultados, os novos empregados são os mais suscetíveis; 20% apontam os assistentes executivos como mais suscetíveis; outros 20% respondem ser a alta diretoria mais suscetível e apenas 10% apontam os terceirizados enquanto mais suscetíveis a ataques de Engenharia Social, apresentado na Figura 48.

Figura 48 – Q21 Formulário 04

Fonte: Autores, 2022

A pergunta 22, na qual o consultado emite opinião acerca da fonte mais comum de ataques de Engenharia Social, tendo como opções de respostas Phishing, Internet, redes sociais, contatos telefônicos e abordagem pessoal, retornou 80% para Phising (e-mails falsos); 10% para Internet / redes Sociais e outros 10% para contatos telefônicos e abordagem pessoal, abordado na Figura 49.

Figura 49 – Q22 Formulário 04



Fonte: Autores, 2022

A pergunta 23, acerca do que a sua organização vem fazendo para prevenir ataques de Engenharia Social, cujas opções: promovendo treinamentos de segurança de Informação com os empregados; a política de segurança inclui direcionamentos para prevenir ataques de Engenharia Social; atualmente nada, mas temos planos de fazer; não estamos fazendo nada, nem temos plano de fazer, 50% dos consultados afirmam que a organização vem promovendo treinamentos de Segurança de Informação com os empregados; 30% Afirmam possuir uma política de segurança que inclui direcionamentos para prevenir ataques de Engenharia Social; enquanto 20%, declaram que a organização não faz nada mas possui um plano para desenvolver algo neste sentido, como aborda a Figura 50.

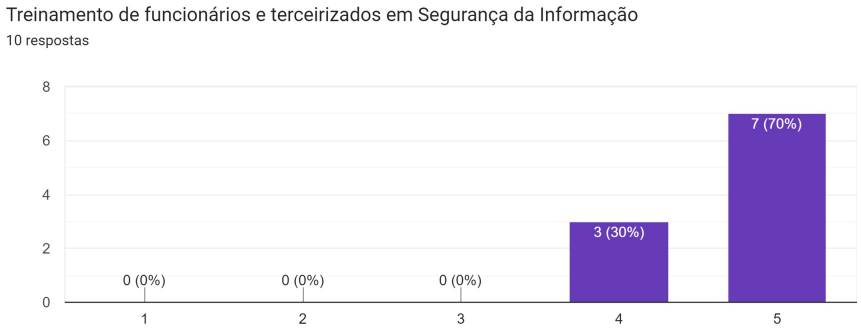
Figura 50 – Q23 Formulário 04

Fonte: Autores, 2022

A abordagem presente na questão 24: Em uma escala de 1 a 5, onde 1 está para menos importante e 5 para muito importante que conceito você atribui para “Treinamento de funcionários

e terceirizados em Segurança da Informação" enquanto meio de proteção contra a Engenharia Social, obteve como retorno: 70% de conceito 5 e 30% de conceito 4, como mostra a **??**.

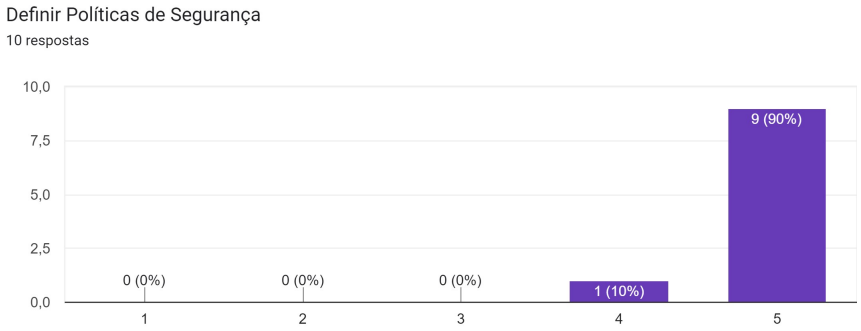
Figura 51 – Q24 Formulário 04



Fonte: Autores, 2022

Na questão 25, cuja abordagem: Em uma escala de 1 a 5, onde 1 está para menos importante e 5 para totalmente importante, que conceito você atribui para "definir Políticas de Segurança" enquanto meio de proteção contra a Engenharia Social? 90% dos consultados atribui conceito 5, enquanto 10% atribui conceito 4, mostrado na Figura 52.

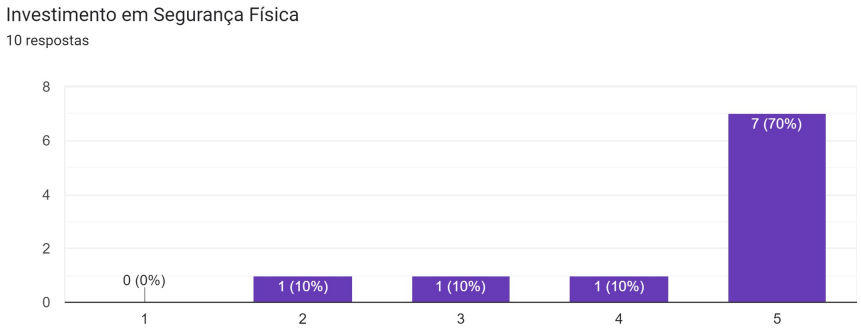
Figura 52 – Q25 Formulário 04



Fonte: Autores, 2022

Na questão 26: Em uma escala de 1 a 5, onde 1 está par menos importante,e 5 para totalmente importante), que conceito você atribui para “Investimento em Segurança Física” enquanto meio de proteção contra a Engenharia Social? obteve-se: 70 % dos para o conceito 5, 10 % para o conceito 4, mais 10% para conceito 3, e outros 10 % para o conceito 2, abordado na Figura 53.

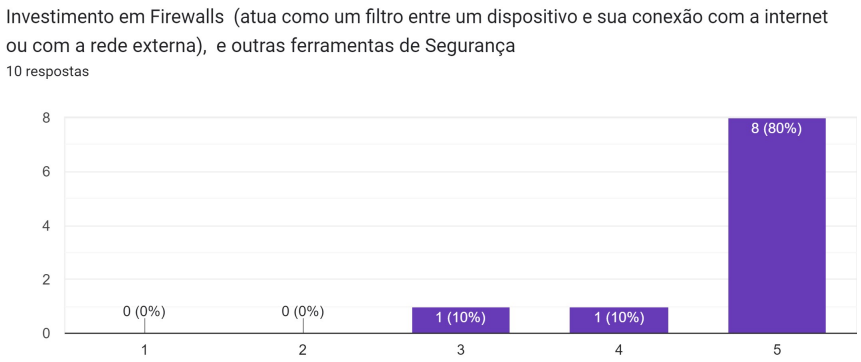
Figura 53 – Q26 Formulário 04



Fonte: Autores, 2022

Analisando o retorno da questão 27, que versa sobre Investimento em Firewalls (ferramenta que atua como um filtro entre um dispositivo e sua conexão com a internet ou com a rede externa), e outras ferramentas de Segurança, em uma escala de 1 a 5, onde 1 está para menos importante e 5 para totalmente importante, que conceito você atribui para “Investimento em Firewalls” enquanto meio de proteção contra a Engenharia Social? Para esta abordagem os dados apontam: 80% para o conceito 5, 10% para o conceito 4, e, outros 10%, para o conceito 2, como mostra a Figura 54 .

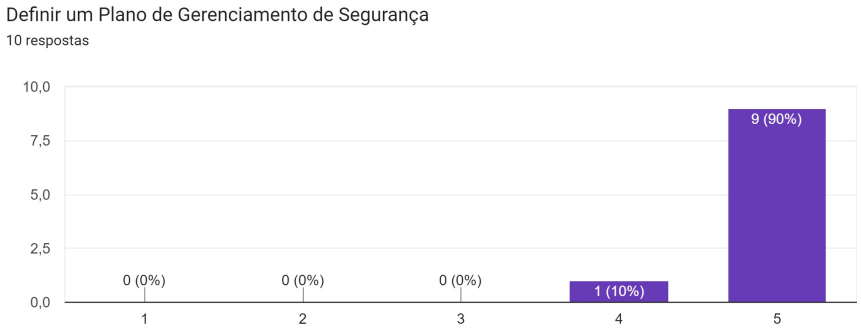
Figura 54 – Q27 Formulário 04



Fonte: Autores, 2022

Na questão 28, cuja abordagem consiste na seguinte pergunta: Em uma escala de 1 a 5, onde 1 está para menos importante, e 5 para totalmente importante, que conceito você atribui para “Definir um Plano de Gerenciamento de Segurança” enquanto meio de proteção contra a Engenharia Social? obteve-se enquanto dados: 90% para o conceito 5, 10% para o conceito 4, abordados na Figura 55.

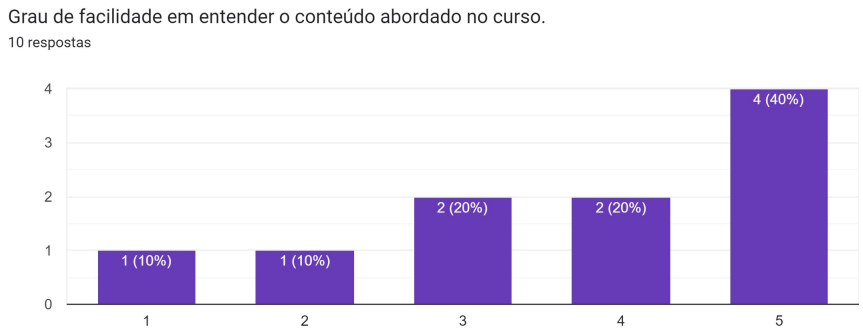
Figura 55 – Q28 Formulário 04



Fonte: Autores, 2022

A questão 29, de caráter específico: Em uma escala de 1 a 5, onde 1 está para muito fácil, e 5 para muito difícil, que conceito você atribui para " O Grau de facilidade em entender o conteúdo abordado no curso? ", retornou 40% de conceito 5, 20% de conceito 4, 20% de conceito 3, 10% de conceito 2 e 10% de conceito 1, explicito na Figura 56.

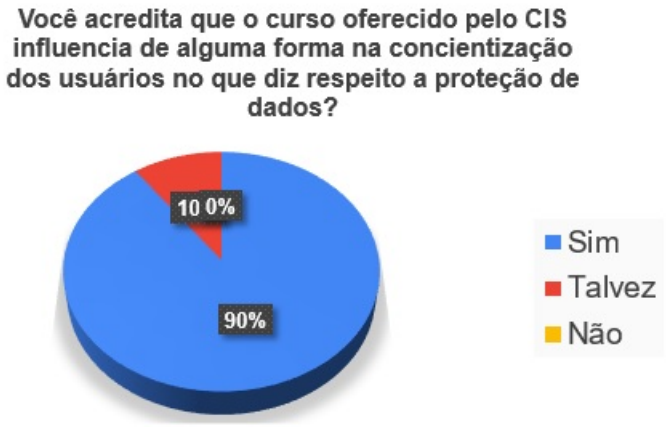
Figura 56 – Q29 Formulário 04



Fonte: Autores, 2022

A abordagem da pergunta 30, que buscou captar a opinião do público-alvo acerca da eficiência do curso oferecido pelo Portal CIS enquanto influenciador de alguma forma na conscientização dos usuários, no que diz respeito a proteção de dados, obteve retorno de 90% para sim e 10% para talvez, abordado na Figura 57.

Figura 57 – Q29 Formulário 04



Fonte: Autores, 2022

8

Considerações Finais

Este capítulo descreve as considerações finais acerca dos estudos empreendidos na elaboração desta dissertação trazendo em seguida duas seções descritas enquanto: 7.1 Trabalhos futuros; e 7.2 Trabalhos relacionados à dissertação.

O objetivo macro desta pesquisa foi desenvolver uma ferramenta informativa capaz de conscientizar usuários de IoT e outros dispositivos inteligentes, acerca da importância de identificar e prevenir ataques em rede. Para o alcance deste objetivo, a primeira etapa deste trabalho consiste em uma análise aprofundada acerca do nível de conhecimento de usuários de dispositivos tais com IoT a fim de descrever riscos e vulnerabilidades aos quais estes possam estar expostos, bem como propor ações de mitigação de tais riscos.

Ainda na primeira etapa, foram descritos os desafios da Segurança da Informação em IoT frente ao estudo de vulnerabilidades e mecanismos de proteção, no qual analisou-se a eficiência destes mecanismos em infra-estruturas que utilizam IoT e tecnologias similares.

Para o desenvolvimento da primeira etapa, elaborou-se uma questão norteadora capaz de definir o que estaria sendo procurado e quais resultados se pretendia alcançar, para assim, selecionar as bibliografias pertinentes. A questão norteadora possibilitou traçar um panorama da pesquisa e construir uma string de busca que definiu critérios de exclusão e inclusão de publicações dada a relevância acerca do tema.

Já na segunda etapa, a de revisão bibliográfica, buscou-se concentrar um maior número de trabalhos relacionados à Engenharia Social e aos desafios da Segurança da Informação no contexto de Internet das Coisas. No desenvolvimento dessa revisão bibliográfica, utilizou-se as bases de dados SpringerLink 1, ACM Digital Library 2, IEEE Digital Library 3, ISI Web Of Science 4, Science Direct 5 e Scopus. Esta etapa consolidou a revisão sistemática.

A terceira etapa consiste no desenvolvimento de um curso composto por cinco módulos cujo foco principal foi facilitar a identificação dos principais ataques de engenharia social em IoT

promovendo um estudo acerca dos tipos e técnicas de defesa, os quais , através de mecanismos de controle, possam ser usados para inibir comportamentos facilitadores referentes ao fator humano. Intercalados às aulas, foram aplicados formulários disponibilizados via Google forms, através do qual aferia-se o nível de conhecimento do aluno antes e depois da aplicação dos conteúdos.

A quarta etapa visa armazenar e disseminar o conteúdo elaborado na etapa anterior e consiste em um ambiente virtual, composto por 6 abas, dentre as quais disponibiliza-se o referido curso. A plataforma deverá ser atualizada periodicamente e alimentada com novos cursos e informações relevantes.

Para a validação da ferramenta ora desenvolvida, direcionou-se um formulário aplicado a gestores de TI, que buscou captar a opinião do público-alvo acerca da eficiência do curso oferecido pelo CIS. No quesito influenciador na conscientização dos usuários, no que diz respeito a proteção de dados, obteve-se retorno de 90% para sim e 10% para talvez. Esta avaliação permite concluir que se trata de uma ferramenta relevante, cuja utilização contribui com a segurança em Redes de Internet das Coisas e tecnologias similares.

8.1 Trabalhos Futuros

Nesta seção serão apresentadas algumas contribuições para trabalhos futuros.

São elas:

- Patentear e registrar a marca CIS;
- Elaborar e disponibilizar outros cursos e micro aulas;
- Promover lives em redes sociais sobre os temas propostos.

8.2 Produções Relacionadas

Nesta seção são apresentadas as produções relacionadas à dissertação.

- Artigo Submetidos e em Avaliação: Social Engineering and Defense Techniques: an approach on the level of the knowledge and awareness of the users of IoT devices;
- Artigos a serem submetidos: Desafios da Segurança no Contexto de Internet das Coisas: Um mapeamento Sistemático;

  Conscientização sobre a importância da Segurança da Informação;
- Portal CIS.

Referências

ALEXANDROV, V.; DESNITSKY, V.; CHALY, D. Design and security analysis of a fragment of internet of things telecommunication system. *Automatic Control and Computer Sciences*, Springer, v. 53, n. 7, p. 851–856, 2019. Citado 4 vezes nas páginas 12, 17, 18 e 34.

ANDRADE, R. O.; YOO, S. G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, Elsevier, v. 48, p. 102352, 2019. Citado na página 23.

ARABO, A. Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, Elsevier, v. 61, p. 227–232, 2015. Citado 2 vezes nas páginas 19 e 40.

ARAMUNI, J. P. C.; MAIA, L. C. O impacto da engenharia social na segurança da informação: uma abordagem orientada à gestão corporativa. *AtoZ: novas práticas em informação e conhecimento*, v. 7, n. 1, p. 31–37, 2020. Citado na página 25.

BELLI, L. *CyberBRICS: Cybersecurity regulations in the BRICS countries*. [S.l.]: Springer Nature, 2021. Citado na página 28.

BICKMAN, L.; ROG, D. J. *The SAGE handbook of applied social research methods*. [S.l.]: Sage publications, 2008. Citado 2 vezes nas páginas 30 e 42.

BOAVENTURA, E. M. *Metodologia da pesquisa: monografia, dissertação, tese*. [S.l.]: Atlas, 2004. Citado na página 29.

CAMPHOUSE, A.; NGALAMOU, L. Securing a connected home. In: IEEE. *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. [S.l.], 2019. p. 0250–0256. Citado 2 vezes nas páginas 18 e 21.

CARNEIRO, L. E. S.; ALMEIDA, M. B. Gestão da informação e do conhecimento no âmbito das práticas de segurança da informação: O fator humano nas organizações. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*, Universidade Federal de Santa Catarina, v. 18, n. 37, p. 175–202, 2013. Citado 2 vezes nas páginas 45 e 46.

CASTILHO, W. *Manual Do Detetive Virtual*. 2°. ed. Endereço: Matrix, 2012. (serie). ISBN 9788563536723. Citado na página 20.

CAVALLI, O. Internet das coisas e inovação na américa latina. *Sl: sn*, 2016. Citado na página 12.

CHANG, S.-I.; CHANG, L.-M.; LIAO, J.-C. Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, Elsevier, v. 57, n. 6, p. 103335, 2020. Citado na página 22.

COELHO, C. F.; RASMA, E. T.; MORALES, G. Engenharia social: uma ameaça à sociedade da informação. *Exatas & Engenharias*, Institutos Superiores de Ensino do Censa, v. 3, n. 05, 2013. Citado na página 24.

CÔRTE, K. Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos. 2014. Citado na página 45.

COSTA, L.; BARROS, J. P.; TAVARES, M. Vulnerabilities in iot devices for smart home environment. In: SCITEPRESS. *Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019*. [S.l.], 2019. v. 1, p. 615–622. Citado 3 vezes nas páginas 14, 19 e 35.

DANTAS, A. R. P. Cyrm: cyber range para auxiliar o ensino de defesa para alunos da disciplina de segurança da informação. 2022. Citado na página 26.

DONG, M. et al. Cloak: visible touching and invisible protecting: cloud privacy protection based on lsb and chaotic approach. In: IEEE. *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*. [S.l.], 2018. p. 225–229. Citado 3 vezes nas páginas 12, 13 e 35.

EIRAS, M. C. Engenharia social e estelionato eletrônico. *IBPI Internet School*, 2004. Citado na página 25.

GAMA, G. A. d. Design arquitetural de software aplicado a sistemas de larga escala: revisão de literatura cinzenta. 2022. Citado na página 30.

GARTNER. 4.9 billion connected"things"will be in use in 2015. *Gartner [online].[cit. 2015-11-09]. Dostupné z: http://www. gartner. com/newsroom/id/2905717*, p. 31, 2014. Citado na página 13.

GIL, A. C. Métodos e técnicas de pesquisa social. -são paulo: Editora atlas, 1999. gil, antónio carlos. *Métodos e Técnicas de Pesquisa social*, 2008. Citado na página 29.

GRAMMATIKIS, P. I. R.; SARIGIANNIDIS, P. G.; MOSCHOLIOS, I. D. Securing the internet of things: Challenges, threats and solutions. *Internet of Things*, Elsevier, v. 5, p. 41–70, 2019. Citado 2 vezes nas páginas 21 e 40.

GUNDUZ, M. Z.; DAS, R. Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, Elsevier, v. 169, p. 107094, 2020. Citado na página 22.

HABIBI, J. et al. Heimdall: Mitigating the internet of insecure things. *IEEE Internet of Things Journal*, IEEE, v. 4, n. 4, p. 968–978, 2017. Citado na página 23.

HADNAGY, C. *Social engineering: The art of human hacking*. [S.l.]: John Wiley & Sons, 2010. Citado na página 24.

HAMDI, Z. et al. A comparative review of isms implementation based on iso 27000 series in organizations of different business sectors. In: *Journal of Physics: Conference Series*. [S.l.: s.n.], 2019. v. 1339, n. 1, p. 012103. Citado na página 20.

HEARTFIELD, R.; LOUKAS, G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, Elsevier, v. 76, p. 101–127, 2018. Citado na página 40.

HENRIQUES, F. d. A. F. *A influência da Engenharia Social no fator humano das organizações*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2017. Citado 3 vezes nas páginas 43, 44 e 46.

HONÓRIO, T. J. O uso de ciberataques em eleições e as relações internacionais| the use of cyberattacks in elections and international relations. *Mural Internacional*, v. 9, n. 1, p. 85–98, 2018. Citado na página 27.

JACOBSSON, A.; BOLDT, M.; CARLSSON, B. A risk analysis of a smart home automation system. *Future Generation Computer Systems*, Elsevier, v. 56, p. 719–733, 2016. Citado na página 23.

JINHONG, Y.; CHUL-SOO, K.; ONIK, M. M. H. Aggregated risk modelling of personal data privacy in internet of things. In: IEEE. *2019 21st International Conference on Advanced Communication Technology (ICACT)*. [S.l.], 2019. p. 425–430. Citado na página 22.

JÚNIOR, J. V. C. Ambiente de análise de ameaças para geração de inteligência de ameaças usando fontes abertas. 2018. Citado na página 26.

JUNIOR, S. L. S.; FARINELLI, F. A. *DOMÓTICA-Automação Residencial e Casas Inteligentes com Arduíno e ESP8266*. [S.l.]: Saraiva Educação SA, 2018. Citado na página 14.

KETTANI, H.; CANNISTRA, R. M. On cyber threats to smart digital environments. In: *Proceedings of the 2nd International Conference on Smart Digital Environment*. [S.l.: s.n.], 2018. p. 183–188. Citado 2 vezes nas páginas 22 e 40.

KITCHENHAM, B. Procedures for performing systematic reviews. *Keele, UK, Keele University*, v. 33, n. 2004, p. 1–26, 2004. Citado 2 vezes nas páginas 30 e 38.

KLOBAS, J. E.; MCGILL, T.; WANG, X. How perceived security risk affects intention to use smart home devices: A reasoned action explanation. *Computers & Security*, Elsevier, v. 87, p. 101571, 2019. Citado na página 19.

KUMAR, A.; CHAUDHARY, M.; KUMAR, N. Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology*, Citeseer, v. 2, n. 11, p. 15–19, 2015. Citado 2 vezes nas páginas 44 e 45.

LALLIE, H. S. et al. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, Elsevier, v. 105, p. 102248, 2021. Citado 2 vezes nas páginas 25 e 40.

LEE, H. Home iot resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics*, Elsevier, v. 49, p. 101377, 2020. Citado na página 22.

LEMOS, A.; MARQUES, D. Questoes sobre privacidade na internet das coisas. In: *Congresso do INCT. DD*. [S.l.: s.n.], 2018. Citado na página 17.

LIMA, F. S. et al. Vpn: Uma solução prática e economicamente viável. *TECNOLOGIAS EM PROJEÇÃO*, v. 4, n. 1, p. 30–40, 2013. Citado na página 28.

LOUREÇO, R. M.; DUARTE, R. P. Gestão de segurança da informação. 004, 2020. Citado na página 18.

LYRA, M. R. et al. Segurança e auditoria em sistemas de informação. *Rio de Janeiro: Ciência Moderna*, 2008. Citado na página 20.

MACHADO, J.; BIONI, B. R. et al. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso do "nota fiscal paulista"| protection of personal data in programs for tax-evasion prevention by collecting invoices: the case of são paulo. *Liinc em Revista*, Instituto Brasileiro de Informação em Ciência e Tecnologia, v. 12, n. 2, 2016. Citado na página 28.

MAGRANI, E. A internet das coisas. 1ª edição. *Rio de Janeiro: Editora FGV*, 2018. Citado 3 vezes nas páginas 12, 13 e 24.

MAHAINI, M. I.; LI, S.; SAĞLAM, R. B. Building taxonomies based on human-machine teaming: Cyber security as an example. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. [S.l.: s.n.], 2019. p. 1–9. Citado 2 vezes nas páginas 21 e 40.

MAVROPOULOS, O. et al. Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks*, Elsevier, v. 92, p. 101743, 2019. Citado na página 22.

MITNICK, K. D.; SIMON, W. L. *The art of deception: Controlling the human element of security*. [S.l.]: John Wiley & Sons, 2003. Citado na página 24.

MORAES, I. H. S. d.; PRADO, L. A. Saúde coletiva e uma escolha de sofia: defender a privacidade no ciberespaço. *Ciência & Saúde Coletiva*, SciELO Brasil, v. 23, p. 3267–3276, 2018. Citado na página 28.

MOURA, T. M.; NEVES, J. E. D. Análise de segurança em dispositivos internet das coisas. *Revista Interface Tecnológica*, v. 18, n. 2, p. 15–27, 2021. Citado na página 28.

OLIVEIRA, R. S. d. Engenharia social e segurança da informação: análise das questões relacionadas ao uso das redes sociais online. Niterói, 2019. Citado 3 vezes nas páginas 43, 45 e 46.

PASCHOAL, D. A. C.; PEREIRA, G. F. Segurança da informação na indústria 4.0: framework nist. Faculdade de Tecnologia de Americana, 2019. Citado na página 26.

PEIXOTO, M. C. P. Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações. *Monografia (Bacharelado)–Curso de Ciência da Computação–Pró-Reitoria de Ensino de Graduação do Centro Universitário do Triângulo. Uberlândia: Unitri*, 2004. Citado na página 24.

PETERSEN, K. et al. Systematic mapping studies in software engineering. In: *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*. [S.l.: s.n.], 2008. p. 1–10. Citado na página 30.

PINHEIRO, A. D. A influência da internet das coisas para a guerra cibernética. 2018. Citado na página 27.

PINHEIRO, P. P. *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD*. [S.l.]: Saraiva Educação SA, 2020. Citado na página 28.

PINZÓN, J. J. S. et al. La ingeniería social, el antes y el ahora de un problema global. Universidad Nacional Abierta ya Distancia UNAD, 2015. Citado na página 27.

PLACHKINOVA, M.; MENARD, P. An examination of gain-and loss-framed messaging on smart home security training programs. *Information Systems Frontiers*, Springer, p. 1–22, 2019. Citado 2 vezes nas páginas 14 e 36.

QUSA, H. et al. Secure smart home using open security intelligence systems. In: IEEE. *2019 Sixth HCT Information Technology Trends (ITT)*. [S.l.], 2019. p. 12–17. Citado 4 vezes nas páginas 13, 18, 24 e 36.

RAFFERTY, L. et al. Intelligent multi-agent collaboration model for smart home iot security. In: IEEE. *2018 IEEE International Congress on Internet of Things (ICIOT)*. [S.l.], 2018. p. 65–71. Citado na página 23.

RIBEIRO, R. M. O. et al. Segurança em iot: simulação de ataque em uma rede rpl utilizando contiki. Universidade Federal de Uberlândia, 2018. Citado na página 18.

ROSNER, G. *Privacy and the Internet of Things*. [S.l.]: O'Reilly Media, Incorporated, 2016. Citado na página 12.

SANTOS, M. de C. *O Sucesso Empresarial baseado na Gestão de Segurança da Informação*. [S.l.], 2019. Citado na página 20.

SANTOS, N. d. S. dos et al. Um objeto de aprendizagem sobre medidas de prevenção na internet: conscientização do usuário. In: SBC. *Anais do XX Workshop de Informática na Escola*. [S.l.], 2014. p. 562–565. Citado 3 vezes nas páginas 43, 44 e 46.

SILVA, A. G. d.; MESQUITA, A. R. d. S.; PAIVA, C. E. Tecnologias e ferramentas para prevenção de ataques em redes de computadores. 109, 2018. Citado 2 vezes nas páginas 43 e 44.

SILVA, N. B. X.; ARAÚJO, W. J. d.; AZEVEDO, P. M. d. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. *Revista Ibero-Americana de Ciência da Informação*, v. 6, n. 2, 2013. Citado na página 25.

SILVA, S. M. Trabalho de conscientização sobre segurança da informação no uso de redes sociais aos alunos da aprendizagem insdustrial senai itajaí/sc. 2020. Citado 2 vezes nas páginas 43 e 44.

SILVEIRA, D. T.; CÓRDOVA, F. P. A pesquisa científica. *Métodos de pesquisa. Porto Alegre: Editora da UFRGS, 2009. p. 33-44*, 2009. Citado na página 29.

SOUZA, G. M. d. Implantação de ferramenta livre para controle e segurança de rede local. Universidade Tecnológica Federal do Paraná, 2018. Citado na página 27.

SOUZA, R. C. de; FERNANDES, J. H. C. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. *Brazilian Journal of Information Science: research trends*, v. 10, n. 1, 2016. Citado na página 25.

SPANOS, G. et al. Combining statistical and machine learning techniques in iot anomaly detection for smart homes. In: IEEE. *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. [S.l.], 2019. p. 1–6. Citado 4 vezes nas páginas 18, 19, 21 e 23.

VERISIGN. Tendências e ameaças técnicas. *Verisign iDefense Security Intelligence Service*, 2016. Citado 2 vezes nas páginas 44 e 45.

VINUTO, J. A amostragem em bola de neve na pesquisa qualitativa. *Um Debate em*, 2016. Citado na página 42.

VOLKMANN, T. B. Implantação de sistema iot para automação residencial e irrigação de jardins. 2022. Citado na página 17.

WARAGA, O. A. et al. Design and implementation of automated iot security testbed. *Computers & Security*, Elsevier, v. 88, p. 101648, 2020. Citado na página 26.

WEN, M. et al. Understanding floss through community publications: strategies for grey literature review. In: IEEE. *2020 IEEE/ACM 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*. [S.l.], 2020. p. 89–92. Citado na página 31.

YANG, H.; LEE, H.; ZO, H. User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems*, Emerald Publishing Limited, 2017. Citado na página 40.

YIĞIT, B. et al. Cost-aware securing of iot systems using attack graphs. *Ad Hoc Networks*, Elsevier, v. 86, p. 23–35, 2019. Citado 2 vezes nas páginas 21 e 40.

ZHOU, W. et al. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 2, p. 1606–1616, 2018. Citado 2 vezes nas páginas 19 e 40.

Apêndices

APÊNDICE A – Questionário 1

Formulário 01

Formulário avaliativo

*Obrigatório

1. Nome completo: *

2. e-mail *

3. Idade (faixa etária) *

Marcar apenas uma oval.

- ◯ menos de 18
- ◯ 18 a 25
- ◯ 26 a 33
- ◯ 24 a 41
- ◯ 42 ou mais

4. Qual seu nível de conhecimento em Segurança da Informação: *

Marcar apenas uma oval.

- ◯ nenhum
- ◯ pouco
- ◯ mediano
- ◯ bom
- ◯ excelente

5. Em qual nível você avalia seu conhecimento em relação a Tecnologia da informação? *

Marcar apenas uma oval.

- ◯ nenhum
- ◯ pouco
- ◯ razoável
- ◯ bom
- ◯ excelente

6. Com que frequência você utiliza redes sociais? *

Marcar apenas uma oval.

- ◯ nunca
- ◯ raramente
- ◯ às vezes
- ◯ quase sempre
- ◯ sempre

7. Com que frequência você publica informações pessoais nas redes sociais ? *

Marcar apenas uma oval.

- ◯ nunca
- ◯ raramente
- ◯ às vezes
- ◯ quase sempre
- ◯ sempre

8. Você já recebeu algum contrato através de email, chamadas telefônicas, SMS ou WhatsApp e desconfiou que tenha sido um "trote" para capturar informações suas? *

Marcar apenas uma oval.

- ◯ sim
- ◯ não
- ◯ não lembro

9. Você utiliza datas comemorativas como senhas? *

Marcar apenas uma oval.

- ◯ nunca
- ◯ raramente
- ◯ às vezes
- ◯ quase sempre
- ◯ sempre

10. Você já ouviu falar sobre Engenharia Social? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

11. Com suas palavras defina o que você acredita ser Engenharia Social? *

_____

_____

APÊNDICE B – Questionário 2

Formulário 02

Formulário avaliativo.

*Obrigatório

1. Nome completo: *

2. e-mail *

3. Qual o nível de consciência que você possui a respeito de potencial ameaça de ataques de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Nunca ouvir falar
- ◯ Pouco consciente
- ◯ Já ouvi falar, mas não dei muita importância ao tema
- ◯ Muito consciente
- ◯ Totalmente consciente

4. Você já sofreu algum ataque de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento

5. Qual sua opinião em relação a motivação por trás de ataques de Engenharia Social: *

Marcar apenas uma oval.

- ◯ Ganhos financeiros
- ◯ Vingança
- ◯ Acesso a informações privilegiadas
- ◯ Outro: _____

6. Em sua opinião que tipo de pessoa é mais suscetível a ataques de Engenharia Social? *

_____

7. Conhece alguém que já foi vítima de Engenharia Social (fraudes eletrônicas, golpes, vazamento, de informações, etc) *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

8. Você acessa suas redes sociais usando Internet pública (Universidade,shopping, bar, restaurantes, rodoviárias) *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

9. Você desconfia de mensagens atrativas recebidas em mídias sociais? *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

APÊNDICE C – Questionário 3

Formulário 03

Formulário avaliativo.

*Obrigatório

1. Nome completo: *

2. e-mail: *

3. Você fornece dados financeiros ou informações pessoais em mídias sociais? *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

4. Você utiliza recursos de privacidade (marcação de pessoas, verificação de duas etapas? *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

5. Você altera o nome de usuário e senha padrão dos dispositivos de internet? *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

6. Antes de comprar um novo dispositivo você busca ter informações sobre o nível de proteção e segurança? *

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Muitas vezes
- ◯ Sempre

7. Todos seus dispositivos (computadores, Smartphones...) são protegidos por senha? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

8. Você sabia que a troca de senhas a cada seis meses aumenta a segurança de forma significativa? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

9. Você sabe identificar um link fraudulento? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

10. Quando você utiliza tecnologia, quais medidas de segurança considera importantes para evitar ser alvo de criminosos? *

APÊNDICE D – Termo de Consentimento Livre e Esclarecido (T.C.L.E.)

Este formulário, tem como objetivo, coletar informações para validar o uso do Checklist IoT Security (CIS) como ferramenta de auxilio no que diz respeito a utilizar técnicas de Segurança da Informação, que será desenvolvida durante uma pesquisa de mestrado do programa de Pós Graduação em Ciencia da Computação da Universidade Federal de Sergipe (DCOMP/UFS) como requisito parcial para a obtenção do título de Mestrado em Ciência da Computação.

A(O) sra. (sr.) está sendo convidado(a) a participar desta pesquisa que tem como finalidade validar o uso do portal CIS - Checklist IoT Security , que tem como objetivo ser um espaço onde os usuário de tecnologias, IoT entre outras, possam conhecer melhores práticas de uso, para assim se sentirem mais seguros em rede, surgiu da observação que há poucos estudos sobre o comportamento do usuário em relação a Segurança da Informação. Ao participar deste estudo a(o) sra. (sr.) irá colaborar com os orientadores Prof. Dr. Admilson de Ribeiro Lima Ribeiro, Prof. Dr. Gilton José Ferreira da Silva, e discente Maiara de Castro Santos na validação do material desenvolvido durante uma pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação - PROCC/UFS da aluna Maiara de Castro Santos para aplicação em pesquisas futuras. O presente formulário tomará um tempo médio entre 10 e 16 minutos para ser respondida. Ao conciliar em responder as seguintes questões, a (o) sra (sr.) tem liberdade de se recusar a participar e ainda se continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo para a(o) sra. (sr.). Sempre que quiser pedir mais informações sobre a pesquisa por meio do e-mail maiaracs@dcomp.ufs.br. As informações coletadas neste estudo serão tratadas como confidenciais, somente a aluna e orientadores terão conhecimento dos dados. Ao participar desta pesquisa a sra. (sr)não terá nenhum benefício direto nem prejuízos. Entretanto, esperamos que este estudo tenha informações sobre a utilização de Técnicas de Segurança da Informação importante de forma que o conhecimento que será construído a este material pode auxiliar na utilização destas para auxílio de prática.

APÊNDICE E – Questionário - Avaliação CIS

Avaliação CIS

Este formulário, tem como objetivo, coletar informações para validar o uso doChecklist IoT Security (CIS) como ferramenta de auxilio no que diz respeito a utilizar técnicas de Segurança da Informação, que será desenvolvida durante uma pesquisa de mestrado do programa de Pós Graduação em Ciencia da Computação da Universidade Federal de Sergipe (DCOMP/UFS) como requisito parcial para a obtenção do título de Mestrado em Ciência da Computação.

*Obrigatório

1. A(O) sra. (sr.) está sendo convidado(a) a participar desta pesquisa que tem como finalidade validar o uso do portal CIS - Checklist IoT Security , que tem como objetivo ser um espaço onde os usuário de tecnologias, IoT entre outras, possam conhecer melhores práticas de uso, para assim se sentirem mais seguros em rede, surgiu da observação que há poucos estudos sobre o comportamento do usuário em relação a Segurança da Informação. Ao participar deste estudo a(o) sra. (sr.) irá colaborar com os orientadores Prof. Dr. Admilson de Ribeiro Lima Ribeiro, Prof. Dr. Gilton José Ferreira da Silva, e discente Maiara de Castro Santos na validação do material desenvolvido durante uma pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação - PROCC/UFS da aluna Maiara de Castro Santos para aplicação em pesquisas futuras. O presente formulário tomará um tempo médio entre 10 e 16 minutos para ser respondida. Ao conciliar em responder as seguintes questões, a (o) sra (sr.) tem liberdade de se recusar a participar e ainda se continuar participando em qualquer fase da pesquisa, sem qualquer prejuízo para a(o) sra. (sr.). Sempre que quiser pedir mais informações sobre a pesquisa por meio do e-mail maiaracs@dcomp.ufs.br. As informações coletadas neste estudo serão tratadas como confidenciais, somente a aluna e orientadores terão conhecimento dos dados. Ao participar desta pesquisa a sra. (sr)não terá nenhum benefício direto nem prejuízos. Entretanto, esperamos que este estudo tenha informações sobre a utilização de Técnicas de Segurança da Informação importante de forma que o conhecimento que será construído a este material pode auxiliar na utilização destas para auxílio de prática. *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

Identificação do Usuário

2. Nome e e-mail *

3. Qual sua faixa etária? *

Marcar apenas uma oval.

- 18 a 25 anos
- 26 a 33 anos
- 34 a 41anos
- 42 a 49 anos
- 50 anos ou mais

4. Qual seu último nível de escolaridade completo ? *

Marcar apenas uma oval.

- 1º Grau Completo (Fundamental)
- 2º Grau Completo (Ensino Médio)
- Superior
- Especialização
- Mestrado
- Doutorado
- Pós Doutorado

5. Em qual cidade / estado você mora: *

6. Em qual cidade / estado sua empresa ou filial está localizada: *

_____

Identificação da Empresa

7. Qual das opções descreve a área de atuação principal da sua empresa? *

Marcar apenas uma oval.

- ◯ Agricultura
- ◯ Alimentício e de bebidas
- ◯ Automobilístico
- ◯ Comércio e logística
- ◯ Construção
- ◯ Educação
- ◯ Eletrônicos
- ◯ Energia e extração
- ◯ Entretenimento e Lazer
- ◯ Governamental
- ◯ ONGs
- ◯ Publicidade e marketing
- ◯ Saúde e farmacêutico
- ◯ Seguros
- ◯ Serviços de utilidade pública
- ◯ Serviços financeiros
- ◯ Serviços imobiliários
- ◯ Tecnologia da informação
- ◯ Telecomunicações
- ◯ Transporte aéreo e indústria aeroespacial (incluindo defesa)
- ◯ Transporte e entrega
- ◯ Varejo e bens duráveis de consumo
- ◯ Outros.
- ◯ Outro: _____

8. Como você classifiqua a empresa que trabalha quanto ao porte: *

Marcar apenas uma oval.

- ◯ Microempresa
- ◯ Pequena empresa
- ◯ Média empresa
- ◯ Grande empresa

Conhecimentos sobre Segurança da Informação

9. Quanto possui de conhecimento em relação a Segurança da Informação em sua empresa? *

Marcar apenas uma oval.

- ◯ Nenhum conhecimento
- ◯ Pouco conhecimento
- ◯ Conhecimento mediano
- ◯ Bom conhecimento
- ◯ Total conhecimento

10. Quanto possui de conhecimento acerca de normas de Segurança da Informação relacionadas à atividade na empresa? *

Marcar apenas uma oval.

- ◯ Nenhum conhecimento
- ◯ Pouco conhecimento
- ◯ Conhecimento mediano
- ◯ Bom conhecimento
- ◯ Total conhecimento

11. Conhece as informações que devem ser protegidas na empresa em que trabalha? *

Marcar apenas uma oval.

- ◯ Nenhum conhecimento
- ◯ Pouco conhecimento
- ◯ Conhecimento mediano
- ◯ Bom conhecimento
- ◯ Total conhecimento

12. Sua empresa realiza treinamento de conscientização em Segurança da Informação para funcionários e parceiros de negócio? *

Marcar apenas uma oval.

- ◯ Não existe política de treinamentos em Segurança da Informação
- ◯ Existe projeto para realizar treinamentos em Segurança da Informação
- ◯ Existe um processo definido e totalmente aplicado de treinamentos em Segurançada Informação

13. Você tem percepção que o assunto "Segurança da Informação" é debatido de forma estratégica na sua empresa? *

Marcar apenas uma oval.

- ◯ Não.A empresa não dá a importância devida .
- ◯ Não. Mas a empresa já possui planos para tratar o assunto.
- ◯ Desconheço.
- ◯ Sim. O assunto é debatido mas não sai do papel
- ◯ Sim. É tratado com importância total

Conhecimentos sobre Engenharia Social

14. Você recebeu nos últimos 6 meses algum contato através de email , chamadas telefônicas ou SMS e desconfiou que tenha sido um "trote" para capturar informações suas? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não lembro

15. Você publica informações pessoais nas redes sociais?

Marcar apenas uma oval.

- ◯ Nunca
- ◯ Raramente
- ◯ Ocasionalmente
- ◯ Frequentemente
- ◯ Sempre

16. Você já tinha ouvido falar no termo "Engenharia Social"? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não tenho certeza

17. Conhece alguém que já foi vítima de Engenharia Social? (Fraudes Eletrônicas,Golpes, Vazamento de Informações, etc) *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

18. Qual o nível de consciência que você possui a respeito de potenciais ameaças de ataques de Engenharia Social ? *

Marcar apenas uma oval.

- ◯ Nunca ouvi falar em Engenharia Social
- ◯ Pouco consciente
- ◯ Já ouvi falar mas não dou importância ao tema.
- ◯ Muito consciente
- ◯ Totalmente consciente

19. Sua organização já sofreu algum ataque de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não tenho conhecimento.

20. Na sua opinião, qual a motivação por trás de ataques de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Ganhos financeiros
- ◯ Acesso a informações privilegiadas
- ◯ Vantagem competitiva
- ◯ Vingança Pessoal
- ◯ Outro: _____

21. Na sua opinião, que tipo de pessoal é o mais suscetível a ataques de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Novos empregados
- ◯ Terceirizados
- ◯ Assistentes Executivos
- ◯ Pessoal de TI
- ◯ Alta diretoria

22. Na sua opinião qual é a fonte mais comum de ataques de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Phishing (E-mails Falsos)
- ◯ Internet / Redes Sociais
- ◯ Contatos Telefônicos Abordagem Pessoal
- ◯ Outro: _____

23. O que sua organização está fazendo para prevenir ataques de Engenharia Social? *

Marcar apenas uma oval.

- ◯ Promovendo treinamentos de Segurança de Informação com os empregados.
- ◯ A política de segurança inclui direcionamentos para prevenir ataques de Engenharia Social.
- ◯ Atualmente nada, mas temos planos de fazer.
- ◯ Não estamos fazendo nada, nem temos plano de fazer.
- ◯ Outro: _____

Na sua opinião, qual o nível de importância dos seguintes meios de proteção contra a Engenharia Social.

24. Treinamento de funcionários e terceirizados em Segurança da Informação *

Marcar apenas uma oval.

	1	2	3	4	5	
Menos importante	◯	◯	◯	◯	◯	mais importante

25. Definir Políticas de Segurança *

Marcar apenas uma oval.

	1	2	3	4	5	
Menos importante	◯	◯	◯	◯	◯	Mais importante

26. Investimento em Segurança Física *

Marcar apenas uma oval.

	1	2	3	4	5	
Menos importante	◯	◯	◯	◯	◯	Mais importante

27. Investimento em Firewalls (atua como um filtro entre um dispositivo e sua conexão com a internet ou com a rede externa), e outras ferramentas de Segurança *

Marcar apenas uma oval.

	1	2	3	4	5	
Menos importante	◯	◯	◯	◯	◯	Mais importante

28. Definir um Plano de Gerenciamento de Segurança *

Marcar apenas uma oval.

	1	2	3	4	5	
Menos importante	◯	◯	◯	◯	◯	Mais importante

Avaliação do CIS

29. Grau de facilidade em entender o conteúdo abordado no curso. *

Marcar apenas uma oval.

	1	2	3	4	5	
Muito fácil	◯	◯	◯	◯	◯	Muito Dificil.

30. Você acredita que o curso oferecido pelo CIS influencia de alguma forma na concientização dos usuários no que diz respeito a proteção de dados? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Talvez
- ◯ Não

31. A partir do conteúdo abordado, na sua opinião o que poderia melhorar ou ser fornecido? *