UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

APSEA: Um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social

Dissertação de Mestrado

Waldson Rodrigues Cardoso

São Cristóvão – Sergipe

2024

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Waldson Rodrigues Cardoso

APSEA: Um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social

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): Drº. Admilson de Ribamar Lima Ribeiro
Coorientador(a): Drº. João Marco Cardoso Silva

São Cristóvão – Sergipe

2024

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Cardoso, Waldson Rodrigues
C268a APSEA: Um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social / Waldson Rodrigues Cardoso ; orientador Admilson de Ribamar Lima Ribeiro. - São Cristóvão, 2024.
115 f.

Dissertação (mestrado em Ciência da Computação) – Universidade Federal de Sergipe, 2024.

1. Engenharia social. 2. Segurança da informação e criptografia. I. Ribeiro, Admilson de Ribamar Lima orient. II. Título.

CDU 004

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
COORDENAÇÃO DE PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Ata da Sessão Solene de Defesa da Dissertação do Curso de Mestrado em Ciência da Computação-UFS.
Candidato: Waldson Rodrigues Cardoso

Em 28 dias do mês de fevereiro do ano de dois mil e vinte quatro, com início às 14hs, realizou-se na Sala de Seminários do PROCC da Universidade Federal de Sergipe, na Cidade Universitária Prof. José Aloísio de Campos, a Sessão Pública de Defesa de Dissertação de Mestrado do candidato **Waldson Rodrigues Cardoso**, que desenvolveu o trabalho intitulado: ***"APSEA: Um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social"***, sob a orientação do Prof. Dr. **Admilson de Ribamar Lima Ribeiro.** A Sessão foi presidida pelo Prof. Dr. **Admilson de Ribamar Lima Ribeiro** (PROCC/UFS), que após a apresentação da dissertação passou a palavra aos outros membros da Banca Examinadora, Prof. Dr. **João Marco Cardoso da Silva (Uminho)** , posteriormente o Prof. Dr. **Igor Medeiros Vanderlei** (UFAPE) e, em seguida, Dr. **Gilton José Ferreira da Silva** (PROCC/UFS) . Após as discussões, a Banca Examinadora reuniu-se e considerou o mestrando (a) APROVADO "*(aprovado/reprovado)*". Atendidas as exigências da Instrução Normativa 05/2019/PROCC, do Regimento Interno do PROCC (Resolução 67/2014/CONEPE), e da Resolução nº 04/2021/CONEPE que regulamentam a Apresentação e Defesa de Dissertação, e nada mais havendo a tratar, a Banca Examinadora elaborou esta Ata que será assinada pelos seus membros e pelo mestrando.

Cidade Universitária "*Prof. José Aloísio de Campos*", 28 de fevereiro de 2024.

Prof. Dr. Admilson de Ribamar Lima Ribeiro
(PROCC/UFS)
Presidente

Documento assinado digitalmente
gov.br
GILTON JOSE FERREIRA DA SILVA
Data: 29/05/2024 10:49:57-0300
Verifique em https://validar.iti.gov.br

Prof. Dr.Gilton José Ferreira da Silva
(PROCC/UFS)
Examinador Interno

Documento assinado digitalmente
gov.br
IGOR MEDEIROS VANDERLEI
Data: 06/03/2024 14:34:50-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Igor Medeiros Vanderlei
(UFAPE)
Examinador Externo

Prof. Dr. João Marco Cardoso da Silva
(Uminho)
Examinador Externo

Documento assinado digitalmente
gov.br
WALDSON RODRIGUES CARDOSO
Data: 29/05/2024 11:21:01-0300
Verifique em https://validar.iti.gov.br

Waldson Rodrigues Cardoso
Candidato

"Albert Einstein disse uma vez: 'A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.' Com esta frase em mente, dedico este trabalho a todos aqueles que buscam o conhecimento e a inovação, contribuindo assim para expandir as fronteiras do entendimento humano. Cada pesquisa é uma gota no oceano do saber, mas, juntas, essas gotas formam um mar de descobertas."

Agradecimentos

Primeiramente a Deus, por guiar meus passos neste e em todos os momentos da minha vida. Por ter me proporcionado saúde e forças para superar todos os obstáculos e alcançar a realização deste objetivo.

Aos meus pais, Rosa Meire Rodrigues Cardoso e José Walter Cardoso, pelo suporte, amor e ensinamentos de sempre. Ao meu irmão, Wagner Paixão Cardoso, por todo companheirismo e apoio.

A minha esposa e amiga, Ana Gleice. A sua gentileza, compreensão e amor foram a força motriz por trás de cada página escrita e de cada desafio superado durante este percurso. Obrigado por ser minha inspiração, meu porto seguro e minha eterna fonte de apoio.

A minha sogra, Maria, por seu carinho e acolhimento. Obrigado por estar sempre presente.

Ao meu orientador, Prof. Dr. Admilson de Ribamar Lima Ribeiro, por toda paciência, dedicação e conhecimento compartilhado. Saiba que tem todo meu respeito e agradecimento. Sem sua orientação, nada disso seria possível. E ao coorientador, João Marco Cardoso Silva, pelo apoio e contribuições ao longo deste percurso acadêmico.

Aos meus colegas de trabalho da AGIN, setor que integra o DETRAN/SE, que me acolheram e compreenderam sempre da melhor forma, possibilitando a realização desta conquista.

Aos meus amigos e familiares, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

A todos vocês, meu muito obrigado!

Resumo

Introdução: A crescente preocupação com a segurança da informação decorre dos riscos associados à disseminação de dados pessoais na Internet e ao aumento dos ataques de engenharia social, que exploram vulnerabilidades psicológicas. Esses ataques representam uma ameaça substancial para indivíduos e organizações, podendo resultar em prejuízos financeiros significativos. A abordagem para enfrentar a engenharia social envolve a conscientização de funcionários, e um sistema especialista se destaca como uma ferramenta valiosa para simular o raciocínio humano e fornecer recomendações baseadas nas interações do usuário. Esta dissertação é motivada pela necessidade premente de conscientizar as pessoas sobre as ameaças da engenharia social e fornecer mecanismos eficazes para proteger informações pessoais e organizacionais contra esses ataques. **Objetivo:** O objetivo principal é desenvolver um sistema especialista de segurança da informação, com foco em engenharia social, a fim de conscientizar usuários e prevenir vulnerabilidades. **Metodologia:** Esta pesquisa adota uma abordagem aplicada de desenvolvimento tecnológico, dividida em duas fases distintas. A primeira fase compreende o mapeamento sistemático, o estudo exploratório e a coleta de dados. Na segunda etapa, o foco é direcionado para o desenvolvimento do sistema, sendo validado por meio da aplicação de um questionário utilizando a escala *Likert* e análise dos dados resultantes. **Resultados:** Os resultados revelam a eficácia da metodologia adotada. O mapeamento sistemático proporcionou *insights* valiosos sobre os ataques de engenharia social, enquanto o sistema especialista foi validado para assegurar que atenda aos requisitos e expectativas dos usuários, especialmente no contexto de conscientização e prevenção de ameaças de engenharia social. A aplicação do questionário utilizando a escala *Likert* confirmou a aceitação positiva pelos usuários, solidificando a utilidade percebida do sistema. **Conclusão:** A avaliação conclusiva destaca a relevância da ferramenta desenvolvida, que se revela uma contribuição significativa para a estratégia de conscientização contra ameaças de engenharia social. Além de reafirmar os resultados obtidos, são discutidas as limitações do estudo, proporcionando um contexto mais abrangente, e são sugeridas possíveis direções para pesquisas futuras, visando a contínua melhoria da segurança da informação em um cenário dinâmico e desafiador.

Palavras-chave: Engenharia social, Vulnerabilidades, Segurança da informação, Sistema Especialista, Conscientização.

Abstract

Introduction: The growing concern for information security arises from the risks associated with the dissemination of personal data on the Internet and the increase in social engineering attacks, which exploit psychological vulnerabilities. These attacks represent a substantial threat to individuals and organizations, potentially resulting in significant financial losses. The approach to tackling social engineering involves raising employee awareness, and an expert system stands out as a valuable tool for simulating human reasoning and providing recommendations based on user interactions. This dissertation is motivated by the urgent need to raise awareness about social engineering threats and to provide effective mechanisms to protect personal and organizational information from these attacks. **Objective:** The main objective is to develop an expert system for information security, focusing on social engineering, in order to raise user awareness and prevent vulnerabilities. **Methodology:** This research adopts an applied technological development approach, divided into two distinct phases. The first phase comprises systematic mapping, exploratory study, and data collection. In the second stage, the focus is directed to the development of the system, being validated through the application of a questionnaire using the *Likert* scale and analysis of the resulting data. **Results:** The results demonstrate the effectiveness of the adopted methodology. The systematic mapping provided valuable insights into social engineering attacks, while the expert system was validated to ensure it meets the requirements and expectations of users, especially in the context of awareness and prevention of social engineering threats. The application of the questionnaire using the *Likert* scale confirmed the positive acceptance by users, solidifying the perceived usefulness of the system. **Conclusion:** The concluding assessment highlights the relevance of the developed tool, which proves to be a significant contribution to the strategy of raising awareness against social engineering threats. In addition to reaffirming the results obtained, the study discusses its limitations, providing a broader context, and suggests possible directions for future research, aiming at the continuous improvement of information security in a dynamic and challenging scenario.

Keywords: Social Engineering, Vulnerabilities, Information Security, Expert System, Awareness.

Lista de ilustrações

Lista de quadros

Lista de tabelas

Lista de abreviaturas e siglas

AGIN	Assessoria Geral de Tecnologia da Informação e Comunicação
APSEA	*Awareness and Prevention Expert System against Social Engineering Attacks*
CRUD	*Create, Read, Update and Delete*
DCOMP	Departamento de Computação
DETRAN/SE	Departamento Estadual de Trânsito de Sergipe
ES	Engenharia Social
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
IA	Inteligência Artificial
LDAP	*Lightweight Directory Access Protocol*
MER	Modelo Entidade e Relacionamento
MVC	Modelo-Visão-Controlador
UML	Unified Modeling Language
LGPD	Lei Geral de Proteção dos Dados Pessoais
UFS	Universidade Federal de Sergipe
SE	Sistema Especialista

Sumário

1

Introdução

A crescente importância da informação digital apresenta não apenas oportunidades, mas também riscos de segurança. A disseminação de plataformas de redes sociais permite que invasores coletem dados pessoais de funcionários por meio de suas pegadas *online*. As informações obtidas dessa maneira podem ser usadas para facilitar ataques a uma organização. À medida que os seres humanos tomam decisões e assumem responsabilidades, o fator humano está dando uma importante contribuição para o aspecto da segurança da informação. Mesmo as medidas de proteção técnica mais fortes são inúteis se um invasor puder influenciar os funcionários com sucesso (GRASSEGGER; NEDBAL, 2021).

A engenharia social é entendida no contexto da segurança da informação como uma manipulação psicológica e emocional das pessoas para que divulguem informações confidenciais (WILSON, 2018).

O ataque de engenharia social é o método de ataque mais comum usado por *hackers*. Para *hackear* um sistema e executar código malicioso, é necessário ter uma compreensão clara das vulnerabilidades presentes no sistema em questão. No entanto, com o uso de controles avançados, o sucesso desses tipos de ataques técnicos tem sido minimizado. Como resultado, os *hackers* têm recorrido a métodos alternativos, como a engenharia social, que busca explorar as vulnerabilidades psicológicas das pessoas e as potenciais vulnerabilidades técnicas de vários sistemas. Os ataques de engenharia social são agora considerados uma séria ameaça para pessoas e organizações (LEONOV et al., 2021).

De acordo com Astakhova e Medvedev (2020) nos ataques a clientes (pessoas jurídicas) de instituições financeiras, os invasores, via de regra, não utilizam ferramentas técnicas sofisticadas. Eles prestam muito mais atenção à preparação de ataques de uma perspectiva de engenharia social.

A engenharia social é uma técnica em desenvolvimento baseada no impacto psicológico em uma pessoa e seus “pontos fracos”. As consequências de ataques usando engenharia social

são caras para indivíduos, bem como para empresas e nações inteiras. Os prejuízos deles podem chegar a centenas de milhões de dólares, e surgem devido ao simples descuido e ingenuidade dos usuários dos sistemas de informação (LEONOV et al., 2021).

É a partir da necessidade do fortalecimento de mecanismos que auxiliem os indivíduos e as organizações contra ataques de engenharia social que essa dissertação é proposta. Em um primeiro momento, um mapeamento sistemático da literatura foi conduzido para investigar os principais ataques de engenharia social, bem como métodos e/ou técnicas de defesa utilizadas para evitar os desvios de informações de valor organizacional. Conforme o mapeamento realizado, foi percebido que atualmente a engenharia social vem se tornando uma das grandes ameaças à segurança da informação, sendo assim uma poderosa forma de invadir sistemas seguros. Porém, como forma de mitigar essas ameaças, os autores enfatizam os programas e treinamentos de conscientização do usuário humano.

Neste contexto, surge a necessidade de explorar abordagens inovadoras para combater a engenharia social. Um componente vital desse esforço é a implementação de um "Sistema Especialista de Segurança da Informação com foco em consientização contra ataques de engenharia social". O termo "sistema especialista"refere-se a um tipo de *software* inteligente que utiliza conhecimento especializado e regras para imitar o raciocínio humano em um domínio específico. Em outras palavras, é um recurso tecnológico projetado para resolver problemas complexos em um campo particular, como diagnóstico médico, suporte técnico ou análise financeira. No contexto desta dissertação, um sistema especialista pode ser uma ferramenta fundamental para conscientizar e treinar funcionários e colaboradores, capacitando-os a reconhecer e prevenir eficazmente ataques de engenharia social. A escolha dessa abordagem específica será explorada detalhadamente ao longo deste trabalho, respondendo à necessidade urgente de fortalecer as defesas organizacionais contra ameaças crescentes. (RUSSELL; NORVIG, 2010)

Além do aprimoramento na eficácia das defesas, a implementação de um sistema especialista pode oferecer benefícios financeiros substanciais para organizações. Ao reduzir os custos associados à realização de treinamentos extensivos e campanhas de conscientização, as organizações podem direcionar recursos para outras áreas críticas. Essa abordagem proativa não apenas fortalece a segurança contra ataques de engenharia social, mas também demonstra um compromisso com a eficiência operacional e o uso inteligente dos recursos disponíveis. A importância de adotar medidas proativas torna-se evidente diante das crescentes ameaças à segurança da informação, e a implementação de um sistema especialista representa um passo significativo na busca pela segurança abrangente de informações e recursos organizacionais.

1.1 Contextualização e justificativa do estudo

A introdução delineou de maneira abrangente a crescente importância da informação digital e os desafios de segurança associados, com foco especial nos riscos representados pelos

ataques de engenharia social. Este segmento se propõe a expandir e aprofundar esses aspectos, fornecendo uma contextualização mais detalhada e justificando a necessidade de explorar uma abordagem inovadora, representada pela implementação de um "Sistema Especialista em Segurança da Informação com foco em conscientização contra ataques de engenharia social".

1.1.1 Ampliando o Contexto

Como observado na introdução, a disseminação de plataformas de redes sociais e a crescente interconectividade digital criaram um ambiente propício para a coleta de dados pessoais por invasores. A análise desses dados é frequentemente utilizada como uma etapa inicial para a realização de ataques a organizações, aproveitando-se das vulnerabilidades não apenas dos sistemas técnicos, mas, crucialmente, do fator humano. O entendimento dessa dinâmica complexa é vital para formular estratégias eficazes de defesa.

1.1.2 Justificativa para a Escolha do Sistema Especialista

A decisão de propor um "Sistema Especialista em Segurança da Informação"como componente central deste estudo é fundamentada na necessidade de uma resposta mais avançada e proativa aos desafios impostos pela engenharia social. Este sistema, baseado em inteligência artificial e conhecimento especializado, visa oferecer uma abordagem atual para conscientizar e treinar indivíduos, capacitando-os a reconhecer e prevenir ataques dessa natureza.

A escolha de um Sistema Especialista em Segurança da Informação é respaldada pela necessidade de uma resposta avançada e proativa à engenharia social. Embora outras abordagens, como treinamento convencional e medidas de segurança tecnológica, tenham sido consideradas, um sistema baseado em inteligência artificial e conhecimento especializado oferece uma solução inovadora para conscientização e prevenção de ataques, destacando-se pela capacidade de adaptar-se dinamicamente às ameaças em constante evolução e de fornecer orientações personalizadas aos usuários, fundamentais na mitigação eficaz dos riscos associados à engenharia social.

Ao expandir e aprofundar esses pontos, buscamos consolidar a base teórica e prática que sustenta esta pesquisa, demonstrando sua relevância em face das crescentes ameaças à segurança da informação.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo principal é desenvolver um sistema especialista de segurança da informação, com foco em engenharia social, a fim de conscientizar usuários e prevenir vulnerabilidades.

1.2.2 Objetivos Específicos

Para possibilitar a realização do objetivo geral, podemos enumerar os seguintes objetivos específicos:

- Identificar e categorizar os estudos existentes sobre o tipo de organização que mais aparece como alvo de ataques de engenharia social, os seus principais ataques, bem como analisar métodos e/ou técnicas de defesa;
- Construir uma base de conhecimento a cerca das ameaças de engenharia social;
- Desenvolver um sistema que ajude a conscientizar os usuários sobre as técnicas de engenharia social, prevenir ataques e diagnosticar vulnerabilidades relacionadas a esse tipo de ameaça, contribuindo para a melhoria da segurança da informação em uma organização.
- Realizar a validação do sistema desenvolvido por meio da aplicação de um questionário utilizando a escala *Likert*.

1.3 Estrutura da dissertação

Para além deste capítulo introdutório, esta dissertação de mestrado apresenta mais 9 capítulos. Esses capítulos são descritos a seguir:

- Capítulo 2 - Fundamentação teórica: que consiste na revisão de literatura pertinente a estudos que envolvem Segurança da Informação, Engenharia Social e Sistemas Especialistas;
- Capítulo 3 - Metodologia, métodos e materiais utilizados na elaboração da pesquisa;;
- Capítulo 4 - Trabalhos relacionados: demonstra os trabalhos correlatos de acordo com o mapeamento sistemático, bem como são apresentados os resultados desse mapeamento e a síntese do processo de sumarização dos trabalhos estudados;
- Capítulo 5 - Uma Exploração Abrangente de Estratégias de Conscientização Contra Ataques de Engenharia Social;
- Capítulo 6 - Projeto do APSEA: base de conhecimento, representação do conhecimento, aquisição e formação do conhecimento, definição das perguntas, definição das regras, mecanismo de inferência, interface de interação com usuário, modelagem do sistema, arquitetura e funcionamento do sistema, e por fim as funcionalidades;
- Capítulo 7 - Implementação: protótipos, CRUD dos registros, validações, e por fim a apresentação do APSEA com a explicação das principais telas do sistema;
- Capítulo 8 - Validação do APSEA: local do estudo e procedimento da aplicação do questionário *Likert*;

- Capítulo 9 - Resultados e Discussões;
- Capítulo 10 - Conclusão: síntese dos resultados obtidos, trabalhos futuros, limitações, e por fim contribuições e produções relacionadas.

2

Fundamentação teórica

2.1 Segurança da Informação

A informação é um dos ativos mais valiosos nas organizações, porque as organizações dependem da informação para operar e tomar as decisões corretas. Para proteger informações confidenciais, muitas organizações seguem padrões e práticas recomendadas, como ISO27001, ISO27002, COBIT, etc. Embora tais medidas ajudem a controlar o acesso e manter as informações protegidas até certo ponto, as violações de segurança da informação, a invasão de redes/armazenamento de computadores das organizações para roubar informações continuam, porque os processos são executados por pessoas e as pessoas são o elo mais fraco, quando trata de segurança em uma organização (OSUAGWU et al., 2015).

Pode-se definir Segurança da Informação como a "Área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

A norma NBR ISO 27002 define da seguinte forma: "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A definição geral de segurança da informação, de acordo Werlinger et al. (2009), compreende disponibilidade, integridade e confidencialidade. A segurança cibernética inclui dimensões adicionais, que se estendem além dos limites formais da segurança da informação, incluindo humanos em sua capacidade pessoal e a sociedade em geral.

A Internet e a tecnologia da informação influenciaram significativamente a vida humana. No entanto, a segurança da informação ainda é uma preocupação importante para usuários e organizações. A tecnologia não pode apenas garantir um ambiente seguro para as informações;

os aspectos humanos da segurança da informação devem ser levados em consideração, além dos aspectos tecnológicos. A falta de conscientização sobre segurança da informação, ignorância, negligência, apatia, malícia e resistência são as raízes dos erros dos usuários (Sohrabi Safa; Von Solms; FURNELL, 2016).

As violações de segurança da informação não apenas acarretam custos extras para as organizações, mas também afetam significativamente sua reputação. O comportamento adequado de segurança da informação, além dos aspectos tecnológicos da segurança da informação, mitiga o risco de falhas de segurança da informação nas organizações (Sohrabi Safa; Von Solms; FURNELL, 2016).

A segurança da informação é uma área crucial para proteger os recursos de uma organização contra ameaças potenciais. Para compreender adequadamente esse campo, é essencial definir alguns conceitos fundamentais.

Primeiramente, a vulnerabilidade pode ser definida como uma fraqueza em um sistema de segurança que pode ser explorada por ameaças para causar danos ou violações de segurança (WHITMAN; MATTORD, 2019). Por outro lado, o risco refere-se à probabilidade de que uma vulnerabilidade seja explorada por uma ameaça, resultando em um impacto negativo para um sistema ou organização (STALLINGS; BROWN, 2015).

Os ataques, por sua vez, são ações deliberadas realizadas por ameaças com o objetivo de explorar uma vulnerabilidade e comprometer a segurança de um sistema, rede ou organização (NIST, 2020). Por fim, um incidente de segurança é qualquer evento que comprometa, ou tenha o potencial de comprometer, a confidencialidade, integridade ou disponibilidade de informações ou recursos de uma organização (ISO/IEC, 2019).

Essas definições fornecem uma base sólida para a compreensão dos desafios enfrentados na área de segurança da informação e destacam a importância de implementar medidas eficazes para mitigar os riscos associados.

2.1.1 Política de Segurança da Informação (ISP)

Para operacionalizar e formalizar a implementação dessas práticas de segurança, as organizações desenvolvem a chamada Política de Segurança da Informação (ISP). Essa política serve como um compêndio formalizado de procedimentos, diretrizes, funções e responsabilidades que direcionam as ações dos funcionários no que tange à preservação e ao uso apropriado dos recursos de informação e tecnologia da organização (ALASSAF; ALKHALIFAH, 2021).

Contudo, a mera elaboração da ISP não garante, por si só, a proteção efetiva dos ativos organizacionais. A conformidade com a Política de Segurança da Informação (ISP) emerge como fator crucial nesse contexto. Refere-se à extensão em que os colaboradores aderem às diretrizes delineadas na ISP para salvaguardar os ativos de informação e tecnologia. Estudos, como o realizado por Alassaf e Alkhalifah (2021), ressaltam que o não cumprimento da ISP figura como

um dos fatores preponderantes em violações de segurança, podendo culminar na interrupção das operações organizacionais.

Portanto, a eficácia da ISP não reside apenas em sua formulação abrangente, mas, sobretudo, no comprometimento e na observância por parte dos funcionários. Além disso, a gestão de riscos desempenha um papel fundamental na manutenção da segurança da informação. Identificar, avaliar e mitigar riscos potenciais são atividades contínuas que contribuem significativamente para a eficácia da ISP.

Adicionalmente, é essencial estabelecer mecanismos de monitoramento e auditoria regulares para garantir a conformidade contínua com a ISP. Isso envolve a revisão constante das políticas, a avaliação da eficácia dos controles implementados e a adaptação às mudanças no ambiente de segurança da informação.

Além disso, a comunicação transparente sobre as políticas de segurança da informação, bem como as consequências do não cumprimento, é crucial para promover a compreensão e a responsabilidade entre os membros da organização. Iniciativas educativas contínuas, *workshops* e simulações de incidentes podem fortalecer ainda mais a conscientização e preparar os funcionários para lidar com ameaças em constante evolução.

Assim, a conformidade com a ISP não apenas reforça a segurança organizacional, mas também representa uma abordagem essencial para mitigar ameaças à segurança da informação, promovendo uma cultura de responsabilidade e conscientização em todos os níveis da organização.

2.1.2 Lei Geral de Proteção de Dados Pessoais - LGPD

Atualmente, muitas organizações fazem uso dos dados pessoais de seus usuários. Dados pessoais são o conjunto de informações que podem levar à identificação de uma determinada pessoa e, portanto, essas informações geralmente são vitais para as operações e continuidade dos negócios das organizações. Consequentemente, a relevância da adoção de metodologias que garantam a proteção e privacidade das informações dos usuários é indispensável para evitar o vazamento de informações sensíveis. Por isso, foram criadas leis para estabelecer requisitos essenciais para que as organizações forneçam suporte e proteção aos dados pessoais dos usuários, como o Regulamento Geral Europeu de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados Brasileira (LGPD) (CASTRO; SILVA; CANEDO, 2022).

Nesse contexto, as discussões sobre a temática têm se expandido, destacando-se algumas obras relevantes diante desse novo panorama. Em sua busca por mapear políticas de proteção de dados pessoais em programas de nota fiscal, Machado, Bioni et al. (2016) conduziu uma pesquisa de campo abrangendo 12 Estados da Federação, culminando no desenvolvimento do projeto intitulado "Programa Nota Fiscal".

No trabalho de Moraes e Prado (2018), a discussão se volta para o uso de dados individuais, a opacidade em relação ao faturamento dos gastos públicos no âmbito da tecnologia, segurança,

privacidade e acesso aos dados.

Por isso, foram criadas leis para estabelecer requisitos essenciais para que as organizações forneçam suporte e proteção aos dados pessoais dos usuários, como o Regulamento Geral Europeu de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados Brasileira (LGPD) (CASTRO; SILVA; CANEDO, 2022).

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde setembro de 2020, representa um marco regulatório importante no que diz respeito à proteção de dados pessoais. Inspirada no GDPR europeu, a LGPD estabelece diretrizes claras para a coleta, processamento, armazenamento e compartilhamento de informações pessoais, atribuindo direitos aos titulares desses dados e responsabilidades às organizações que os manipulam.

Dentre os princípios fundamentais da LGPD estão a transparência no tratamento dos dados, a finalidade específica da coleta, a necessidade de consentimento do titular, a minimização da quantidade de dados coletados, a garantia da segurança da informação e a responsabilidade das organizações em caso de incidentes de segurança.

Além disso, a LGPD prevê a figura do Encarregado de Proteção de Dados (DPO), um profissional responsável por assegurar o cumprimento da legislação dentro das organizações. A não conformidade com as disposições da LGPD pode resultar em sanções significativas, incluindo multas substanciais.

Nesse cenário, muitas organizações têm buscado adaptar suas práticas e processos para garantir a conformidade com os requisitos da LGPD, implementando políticas de privacidade, revisando procedimentos de segurança da informação e promovendo a conscientização sobre a importância da proteção de dados pessoais.

Essa abordagem proativa em relação à proteção de dados não apenas atende aos requisitos legais, mas também fortalece a confiança dos usuários e consumidores nas organizações, contribuindo para uma cultura de respeito à privacidade e segurança da informação.

2.2 Conceitos e definições de engenharia social

A engenharia social é a arte de fazer com que os usuários comprometam os sistemas de informação. Em vez de ataques técnicos a sistemas, os engenheiros sociais visam humanos com acesso a informações, manipulando-os para divulgar informações confidenciais ou até mesmo para realizar seus ataques maliciosos por meio de influência e persuasão. As medidas de proteção técnica geralmente são ineficazes contra esse tipo de ataque. Além disso, as pessoas geralmente acreditam que são boas em detectar esses ataques. No entanto, as elas também têm um desempenho ruim na detecção de mentiras e enganos (KROMBHOLZ et al., 2015).

Para Rocha Flores e Ekstedt (2016) a engenharia social é uma ameaça externa à segurança da informação que inclui a exploração de fraquezas humanas, manipulando as pessoas para que

executem ações que beneficiem um invasor.

De acordo com Cullen e Armitage (2018) a engenharia social é, portanto, a capacidade de enganar os usuários para que façam algo que vá contra o interesse da segurança usando influência e persuasão.

Especialistas fundamentam os princípios da engenharia social com o auxílio da teoria da influência e atribuem a eles reciprocidade, comprometimento, prova social, autoridade, simpatia e deficiência (ASTAKHOVA; MEDVEDEV, 2020).

Segundo Wilcox e Bhattacharya (2020) o ciclo de vida da engenharia social inclui quatro fases a seguir: (a) Apuração de fatos – A fase para coletar informações sobre o alvo e então usar essas informações para construir um relacionamento com o alvo ou alguém relevante para o sucesso do ataque. (b) Confiança – Nesta fase, o agressor posicionar-se com um papel de confiança. (c) Manipulação – O alvo é manipulado pelo agressor "confiável" para revelar informações, como senha ou realizar uma ação em benefício do agressor. (d) Execução: O ciclo se completa à medida que o alvo/vítima completa a tarefa ou tarefas solicitadas pelo agressor.

Wilcox e Bhattacharya (2020) ainda afirmam que engenharia social por meio de canais de mídia social direcionados aos funcionários da organização está emergindo como uma das ameaças mais desafiadoras à segurança da informação. A engenharia social desafia os esforços tradicionais de segurança devido ao método de ataque baseado na ingenuidade ou erro humano. Os engenheiros sociais agora estão usando predominantemente as mídias sociais para perseguir e atingir as vítimas, usando as informações coletadas para atrair suas vítimas com técnicas de *phishing* – aplicadas através do próprio site ou por e-mail tradicional. Além disso, as inseguranças inerentes às tecnologias móveis estão contribuindo de forma monumental para o sucesso e a dissimulação desses ataques.

Para minimizar as perdas referentes aos ataques da engenharia social, deve-se: programar políticas de segurança nas organizações e sua ampla divulgação; promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social. A conscientização peculiar, portanto, é a conscientização adaptada à realidade específica da organização e setor em que atua, visando minimizar os riscos de segurança da informação relacionados à engenharia social; realizar a classificação e armazenamento da informação conforme o seu nível; executar a implementação e monitoramento dos mecanismos de segurança; não manusear informações corporativas fora da empresa e nem fornecer informações pessoais ou secretas; tomar cuidados especiais com o lixo eletrônico, assim como em qualquer outro meio, através de regras de descarte (ARAMUNI; MAIA, 2020b apud COELHO; RASMA; MORALES, 2013b).

2.3 Tipos de ataques de engenharia social

Os ataques de engenharia social são multifacetados e incluem aspectos físicos, sociais, técnicos e sociotécnicos, usados em diferentes estágios do ataque real (KROMBHOLZ et al., 2015).

2.3.1 Abordagens Físicas

As abordagens físicas, conforme destacado por Salahdine e Kaabouch (2019), são formas de ação em que o invasor realiza atividades como vasculhar o lixo, também conhecido como mergulho em lixeiras. Essa prática pode revelar-se uma fonte valiosa de informações diversas para os invasores, abrangendo desde dados pessoais até detalhes que possibilitam o acesso não autorizado.

Além do mergulho em lixeiras, abordagens físicas, como mencionado por Osuagwu et al. (2015), também podem envolver outras táticas, como roubo, extorsão ou acesso não autorizado a ambientes físicos da vítima. Em ambientes corporativos com espaços de trabalho de plano aberto, por exemplo, um invasor pode explorar a disposição do local para encontrar informações sensíveis, como senhas anotadas em *post-its*. Essa prática revela a versatilidade das abordagens físicas, que podem variar de técnicas relativamente simples, como vasculhar lixeiras, a estratégias mais complexas, como o acesso físico a ambientes restritos.

Essa compreensão abrangente das abordagens físicas destaca a importância de medidas de segurança não apenas em ambientes digitais, mas também no controle físico de espaços, minimizando vulnerabilidades exploráveis por meio de acesso não autorizado, roubo ou extorsão.

2.3.2 Abordagens Sociais

As abordagens sociais representam o aspecto mais crítico dos ataques de engenharia social, pois envolvem técnicas sociopsicológicas para manipular as vítimas. Conforme destacado por Koyun e Janabi (2017), os agressores buscam frequentemente estabelecer relacionamentos com suas futuras vítimas, fazendo uso de princípios persuasivos, como a exploração da autoridade suposta. Além disso, Salahdine e Kaabouch (2019) destacou, na época do estudo, que o tipo mais prevalente de ataque social era realizado por telefone.

O sucesso dessas abordagens sociais muitas vezes depende da aplicação eficaz dos princípios de persuasão, como os delineados por Cialdini Krombholz et al. (2015). Entre esses princípios, destaca-se o uso da autoridade suposta, onde os agressores podem se passar por figuras de autoridade para ganhar a confiança das vítimas. É relevante observar que, além dos princípios de Cialdini, outros fatores sociais, como a curiosidade, desempenham um papel crucial. Por exemplo, a curiosidade é explorada em ataques de *spear phishing* e *baiting*, revelando-se um vetor social significativo.

A construção de relacionamentos com as vítimas é uma estratégia comum para aumentar as chances de sucesso desses ataques. Esse envolvimento emocional pode tornar as vítimas mais propensas a compartilhar informações sensíveis ou realizar ações indesejadas. Assim, a compreensão dessas abordagens sociais, conforme discutido por Salahdine e Kaabouch (2019), é essencial para fortalecer a conscientização e a resistência contra manipulações psicológicas.

2.3.3 Abordagens Técnicas

Os ataques técnicos, como discutido por Koyun e Janabi (2017), são predominantemente realizados pela Internet. Este meio oferece uma plataforma atrativa para engenheiros sociais coletarem senhas, dado que os usuários frequentemente utilizam senhas simples que são compartilhadas entre várias contas. Essa prática torna mais fácil para os invasores comprometerem a segurança, uma vez que, uma vez obtida a senha, ela pode ser testada em diferentes serviços online.

Mecanismos de pesquisa desempenham um papel fundamental nesse tipo de abordagem técnica, sendo amplamente empregados pelos invasores para coletar informações pessoais sobre as vítimas. A análise de Krombholz et al. (2015) destaca que a maioria das pessoas não está plenamente consciente de que, ao realizar buscas online ou compartilhar informações em várias plataformas, estão fornecendo dados valiosos aos invasores. Essa falta de conscientização contribui para a eficácia desses ataques.

Ferramentas especializadas, como o Maltego, ganham destaque nesse contexto. O Maltego é uma ferramenta popular entre os engenheiros sociais, permitindo a coleta, correlação e análise de informações de diferentes fontes na Internet. Sua capacidade de agregar dados de maneira abrangente facilita a criação de perfis detalhados das vítimas, aumentando a eficácia dos ataques (KROMBHOLZ et al., 2015). Essas abordagens técnicas destacam a importância de práticas de segurança online e a necessidade de conscientização sobre o compartilhamento de informações pessoais na era digital.

2.3.4 Abordagens Sociotécnicas

Abordagens sociotécnicas representam um campo complexo e dinâmico, onde os engenheiros sociais combinam diversas estratégias para criar ferramentas poderosas (KROMBHOLZ et al., 2015). A análise de Salahdine e Kaabouch (2019) e a classificação proposta dividem os ataques sociotécnicos em duas categorias principais: diretos e indiretos.

Na categoria de ataques **diretos**, o invasor estabelece contato direto com a vítima, envolvendo interações que podem ocorrer fisicamente ou virtualmente. Exemplos emblemáticos desses ataques incluem:

1. ***Physical Access:*** O invasor busca acesso físico ao ambiente da vítima, frequentemente

exigindo presença física para realizar o ataque.

2. ***Shoulder Surfing:*** Envolve observação direta, como olhar sobre o ombro de alguém para obter informações.
3. ***Dumpster Diving:*** Consiste em vasculhar o lixo da vítima em busca de informações sensíveis.
4. ***Phone Social Engineering:*** O atacante manipula a vítima por meio de interações telefônicas persuasivas.
5. ***Pretexting:*** O invasor cria uma situação inventada para convencer a vítima a divulgar informações ou conceder acesso.
6. ***Impersonation on Help Desk Calls:*** O atacante se passa por um representante de suporte técnico para obter informações confidenciais.
7. ***Stealing Important Documents:*** Envolve o furto físico de documentos que contêm informações sensíveis.

Já na categoria **indireta**, os ataques são lançados remotamente, eliminando a necessidade de contato físico. Exemplos característicos desses ataques incluem:

1. ***Phishing:*** Os ataques de phishing buscam obter dados de autenticação por meio de mensagens enganosas.
2. ***Fake Software:*** Envolve a distribuição de software fraudulento para explorar vulnerabilidades.
3. ***Pop-Up Windows:*** Utilização de janelas pop-up para induzir ações indesejadas.
4. ***Ransomware:*** Ataques que visam criptografar dados e exigir resgate para sua liberação.
5. ***SMSishing:*** Similar ao phishing, mas realizado por meio de mensagens SMS.
6. ***Online Social Engineering:*** Manipulação psicológica conduzida virtualmente para obter informações.
7. ***Reverse Social Engineering:*** Estabelece confiança entre o invasor e a vítima para obter informações privilegiadas remotamente.

A distinção entre ataques diretos e indiretos fornece *insights* cruciais sobre a variedade de estratégias empregadas pelos engenheiros sociais, abrangendo tanto interações pessoais quanto a exploração remota de vulnerabilidades. Essa abordagem holística evidencia a complexidade do cenário sociotécnico, onde a criatividade dos invasores é uma força motriz constante.

2.3.5 Principais exemplos de ataques

Ao explorar as diversas abordagens dos ataques de engenharia social, torna-se evidente a amplitude de estratégias utilizadas para manipular indivíduos e obter informações sensíveis. Nesta seção, aprofundaremos os principais exemplos desses ataques, destacando suas nuances e táticas específicas. A compreensão desses métodos é crucial para fortalecer a resistência contra ameaças cibernéticas que exploram a natureza humana.

- ***Phishing***: O *phishing*, conforme descrito por Krombholz et al. (2015), é uma fraude online em que um invasor busca obter dados de autenticação da vítima. Já o estudo de Salahdine e Kaabouch (2019) adiciona que esses ataques frequentemente envolvem envio em massa de e-mails ou mensagens SMS, simulando instituições confiáveis.

- ***Spear Phishing***: O *spear phishing*, conforme definido por Krombholz et al. (2015), é uma forma altamente direcionada de ataque por e-mail ou telefone, frequentemente empregada em ambientes de negócios. Salahdine e Kaabouch (2019) destaca que esse tipo de ataque pode incluir mensagens que parecem vir de figuras de autoridade dentro da organização.

- ***Pretexting***: é o ato de criar e usar uma situação inventada para convencer um alvo a liberar informações ou conceder acesso a materiais sensíveis. Muitas vezes, esse tipo de ataque geralmente é implementado por telefone. Ao responder a perguntas, a vítima, sem saber, fornecerá ao invasor todas as informações de que o *hacker* precisa para realizar o ataque (OSUAGWU et al., 2015).

- ***Quid Pro Quo***: O termo "*Quid Pro Quo*,"que em Latim significa 'uma coisa por outra', descreve uma tática específica de ataque de engenharia social. Nesse contexto, um ataque *Quid Pro Quo* ocorre quando um atacante oferece um benefício tangível em troca de acesso a sistemas ou informações sensíveis. Essa técnica compartilha semelhanças com o *Baiting*, mas se diferencia na natureza da transação proposta. Ao contrário do *Baiting*, onde a isca é um dispositivo ou meio de armazenamento infectado, no ataque *Quid Pro Quo*, o atacante promete um serviço ou benefício específico como contrapartida para induzir a vítima a realizar uma ação desejada, como fornecer credenciais de login ou informações confidenciais.

- ***Baiting***: é uma técnica de ataque que envolve a disponibilização de um meio de armazenamento, como um USB infectado por *malware*, em um local estratégico onde é provável que seja encontrado por potenciais vítimas. O termo "*baiting*"deriva da ideia de isca, onde o atacante utiliza um objeto ou dispositivo contaminado como isca para atrair a curiosidade das pessoas. Ao encontrar esse meio de armazenamento, as vítimas podem ser tentadas a conectá-lo aos seus próprios dispositivos, como computadores pessoais ou sistemas de trabalho, com o objetivo de descobrir seu conteúdo ou encontrar informações sobre seu

proprietário. No entanto, ao conectar o dispositivo comprometido, o *malware* contido nele é ativado, permitindo que o atacante ganhe acesso não autorizado ao sistema da vítima.

- ***Tailgating***: esse tipo de ataque envolve um indivíduo não autorizado que segue um funcionário autorizado em uma área restrita. Personificando um mensageiro ou entregador, o atacante espera fora do edifício. O ser humano tem uma tendência natural para ajudar aqueles que precisam de alguma ajuda. Isso é muito bem aproveitado por engenheiros sociais. Por exemplo, o atacante faz-se passar por um entregador com muitas caixas na mão e obtém acesso a um prédio enquanto um funcionário decide ajudá-lo mantendo a porta aberta.

- ***Waterholing***: descreve um ataque direcionado em que os invasores comprometem um site que provavelmente será de interesse da vítima escolhida. Os atacantes então esperam no charco por sua vítima (KROMBHOLZ et al., 2015).

- ***Spoofing***: é o processo de falsificar a identidade de alguém e se passar por outra pessoa. O engenheiro social desenvolve um site que espelha um site confiável, mas pode ser usado para roubo de identidade, geralmente pedindo aos usuários que enviem informações de *login* para o site duplicado ou instalem *malware* no computador do usuário (OSUAGWU et al., 2015).

- ***Dumpster Diving***: é a prática de vasculhar o lixo de indivíduos ou empresas para encontrar itens descartados que incluem informações confidenciais que podem ser usadas para comprometer um sistema ou uma conta de usuário específica (KROMBHOLZ et al., 2015).

- ***Shoulder surfing***: refere-se ao uso de técnicas de observação direta para obter informações, como olhar por cima do ombro de alguém na tela ou no teclado (KROMBHOLZ et al., 2015).

- ***Road Apples***: refere-se a situações em que o cibercriminoso descarta uma mídia física, como CD ou memória *Flash* USB, rotulada para atrair curiosidade (“Pesquisa Salarial Executiva”, “Plano de Redução de Pessoal de RH”, “Mudanças Organizacionais Confidenciais”). Uma vez que uma equipe escolhe a mídia e os *slots* em um PC para visualizar, o recurso “autorun” carregará *Trojan* ou vírus para rastrear pressionamentos de tecla e coletar IDs e senhas (OSUAGWU et al., 2015).

- ***Reverse social engineering***: é um ataque em que geralmente a confiança é estabelecida entre o invasor e a vítima. Os atacantes criam uma situação em que a vítima precisa de ajuda e depois se apresenta como alguém que a vítima considerará alguém que pode resolver seu problema e receber informações privilegiadas. É claro que os invasores tentam escolher um indivíduo que eles acreditam ter informações que os ajudarão (KROMBHOLZ et al., 2015).

- ***Advanced Persistent Threat***: refere-se a ataques de espionagem de longo prazo, principalmente baseados na Internet, conduzidos por um invasor que tem os recursos e a intenção de incluir um sistema de forma persistente (KROMBHOLZ et al., 2015).

2.4 Mitigação de Ataques de Engenharia Social

As estratégias para lidar com ataques de engenharia social podem ser classificadas em prevenção, detecção e mitigação (ARABIA-OBEDOZA et al., 2020a). No âmbito da prevenção, existem duas categorias: sistemas de prevenção para usuários humanos e sistemas de prevenção tecnológica. Os sistemas de prevenção para usuários humanos envolvem a implementação de políticas e processos dentro da organização, além de programas de conscientização e treinamento em cibersegurança. Os sistemas de prevenção tecnológica incluem varreduras e pesquisas de sites, o uso de extensões de navegador como o TabShots e a implementação de uma lista negra para o tráfego malicioso.

As estratégias de detecção podem ser divididas em técnicas de detecção humanas e técnicas de detecção tecnológicas. As técnicas de detecção humanas envolvem o uso de humanos como sensores de segurança, coberturas dinâmicas de segurança e avaliação de riscos centrada em engenharia social. As técnicas de detecção tecnológicas incluem a detecção de páginas da web de phishing visualmente semelhantes usando a distância do transportador de terra e proteção contra falsificações.

Quanto às estratégias de mitigação, elas abrangem fraudes cibernéticas, detecção de contas falsas em redes sociais, conscientização em redes sociais, contramedidas contra cavalos de Troia, conscientização em segurança aplicada a indivíduos e organizações, e contramedidas contra fraudes bancárias baseadas em dispositivos. Portanto, as estratégias para lidar com ataques de engenharia social envolvem uma combinação de medidas preventivas, técnicas de detecção e ações de mitigação.

2.5 Sistemas especialistas

Os sistemas especialistas começaram a aparecer no final do século XX, como pesquisas privadas sobre a criação e aplicação de inteligência artificial (MANDRAKOV; VASILIEV; DUDINA, 2021).

De acordo com Sihwi, Andriyanto e Anggrainingsih (2016), sistema Especialista (SE) é um ramo da Inteligência Artificial que faz uso extensivo de conhecimento especializado para resolver problemas no nível do especialista humano em um domínio específico.

Para Yu et al. (2018), o sistema especialista pode ser considerado como uma linguagem de programação descritiva porque os programadores não precisam especificar como realizar o algoritmo específico. Agora, existem vários tipos de sistemas especialistas, como sistemas

especialistas baseados em *frameworks*, sistemas especialistas baseados em raciocínio e sistemas especialistas baseados em regras, e assim por diante.

Segundo Rani e Goel (2015), o conhecimento deve ser apresentado em um formato compreensível para realizar qualquer tipo de raciocínio no sistema especialista, o que é conhecido como representação do conhecimento. O sistema especialista consiste em dois componentes: base de conhecimento e raciocínio lógico. A base de conhecimento é o primeiro componente de um sistema especialista e é uma coleção de informações que estão em uma representação bem definida. O segundo componente de um sistema especialista é o raciocinador lógico que realiza todo o raciocínio necessário sobre a base de conhecimento previamente construída. Com este raciocinador lógico concluímos novas informações da base de conhecimento construída anteriormente.

Dentre os diversos tipos de sistemas especialistas, os Sistemas Especialistas Baseados em Regras (SEBR) são uma abordagem comum. Nesse tipo de sistema, o conhecimento é representado por meio de regras do tipo "SE... ENTAO...", onde condições (premissas) levam a conclusões. Cada regra é projetada para capturar o conhecimento específico de um especialista humano no domínio em questão (CARRICO; GIRARD; JONES, 1989).

Vários métodos têm sido adotados na construção do sistema especialista em diversos domínios, como *Forward Chaining*, *Backward Chaining*, *Fuzzy* e Método da Certeza (SIHWI; ANDRIYANTO; ANGGRAININGSIH, 2016).

O *Forward Chaining*, também conhecido como Encadeamento Progressivo, caracteriza-se pelo início com informações iniciais, avançando por meio de regras para alcançar uma conclusão. Este método opera a partir de fatos conhecidos, expandindo-se até alcançar uma solução (NILSSON, 1982).

Por outro lado, o *Backward Chaining*, ou Encadeamento Regressivo, adota uma abordagem inversa. Inicia com uma meta ou conclusão desejada e retrocede para encontrar os fatos ou regras necessários que suportam essa conclusão (GIARRATANO; RILEY, 1989).

A lógica *Fuzzy*, introduzida por Zadeh (1965), é uma abordagem que lida eficientemente com a incerteza e a imprecisão. Em contraste com a lógica booleana tradicional, que opera com valores nítidos (verdadeiro ou falso), a lógica *Fuzzy* permite a representação de graus de verdade, proporcionando uma maneira mais flexível de lidar com a incerteza em sistemas especialistas.

Por fim, o Método da Certeza assume um cenário em que todas as informações disponíveis são conhecidas com precisão e confiabilidade. Em situações onde a incerteza não é uma preocupação central, este método oferece uma abordagem mais determinística para a construção de sistemas especialistas (JACKSON, 1986). Cada um desses métodos desempenha um papel distinto na modelagem e implementação de sistemas especialistas, proporcionando escolhas flexíveis para atender às necessidades específicas de diferentes domínios de aplicação.

3
Metodologia

3.1 Métodos

Este trabalho adota uma abordagem de pesquisa que é simultaneamente básica e aplicada. Seguindo a definição de Gil (2008), a pesquisa básica procura gerar novos conhecimentos que possam contribuir para avanços na ciência, ainda que não tenha uma aplicação prática imediata. No contexto deste estudo, a pesquisa básica foi adotada para definir os temas de pesquisa, como Segurança da Informação e Engenharia Social, que são destacados no escopo. Esses estudos visam mitigar os ataques de engenharia social por meio da conscientização dos usuários.

A metodologia proposta para o desenvolvimento deste trabalho é uma pesquisa básica e aplicada de desenvolvimento tecnológico, que envolve a sistematização do processo de conscientização em segurança da informação, com foco na prevenção de ataques de engenharia social. 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) e Boaventura (2004), como 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. A metodologia adotada envolve duas etapas principais:

A primeira etapa envolve: Execução do Mapeamento Sistemático da Literatura; Realização de um estudo exploratório sobre desenvolvimento de sistema especialista relacionado à segurança da informação e Coleta de dados em diferentes fontes, como livros, artigos de periódicos e conferências.

A segunda etapa envolve: Desenvolver um sistema que ajude a conscientizar os usuários sobre as técnicas de engenharia social, prevenção de ataques e diagnóstico de vulnerabilidades, além de realizar validação do sistema desenvolvido.

A validação do sistema especialista em segurança da informação será realizada por meio da aplicação de um questionário utilizando a escala *Likert* e posterior análise dos dados.

A metodologia utilizada no desenvolvimento deste trabalho tem como objetivo proporcionar uma abordagem sistemática e prática para alcançar o objetivo principal: desenvolver um sistema especialista de segurança da informação, com foco em engenharia social, a fim de conscientizar usuários e prevenir vulnerabilidades. Esta metodologia permitirá não apenas a sistematização do processo de conscientização, mas também a aplicação prática dos conhecimentos adquiridos para a prevenção de ataques de engenharia social, além de fornecer uma análise dos resultados da validação do sistema desenvolvido.

3.2 Materiais

Uma aplicação *web* é formada por um grupo de linguagens, bibliotecas, *plugins* e banco de dados que permitem, com a escolha correta de tais ferramentas, propiciar ao usuário o *kit* essencial para atingir seus objetivos. O processo de desenvolver uma aplicação de qualidade, já se inicia mesmo na escolha de tais tecnologias. Deste modo, esta seção apresenta o conjunto de tecnologias que foram utilizadas, tanto no auxílio do desenvolvimento em si, quanto em relação aos *softwares* e elementos que compõem a aplicação.

Durante o desenvolvimento deste trabalho, foram selecionadas cuidadosamente diversas tecnologias e ferramentas para atender aos requisitos específicos do projeto. Cada escolha foi baseada em critérios como funcionalidade, desempenho e facilidade de manutenção da aplicação.

O *Visual Studio Code* foi adotado como editor de código fonte devido à sua ampla gama de funcionalidades e suporte para várias linguagens de programação. Sua extensibilidade e integração com ferramentas essenciais para o desenvolvimento *web* o tornam uma opção poderosa e versátil para desenvolvedores.

Para o desenvolvimento do *backend* da aplicação, optamos pelo Laravel como *framework* PHP. Sua sintaxe expressiva, rico conjunto de funcionalidades e suporte ao padrão Modelo-Visão-Controlador (MVC) foram fatores determinantes para essa escolha. O Laravel oferece ferramentas robustas para o desenvolvimento de aplicações web modernas, incluindo roteamento simplificado, sistema de autenticação integrado e uma ORM elegante para interação com o banco de dados.

A modelagem das páginas da aplicação foi realizada utilizando o template *attex*. Sua facilidade de implementação, visual atraente e ampla variedade de elementos visuais úteis foram aspectos-chave que influenciaram essa decisão. O attex fornece uma estrutura sólida e flexível para a construção de interfaces de usuário intuitivas e responsivas.

Quanto ao banco de dados, o *PostgreSQL* foi escolhido como sistema de gerenciamento devido à sua confiabilidade, desempenho e robustez. Para administração do banco de dados,

utilizamos o *DBeaver Community*, uma ferramenta de código aberto com interface intuitiva e suporte a uma ampla gama de sistemas de gerenciamento de banco de dados.

Essas escolhas foram fundamentais para o sucesso do projeto, permitindo o desenvolvimento de uma aplicação web eficiente, segura e de fácil manutenção.

3.2.1 Ambiente de Desenvolvimento

O *Visual Studio Code* é um editor de código fonte, que possui uma enorme gama de ferramentas e funcionalidades úteis no desenvolvimento de aplicações em diversas linguagens. Ele é um *software* livre e foi desenvolvido pela *Microsoft*. Entre o conjunto de linguagens que ele provê suporte, dado o seu rico ecossistema de extensões, pode ser citado: *JavaScript*, *TypeScript*, *Node.js*, *C++*, *C#*, *Java*, *Python*, *PHP*. Além de possuir um terminal integrado, extensões como *PHP IntelliSense*, *PHP Debug*, Laravel 10 *Snippets*, se mostraram bastante convenientes no processo de desenvolvimento.

O *WampServer* é uma plataforma para desenvolvimento *web* que contém as aplicações *Apache*, *Mysql* e *PHP*, de modo que o *software* simule o comportamento de um servidor, e pudesse portanto testar a aplicação desenvolvida. As versões utilizadas foram:

- WampServer – 3.3.1 - 64bit
- Apache – 2.4.54.2
- MySQL – 8.0.31
- PHP – 8.2.4

3.2.2 Framework PHP

Um *frameworks*, sob a visão de programação, é um conjunto de classes desenvolvidas e organizadas de tal modo que fornecem auxílio na criação de outras aplicações, com propósitos mais específicos. O uso de *frameworks* para o desenvolvimento *web* traz agilidade, segurança e organização de código. Sommerville (2011) afirma que, “os *frameworks* dão suporte ao reúso de projeto, bem como ao reúso de classes específicas de sistema, pois fornecem uma arquitetura de esqueleto para a aplicação”

Laravel, de acordo com Otwell (2016), é um *framework* de aplicação *web* com sintaxe expressiva e elegante, além de que fornecer ferramentas necessárias para aplicações grandes e robustas. Baseado no padrão Modelo-Visão-Controlador (MVC), o Laravel consegue manter o código limpo e simples, provê funcionalidades que auxiliam o roteamento de páginas *web*, sistema de autenticação, validação de requisições, acesso e operações ao banco de dados, além de muitas outras tarefas comuns na programação *web*. A versão utilizada neste trabalho foi o Laravel 10.0.

3.2.3 Template

Para a modelagem das páginas foi utilizado o template *attex*, ele cria um painel administrativo composto de vários *plugins* e dependências advindos de *frameworks* como *Bootstrap* 4 e *JQuery*. Com a grande vantagem de ser fácil de implementar e customizar, somadas com um visual agradável e uma grande quantidade de elementos visuais úteis ao sistema, o *attex* foi escolhido para agilizar a construção do *CSS* e padronizar as páginas da aplicação.

3.2.4 Banco de Dados

No Laravel, o processo de criação e atualização do banco de dados é facilitado pelo uso de classes chamadas *migrations*. As *migrations* são uma forma conveniente e controlada de gerenciar o esquema do banco de dados ao longo do tempo, garantindo consistência e facilitando o trabalho colaborativo entre desenvolvedores.

Utilizando o *PostgreSQL* como sistema de gerenciamento de banco de dados, especificamente na versão 15.6, as *migrations* no Laravel são responsáveis por automatizar a criação e atualização do esquema conforme necessário. Cada *migrations* corresponde a uma alteração específica no esquema do banco de dados, como a criação de uma tabela, a adição de uma coluna ou a definição de um índice. As *migrations* são escritas em código PHP e seguem uma convenção de nomenclatura que inclui um timestamp para garantir a ordem de execução.

Durante o processo de desenvolvimento, as *migrations* são executadas sequencialmente conforme necessário, criando ou atualizando automaticamente o esquema do banco de dados de acordo com as mudanças no código-fonte. Isso simplifica o processo de gerenciamento do banco de dados e elimina a necessidade de executar scripts SQL manualmente.

Além disso, as *migrations* são reversíveis, o que significa que é possível reverter ou desfazer uma migração anterior, se necessário, facilitando o processo de *rollback* em caso de erro ou necessidade de retroceder para uma versão anterior do esquema do banco de dados.

Em resumo, as *migrations* no Laravel, em conjunto com o *PostgreSQL* 15.6, fornecem uma abordagem eficaz e organizada para gerenciar o esquema do banco de dados durante o desenvolvimento, promovendo consistência, colaboração e facilidade de manutenção.

3.2.5 DBeaver Community

O DBeaver é uma ferramenta de banco de dados universal, gratuita e de código aberto, projetada para desenvolvedores e administradores de banco de dados. Seu principal objetivo é a usabilidade, refletida em uma interface de usuário cuidadosamente projetada e implementada. Baseado em um *framework* de código aberto, o DBeaver é multiplataforma e permite a escrita de várias extensões (*plugins*). Utilizamos a versão 23.0.1 do DBeaver. Ele suporta qualquer banco de dados com um driver JDBC e é capaz de lidar com qualquer fonte de dados externa, com ou

sem um driver JDBC disponível. Além disso, possui um conjunto de *plugins* para diferentes bancos de dados e utilitários de gerenciamento de banco de dados, como modelagem de dados, transferência de dados, comparação, exportação/importação de dados e geração de dados fictícios, entre outros. Com uma grande variedade de recursos, o DBeaver oferece uma solução abrangente para diversas necessidades de gerenciamento de banco de dados.

4

Trabalhos Relacionados

Para a andamento da dissertação ora descrita, definiu-se inicialmente, realizar a elaboração do mapeamento sistemático, que subsidiou a seleção, a revisão e a sintetização dos trabalhos que, de acordo com a relevância, embasaram a pesquisa. Ressalta-se que foram consultadas publicações entre os anos 2012-2022, para que assim fosse aproveitado estudos recentes, respeitando-se os avanços tecnologicos e a necessidade de atualizações.

Na fase de planejamento da pesquisa, o mapeamento sistemático permitiu tomar-se como ponto de partida a questão norteadora. Nesta, define-se o que está sendo procurado e quais resultados se pretende alcançar.

Por meio das questões norteadoras, foi possível traçar um panorama da pesquisa e construir uma *string* de busca. Além disso, foi definido critérios de exclusão e inclusão de publicações dada a relevância acerca do tema através das perguntas formuladas.

Tal paradigma permitiu encontrar as respostas para as questões propostas ainda no mapeamento sistemático com base nas literaturas pertinentes, além de apresentar o objetivo, as estratégias e os critérios adotados.

4.1 Engenharia Social nas Organizações

Para realizar o estudo sobre engenharia social nas organizações, foi empregado o método de Mapeamento Sistemático da Literatura (Systematic Literature Mapping - SLM), conforme destacado por Petersen, Vakkalanka e Kuzniarz (2015). O Mapeamento Sistemático da Literatura busca analisar questões e proporcionar respostas por meio da adição ou indexação de evidências relacionadas às temáticas propostas. Este processo é conduzido com critérios rigorosos de natureza interativa, visando fornecer uma visão abrangente de uma área específica. O principal objetivo do SLM é identificar a quantidade e o caráter da pesquisa existente, permitindo a apresentação de resultados relevantes disponíveis na literatura.

Neste sentido, o processo de mapeamento empreendido para o trabalho ora descrito, percorreu as seguintes etapas:

- Elaboração das questões de pesquisa, que permitem nortear o mapeamento; desenvolvimento da pesquisa por meio da estratégia de busca e de seleção dos estudos primários, através da qual se obtém resultados mais significativos;
- Critérios de seleção, que facilitam a triagem dos artigos relevantes;
- Análise dos resultados, que permite a obtenção dos dados que, por sua vez, respondem as questões de pesquisa;

4.1.1 Questões de Pesquisa

Visualizando-se o alcance dos objetivos traçados para esta pesquisa, levantou-se 3 questões norteadoras cujo mapeamento, através dos dados retirados das bases de dados digitais na área de computação, fornecerá as respostas.

- QP1 - Qual tipo de organização que mais aparece como alvo de ataques de engenharia social?
- QP2 - Quais são os principais tipos de ataques de engenharia social nas organizações?
- QP3 - Quais métodos e/ou técnicas de defesa para evitar ataques de Engenharia Social nas organizações?

4.1.2 Estratégia de Busca e de Seleção

Nesta etapa da pesquisa, foi aplicada uma estratégia de investigação automática em bases de dados digitais na área de computação, tendo como objetivo satisfazer as questões de pesquisa, por intermédio de uma *string* de busca acrescida dos operadores booleanos OR e AND, para realçar as definições de termos ou palavras-chaves a serem utilizadas. IEEE Xplore Digital Library, Scopus, Web of Science, Science Direct, ACM Digital Library e Springer Link foram as bibliotecas digitais selecionadas para execução da *string* de busca, seguindo os critérios de cada biblioteca, dentro da faixa temporal de 2012 a 2022.

Foram utilizadas as seguintes bases de pesquisa:

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

- ACM Digital Library <<http://portal.acm.org>>;
- Springer Link <<http://link.springer.com>>;

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

Tabela 1 – Palavras-Chave utilizadas na *string* de busca

Palavra-chave	**Sinônimo em Inglês**
Engenharia Social	Social Engineering
Ataques	Attacks
Segurança da Informação	Information Security
Ferramentas	Tools
Organização	Company

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

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

((Social Engineering) AND (Attacks) AND (Information Security) AND (Tools) AND ((Organization) OR (Company)))

A seguir os Critérios de Inclusão:

1. CI01: Artigos em que o título esteja dentro do contexto de pesquisa;
2. CI02: Artigos em que o resumo esteja dentro do contexto de pesquisa;
3. CI03: Artigos em que o ano de publicação seja superior a 2011;
4. CI04: Artigos em que as suas fontes sejam de conferências ou *journals*;

A seguir os Critérios de Exclusão:

1. CE01: Artigos publicados antes do ano de 2012;
2. CE02: Estudos duplicados;
3. CE03: Estudos fora do contexto da pesquisa;
4. CE04: Estudos secundários;
5. CE05: Estudos disponíveis com leitura incompleta;
6. CE06: Estudo Inacessível para download;
7. CE07: Artigos sem identificação do autor;

Os artigos selecionados por meio do processo de busca dos estudos primários serão verificados de acordo com critérios estabelecidos de inclusão ou exclusão para a extração dos dados. Para cada estudo selecionado, mediante a execução do processo de seleção dos estudos primários, serão extraídos os seguintes dados:

- Objetivo do artigo;
- Data de publicação;
- Tipos de soluções;
- Sugestão para trabalhos futuros.

A partir da *string* de busca composta pelas palavras-chave Social Engineering, Attacks, Information Security, Organization or Company, os resultados obtidos serão analisados, organizados, agrupados e comparados. Essas palavras-chave foram selecionadas por serem inerentes ao tema em questão, ou seja, a segurança da informação relacionada a ataques de engenharia social. Dessa forma, a análise dos resultados será orientada pelos critérios relevantes para a pesquisa, como tipo de ataque, tipo de organização ou empresa estudada, entre outros.

4.2 Estudos Relevantes

O tema engenharia social nas organizações apresenta-se enquanto proposta a partir da análise dos artigos relacionados que contemplam de estudos mais aprofundados na área. A necessidade de uma ênfase maior neste sentido parte do pressuposto de que o aumento de informações sensíveis e vitais, para o negócio das organizações, ampliam a possibilidade da ação da engenharia social. Cabe a ressalva de que se trata da manipulação psicológica para com tais usuários na intenção de que estes executem ações ou divulguem informações confidenciais.

As ameaças e tendências da Engenharia Social são investigadas e estratégias de mitigação recomendadas (OSUAGWU et al., 2015). A engenharia social, uma técnica pela qual os cibercriminosos enganam suas vítimas para que divulguem informações de *login* sem usar nenhum dispositivo técnico, foi identificada como uma das ameaças mais perigosas do nosso tempo. Devido ao fato de que qualquer roubo de identidade ou violação no sistema de informações de uma organização, resultando na divulgação de informações confidenciais, pode ter consequências de longo alcance, como perdas financeiras, interrupção de serviços, danos à imagem pública.

O trabalho de Krombholz et al. (2015) tem como objetivo fornecer uma visão abrangente e completa dos ataques de engenharia social ao trabalhador do conhecimento, monitorar o estado da arte da pesquisa neste campo e fornecer uma taxonomia abrangente para categorizar os ataques de engenharia social e medir seu impacto.

Mouton, Leenen e Venter (2016) propuseram modelos detalhados de ataque de engenharia social que são derivados de exemplos de engenharia social do mundo real. Os exemplos documentados não incluem todas as etapas e fases do ataque. Os modelos de ataque de engenharia social propostos tentam aliviar o problema da literatura documentada limitada sobre ataques de engenharia social, mapeando os exemplos do mundo real para a estrutura de ataque de engenharia social.

Khlobystova e Abramov (2021) propuseram uma nova abordagem para a análise de ataques de engenharia social em várias etapas, levando em conta o fator de acidentes das ações do malfeitor. O significado teórico do trabalho é criar uma base para posterior modelagem e análise de ataques de engenharia social em várias etapas. O significado prático do estudo está na formação de uma ferramenta de análise abrangente da organização para identificar os cenários mais críticos para o desenvolvimento de ataques de engenharia social.

Hammour et al. (2019) apresentam uma estrutura de governança de tecnologia da informação aplicada em um banco jordaniano para proteger o sistema de ataques de engenharia social. Trabalhamos em um estudo de caso que foca principalmente no ataque de *phishing*, que é considerado uma das ameaças mais comuns em bancos, e a forma como a equipe irá lidar com isso. Os resultados mostram melhorias positivas na conscientização da equipe e na prevenção desses tipos de ataques, bem como um aumento acentuado na comunicação de qualquer atividade suspeita percebida pelos funcionários.

Sohrabi Safa, Von Solms e Furnell (2016) mostram como o cumprimento das políticas de segurança da informação organizacional molda e mitiga o risco de comportamento dos funcionários. O aspecto significativo desta pesquisa é derivado da conceituação de diferentes aspectos de envolvimento, como compartilhamento de conhecimento de segurança da informação, colaboração, intervenção e experiência, bem como apego, compromisso e normas pessoais que são elementos importantes na Teoria do Vínculo Social.

O trabalho de Grassegger e Nedbal (2021) tem como objetivo, portanto, identificar fatores individuais e organizacionais que afetam a conscientização sobre segurança da informação e examina a influência da conscientização sobre segurança da informação na intenção de resistir a ataques de engenharia social.

Wilson (2018) buscou conscientizar sobre o roubo de dados e como as técnicas de engenharia social são utilizadas por *hackers* para vulnerabilizar informações de entidades empresariais.

O estudo de Aldawood e Skinner (2019), destaca alguns dos desafios que as organizações encontram no processo de desenvolvimento do conhecimento humano para lutar contra ataques de engenharia social. Os desafios em relação às ferramentas tradicionais e modernas foram analisados para sugerir a necessidade de traçar perfis de funcionários em risco e desenvolver programas de treinamento em cada nível da hierarquia para garantir que os *hackers* não tenham

sucesso.

A pesquisa de Aldawood e Skinner (2020) se concentra no elemento humano das ameaças de segurança cibernética, reconhecendo que os *hackers* exploram as vulnerabilidades e a falta de conscientização da equipe. Em seguida, usar esses problemas para criar brechas de segurança e projetar ataques cibernéticos que incluem a interrupção ou infecção de sistemas de informação, transferência de fundos não autorizados e roubo de credenciais. Os resultados deste estudo qualitativo destacam que existe uma relação positiva entre a engenharia social e a conscientização do usuário. As descobertas se baseiam no trabalho contínuo dos pesquisadores, que postula que, à medida que o aumento do conhecimento contextual da engenharia social leva a uma diminuição de vítimas da engenharia social, é, portanto, um dos mecanismos mais eficazes para gerenciar a engenharia social.

O artigo de Astakhova e Medvedev (2020) tem como objetivo desenvolver uma ferramenta de *software* baseada em aprendizado de máquina – um *scanner* para testes dinâmicos internos de funcionários de uma organização para aumentar sua resistência a ataques de engenharia social de diferentes tipos, formas e desenvolver sua cultura de segurança da informação. A ferramenta permite que o especialista em segurança da informação não apenas escaneie a resistência dos funcionários da organização a ataques de engenharia social, mas também receba informações sobre os ataques detectados dos funcionários, além de treiná-los e testá-los de forma abrangente para entender os métodos modernos de tais ataques.

Jansen e Fischbach (2020) criaram o *The Social Engineer*, um jogo educacional imersivo em realidade virtual, para conscientizar e sensibilizar os jogadores sobre engenharia social. O jogador se faz passar por um testador de penetração e realiza auditorias de segurança em uma empresa virtualmente simulada. O jogo consiste em um mundo de jogo detalhado contendo três missões distintas que exigem que o jogador aplique diferentes métodos de ataque de engenharia social. O Engenheiro Social pode potencialmente beneficiar as empresas como uma ferramenta imersiva de autotreinamento para seus funcionários, apoiar especialistas em segurança no ensino de conscientização de engenharia social como parte de um curso de treinamento abrangente e entreter indivíduos interessados, aproveitando mecânicas de jogo divertidas e inovadoras.

Alghenaim et al. (2021) propuseram um modelo de conscientização conceitual projetado para aumentar a conscientização dos funcionários no setor público saudita para lidar com falta de conscientização dos funcionários sobre ataques de engenharia social. Além disso, a pesquisa examina um ator do setor público na Arábia Saudita como um estudo de caso. As descobertas levaram à criação de um modelo composto por cinco componentes: um modelo de conscientização de situação para *phishing*, uma ferramenta de conscientização de segurança da informação, um triângulo de poder-conhecimento-prática, métricas de acompanhamento do setor público saudita e fases de implementação.

O trabalho de Mouton, Teixeira e Meyer (2017), descreve como o SEADMv2 foi implementado como um aplicativo *Android* chamado *Social Engineering Prevention Training*

Tool (SEPTT). Ele também descreve o experimento que foi realizado para testar se a implementação *Android* do SEADMv2 atende a sua finalidade e melhora a capacidade das pessoas de detectar ataques maliciosos de engenharia social corretamente. Os resultados obtidos com a realização do experimento foram analisados, usando medidas estatísticas apropriadas, para garantir que os resultados sejam estatisticamente significativos.

No trabalho de Tioh, Mina e Jacobson (2019) foi implementada uma ferramenta extensível de ensino na forma de um jogo sério projetado para ajudar a incutir segurança de computador e relevante práticas para usuários que podem não ter necessariamente formação técnica, em um esforço para se proteger contra alguns dos ataques de engenharia social mais comuns.

Beckers e Pape (2016) propuseram o uso de um jogo de cartas para elicitar esses requisitos, que todos os funcionários de uma empresa podem jogar para entender a ameaça e os requisitos de segurança do documento. O jogo considera o contexto individual de uma empresa e apresenta os princípios subjacentes do comportamento humano que os engenheiros sociais exploram, bem como padrões de ataque concretos. A abordagem avaliou vários grupos de pesquisadores, administradores de TI e profissionais da indústria.

O principal objetivo do estudo de OBUHUMA e ZIVUKU (2020) foi apresentar e demonstrar uma abordagem analítica para a Engenharia Social no Quênia e, em seguida, desenvolver um modelo para controlar a Engenharia Social. Para atingir este objetivo, foram considerados os seguintes objetivos específicos: explorar o nível de compreensão das várias formas de Engenharia Social no Quênia; determinar a prevalência de ataques de Engenharia Social no Quênia e propor um modelo que possa atuar como uma contramedida para a Engenharia Social. O estudo rendeu resultados promissores e em nível mais amplo, levando a uma proposta de modelo de conscientização da Engenharia Social, na forma de um sistema especialista.

A utilização de um sistema especialista como ferramenta de conscientização para evitar ataques de engenharia social se justifica porque esse tipo de ataque é altamente sofisticado e muitas vezes se aproveita da falta de conhecimento dos usuários sobre as melhores práticas de segurança da informação para obter informações sigilosas ou acesso não autorizado a sistemas. Um sistema especialista pode ajudar a conscientizar os usuários sobre as técnicas de engenharia social mais comuns e ensiná-los a identificar sinais de alerta, como por exemplo, pedidos de informações pessoais ou solicitações urgentes e incomuns, que possam indicar a ocorrência de um ataque de engenharia social. Dessa forma, a utilização de um sistema especialista pode ser uma forma efetiva de aumentar a segurança das organizações e proteger informações sensíveis contra ataques mal-intencionados.

4.3 Resultados

O Mapeamento foi realizado entre o mês de março de 2022 e o mês de maio de 2022. Com a aplicação da *string* de busca e palavras-chaves em inglês nas bases foram encontradas

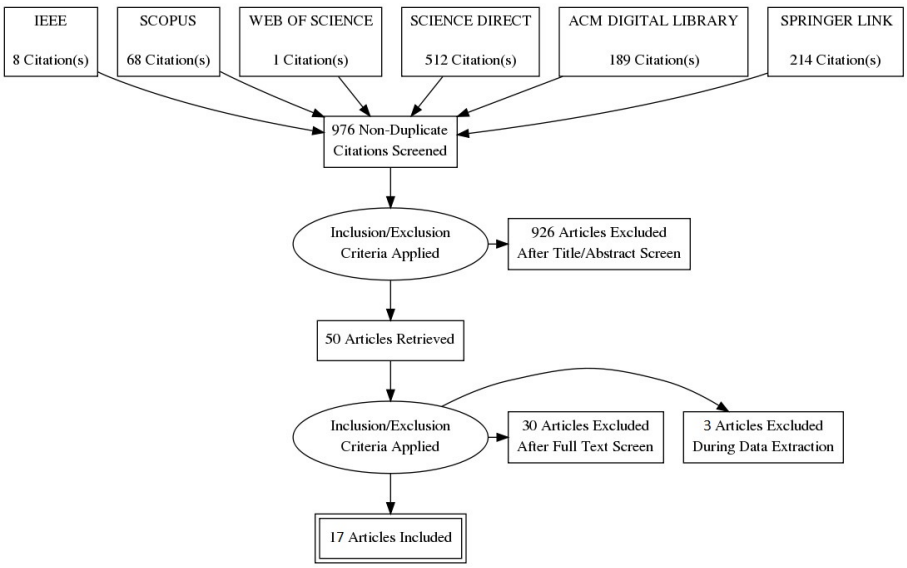
Quadro 1 – Comparação entre os trabalhos relacionados.

Autor	Tipo org.	Ataques	Conscien-tização	Política Seg.	Fer-ramenta
(HAMMOUR et al. 2019)	X	X	X		
(GRASSEGGER; NEDBAL, 2021)		X	X		
(ASTAKHOVA; MEDVEDEV, 2020)	X	X			X
(WILSON, 2018)	X	X	X		
(MOUTON; LEENEN; VENTER, 2016)	X	X			
(SOHRABI SAFA et al. 2016)			X	X	
(KROMBHOLZ et al. 2015)	X	X			
(OSUAGWU et al. 2015)		X	X	X	X
(KHLOBYSTOVA; ABRAMOV, 2021)					
(JANSEN; FISCHBACH, 2020)	X	X	X		X
(OBUHUMA; ZIVUKU, 2020)	X	X	X		X
(ALDAWOOD; SKINNER, 2019)	X	X	X		X
(ALDAWOOD; SKINNER, 2020)	X	X	X		X
(ALGHENAIM et al. 2021)	X	X	X		X
(MOUTON; TEIXERA; MEYER, 2017)	X	X	X		X
(TIOH; MINA; JACOBSON, 2019)	X	X	X		X
(BECKERS; PAPE, 2016)	X	X	X		X
PROPOSTA	X	X	X		X

inicialmente 992 artigos. Com a intenção de determinar um critério para a inclusão e exclusão dos artigos, foram analisados seus principais campos título (*title*), palavras-chave (*key words*), resumo (*abstract*), a introdução (*introduction*) e a conclusão (*conclusion*) para os resultados retornados, obtendo-se 50 artigos nas seis bases utilizadas. Foi realizada uma leitura no artigo por completo resultando em 30 artigos relevantes. Por fim, com a extração dos dados resultou em 17 artigos.

A Figura 1 apresenta um fluxo descrevendo o processo de extração dos artigos desde a base até a análise.

Figura 1 – Gráfico de prisma com a extração de dados



Fonte: Elaborada pelo autor

4.3.1 Resposta da questão de pesquisa 1

A resposta para a questão de pesquisa Q1, Qual tipo de organização que mais aparece como alvo de ataques de engenharia social?, é ilustrada na Quadro 2, a qual apresenta organizações que foram alvo de ataques de engenharia social.

Quadro 2 – Tipo de organização que mais aparece como alvo de ataques de engenharia social.

Tipo de Organizações	**Referências**
Instituições Financeiras	(ASTAKHOVA; MEDVEDEV, 2020) (HAMMOUR et al., 2019)
Não Governamentais	(WILSON, 2018)
Governamentais	(KROMBHOLZ et al., 2015) (WILCOX; BHATTACHARYA, 2020) (ALGHENAIM et al., 2021) (OBUHUMA; ZIVUKU, 2020)
Empresarial	(ASTAKHOVA; MEDVEDEV, 2020) (KROMBHOLZ et al., 2015) (WILCOX; BHATTACHARYA, 2020) (MOUTON; LEENEN; VENTER, 2016) (JANSEN; FISCHBACH, 2020) (ALDAWOOD; SKINNER, 2020) (MOUTON; TEIXEIRA; MEYER, 2017) (TIOH; MINA; JACOBSON, 2019) (BECKERS; PAPE, 2016)

De acordo com esses resultados, verifica-se que os tipos de organizações com maior quantidade de referências sobre alvo de ataques de engenharia social são as empresariais.

4.3.2 Resposta da questão de pesquisa 2

A resposta para a questão de pesquisa Q2, Quais principais ataques de engenharia social nas organizações?, é ilustrada na Quadro 3, a qual mostra o ataque de engenharia social com maior evidência nas organizações.

Quadro 3 – Principais ataques de engenharia Social nas organizações.

Ataques de Engenharia Social	**Referências**
Phishing	(MOUTON; LEENEN; VENTER, 2016) (ASTAKHOVA; MEDVEDEV, 2020) (Rocha Flores; EKSTEDT, 2016) (KROMBHOLZ et al., 2015) (OSUAGWU et al., 2015) (WILSON, 2018) (HAMMOUR et al., 2019) (WILCOX; BHATTACHARYA, 2020) (GRASSEGGER; NEDBAL, 2021) (OBUHUMA; ZIVUKU, 2020) (ALDAWOOD; SKINNER, 2019) (ALDAWOOD; SKINNER, 2020) (ALGHENAIM et al., 2021) (TIOH; MINA; JACOBSON, 2019)
Spear Phishing	(KROMBHOLZ et al., 2015) (OSUAGWU et al., 2015) (GRASSEGGER; NEDBAL, 2021)
Vishing	(WILSON, 2018) (OBUHUMA; ZIVUKU, 2020)
Smishing	(OBUHUMA; ZIVUKU, 2020)
Pretexting	(MOUTON; LEENEN; VENTER, 2016) (WILSON, 2018) (OSUAGWU et al., 2015) (JANSEN; FISCHBACH, 2020) (GRASSEGGER; NEDBAL, 2021) (ALDAWOOD; SKINNER, 2020) (BECKERS; PAPE, 2016)
Quid Pro Quo	(MOUTON; LEENEN; VENTER, 2016) (WILSON, 2018)
Baiting	(MOUTON; LEENEN; VENTER, 2016) (KROMBHOLZ et al., 2015) (WILSON, 2018) (GRASSEGGER; NEDBAL, 2021)
Tailgating	(WILSON, 2018)
Waterholing	(KROMBHOLZ et al., 2015) (WILSON, 2018) (GRASSEGGER; NEDBAL, 2021)
Spoofing	(OSUAGWU et al., 2015)
Dumpster Diving	(KROMBHOLZ et al., 2015) (OSUAGWU et al., 2015) (GRASSEGGER; NEDBAL, 2021)
Shoulder surfing	(KROMBHOLZ et al., 2015) (OSUAGWU et al., 2015) (GRASSEGGER; NEDBAL, 2021)
Road Apples	(OSUAGWU et al., 2015)
Reverse social engineering	(KROMBHOLZ et al., 2015) (GRASSEGGER; NEDBAL, 2021)
Advanced Persistent Threat	(KROMBHOLZ et al., 2015)

De acordo com esses resultados verifica-se que os principais ataques de engenharia social com maiores quantidades de referências com ênfase nas organizações são *Phishing*, *Pretexting* e *Baiting*.

4.3.3 Resposta da questão de pesquisa 3

A reposta para a questão de pesquisa Q3, Quais métodos e/ou técnicas de defesa utilizadas para evitar os desvios de informações de valor organizacional.?,é ilustrada na Quadro 4, a qual mostra os métodos e/ou técnicas de defesa utilizadas para evitar os desvios de informações de valor organizacional.

Quadro 4 – Métodos e/ou técnicas de defesa utilizadas para evitar os desvios de informações de valor organizacional.

Métodos e/ou Técnicas	**Referências**
Aplicação da política e processo dentro da organização	(ARABIA-OBEDOZA et al., 2020b) (OSUAGWU et al., 2015) (Sohrabi Safa; Von Solms; FURNELL, 2016)
Programas e treinamentos de conscientização do usuário humano	(HAMMOUR et al., 2019) (GRASSEGGER; NEDBAL, 2021) (Sohrabi Safa; Von Solms; FURNELL, 2016) (WILSON, 2018) (ARABIA-OBEDOZA et al., 2020b) (OSUAGWU et al., 2015) (JANSEN; FISCHBACH, 2020) (ALDAWOOD; SKINNER, 2020) (ALGHENAIM et al., 2021) (MOUTON; TEIXEIRA; MEYER, 2017) (TIOH; MINA; JACOBSON, 2019) (BECKERS; PAPE, 2016) (OBUHUMA; ZIVUKU, 2020)
Ferramentas	(ASTAKHOVA; MEDVEDEV, 2020) (OSUAGWU et al., 2015) (JANSEN; FISCHBACH, 2020) (ALGHENAIM et al., 2021) (MOUTON; TEIXEIRA; MEYER, 2017) (TIOH; MINA; JACOBSON, 2019) (BECKERS; PAPE, 2016) (OBUHUMA; ZIVUKU, 2020)
Blacklisting	(ARABIA-OBEDOZA et al., 2020b)
Flow whitelisting	(ARABIA-OBEDOZA et al., 2020b)

De acordo com esses resultados verifica-se que os métodos e/ou técnicas com maiores quantidades de referências para aplicação nas organizações com ênfase na defesa utilizadas para evitar os desvios de informações de valor organizacional são programas e treinamentos de conscientização do usuário humano, aplicação da política e processo dentro da organização e ferramentas.

4.4 Síntese Narrativa

A proteção de dados é uma preocupação séria dentro de qualquer empresa ou organização. Os futuros profissionais de segurança cibernética precisam ter experiência tanto no aspecto técnico da segurança quanto no elemento humano da segurança.

Quantitativamente, a observação dos resultados permitiu observar que em primeiro lugar, o tipo de organização que mais aparece são as empresas. Em segundo lugar, os principais tipos de ataques nas organizações são *Phishing*, *Pretexting* e *Baiting*. Terceiro, os métodos e/ou técnicas com ênfase na defesa utilizadas para evitar os desvios de informações de valor organizacional são programas e treinamentos de conscientização do usuário humano, aplicação da política e processo dentro da organização e ferramentas.

Para tais defesas, os trabalhos relatam uma constante busca por soluções frente à vulnerabilidade referente a engenharia social à qual os usuários estão expostos. Grande parte dos trabalhos analisados apontam a falta de treinamentos de conscientização do usuário humano e/ou a aplicação da política e processo dentro da organização sobre engenharia social. Com base nas observações dos estudos, se as pessoas souberem quais são as formas de ataques de engenharia social, elas estarão menos propensas a se tornarem vítimas.

4.5 Ameaças à validade

As ameaças à validade do presente estudo foram:

Viés de seleção: no início do processo, aplicou-se os critérios de inclusão e exclusão com base em nosso julgamento e os estudos foram incluídos ou excluídos neste estudo de mapeamento. Isso significa que alguns estudos podem ter sido categorizados incorretamente. Com a intenção de mitigar esta ameaça, discutimos o protocolo do estudo entre os pesquisadores para garantir o entendimento comum deste.

Validade de construção: pode ser avaliada a partir da definição clara e precisa das questões de pesquisa e da *string* de busca utilizada para coletar os dados. No entanto, é importante ressaltar que essas questões e termos foram definidos pelos pesquisadores, e podem não abranger todas as nuances do tema em questão.

Extração de dados: viés ou problema de extração pode afetar a caracterização das abordagens e análise de estudos selecionados. A fim de reduzir este viés, discutimos profundamente as categorias e as formas de extração. A extração de dados foi realizada conjuntamente por dois pesquisadores. Se os pesquisadores discordarem sobre uma classificação ou informações extraídas, uma terceira opinião foi considerada para resolver as diferenças e para garantir que os dados extraídos sejam válidos e claros para análises posteriores.

Validade externa: realizamos um estudo de mapeamento sistemático sobre os estudos publicados a partir de 2012 nas bases da IEEE Xplore Digital Library, Scopus, Web of Science, Science Direct, ACM Digital Library, Springer Link e Compendex. Este ponto implica que podemos ter perdido alguns estudos relevantes contidos nestas bases de dados e em outras bases que não foram utilizadas. Assim, não podemos generalizar nossas conclusões de todas as abordagens. No entanto, nossos resultados podem apoiar futuras investigações nessa área.

4.6 Considerações do Capítulo

O presente capítulo proporcionou uma análise abrangente sobre a engenharia social, um dos principais desafios enfrentados pelas organizações na proteção de seus dados e recursos. Através do mapeamento sistemático da literatura, foi possível identificar os tipos mais comuns de organizações alvo de ataques de engenharia social, os principais métodos e técnicas de ataque utilizados, bem como as estratégias de defesa adotadas por essas organizações.

Os resultados revelaram que empresas são os principais alvos de ataques de engenharia social, destacando a importância de investir em programas de conscientização do usuário humano e na aplicação de políticas e processos internos para mitigar essas ameaças. Além disso, os ataques mais frequentes incluem *Phishing*, *Pretexting* e *Baiting*, ressaltando a necessidade de medidas proativas para detectar e prevenir tais ataques.

As conclusões deste estudo enfatizam a importância de uma abordagem multidisciplinar na proteção contra engenharia social, que vai além das medidas tecnológicas tradicionais e inclui a conscientização dos usuários. Futuras pesquisas podem se concentrar no desenvolvimento de ferramentas e estratégias mais avançadas para combater essas ameaças e na avaliação da eficácia das medidas de defesa adotadas pelas organizações.

Em suma, este estudo contribui para o entendimento mais profundo da engenharia social e suas implicações para a segurança da informação, fornecendo *insights* valiosos para profissionais de segurança cibernética, gestores de TI e pesquisadores interessados em proteger as organizações contra ameaças cada vez mais sofisticadas.

5

Uma Exploração Abrangente de Estratégias de Conscientização Contra Ataques de Engenharia Social

No cenário digital dinâmico e em constante mudança de hoje, proteger informações confidenciais contra ameaças cibernéticas tornou-se uma prioridade inegável. Entre os vários desafios enfrentados no domínio da segurança da informação, os ataques de engenharia social surgem como uma ameaça particularmente insidiosa, explorando o factor humano para comprometer as defesas digitais. Neste contexto desafiador, os sistemas especialistas, ferramentas que replicam a capacidade de tomada de decisão dos especialistas humanos, destacam-se no campo da inteligência artificial.

Esses sistemas são meticulosamente projetados para enfrentar desafios complexos, operando com base em regras lógicas fundamentadas na estrutura "se-então". Aplicados notavelmente na tomada de decisões educacionais, sua utilidade se estende, conforme demonstrado por Hijji e Alam (2022), para a conscientização e treinamento em segurança cibernética, possibilitando uma abordagem educacional eficaz.

À medida que nos aprofundarmos neste tópico, este capítulo se desenvolverá de forma estruturada. Inicialmente, forneceremos uma breve recapitulação conceitual à engenharia social e exemplos de ataques do mundo real, oferecendo o contexto essencial necessário para a análise subsequente do papel central desempenhado pelos sistemas especialistas no âmbito da segurança da informação. A seguir, elucidaremos a metodologia exploratória adotada em nossa pesquisa, fornecendo *insights* sobre a abordagem empregada para a coleta e análise da literatura relevante. As seções subsequentes aprofundarão os resultados de trabalhos seminais, examinando as sementes identificadas e suas contribuições para a compreensão da interseção entre sistemas especialistas e segurança da informação.

Além disso, dedicaremos uma seção à discussão, onde aprofundaremos as análises realizadas e exploraremos conexões mais profundas entre os resultados. Finalmente, na conclusão,

resumiremos as principais conclusões e destacaremos as implicações práticas. Através desta abordagem estruturada, o nosso objetivo é fornecer uma visão abrangente das estratégias adotadas pelos sistemas especialistas para fortalecer a conscientização e o treinamento contra ataques sofisticados de engenharia social.

5.1 Relembrando o Conceito: Engenharia Social

A engenharia social, conforme elucidado por Mitnick e Simon (2003), envolve a manipulação, decepção e influência de indivíduos dentro de uma organização para atender a solicitações específicas, que vão desde a divulgação de informações sensíveis até a execução de tarefas benéficas ao atacante. Isso inclui interações simples, como chamadas telefônicas, e estratégias mais complexas, como orientar o alvo a visitar um site que explora vulnerabilidades técnicas para assumir o controle de seu computador.

No âmbito da segurança de Tecnologias da Informação e Comunicação (TIC), Hadnagy (2010) fornece contexto para a engenharia social, abordando ações voltadas para a obtenção e exploração de informações valiosas, incluindo dados confidenciais de organizações e sistemas computacionais, tudo isso explorando a confiança das pessoas.

Definida por Coelho, Rasma e Morales (2013a), a engenharia social compreende um conjunto de técnicas para manipular pessoas, levando-as a realizar ações ou divulgar informações que normalmente não revelariam.

Destacando a importância da implementação e monitoramento de mecanismos de segurança, aliados a precauções específicas relacionadas aos resíduos eletrônicos para mitigar ameaças de engenharia social, Aramuni e Maia (2020a) enfatizam a necessidade de tais medidas. Além disso, a conscientização do usuário, conforme destacado por Silva, Araújo e Azevedo (2013), é fundamental para as empresas. Implementar estratégias apropriadas para o uso seguro de redes sociais online é crucial, visando evitar cair vítima de ataques de engenharia social.

5.1.1 Ataques de Engenharia Social

Abaixo estão exemplos reais de ataques de engenharia social, ilustrando sua diversidade e sofisticação:

1. A Ubiquiti Networks em Hong Kong sofreu uma perda de aproximadamente USD 40 milhões em um ataque de phishing, no qual os invasores comprometeram a conta de e-mail de um funcionário de alto escalão, solicitando pagamentos fraudulentos (PINZON et al., 2015).

2. Durante as eleições presidenciais dos EUA em 2016, hackers utilizaram spear phishing para criar um e-mail falso no Gmail, levando os usuários a alterar senhas. O subsequente

vazamento de e-mails influenciou o resultado da eleição, favorecendo Donald Trump em relação a Hillary Clinton (HONORIO, 2018).

3. O condado de Cabarrus, nos Estados Unidos, foi vítima de um ataque de engenharia social resultando em uma perda de USD 1,7 milhão. Hackers usaram e-mails maliciosos, se passando por fornecedores, para solicitar pagamentos para uma nova conta bancária (JUNIOR, 2018).

4. A Toyota Boshoku Corporation teve uma perda de aproximadamente USD 37 milhões em um ataque de engenharia social no Japão. Os invasores persuadiram um executivo financeiro a alterar informações bancárias para uma transferência eletrônica (PASCHOAL; PEREIRA, 2019).

5. Um golpe de phishing resultou em uma perda de aproximadamente USD 400.000, onde um cibercriminoso se passou por assistente de uma vítima, solicitando pagamento relacionado a investimentos imobiliários (DANTAS, 2022).

6. Um hacker de 18 anos obteve acesso à rede interna da Uber. Isso foi resultado direto de um ataque de phishing, e a vítima, que era um funcionário, aprovou uma solicitação de MFA. O invasor então investigou mais profundamente nos sistemas internos da Uber e encontrou um script PowerShell com credenciais de administrador que lhe deu acesso à AWS, OneLogin e GSuite, entre outros (NAIR; ACHARY, 2023).

7. Esse *hack* foi supostamente realizado pelo mesmo hacker que fez o *hack* da Uber. O hacker usou engenharia social para entrar no servidor *Slack* deles, enganando um dos funcionários. Ele conseguiu obter o código-fonte dos jogos GTA V e GTA VI (não lançado) e também divulgou algumas gravações de tela do jogo, que parecem ser uma versão de depuração (NAIR; ACHARY, 2023).

Esses exemplos destacam a necessidade de estratégias robustas de conscientização e segurança para mitigar efetivamente as diversas e sofisticadas ameaças impostas pela engenharia social.

Compreender a diversidade e sofisticação dos ataques de engenharia social destaca a necessidade de estratégias eficazes de conscientização e segurança. Nesse contexto, vamos agora aprofundar na metodologia de pesquisa exploratória, uma abordagem crucial que empregamos para aprofundar nossa compreensão desses desafios e oportunidades.

5.2 Pesquisa Exploratória

Uma pesquisa complementar se fez necessária para elucidar as informações empreendidas neste trabalho. Para tanto, adotamos uma metodologia de pesquisa exploratória. Este método

permite uma investigação detalhada e abrangente de um fenômeno pouco compreendido, proporcionando uma base sólida para futuras investigações.

A insuficiência de resultados na fase de Mapeamento Sistemático na pesquisa empreendida sugere a utilização desta metodologia como um ponto de partida para investigar mais profundamente o papel dos sistemas especialistas na segurança da informação. Inicialmente, a pesquisa concentrou-se em compreender as ameaças de engenharia social, os tipos de ataques predominantes e as técnicas de defesa existentes. No entanto, a análise desses elementos não trouxe à tona, até o momento, *insights* suficientes sobre o impacto dos sistemas especialistas no processo de conscientização e treinamento.

Ao concluir o mapeamento sistemático, tornou-se claro que os programas de conscientização e treinamento foram identificados como estratégias cruciais para fortalecer o fator humano como parte ativa da segurança da informação, conforme destacado por vários autores revisados. Neste ponto, a ausência de uma abordagem mais aprofundada sobre o papel dos sistemas especialistas nesta dinâmica revelou uma lacuna em nossa compreensão do panorama atual da segurança da informação.

Dessa forma, a metodologia exploratória é proposta como um caminho estratégico para preencher essa lacuna e investigar de maneira mais específica como os sistemas especialistas podem ser efetivamente incorporados no contexto da conscientização e treinamento em relação às ameaças de engenharia social. Esta abordagem visa contribuir significativamente para a compreensão da interseção entre sistemas especialistas e práticas de segurança da informação, promovendo uma visão mais abrangente e informada sobre as estratégias de proteção digital.

Para a elaboração desta revisão, realizou-se uma busca no Google Scholar durante o período de 02 a 20 de janeiro de 2023, com os seguintes termos de busca: ("expert system") AND ("information security"OR "cyber security") AND ("social engineering") AND ("education"OR "awareness"OR "training"). A partir dos critérios de seleção, foram escolhidos cinco trabalhos seminais. Os trabalhos selecionados passaram pelos seguintes critérios de seleção:

- Inclusão entre os 10 principais resultados retornados pelo Google Scholar, com a condição de que o artigo seja acessível;
- Publicação entre 2013 e 2023, priorizando trabalhos recentes para resultados e informações atualizados;
- Exclusão de livros ou artigos de sites e blogs das fontes consideradas.

Embora os artigos iniciais selecionados tenham fornecido informações valiosas sobre o panorama mais amplo dos sistemas especialistas e da segurança da informação, é digno de nota mencionar que não geraram sementes adicionais. Esta limitação é atribuída às restrições temáticas e ao recorte temporal especificado para esta pesquisa (2013 a 2023). Consequentemente,

a ausência de sementes derivadas destes artigos iniciais influenciou o escopo e a amplitude da revisão da literatura, particularmente em determinadas áreas temáticas. Essas restrições são reconhecidas como aspectos inerentes ao processo de pesquisa e são explicadas para proporcionar transparência quanto às complexidades da metodologia.

Com a metodologia exploratória estabelecendo as bases para a nossa investigação. Ao aplicar esta abordagem metodológica refinada aos trabalhos selecionados, podemos discernir padrões significativos e colher informações valiosas sobre o papel dos sistemas especialistas na segurança da informação. Vamos nos aprofundar em como cada artigo inicial contribui para uma compreensão mais ampla da interseção entre sistemas especialistas e ameaças à segurança digital.

5.3 Visão Geral da Literatura Selecionada

Antes de nos aprofundarmos nas especificidades de cada artigo inicial, vamos fornecer uma breve visão geral dos principais *insights* obtidos na literatura selecionada.

A tabela 3 descreve os artigos iniciais escolhidos para a revisão, cada um contribuindo com perspectivas únicas para a interseção de sistemas especialistas e segurança da informação.

Tabela 3 – Sementes da revisão

ID	Título	Referência
S1	CSAAES: Um sistema especialista para conscientização sobre ataques de segurança cibernética	(RANI; GOEL, 2015)
S2	Ataques cibernéticos baseados em engenharia social no Quênia	(OBUHUMA; ZIVUKU, 2020)
S3	Desenvolvimento de sistema especializado consultivo baseado em conhecimento para identificar e mitigar ameaças internas não intencionais em instituições financeiras da Etiópia	(ADANE, 2020)
S4	Um Modelo Eficaz de Treinamento de Conscientização em Segurança Cibernética: Primeira Defesa de uma Estratégia de Segurança Organizacional	(DASH; ANSARI, 2022)
S5	Sistema especialista com lógica *Fuzzy* para proteção de recursos de informação científica	(NORMATOV; RAKHMATULLAEV, 2020)

Fonte: Autores, 2023

S-1 ou primeira semente, contempla o artigo de Rani e Goel (2015), foi a primeira semente selecionada. O artigo discute a necessidade de proteção contra ataques cibernéticos, devido à vasta utilização da internet e à exposição de informações. Apresenta um sistema especialista chamado CSAAES, que visa conscientizar os usuários sobre diferentes tipos de ataques e seus sintomas, além de fornecer contramedidas para lidar com esses ataques. O sistema é implementado usando o *framework* Visual Studio 10.0 e ASP.NET, com regras gerenciadas na estrutura dot net no *back-end*. Ele identifica possíveis ataques com base nos sintomas observados e fornece soluções

para os ataques identificados. O sistema especialista pode continuar solicitando ao usuário o próximo sintoma com base no problema enfrentado por ele. O usuário pode inserir problemas adicionais que não estão presentes na lista. O sistema pode ser dinamizado e melhorado com base nos sintomas inseridos pelo usuário. A semente S-1 é baseada no artigo Rani e Goel (2015), cujas sementes são os artigos referenciados. No entanto, observamos que os artigos referenciados estão fora da faixa temporal estabelecida para esta pesquisa (2013 a 2023). Portanto, as possíveis sementes derivadas desse artigo estão limitadas aos artigos publicados fora do intervalo de tempo especificado, resultando na ausência de sementes relevantes durante a busca. Esta semente, portanto, não retornou outras sementes dentro dos critérios estabelecidos.

A S-2, ou segunda semente, se refere ao artigo de OBUHUMA e ZIVUKU (2020), este artigo trata sobre ciberataques baseados em engenharia social no Quênia. Ele destaca que a engenharia social é uma das artes utilizadas pelos cibercriminosos para explorar a camada mais fraca dos sistemas de segurança da informação, que são os usuários. O estudo apresenta as principais técnicas de engenharia social utilizadas pelos cibercriminosos no Quênia, como o uso de autoridade, prova social e a criação de laços à distância. Além disso, o estudo aponta que os quenianos são vítimas da engenharia social devido à falta de conscientização e/ou educação do usuário. O artigo também apresenta um modelo de conscientização da engenharia social na forma de um sistema especialista, que pode ser usado por indivíduos e organizações para incutir uma mentalidade segura sobre como evitar ataques de engenharia social. Por fim, o artigo destaca a importância de trabalhos futuros para a implementação e validação do modelo por um tamanho de amostra maior. Ao analisar as referências do artigo, não foram identificados documentos que estejam especificamente voltados para sistemas especialistas no contexto da segurança da informação. A pesquisa, portanto, não gerou outras sementes devido à limitação temática das referências disponíveis.

A S-3 - ou terceira semente, se refere ao artigo de Adane (2020), ele discute a importância da segurança em instituições financeiras e como a automação pode aumentar a vulnerabilidade a atores maliciosos internos e externos. O texto destaca a dificuldade em detectar, defender ou isolar ameaças internas, uma vez que são funcionários confiáveis que podem cometer erros inocentes ou inadvertidamente passar informações confidenciais. O artigo propõe um sistema especializado baseado em conhecimento para mitigar ameaças internas não intencionais em instituições financeiras na Etiópia, fornecendo orientação e recomendações à equipe de segurança. O artigo tem como objetivo fornecer uma solução prática para mitigar ameaças internas em instituições financeiras.

A S-4 - ou quarta semente, se refere ao artigo Dash e Ansari (2022) este artigo destaca a importância da Educação, Treinamento e Conscientização em Segurança para as organizações promoverem a eficiência e acessibilidade. O modelo proposto no artigo inclui três componentes principais: conscientização em segurança, treinamento em segurança e educação em segurança. O artigo também discute a importância de programas SETA (Security Education Training and

Awareness) eficazes e como eles devem ser constantes, complementares e compensatórios. Além disso, o artigo destaca a importância de programas SETA serem acessíveis e de baixo custo, mas ainda assim fornecerem um grau ótimo de segurança. O *viCyber* é uma ferramenta útil para desenvolver currículos de segurança cibernética de forma rápida e confiável, baseado em um modelo de sistema especialista. O *viCyber* é governado pelo *framework NICE* e possui um mecanismo de *feedback* e recomendação baseado na perspectiva do usuário. O modelo usa um sistema de suporte à decisão baseado na interação humano-computador para descrever o processo de construção e ajudar a modificar a compreensão conceitual do usuário durante o treinamento com *feedback* em tempo real. Este não gerou outras sementes devido à limitação temática das referências disponíveis.

A S-5 - ou quinta semente, se refere ao artigo de Normatov e Rakhmatullaev (2020) este artigo trata de sistemas especialistas com lógica *fuzzy*, também conhecida como lógica difusa, é uma extensão da lógica booleana que permite lidar com incertezas e imprecisões de uma maneira mais flexível, para proteger recursos de informação científica em bibliotecas e redes de informação corporativas. Ele destaca a importância da segurança da informação nessas redes e oferece métodos e ferramentas eficazes para proteger bancos de dados de recursos científicos e educacionais. O arquivo também menciona a coleta de dados primários por especialistas analistas e a colaboração com especialistas em segurança da informação para criar uma base de conhecimento. Em resumo, o arquivo fornece informações valiosas sobre a proteção de recursos de informação em bibliotecas e redes de informação corporativas. De acordo com Normatov e Rakhmatullaev (2020), os benefícios de usar sistemas especialistas para proteger recursos de informação em bibliotecas e centros de informação incluem a capacidade de detectar e prevenir ameaças de segurança, aprimorar a eficiência do sistema de segurança e reduzir o risco de perda de dados. Esses sistemas podem ser usados em conjunto com a conscientização dos usuários para aumentar a segurança da informação. A conscientização dos usuários é importante para garantir que eles entendam as políticas de segurança da informação e saibam como proteger seus dados pessoais. Além disso, a conscientização dos usuários pode ajudar a prevenir ataques de engenharia social, que são uma das principais ameaças à segurança da informação em bibliotecas e centros de informação. Este não gerou outras sementes devido à limitação temática das referências disponíveis

Tabela 4 – Comparação de artigos relacionados à pesquisa realizada

ID	Metodologia	Principais Resultados	Contribuições
S-1	Levantamento sobre programas de conscientização em segurança cibernética; Integração de sistemas especialistas	Identificou lacuna de conscientização; Propôs sistema especialista CSAAES	Insights sobre sistemas especialistas para conscientização em segurança cibernética
S-2	Estudo de caso sobre ataques cibernéticos no Quênia; Análise de técnicas de engenharia social	Revelou táticas de engenharia social; Propôs modelo de sistema especialista	Abordagem específica para lidar com ameaças de engenharia social
S-3	Pesquisa aplicada exploratória com abordagem quantitativa; Representação de conhecimento baseada em regras	Eficácia na detecção de ameaças internas	Solução prática para segurança interna em instituições financeiras
S-4	Pesquisa qualitativa utilizando o Modelo de Aceitação de Tecnologia (TAM); Exame de programas de treinamento em conscientização de segurança baseados em IA	Abordagem inovadora para educação e treinamento em segurança cibernética; Enfatizou a importância do SETA; Apresentou o modelo *viCyber*	Contribuição para treinamento em conscientização de segurança com IA
S-5	Análise do estado de desenvolvimento de pesquisas sobre proteção de bases de dados científicas e educacionais em bibliotecas; Aplicação de métodos de lógica *fuzzy*	Benefícios de sistemas especialistas com lógica *fuzzy*	*Insights* sobre o potencial da lógica *fuzzy* em segurança da informação

Fonte: Autores, 2023

5.4 Discussão

A síntese das descobertas dos artigos semente selecionados lança luz sobre a intricada relação entre sistemas especialistas e segurança da informação, com foco específico em conscientização e treinamento contra ameaças de engenharia social. Aqui, destilamos os principais insights derivados de nossa revisão:

CSAAES: Um sistema especialista para conscientização sobre ataques de segurança cibernética (RANI; GOEL, 2015): O trabalho de Rani e Goel destaca a necessidade crítica de conscientização sobre ataques cibernéticos na era do amplo uso da internet. O sistema especialista

CSAAES serve como uma ferramenta notável para aumentar a conscientização do usuário, enfatizando a importância de entender vários tipos de ataques e implementar contramedidas eficazes.

Ataques cibernéticos baseados em engenharia social no Quênia (OBUHUMA; ZIVUKU, 2020): A exploração de técnicas de engenharia social no contexto queniano, realizada por Obuhuma e Zivuku, ilumina as vulnerabilidades decorrentes da falta de conscientização do usuário. O modelo proposto de conscientização baseado em sistema especialista destaca-se como uma estratégia potencial para promover uma mentalidade segura e combater ataques de engenharia social.

Desenvolvimento de um sistema especialista baseado em conhecimento consultivo para identificar e mitigar ameaças internas não intencionais em instituições financeiras etíopes (ADANE, 2020): O foco de Adane em ameaças internas dentro de instituições financeiras destaca os desafios apresentados por ações não intencionais de funcionários. O sistema especialista baseado em conhecimento oferece uma abordagem prática para identificar e mitigar essas ameaças, fornecendo insights valiosos para aprimorar as medidas de segurança interna.

Um Modelo Eficaz de Treinamento em Conscientização de Segurança Cibernética: Primeira Defesa de uma Estratégia de Segurança Organizacional (DASH; ANSARI, 2022): A ênfase de Dash e Ansari em Educação, Treinamento e Conscientização em Segurança (SETA) está alinhada ao reconhecimento crescente dos fatores humanos na segurança organizacional. O modelo viCyber, incorporando um sistema especialista, apresenta uma abordagem inovadora para desenvolver currículos de cibersegurança e aprimorar a compreensão do usuário, mostrando o potencial de sistemas especialistas em contextos educacionais.

Sistema especialista com lógica *fuzzy* para a proteção de recursos de informação científica (NORMATOV; RAKHMATULLAEV, 2020): A exploração de sistemas especialistas com lógica *fuzzy* para a proteção de recursos de informação por Normatov e Rakhmatullaev enfatiza a sinergia entre tecnologia e conscientização do usuário. A integração de sistemas especialistas, aliada à educação do usuário, surge como uma estratégia multifacetada para aprimorar a segurança da informação em bibliotecas científicas e redes corporativas.

Em essência, esses artigos reforçam coletivamente o papel fundamental dos sistemas especialistas em abordar diversos aspectos dos desafios de cibersegurança. A integração de soluções tecnológicas com conscientização do usuário surge como uma abordagem holística, reconhecendo o fator humano na cibersegurança. Essa síntese fornece uma visão abrangente, preparando o caminho para implementações práticas no campo dinâmico de sistemas especialistas e segurança da informação.

5.5 Considerações do Capítulo

Em conclusão, a revisão de sistemas especialistas no contexto da segurança da informação, com foco especial em conscientização e treinamento contra ameaças de engenharia social, revela um cenário rico em abordagens inovadoras e soluções práticas. Os artigos selecionados enfatizam coletivamente o papel fundamental dos sistemas especialistas em abordar vários aspectos dos desafios de cibersegurança. Desde aumentar a conscientização sobre ataques cibernéticos até mitigar ameaças internas e desenvolver modelos eficazes de treinamento em cibersegurança, esses artigos fornecem *insights* valiosos sobre as diversas aplicações de sistemas especialistas.

A síntese das descobertas destaca a necessidade de uma abordagem holística que combine soluções tecnológicas, como sistemas especialistas, com educação e conscientização do usuário. A eficácia dos sistemas especialistas não está apenas em suas capacidades técnicas, mas também em sua integração em estratégias mais amplas que consideram o fator humano na cibersegurança. Os artigos semente apresentados servem como base para evolução de sistemas especialistas na segurança da informação.

6

Projeto do APSEA

Esta dissertação tem como objetivo desenvolver um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social destinado aos usuários no contexto de funcionários de uma organização pública para instruir sobre como evitar ataques de engenharia social e ainda gerar diagnóstico de vulnerabilidade destes para o gestor. Esse sistema foi chamado de APSEA (**Awareness and Prevention Expert System against Engineering Attacks**). Apesar da maior incidência de ataques de engenharia social ocorrer em empresas privadas, a pesquisa no setor público se justifica pela vulnerabilidade das organizações governamentais a esse tipo de ataque e pela importância da conscientização dos usuários sobre as melhores práticas de segurança da informação para preveni-los e garantir a segurança dos dados e sistemas governamentais. Nesta, será abordado informações sobre engenharia social relacionadas a ataques e contramedidas. Essa ferramenta será composta por três módulos: gerente de TI, usuários e gerente de risco. O módulo do usuário permitirá a interação do usuário com informações, treinamento e questões sobre engenharia social, no qual o método *Forward Chaining* será aplicado durante a realização de questões. O módulo do gerente de TI permite que o mesmo alimente a base de dados da ferramenta. O módulo gerente de risco irá aplicar o *Forward Chaining* como método de inferência com as interações dos usuários e a partir destas gera relatórios que possibilitam ao gerente diagnosticar vulnerabilidade através de uma técnica de inteligência artificial, conhecida como sistema especialista, redirecionando os conteúdos apresentados para que os problemas encontrados sejam mitigados.

O *Forward Chaining* foi selecionado para o presente estudo devido à sua implementação simplificada. Essa técnica consiste em inferir conclusões a partir de fatos pré-existentes, seguindo um processo de raciocínio linear.

A estrutura básica de um Sistema Especialista, apresentada na Figura 2, é normalmente composto por uma base de conhecimento (heurística de informação, etc.), um mecanismo de inferência (analisa a base de conhecimento) e a interface do usuário final (aceita entradas, gera

saídas) (SIHWI; ANDRIYANTO; ANGGRAININGSIH, 2016)

Figura 2 – Estrutura Básica do SE

Fonte: Elaborada pelo autor

6.1 Base de Conhecimento

A Base de Conhecimento é fundamental para um Sistema Especialista, sendo definida como a fonte de informações utilizada por especialistas (FERREIRA et al., 2020). Essencial no núcleo de todo sistema, essa base contém o conhecimento necessário para atingir os objetivos propostos.

A Base de Conhecimento não se limita a ser apenas um depósito de dados, pois engloba uma variedade de regras destinadas a solucionar problemas de maneira direta e lógica. Desse modo, ao receber informações do usuário, esses sistemas são capazes de tomar decisões, agindo de forma análoga a especialistas (ROSSO; SILVA; SCALABRIN, 2009). Trata-se de um módulo principal de todo Sistema Especialista, pois contém o conhecimento necessário para que se consiga alcançar o objetivo pretendido. Pode-se dizer que a base de conhecimentos contém um somatório de crenças, fatos e heurísticas (RITA; AL., 2020).

A Base de Conhecimento é o elemento que armazena o conhecimento abstrato. Este conhecimento é armazenado em um conjunto de regras de produção do tipo [Se] premissa, [Então] conclusão (YANASE; TRIANTAPHYLLOU, 2019).

A Base de Conhecimento do APSEA foi meticulosamente construída por meio da aplicação de uma abordagem abrangente. Práticas fundamentadas nas políticas de segurança e privacidade estabelecidas pelo DETRAN/SE foram adotadas para preenchimento e desenvolvimento dessa base. A construção da base de conhecimento também envolveu a análise e referência a materiais relevantes, incluindo artigos especializados e outras fontes confiáveis.

O objetivo primordial foi abranger um espectro diversificado de tipos de ataques de engenharia social, refletindo as ameaças potenciais que podem impactar a segurança de organizações, especialmente no contexto do DETRAN/SE. Essa abordagem baseada em políticas e orientada por materiais especializados contribuiu para a robustez e relevância da base de

conhecimento, garantindo que as regras e *feedbacks* incorporados refletissem de maneira precisa e atualizada os desafios enfrentados na proteção contra ameaças cibernéticas.

A colaboração estreita com especialistas em segurança e o alinhamento constante com as diretrizes do DETRAN/SE garantiram que a base de conhecimento fosse construída com precisão, considerando as especificidades do ambiente organizacional. Esse processo, centrado em políticas e orientado por materiais confiáveis, foi essencial para estabelecer um sistema especialista robusto e eficaz na conscientização e prevenção de ataques de engenharia social.

A construção da base de conhecimento envolveu uma colaboração ativa entre o pesquisador e o analista de segurança da Informação Armando Douglas. Essa abordagem holística combinou experiência acadêmica e prática, assegurando que a base de conhecimento refletisse tanto a fundamentação teórica quanto as nuances práticas de enfrentar ameaças de engenharia social.

Para garantir a eficácia e a facilidade de gerenciamento, optou-se por empregar regras de produção simples. Essa escolha visou a praticidade e a acessibilidade na administração contínua da base de conhecimento. A simplificação das regras de produção não apenas facilita a manutenção, mas também contribui para uma compreensão clara e direta das orientações fornecidas aos usuários.

Após a construção inicial, a base de conhecimento passou por uma validação para garantir sua precisão e relevância. A colaboração com o analista de segurança da informação Armando Douglas desempenhou um papel fundamental nesse processo, fornecendo uma perspectiva prática valiosa para aprimorar a aplicabilidade das regras no contexto específico do DETRAN/SE.

Dessa forma, a construção da base de conhecimento foi uma iniciativa conjunta, alinhando conhecimentos teóricos e práticos para oferecer uma ferramenta robusta e eficaz na conscientização e prevenção de ataques de engenharia social.

Foi utilizado a base *PostGreSQL* que compreende um dos sistemas de gerenciamento de banco de dados mais utilizado na atualidade. É um sistema *open source* de gerenciamento de banco de dados de grande porte, define os tipos de dados, disponibilizando a manipulação e armazenamento dos mesmos, fornecendo dessa forma funções especiais e índices para consultas e manipulação dos dados.

6.2 Representação do Conhecimento

Durante a fase de Representação do Conhecimento, direcionamos nossos esforços para o desenvolvimento do APSEA destinado a conscientizar os usuários da AGIN no contexto do DETRAN/SE sobre os ataques de engenharia social, bem como fornecer ações educativas de como evitar esses ataques. Essa iniciativa foi impulsionada pelas informações cruciais fornecidas pelo Gestor de TI, em especial, no momento de adequação da LGPD no órgão.

A necessidade emergiu em consonância com as diretrizes da LGPD e outros requisitos

específicos, como os estabelecidos pelo Departamento Estadual de Trâsito de Sergipe (DETRAN/SE), incluindo a Gestão Contínua de Vulnerabilidades, a Conscientização sobre Segurança e Treinamento de Competências, e a Aquisição de Solução para Gestão de Respostas a Incidentes.

No âmbito da LGPD, o DETRAN/SE exige que a conscientização e o treinamento de competências em segurança sejam estabelecidos e mantidos como parte integrante de suas diretrizes. Nesse contexto, o APSEA não apenas atende a essa exigência, mas também se alinha com a necessidade contínua de avaliar e rastrear vulnerabilidades, conforme estabelecido na Gestão Contínua de Vulnerabilidades.

Além disso, o DETRAN/SE demanda a aquisição de uma solução para Gestão de Respostas a Incidentes, para preparar, detectar e responder rapidamente a ataques. O APSEA desenvolvido possui funcionalidades que contribuem diretamente para essa demanda, permitindo uma abordagem proativa na mitigação de riscos de segurança da informação.

Essa abordagem flexível e personalizável, fundamentada nas necessidades específicas da LGPD e das diretrizes do DETRAN/SE, reflete nosso compromisso com a adaptabilidade e eficácia na conscientização e prevenção de ataques de engenharia social.

6.3 Aquisição e Formação do Conhecimento

A fase de Aquisição e Formação do Conhecimento desempenha um papel crucial no desenvolvimento do Sistema Especialista (SE), pois consiste na obtenção e processamento de dados necessários para transformá-los em modelos e conhecimentos aplicáveis. Nessa etapa, realizamos o levantamento das informações fundamentais, seguindo as melhores práticas destacadas por (AZEVEDO; AL., 2019).

Durante esse estágio, buscamos obter dados relevantes para preenchimento e construção da base de conhecimento do SE, uma vez que a qualidade e abrangência dessas informações são essenciais para o desempenho eficaz do sistema. Além disso, como mencionado por Rita e al. (2020), essa etapa é a parte mais significativa do processo, destacando a importância do cuidadoso levantamento de informações.

O processo de Aquisição e Formação do Conhecimento foi fundamentado nas diretrizes e políticas de segurança do DETRAN/SE, garantindo que as informações coletadas estivessem alinhadas com os requisitos e desafios específicos enfrentados pelo órgão. Dessa forma, buscamos não apenas quantidade, mas também relevância e especificidade nas informações adquiridas.

Além disso, consideramos importante integrar *feedbacks* e validações contínuas durante essa fase, colaborando ativamente com o analista de segurança Armando Douglas para garantir a precisão e atualização das informações adquiridas. Essa abordagem colaborativa e iterativa foi essencial para construir uma base de conhecimento robusta e adaptada às necessidades específicas do DETRAN/SE.

Ao considerar a Aquisição e Formação do Conhecimento como uma etapa crucial, destacamos a relevância do cuidado na seleção, processamento e validação das informações, contribuindo diretamente para a eficácia e confiabilidade do APSEA desenvolvido.

6.4 Definição das Perguntas

Nesta etapa, as perguntas foram meticulosamente definidas para abranger os diversos tipos de ataques de engenharia social que representam potenciais ameaças à segurança de organizações públicas. Cada pergunta foi elaborada com base na natureza específica de cada tipo de ataque, considerando a realidade do ambiente organizacional e alinhada com as melhores práticas de prevenção.

Essas perguntas foram desenvolvidas para avaliar a compreensão e o conhecimento dos usuários em relação aos diferentes cenários de ataques, como *Phishing*, *Vishing*, *Pretexting*, *Quid Pro Quo*, entre outros. A abordagem visa não apenas identificar lacunas no entendimento do usuário, mas também fornecer orientações educativas específicas para fortalecer a conscientização e a capacidade de resposta diante dessas ameaças.

As perguntas foram definidas, destacando a diversidade de tópicos abordados e a abrangência das situações de risco contempladas pelo sistema especialista. Esse processo de definição de perguntas visa criar uma base sólida para a avaliação e conscientização dos usuários, contribuindo significativamente para a eficácia do sistema na prevenção de ataques de engenharia social. As perguntas estão apresentadas no (Apêndice A).

6.5 Definição das Regras

Ao desenvolver as regras para o APSEA, optamos por uma abordagem alinhada com o encadeamento para frente, também conhecido como raciocínio progressivo. Nesse modelo, partimos das informações fornecidas pelo usuário, aplicando regras para alcançar conclusões específicas. Cada regra, estruturada como "Se [condições] então [ações]", é composta por condições (premissas) e ações (conclusões), verificando as respostas do usuário e fornecendo *feedback* personalizado.

Essa escolha fundamenta-se em princípios científicos de inteligência artificial e sistemas especialistas, priorizando a simplicidade, adaptabilidade e eficácia na criação de sistemas para conscientização e educação em segurança.

A simplificação da estrutura das regras visa facilitar a interpretação tanto por parte dos usuários quanto pelos gestores encarregados da manutenção contínua. A clareza do *feedback* gerado é crucial para promover a conscientização e incentivar práticas de segurança.

A estrutura flexível das regras permite fácil adaptação a mudanças nas ameaças de

engenharia social, garantindo a eficiência do sistema diante de novos cenários. Essa flexibilidade é vital para a evolução contínua e para enfrentar novos desafios. As regras estão apresentadas no (Apêndice A).

A simplificação atende a um pedido específico do DETRAN/SE, visando garantir uma manutenção eficiente e facilitar a gestão do sistema. Essa abordagem estratégica torna o sistema mais acessível e compreensível para os gestores responsáveis pela manutenção e atualização da base de conhecimento.

Ao manter regras mais diretas, sem a utilização de complexidades, busca-se assegurar que as atualizações na base de conhecimento possam ser realizadas de maneira rápida e intuitiva. A ênfase está na praticidade e na minimização da curva de aprendizado para os administradores do sistema.

A simplificação contribui para a clareza das regras, tornando o sistema mais transparente para todos os envolvidos. A linguagem direta e a estrutura fácil de entender facilitam a identificação e correção de possíveis erros, promovendo uma manutenção eficaz.

Dessa forma, a escolha por uma abordagem mais simples reflete a consideração consciente das demandas específicas do DETRAN/SE, visando uma administração eficiente e descomplicada do APSEA.

6.6 Mecanismo de Inferência

O mecanismo de inferência desempenha um papel crucial na busca e manipulação do conhecimento armazenado, empregando regras heurísticas, esquemas de raciocínio ou inferências. Geralmente, define os algoritmos que determinarão quais regras serão satisfeitas pelos fatos ou objetivos, priorizando e executando aquelas de maior prioridade, conforme destacado por Rosa e al. (2019).

A inferência pode adotar abordagens como o encadeamento progressivo (*forward chaining*) ou o encadeamento regressivo (*backward chaining*) na base de conhecimento para chegar a uma decisão ou recomendação. O encadeamento regressivo, amplamente utilizado em Sistemas Especialistas (SE), exige que o desenvolvedor especifique na definição da base quais atributos devem ser encontrados, ou seja, os objetivos do SE. Nesse método, os consequentes das regras direcionam a busca, trabalhando de trás para frente para identificar os fatos que sustentam as hipóteses levantadas, como indicado por Yanase e Triantaphyllou (2019).

A máquina de inferência é responsável por encontrar uma atribuição para o atributo desejado nas conclusões das regras (após o ENTÃO...). Para que uma regra seja aprovada, suas premissas devem ser atendidas, desencadeando um processo recursivo em que a máquina busca os atributos das premissas para avaliação. Se o atributo procurado não for encontrado em nenhuma conclusão de regra, uma pergunta direta é feita ao usuário, conforme explicado por Yanase e

Triantaphyllou (2019).

Nossa abordagem para o mecanismo de inferência baseia-se no encadeamento progressivo (*forward chaining*), que é adequado para a natureza do APSEA. No encadeamento progressivo, começamos com as informações fornecidas pelo usuário e, em seguida, aplicamos as regras para chegar a conclusões específicas. Cada regra consiste em condições (premissas) e ações (conclusões), seguindo a estrutura "Se [condições] então [ações]".

A máquina de inferência percorre as regras na base de conhecimento, verificando se as condições são atendidas em relação às respostas do usuário. Quando uma regra é acionada, as ações correspondentes são executadas, gerando *feedback* personalizado para o usuário. Este processo é iterativo e continua até que todas as regras relevantes sejam consideradas.

Essa abordagem permite que o sistema progrida de maneira eficiente, adaptando-se dinamicamente às respostas do usuário e fornecendo orientações personalizadas com base nas condições específicas de cada caso.

A escolha do encadeamento progressivo é respaldada pela simplicidade, adaptabilidade e eficácia na geração de *feedback* personalizado. Além disso, essa abordagem é mais intuitiva para os usuários, uma vez que começa com as informações que forneceram, refletindo um fluxo natural de interação.

Em resumo, nossa máquina de inferência utiliza o encadeamento progressivo para proporcionar uma experiência de conscientização coerente e eficaz, adaptando-se dinamicamente às respostas do usuário e garantindo a relevância e personalização do *feedback* fornecido. Essa abordagem reflete nossa preocupação em tornar o sistema acessível e eficiente na conscientização contra ataques de engenharia social.

6.7 Interface de Interação com Usuário

A Interface de Interação com o Usuário (IU) desempenha um papel central na comunicação entre o Sistema Especialista (SE) e os usuários, servindo como o canal vital para a troca de informações. Este componente, acessível por meio do software, oferece uma interface que facilita a comunicação automática, seguindo uma abordagem que inicia com perguntas fundamentais. As respostas a essas perguntas são então registradas nas variáveis previamente definidas, conforme discutido por Rita e al. (2020).

A interface do usuário é crucial não apenas para coletar informações dos usuários, mas também para encaminhar solicitações à máquina de inferência, desempenhando um papel vital na exibição das respostas do SE em relação às perguntas do usuário, conforme destacado por Ferreira e al. (2020).

No desenvolvimento dessa interação eficaz, optamos por utilizar o *framework* Laravel, que é um *framework* de aplicativo *web* em *PHP*, e a linguagem de programação *PHP* para

implementar a lógica do APSEA. O Laravel é reconhecido por sua elegância, simplicidade e eficiência, fornecendo uma estrutura robusta para o desenvolvimento ágil de aplicativos *web*.

Além disso, para a criação da interface do usuário, escolhemos o *Blade*, que é o mecanismo de *template* do Laravel. O *Blade* oferece uma sintaxe concisa e expressiva para criar as views (visões) do APSEA, tornando o processo de desenvolvimento de interfaces mais intuitivo e eficiente.

Ao adotar o Laravel, *PHP e o Blade*, buscamos não apenas uma implementação técnica eficaz, mas também uma experiência de desenvolvimento facilitada e uma interface do usuário amigável. Essas escolhas tecnológicas foram feitas com base na robustez, flexibilidade e eficiência que essas ferramentas oferecem, contribuindo para o sucesso da interação entre os usuários e o APSEA.

6.8 Modelagem do Sistema

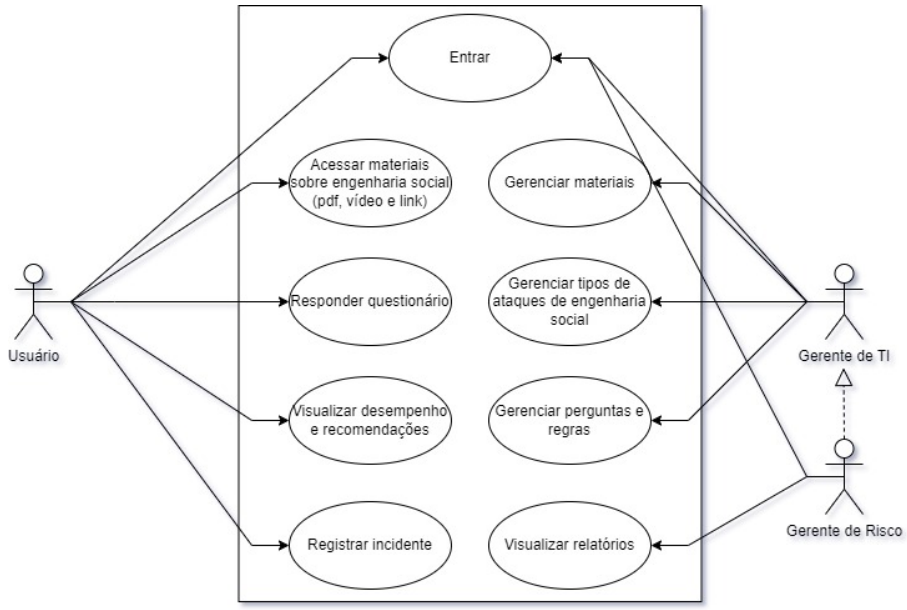
Os casos de uso identificam as interações individuais entre o sistema e seus usuários ou outros sistemas (SOMMERVILLE, 2007). Sendo assim, os casos de usos são importantes para descreverem o funcionamento das funcionalidades do sistema, ou seja, eles podem auxiliar no entendimento das opções fornecidas, para os interessados e mantenedores desta ou de novas versões do *software*.

O diagrama de casos de uso é um artefato da linguagem *Unified Modeling Language (UML)* que por meio de atores, casos de uso e relacionamentos, permitem auxiliar na comunicação dos desenvolvedores sobre o escopo do *software* de forma gráfica. Os diagramas de casos de uso representam diretamente os casos de usos construídos de modo textual.

Os atores são representados como figuras ‘palito’. Os casos de uso são representados por uma elipse contendo seu nome no interior. Já os relacionamentos são linhas que ligam os atores aos casos de usos e determinam os responsáveis por realizarem cada funcionalidade.

Para melhor entendimento de como deve ser o fluxo da aplicação foi criado um diagrama de casos de uso. Os casos de uso constituem uma técnica baseada em cenários. A Figura 3 representa o diagrama geral de casos de uso do sistema.

Figura 3 – Diagrama de Caso de Uso



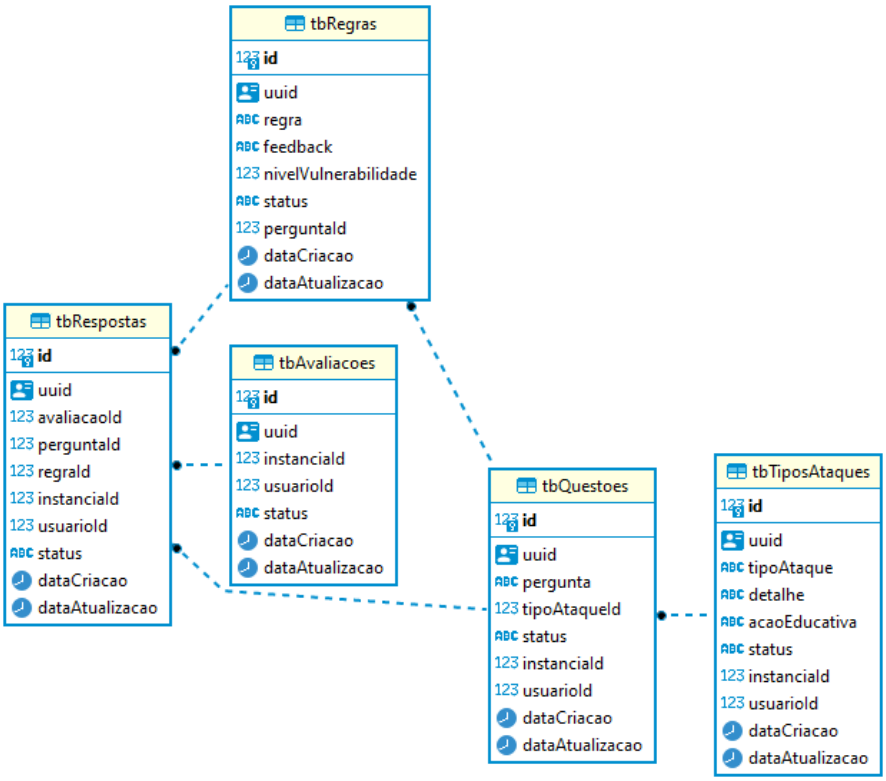
Fonte: Elaborada pelo autor

6.9 Modelo Entidade e Relacionamento

De acordo com Elmasri e Navathe (2011), o Modelo Entidade e Relacionamento (MER) descreve os dados como entidades, relacionamentos e atributos. Uma entidade representa um objeto ou conceito abstrato. Um atributo corresponde a alguma propriedade de interesse e que descreve uma entidade. Já um relacionamento representa uma associação entre entidades.

No banco de dados cada entidade é armazenada em forma de tabela, os atributos são as colunas de cada entidade, enquanto que os relacionamentos são estabelecidos a partir de chaves primárias (valores únicos que representam os registros) e chaves estrangeiras (valor de referência à uma chave primária de outra entidade). O diagrama de entidade e relacionamento do questionário de avaliação do sistema especialista, representa graficamente o MER e está apresentado na Figura 4.

Figura 4 – Diagrama de Entidade e Relacionamento do Questionário - APSEA



Fonte: Elaborada pelo autor

6.10 Requisitos

De acordo com Maxim e PRESSMAN (2021), os requisitos de *software* são descrições e especificações das funções que um sistema de *software* deve fornecer, das restrições sob as quais ele deve operar e dos atributos que ele deve exibir. Esses requisitos desempenham um papel crucial no ciclo de vida do desenvolvimento de *software*, servindo como a base para o projeto, implementação e teste do sistema. Eles ajudam a garantir que o produto final atenda às necessidades e expectativas dos usuários e das partes interessadas, além de fornecer uma estrutura para avaliar o sucesso do projeto de desenvolvimento de *software*.

Esta expansão fornece uma visão mais abrangente do papel dos requisitos de *software* no processo de desenvolvimento e destaca sua importância em garantir o sucesso do projeto.

6.10.1 Requisitos Funcionais

Os requisitos funcionais, essenciais para definir as funcionalidades do sistema, são apresentados na Tabela 5.

Tabela 5 – Requisitos Funcionais

ID	**Descrição**
RF001	O sistema deve permitir o cadastro, edição e exclusão de tipos de ataques.
RF002	O sistema deve permitir o cadastro, edição e exclusão de materiais relacionados à engenharia social.
RF003	O sistema deve permitir o cadastro, edição e exclusão de perguntas e regras para avaliação de usuários.
RF004	O sistema deve permitir o cadastro, edição e exclusão de usuários com diferentes níveis de permissão.
RF005	O sistema deve permitir a consulta de registros de incidentes.
RF006	O sistema deve permitir a visualização de resultados de avaliações.
RF007	O sistema deve permitir o acesso e visualização de materiais relacionados à engenharia social pelos usuários.
RF008	O sistema deve permitir aos usuários realizar avaliações de seu próprio desempenho e nível de vulnerabilidade.
RF009	O sistema deve permitir aos usuários registrar incidentes e receber instruções pertinentes.
RF010	O sistema deve permitir aos gerentes de risco consultar relatórios de avaliação dos usuários.

Os requisitos funcionais apresentados na Tabela 5 estabelecem as funcionalidades específicas que o sistema deve fornecer, abrangendo desde o cadastro de informações até a consulta e análise de dados pelos usuários.

6.10.2 Requisitos Não Funcionais

Os requisitos não funcionais, que delineiam os critérios de qualidade e desempenho do sistema, são descritos na Tabela 6.

Tabela 6 – Requisitos Não Funcionais

ID	**Descrição**
RNF001	O sistema deve ser intuitivo e de fácil utilização.
RNF002	O sistema deve ser responsivo, funcionando em diferentes dispositivos e tamanhos de tela.
RNF003	O sistema deve garantir a segurança das informações, utilizando mecanismos de autenticação e autorização.
RNF004	O sistema deve ser eficiente, garantindo tempos de resposta rápidos mesmo em momentos de alta demanda.
RNF005	O sistema deve ser escalável, suportando um aumento no número de usuários e dados sem perda significativa de performance.
RNF006	O sistema deve ser confiável, garantindo disponibilidade adequada e baixa taxa de falhas.
RNF007	O sistema deve ser compatível com os principais navegadores web do mercado.

Os requisitos não funcionais listados na Tabela 6 estabelecem os critérios de qualidade, desempenho e segurança que o sistema deve atender para garantir uma experiência satisfatória aos usuários.

6.11 Estruturas de Desenvolvimento do APSEA

A arquitetura do APSEA é fundamental para compreender o funcionamento eficaz dessa ferramenta. Nesta seção, exploraremos a estrutura do sistema, destacando sua arquitetura geral e como ele opera para alcançar seus objetivos.

6.11.1 Arquitetura MVC

O sistema APSEA foi desenvolvido utilizando o padrão arquitetural *MVC (Model-View-Controller)*, que separa a aplicação em três componentes principais: *Model, View e Controller*. Segundo Gamma et al. (1994), o padrão MVC promove uma separação clara entre a lógica de negócios, a interface do usuário e o controle das interações, facilitando a manutenção e a escalabilidade do sistema.

- ***Model***: Esta camada é responsável pela lógica de dados do sistema, incluindo interações com o banco de dados, validações e operações de negócios. No APSEA, o *Model* armazena informações relacionadas a incidentes de engenharia social, questionários e resultados das interações do usuário.

- ***View***: A *View* cuida da interface do usuário, apresentando informações do Model e recebendo entrada dos usuários. No APSEA, a *View* inclui componentes de interface gráfica que permitem aos usuários responder a questionários, visualizar resultados e acessar materiais informativos.

- ***Controller***: O *Controller* atua como intermediário entre o *Model* e a *View*. Ele recebe comandos dos usuários pela View, processa a lógica necessária e atualiza o *Model* e a *View* conforme necessário. No APSEA, o *Controller* coordena as ações quando os usuários interagem com o sistema, como quando respondem a questionários ou registram incidentes.

A escolha do padrão MVC para o APSEA trouxe benefícios como uma estrutura modular, facilidade de expansão e um processo de desenvolvimento mais eficiente (FOWLER, 2002). Esta estrutura em camadas facilita a manutenção e a expansão do sistema, pois a separação de preocupações permite que cada componente seja desenvolvido e testado de forma independente. Além disso, o padrão MVC possibilita uma maior escalabilidade e flexibilidade no desenvolvimento de novas funcionalidades. Esses benefícios reforçam o uso do MVC como uma solução robusta para projetos de software complexos.

6.11.2 Módulos do APSEA

O APSEA é composto por três módulos interconectados, cada um desempenhando um papel específico na conscientização e prevenção de ataques de engenharia social. A estrutura geral da arquitetura é a seguinte:

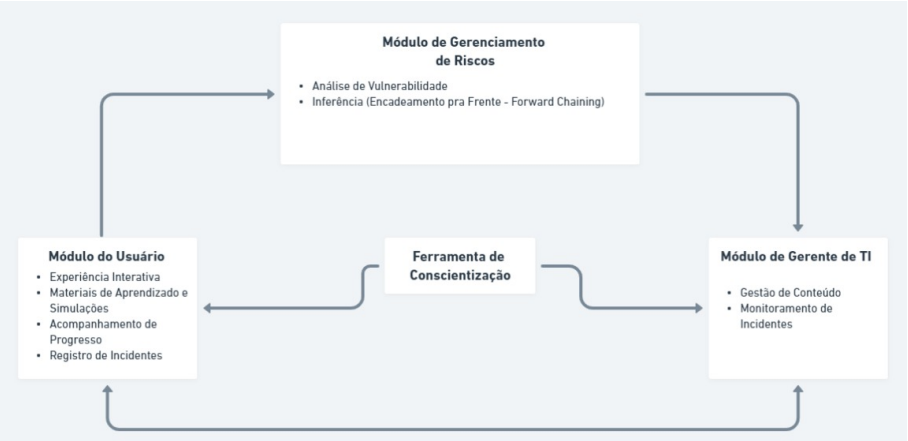
1. **Módulo do Usuário:** Projetado para a aquisição de conhecimento, este módulo interage diretamente com os usuários finais. Sua função principal é fornecer informações, materiais, registro de incidentes e questionários relacionados à engenharia social. Durante a realização de questões, o método *Forward Chaining* é aplicado, permitindo assim aumentar a conscientização dos usuários sobre os riscos de segurança da informação e como evitar ataques de engenharia social. Além disso, os usuários podem acompanhar seu progresso no sistema.

2. **Módulo do Gerente de TI:** Este módulo desempenha um papel crítico na gestão da base de conhecimento do sistema. Ele permite que os responsáveis pela gestão de TI a gerenciar informações relevantes para o sistema, incluindo dados sobre ameaças de engenharia social, técnicas de ataque, perguntas e regras.

3. **Módulo do Gerente de Risco:** Este módulo é responsável por aplicar o método de inferência *Forward Chaining* com base nas interações dos usuários e nos dados fornecidos pelo Gerente de TI. A partir dessas interações, o Módulo do Gerente de Risco gera relatórios que permitem ao gerente diagnosticar vulnerabilidades e identificar áreas de melhoria

específicas para o setor. Isso é alcançado por meio do uso de técnicas de inteligência artificial, permitindo que o APSEA forneça orientações para mitigar os problemas encontrados.

Figura 5 – Disposição dos Módulos do APSEA



Fonte: Elaborada pelo autor

Para visualizar a interação entre os módulos e como a ferramenta abordará a conscientização e prevenção contra ataques de engenharia social em organizações públicas, consulte a Figura 5.

Quando um usuário interage com o APSEA, ele tem a opção de acessar materiais informativos, registrar incidentes, bem como realizar uma das principais ações, que é responder ao questionário proposto. Ao responder ao questionário, o Encadeamento para Frente analisa suas respostas. Se uma sequência de interações indicar um cenário potencial de ataque de engenharia social, o sistema pode tomar medidas preventivas ou alertar o usuário sobre a ameaça potencial. Dessa maneira, o Encadeamento para Frente possibilita uma detecção mais rápida e proativa de tentativas de manipulação psicológica e ataques maliciosos. Após a conclusão do questionário, o sistema fornece *feedbacks* e recomendações ao usuário, visando aumentar a consciência sobre possíveis riscos e melhorar a segurança geral.

A integração desses três módulos cria uma estrutura sólida que permite ao APSEA conscientizar e fornecer soluções para a prevenção de ataques de engenharia social.

6.12 Operações do Módulo

As operações do APSEA estão apresentadas nos quadros Quadro 5, Quadro 6, Quadro 7 pelas quais as divide por usuário responsável. Essas operações representam as ações específicas que os usuários podem executar dentro do sistema para atender aos requisitos funcionais estabelecidos.

6.12.1 Módulo do Gerente de TI

O Quadro 5 apresenta as operações que são de responsabilidade do usuário categorizado como gerente de TI.

Quadro 5 – Operações - Módulo do Gerente de TI

Operação	**Descrição**
Gerenciar Tipos de Ataques	Cadastro, edição e exclusão dos registros da tabela
Gerenciar Materiais	Cadastro, edição e exclusão dos registros da tabela
Gerenciar Perguntas e Regras	Cadastro, edição e exclusão dos registros da tabela
Gerenciar Usuários	Cadastro, edição e exclusão dos registros da tabela
Consultar Incidentes	Consulta registros de incidentes
Analisar Avaliações	Visualizar Resultados

Fonte: Elaborada pelo autor

6.12.2 Módulo do Usuário

O Quadro 6 apresenta as operações que são de responsabilidade do usuário categorizado como usuários.

Quadro 6 – Operações - Módulo do Usuário

Operação	**Descrição**
Acessar Materiais	Visualizar os materiais disponíveis relacionados a engenharia social.
Realizar Avaliação	Aprender com as perguntas e *feedbacks*, Avaliar o nível de vulnerabilidade.
Visualizar Desempenho	Visualiza o desempenho da avaliação, Receber recomendações de como evitar tipos de ataques
Registrar Incidentes	Registrar incidentes, Receber instruções necessárias caso precise.

Fonte: Elaborada pelo autor

6.12.3 Módulo do Gerente de Risco

O Quadro 7 apresenta as operações que são de responsabilidade do usuário categorizado como gerente de Risco.

Quadro 7 – Operações - Módulo do Gerente de Risco

Operação	**Descrição**
Consultar Relatório de Avaliação dos usuários	Diagnosticar vulnerabilidades e identificar áreas de melhoria específicas.

Fonte: Elaborada pelo autor

7

Implementação

Neste capítulo são apresentados os detalhes da implementação do APSEA, as etapas e aspectos de destaque. São abordadas as seções de Protótipos, CRUD (Create, Read, Update, Delete) dos Registros, Validações, e por fim a apresentação do APSEA com a explicação das principais telas do sistema.

7.1 Protótipos

Em primeira instância foi realizada a prototipagem das telas, a qual consistiu na criação de páginas básicas do sistema, sem muita codificação em nível *back-end*. Os protótipos até então não possuíam nenhum tipo de acesso ao banco de dados, validações ou regras de negócio. Os protótipos apenas representavam graficamente aspectos e recursos que seriam implementados nos próximos passos de desenvolvimento. O intuito era obter uma familiaridade com a estrutura do sistema, além de identificar a necessidade de novas funcionalidades.

7.2 CRUD dos registros

Os CRUDs das tabelas foram construídos seguindo o modelo de arquitetura de *software* MVC, adotado pelo Laravel como padrão. Nesse modelo, as páginas são geradas nos arquivos de visão, utilizando a extensão *.blade.php, característica específica do Laravel. As requisições GET e/ou POST são direcionadas às classes controladoras, que coordenam a interação entre os *Models*, *Views* e o restante da aplicação. No Laravel, é importante destacar que são os *Models* que gerenciam o banco de dados, representando e interagindo com os dados do banco, enquanto os *Controllers* recebem as requisições e coordenam as operações entre os *Models* e as *Views*. Portanto, os *Controllers* não são responsáveis pela busca, alteração e salvamento dos registros no banco de dados; essa função cabe exclusivamente aos *Models*. As classes modelo contêm

informações sobre a estrutura das tabelas no banco de dados e definem como esses dados são manipulados.

Foi estabelecido que o usuário com a função de Gerente de TI será responsável pelo gerenciamento dos CRUDs das tabelas relacionadas a tipos de ataques, materiais, perguntas e regras, usuários, consultas de incidentes e análises de avaliações.

7.3 Validações

Um dos objetivos do sistema é auxiliar o usuário, especialmente o Gerente de TI, os Usuários e o Gerente de Risco, a alcançar a corretude do conteúdo do plano de segurança da informação relacionado a engeharia social. Durante a implementação do sistema, enfatizamos a importância das verificações e validações de campos nos formulários para garantir a integridade e qualidade dos dados inseridos. Utilizando a estrutura do Laravel, o sistema emprega classes padrão para validar as solicitações *HTTP*, oferecendo uma ampla gama de regras predefinidas.

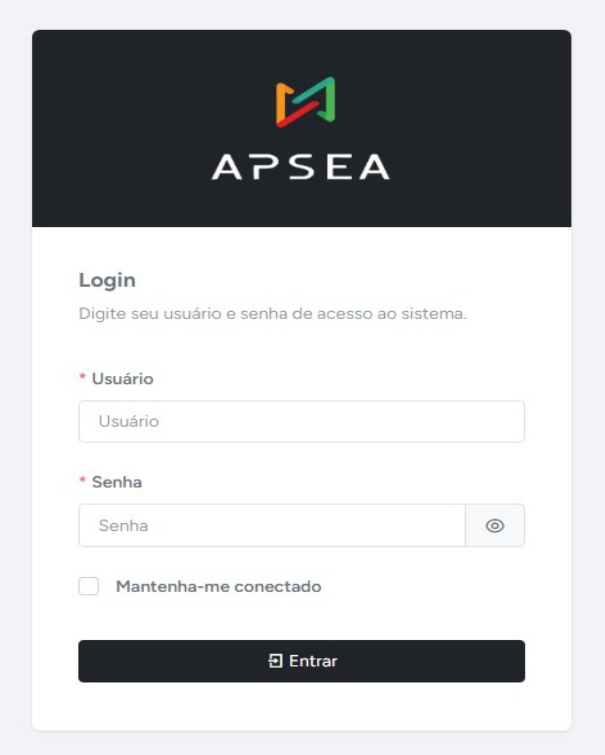
No contexto do Gerente de TI, as classes de validação do Laravel são aplicadas para garantir a consistência dos dados relacionados a tipos de ataques, materiais, perguntas e regras, usuários, consultas de incidentes e análises de avaliações. Essas validações são essenciais para manter a precisão das informações cruciais para a conscientização sobre segurança da informação.

O Gerente de Risco, ao consultar relatórios de avaliação de usuários, diagnosticar vulnerabilidades e tomar decisões em nível gerencial, pode confiar na integridade dos dados validados pelo sistema. O Laravel proporciona a flexibilidade necessária para estender as regras de validação de acordo com as especificidades do *software*, assegurando que a análise de riscos seja precisa e abrangente.

7.4 O Sistema

A Figura 6 exibe a tela de *login* do sistema. Atualmente o sistema se encontra com registros manuais de usuários, para a implantação do sistema no DETRAN/SE se faz necessário a implementação de vínculo com a versão do protocolo de acesso a diretórios *Lightweight Directory Access Protocol* (LDAP), usada nos servidores do orgão.

Figura 6 – Tela de Login do Sistema APSEA



Fonte: Elaborada pelo autor

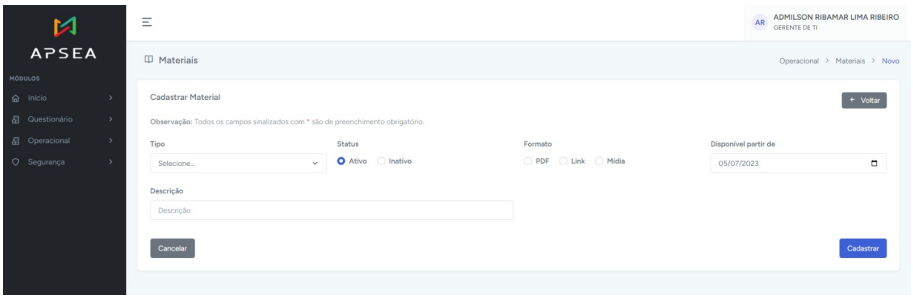
7.4.1 Módulo do Gerente de TI

O módulo administrativo, sob a supervisão do Gerente de TI, é especialmente projetado para fortalecer a conscientização e prevenção contra ataques de engenharia social (ES). As funcionalidades críticas, como Tipos de Ataques, Materiais, Perguntas e Regras, Usuários, Consulta de Incidentes e Análises de Avaliações, são estrategicamente desenvolvidas para atender às necessidades específicas de combate a ameaças provenientes da ES.

O Gerente de TI, por meio desta interface, pode cadastrar, editar e excluir informações relacionadas a ataques de ES, fornecer materiais instrutivos específicos para essa forma de ataque, criar perguntas e regras direcionadas, gerenciar usuários e realizar consultas detalhadas sobre incidentes relacionados à ES. Além disso, a capacidade de analisar avaliações permite ao Gerente de TI avaliar a eficácia das estratégias de conscientização implementadas.

Esse módulo administrativo se torna, assim, uma ferramenta central na defesa proativa contra os riscos associados à ES. O Gerente de TI desempenha um papel crucial na garantia da correta implementação e eficácia das iniciativas de conscientização, promovendo um ambiente mais seguro e resiliente contra esse tipo específico de ameaça.

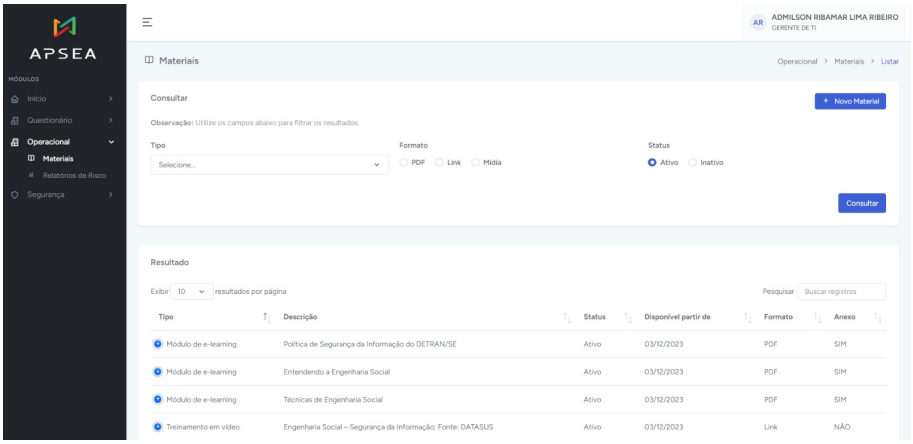
Figura 7 – Tela de Cadastro de Materiais



Fonte: Elaborada pelo autor

Nesta tela, como apresentado na Figura 7, o Gerente de TI pode cadastrar materiais variados destinados à conscientização contra ataques de ES. Os tipos de materiais incluem vídeos, *links* e documentos PDF. Para cada material, o Gerente de TI pode fornecer informações como título, descrição e selecionar o formato do material. Essa funcionalidade permite a inclusão de políticas de segurança da organização, políticas de privacidade e materiais informativos sobre como evitar ataques de ES. A tela oferece uma maneira eficiente de centralizar e gerenciar recursos de conscientização, facilitando o acesso dos usuários a informações cruciais para fortalecer a segurança da informação na organização.

Figura 8 – Tela de Gerenciamento de Materiais

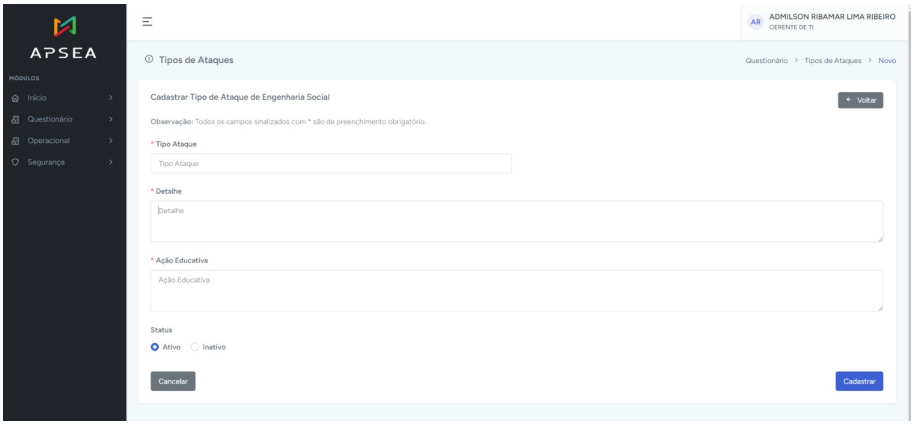


Fonte: Elaborada pelo autor

Na tela de gerenciamento de materiais, como apresentada na Figura 8, o Gerente de TI tem acesso a uma visão abrangente e intuitiva de todos os materiais cadastrados. Além disso, a interface inclui filtros de busca que permitem uma localização eficiente de materiais específicos com base em critérios como categoria, status ou qualquer outro parâmetro relevante. Essa interface possibilita a visualização, edição e exclusão de materiais existentes, fornecendo controle total sobre o conteúdo disponível para conscientização. Para cada material, é possível verificar informações detalhadas, como título, descrição e o formato do material (vídeo, *links*

ou PDF). A facilidade de gerenciar materiais permite uma rápida atualização de políticas de segurança do órgão, políticas de privacidade e outros recursos informativos destinados a prevenir ataques de ES. Essa tela é fundamental para manter a relevância e a eficácia dos materiais de conscientização, contribuindo significativamente para a segurança informação na organização.

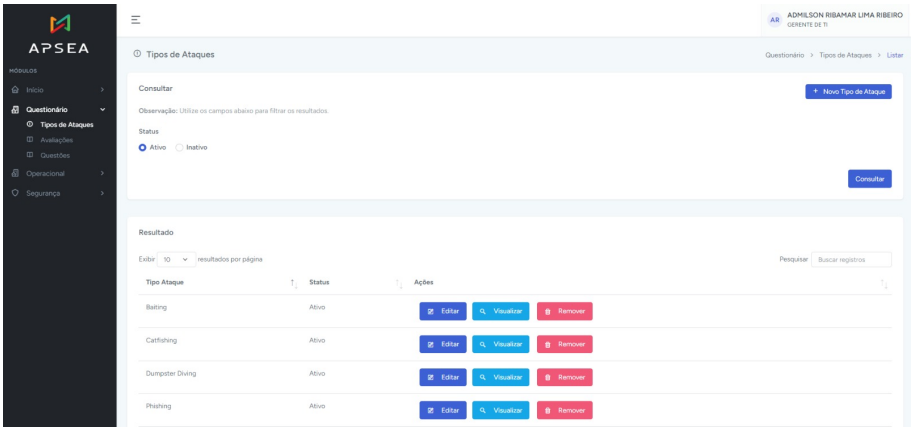
Figura 9 – Tela de Cadastro dos Tipos de Ataques de Engenharia Social



Fonte: Elaborada pelo autor

Nesta tela, como apresentada na Figura 9 o Gerente de TI tem a capacidade de cadastrar novos tipos de ataques de ES, bem como detalhe do tipo de ataque e recomendações de como fazer para evita-lós. O formulário inclui campos específicos para nomear o tipo de ataque, descrever suas características distintivas e fornecer detalhes sobre os métodos comuns utilizados. Essa funcionalidade permite uma catalogação abrangente, possibilitando a organização e a compreensão detalhada de diferentes estratégias de ES. Além disso, o Gerente de TI pode atualizar ou remover tipos de ataques existentes para manter a base de dados sempre atualizada e relevante. Essa tela serve como ponto de partida essencial para personalizar as estratégias de conscientização e fortalecer a segurança contra ameaças específicas de ES.

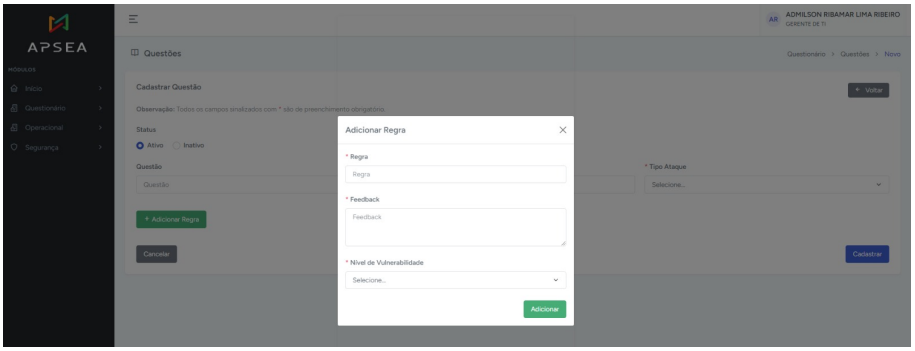
Figura 10 – Tela de Gerenciamento dos Tipos de Ataques de Engenharia Social



Fonte: Elaborada pelo autor

Na tela de gerenciamento dos tipos de ataques de ES, como apresentada na Figura 10, o Gerente de TI pode visualizar, editar e excluir tipos de ataques de ES previamente cadastrados. Essa interface simplificada oferece uma visão geral dos tipos existentes, permitindo rápida edição para atualizações necessárias e a exclusão de tipos desatualizados ou irrelevantes. A capacidade de gerenciar esses tipos de ataques proporciona flexibilidade ao adaptar estratégias de conscientização e manter a base de dados alinhada com as ameaças mais recentes. Essa tela é essencial para garantir uma resposta ágil e eficaz na evolução constante das táticas de ES.

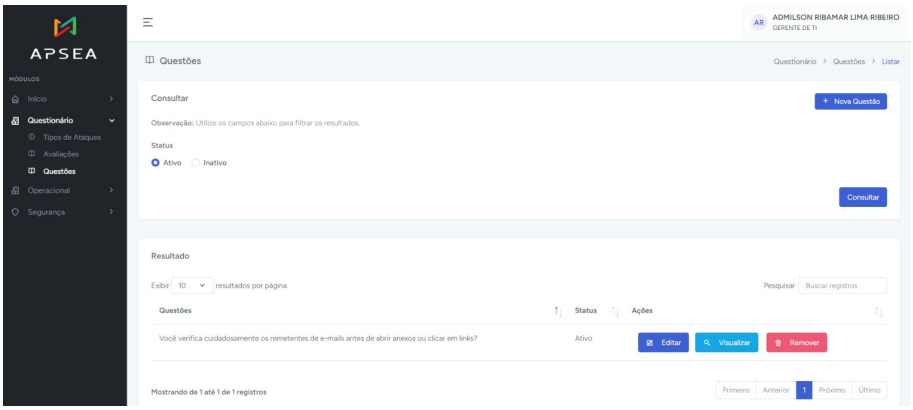
Figura 11 – Tela de Cadastro de Perguntas e Regras



Fonte: Elaborada pelo autor

Essa tela, como apresentada na Figura 11, desempenha um papel crucial no fortalecimento da base de conhecimento do APSEA contra ataques de ES. O Gerente de TI, na tela de registro, pode inserir perguntas específicas e regras de conscientização. As perguntas são formuladas para avaliar o entendimento dos usuários sobre ameaças de ES, enquanto as regras estabelecem diretrizes claras para comportamentos seguros. O formulário na tela permite ao Gerente de TI elaborar questões relevantes, fornecer respostas corretas esperadas e definir condições específicas para aplicação das regras. Essa funcionalidade não apenas personaliza as estratégias de treinamento, mas também fortalece a capacidade do APSEA em oferecer orientações precisas e relevantes aos usuários. Dessa forma, a tela de registro de perguntas e regras é uma peça central na construção da inteligência do sistema, proporcionando uma abordagem proativa contra ameaças de ES.

Figura 12 – Tela de Gerenciamento de Perguntas e Regras



Fonte: Elaborada pelo autor

Na tela de gerenciamento de perguntas e regras, como apresentada na Figura 12, o Gerente de TI tem controle total sobre o conteúdo crítico destinado à conscientização contra ataques de ES. Essa interface oferece uma visão completa de todas as perguntas e regras cadastradas, permitindo a consulta, visualização, edição e exclusão eficientes. Para cada item, o Gerente de TI pode revisar a pergunta, fornecer respostas corretas esperadas e definir condições específicas para aplicação das regras. A facilidade de gerenciar perguntas e regras possibilita uma personalização contínua das estratégias de treinamento, adaptando-se às mudanças nas ameaças de ES. Essa tela é central para a construção da inteligência do APSEA, proporcionando uma abordagem proativa na prevenção de ataques e na promoção da conscientização organizacional.

7.4.2 Módulo do Usuário

O módulo do usuário foi projetado para proporcionar uma experiência interativa e informativa aos usuários finais, com foco na conscientização e prevenção contra ataques de ES. Nesse módulo, os usuários têm acesso a materiais instrutivos, como vídeos, documentos e *links*, que visam fortalecer o entendimento sobre boas práticas de segurança da informação.

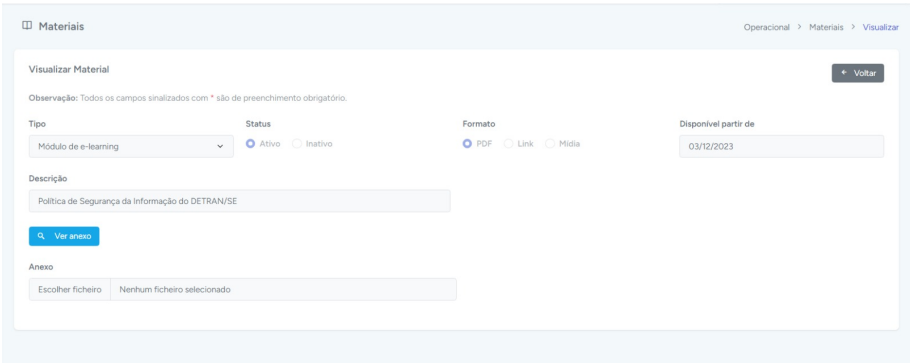
Além disso, os usuários têm a oportunidade de participar de avaliações que testam seus conhecimentos específicos sobre segurança e práticas para evitar ataques de ES. A visualização do desempenho nas avaliações proporciona *feedback* imediato, destacando pontos fortes e possíveis melhorias.

A funcionalidade de registrar incidentes permite que os usuários comuniquem atividades suspeitas ou identifiquem potenciais ameaças à segurança da informação. Ao registrar incidentes, os usuários contribuem para a coleta de dados valiosos que auxiliam na detecção e resposta eficientes a possíveis ameaças.

Adicionalmente, os usuários têm acesso a recomendações personalizadas, fornecendo orientações práticas sobre como evitar diferentes tipos de ataques. Essas recomendações são

adaptadas com base no desempenho do usuário e nos incidentes registrados, proporcionando um ambiente de aprendizado contínuo e personalizado.

Figura 13 – Tela de Visualização de Materiais



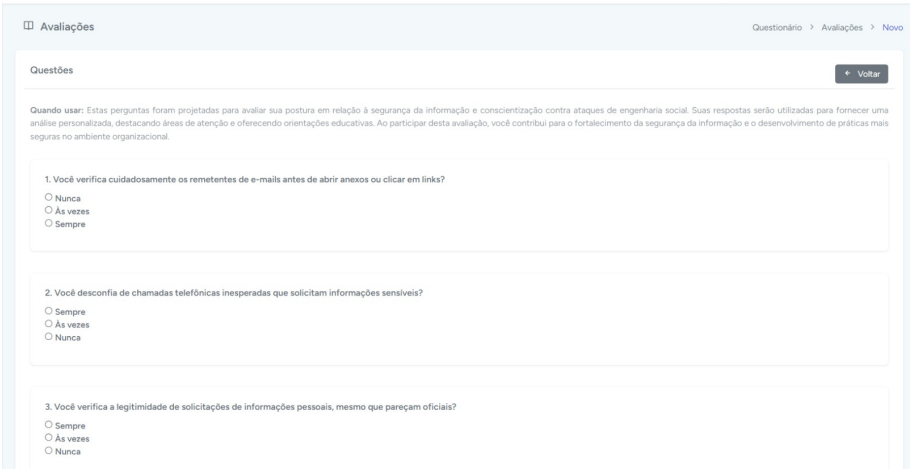
Fonte: Elaborada pelo autor

Na tela de visualização de materiais, como apresentada na Figura 13, os usuários têm acesso a alguns recursos educativos projetados para fortalecer sua conscientização contra ataques de ES. Nesta interface intuitiva, os materiais são organizados de maneira clara, permitindo que os usuários explorem vídeos informativos, documentos importantes, e *links* relevantes.

Cada recurso é acompanhado por informações descritivas, proporcionando contexto sobre o conteúdo. Os usuários podem facilmente selecionar e visualizar materiais específicos, oferecendo uma experiência personalizada e adaptada às suas necessidades de aprendizado.

Essa tela foi desenvolvida para criar um ambiente de aprendizado acessível, incentivando os usuários a se informarem de maneira eficaz sobre as melhores práticas de segurança da informação. A visualização de materiais é um serviço valioso para fortalecer a conscientização e promover uma cultura de segurança dentro da organização.

Figura 14 – Tela do Questionário Avaliativo



Fonte: Elaborada pelo autor

A tela do Questionário Avaliativo, como apresentada na Figura 14 representa um momento crucial no sistema, onde a avaliação do conhecimento do usuário é realizada de maneira abrangente. Desenvolvida com a finalidade de aprimorar a conscientização e compreensão dos usuários em relação às ameaças de ES, esta tela proporciona uma experiência interativa e informativa.

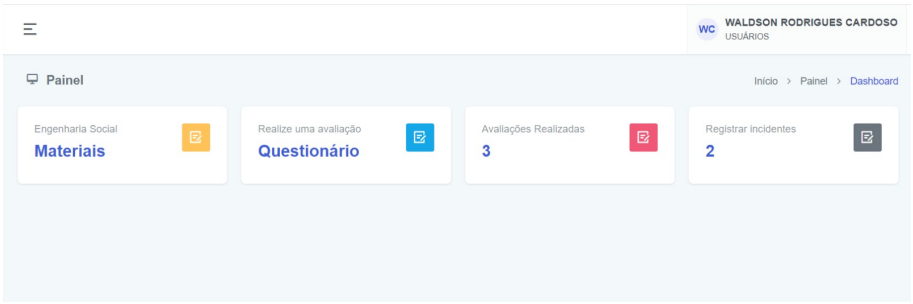
Ao iniciar o questionário, os usuários são apresentados a uma série de perguntas estrategicamente elaboradas, cada uma abordando aspectos específicos de segurança da informação, desde a identificação de ataques até práticas seguras de prevenção. A diversidade das questões permite uma avaliação abrangente do conhecimento, abordando diversas técnicas de ES.

Após a conclusão do questionário, o APSEA utiliza o método de encadeamento pra frente para avaliar as respostas. O *feedback* instantâneo é fornecido aos usuários, destacando áreas de conhecimento sólido e identificando possíveis lacunas. Essa abordagem educativa não apenas informa os usuários sobre os aspectos corretos, mas também educa sobre os erros, promovendo uma aprendizagem contínua.

Além disso, com base nas respostas fornecidas, o APSEA gera recomendações. Essas recomendações visam fortalecer as áreas identificadas como vulneráveis, sugerindo práticas recomendadas para aprimorar a conscientização e resistência contra ataques de ES.

Essa tela do Questionário Avaliativo, portanto, não apenas avalia o conhecimento do usuário, mas também cumpre a missão de ser uma ferramenta educativa e proativa. Ao proporcionar conhecimento, *feedback* construtivo e recomendações personalizadas, ela desempenha um papel fundamental na construção de uma postura segura e consciente diante das ameaças da ES.

Figura 15 – Tela do Painel do Usuário

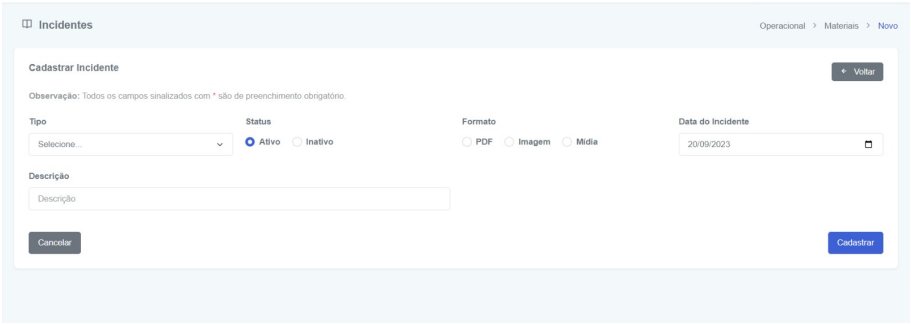


Fonte: Elaborada pelo autor

Dentro do painel do usuário, como apresentado na Figura 15, os atalhos oferecem acesso rápido e direto aos principais serviços. Os usuários podem facilmente acessar materiais relevantes, iniciando a avaliação de segurança através do respectivo serviço. O painel também fornece uma visão clara da quantidade de avaliações realizadas, permitindo um acompanhamento eficiente do progresso. Além disso, a funcionalidade de registro de incidente está acessível, possibilitando aos usuários reportar eventuais problemas ou preocupações de forma direta e descomplicada.

Esses atalhos otimizam a experiência do usuário, promovendo uma navegação intuitiva e eficaz dentro do APSEA.

Figura 16 – Tela de Registro/Cadastro de Incidentes



Fonte: Elaborada pelo autor

A tela de registro de incidentes de segurança da informação, como apresentada na Figura 16, é um componente essencial no sistema, proporcionando aos usuários uma interface clara e eficiente para reportar eventos adversos. Nessa tela, os usuários podem fornecer detalhes específicos sobre incidentes ocorridos, como descrição do incidente, data, hora e categorização do evento. Além disso, a tela permite anexar evidências relevantes, como capturas de tela ou documentos, para uma compreensão mais abrangente do incidente.

A interface é projetada para simplificar o processo de registro, tornando-o acessível a usuários de diferentes níveis de habilidade. A categorização cuidadosa dos incidentes facilita a análise posterior por parte do Gerente de Risco, contribuindo para uma resposta eficaz e a implementação de medidas corretivas. Essa tela reforça o compromisso do sistema com a segurança proativa, incentivando a colaboração dos usuários na identificação e mitigação de possíveis ameaças à segurança da informação.

7.4.3 Módulo do Gerente de Risco

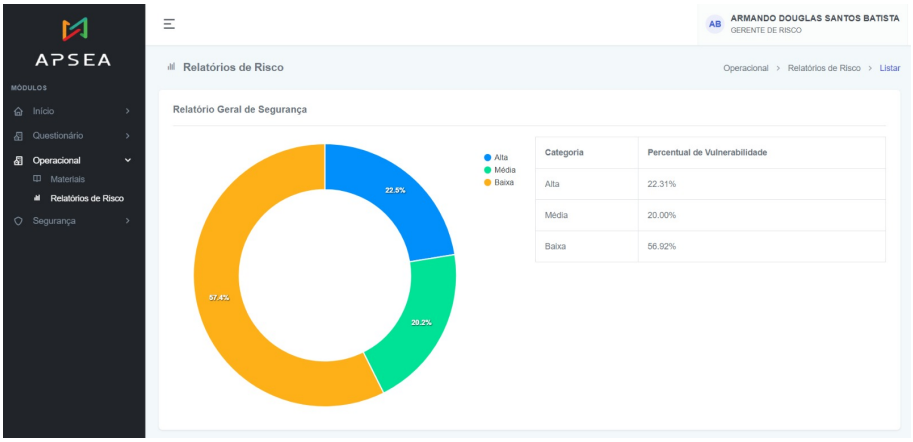
O módulo dedicado ao Gerente de Risco foi meticulosamente projetado para oferecer funcionalidades específicas, para que esse profissional possa conduzir avaliações detalhadas, diagnosticar vulnerabilidades e tomar decisões estratégicas no que diz respeito à segurança da informação na organização.

Uma das funcionalidades essenciais é a capacidade de consultar relatórios detalhados de avaliações realizadas pelos usuários. Esses relatórios fornecem uma análise aprofundada do nível de conscientização e conhecimento dos usuários em relação às ameaças de ES. Essa informação é fundamental para que o Gerente de Risco compreenda o panorama atual de segurança da informação da organização.

Além disso, o módulo do Gerente de Risco permite tomar decisões em nível gerencial com base nos relatórios de avaliação e incidentes registrados. Essas decisões estratégicas podem

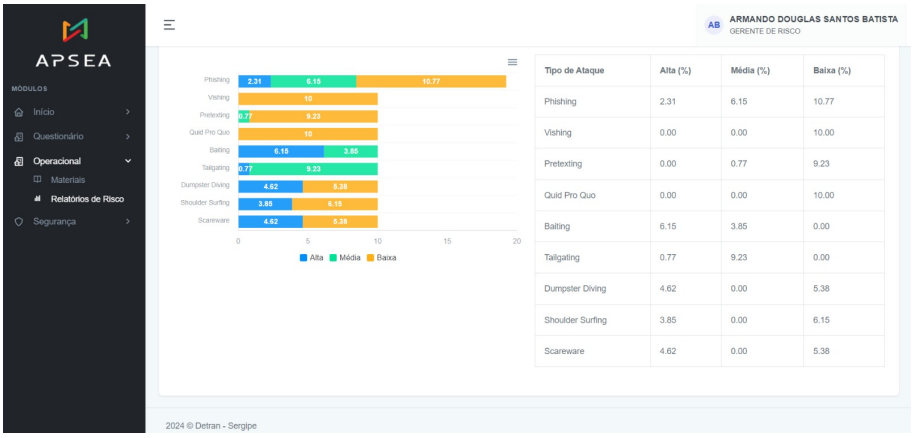
incluir a implementação de medidas de mitigação específicas, visando fortalecer a postura de segurança da informação da organização diante das ameaças de ES.

Figura 17 – Tela do Relatório Geral de Vulnerabilidade



Fonte: Elaborada pelo autor

Figura 18 – Tela do Relatório Geral de Vulnerabilidade por Tipo de Ataque



Fonte: Elaborada pelo autor

O relatório geral de vulnerabilidade, como apresentado na Figura 17 e 18, compilando os resultados das avaliações realizadas pelos 15 participantes, destaca uma visão abrangente do panorama de segurança da informação de um setor da organização. Os dados revelam que 22,31% das respostas indicaram uma vulnerabilidade considerada alta, enquanto 20,00% apontaram para um nível médio de vulnerabilidade. Por outro lado, uma parcela significativa de 56,92% demonstrou um nível baixo de vulnerabilidade.

Esses resultados oferecem *insights* valiosos para o Gerente de Risco, possibilitando uma análise estratégica das áreas específicas que demandam maior atenção e potencial mitigação. A predominância de respostas indicando um nível baixo de vulnerabilidade é encorajadora,

sugerindo uma conscientização robusta e práticas de segurança eficazes entre os participantes. Contudo, a identificação de áreas com vulnerabilidades médias e altas destaca oportunidades para a implementação de medidas preventivas direcionadas, fortalecendo ainda mais a postura de segurança da informação no setor da organização como um todo. Este relatório, fundamentado nas respostas coletivas, representa uma ferramenta valiosa para embasar decisões informadas e estratégicas no âmbito da segurança da informação.

8

Validação Qualitativa do APSEA

Neste capítulo, apresentamos uma validação qualitativa que confirma a eficácia do APSEA (*Awareness and Prevention Expert System against Social Engineering Attacks*). A validação qualitativa é uma abordagem de pesquisa essencial para verificar a aplicação prática do sistema desenvolvido. Essa análise produz informações detalhadas e ilustrativas sobre o objeto de estudo da pesquisa. A pesquisa qualitativa concentra-se na compreensão e explicação dinâmica das relações sociais (SILVEIRA; CÓRDOVA, 2009).

Este método de pesquisa envolve a análise e validação do APSEA no contexto do Departamento Estadual de Trânsito de Sergipe (DETRAN/SE), especificamente na Assessoria Geral de Tecnologia da Informação e Comunicação (AGIN). Detalhamos o local do estudo da validação, os procedimentos adotados na pesquisa e, no Capítulo 9, os resultados e discussões da validação da eficácia do APSEA. Esta validação qualitativa oferece *insights* valiosos sobre a eficácia do sistema na conscientização e prevenção contra ataques de Engenharia Social (ES).

8.1 Local do Estudo

A pesquisa foi realizada no ano de 2023, no Departamento Estadual de Trânsito de Sergipe- DETRAN-SE situado em Aracaju/Sergipe, Região Nordeste do Brasil. O Departamento Estadual de Trânsito de Sergipe – DETRAN/SE, órgão integrante da Administração Pública Estadual, do Poder Executivo do Estado de Sergipe tem sua origem ligada a Inspetoria Geral da Guarda Civil e de Veículos da Secretaria de Segurança Pública, com a finalidade de atender o Código Nacional de Trânsito, aprovado pela Lei federal 5.108 de 21 de setembro de 1966.

Através do Decreto Lei nº 170, de 21 de outubro de 1969, foi transformado em Departamento Geral da Guarda Civil e de Veículos subordinado aSecretaria de Segurança Pública.

Nos termos da Lei nº 2.608, de 27 de fevereiro de 1987, que dispõe sobre a estrutura e o funcionamento da Administração do Estado de Sergipe foi reestruturados como autarquia

estadual, como órgão da administração indireta.

Por Decreto Governamental de nº 8.358 de 30.03.87 ficou definida a finalidade, as atribuições, a organização básica, a competência, a estrutura de seus órgãos e as normas estruturais da situação ou regime jurídico do seu pessoal e da sua administração patrimonial e financeira.

Por força do citado Decreto, o DETRAN/SE é uma Autarquia integrante da Administração Indireta do Poder Executivo Estadual e vinculado à Secretaria de Estado da Segurança Pública, tendo por finalidade o planejamento, coordenação, fiscalização, controle e execução da política estadual de trânsito.

A Assessoria Geral de Tecnologia da Informação e Comunicação (AGIN), situada no âmbito do Departamento Estadual de Trânsito de Sergipe (DETRAN/SE), emerge como o foco central do nosso estudo.

A amostra para o nosso estudo foi retirada diretamente das operações da AGIN no DETRAN/SE, validando assim as ações implementadas para combater a ES. A sensibilidade e segurança das informações demandam estratégias robustas para prevenir ataques e manipulações por meio da ES. Com base no estudo aplicado foi possível analisar como as equipes lidam com ameaças que buscam explorar aspectos psicológicos e sociais para obter informações confidenciais. Isso inclui desde a conscientização dos colaboradores até a implementação de protocolos avançados de segurança cibernética.

A AGIN, dentro do contexto do DETRAN/SE, assume um papel vital na proteção dessas informações sensíveis. Sua atuação não apenas se destaca na implementação de soluções tecnológicas inovadoras, mas também na promoção de medidas e práticas que visam mitigar os riscos associados à ES. Dessa forma, a AGIN no DETRAN/SE não apenas impulsiona a eficiência operacional, mas também salvaguarda a integridade e a confidencialidade das informações, protegendo os usuários contra potenciais ataques de ES.

8.2 Validação do APSEA

A segunda etapa compreende as fases de testes e preenchimento da Escala *Likert* de Avaliação para Validação do APSEA, (Apêndice D), e posteriormente a Análise dos Dados.

No âmbito deste estudo, é fornecido um exemplo representativo do Resultado Individual da Avaliação do APSEA (Apêndice B). Neste documento suplementar, os detalhes específicos e as nuances do resultado da avaliação individual são minuciosamente descritos.

Previamente foi criado, pelo pesquisador, um grupo em um aplicativo de mensagens instantâneas com todos os participantes do estudo para facilitar a comuniação.

Após finalizar as etapas de modelagem e implementação do APSEA o mesmo foi testado primeiramente pelos pesquisadores e posteriormente foi disponibilizado, através de *link* próprio,

para que os usuários participantes pudessem criar uma conta exclusiva, obter acesso e testar o APSEA.

No decorrer da segunda etapa os participantes receberam instruções e orientações de forma escrita, do pesquisador, sobre como utilizar o *software* desenvolvido, desse modo cada usuário foi convidado a explorar e experienciar o APSEA de forma ilimitada.

Posteriormente aos testes, foi pedido aos participantes da pesquisa que respondessem, através de um *link* disponibilizado, um questionário de avaliação para validação do APSEA, utilizando a escala Likert (Apêndice D).

O referido Questionário contém duas partes, a primeira parte inclui dados pessoais, como nome, e-mail, função e a opção de ler na íntegra o Termo de Consentimento Livre e Esclarecido (TCLE) disponível (Apêndice C), concordando ou não, sendo necessário concordar para dar seguimento na avaliação.

Na segunda parte foram avaliados 6 atributos de desempenho funcional, sendo eles Adequação Funcional, Confiabilidade, Usabilidade, Nível de Desempenho, Compatibilidade e Segurança.

Os atributos do grau de satisfação da escala definida variam de 1 (Não Apropriado) a 5 (Completamente Apropriado) expressos no Quadro 1, respeitando as recomendações de modelo de qualidade de software dispostos na ISO/IEC 25010 (*System and Software Engineering - System and Software Quality Requirements and Evaluation - SQuaRE - System and Software Quality Models*) (FELIPE et al., 2020).

A ISO/IEC 25040 (*System and Software Engineering – SQuaRE – Evaluation Process*) é uma norma internacional que estabelece um conjunto de 8 características voltadas para avaliação de *software*, cada característica é composta por subcaracterísticas, totalizando 31 subcaracterísticas, relacionadas às propriedades a serem mensuradas e avaliadas para o estabelecimento da qualidade do produto de *software* (ISO/IEC, 2011)

O Questionário foi criado utilizando o *Google Forms* e as respostas foram armazenadas no *Google Drive* do pesquisador e mantidas em sigilo, a fim de serem utilizadas exclusivamente para avaliação, resultados, futuras adequações e atualizações do APSEA.

O *Google Forms* é um aplicativo que pode criar formulários através de uma planilha no *Google Drive*. É um serviço gratuito, basta apenas ter uma conta no *Gmail*. Estes formulários podem ser questionários de pesquisa elaborados pelo próprio usuário, ou podem ser utilizados os formulários já existentes. Dessa forma, os formulários ficam armazenados no servidor do *Google*, podendo ser acessado de qualquer lugar e não ocupam espaço no computador.

Trata-se, igualmente, de uma aplicação de gestão de pesquisas desenvolvida pelo *Google*. Os utilizadores têm a possibilidade de participar em questionários e preencher formulários de registo, além de poder ser utilizado para realizar pesquisas e recolher informações sobre terceiros.

Tabela 7 – Escala *Likert* para avaliar grau de satisfação do usuário.

Item da Escala	**Definição**	**Pontuação**
Não Apropriado	Não adaptado, não corresponde em nada ao objetivo proposto.	1
Pouco Apropriado	Corresponde muito pouco ao objetivo proposto.	2
Moderadamente Apropriado	Corresponde moderadamente ao objetivo proposto.	3
Muito Apropriado	Corresponde intensamente ao objetivo proposto.	4
Completamente Apropriado	Corresponde perfeitamente ao objetivo proposto.	5

Fonte: Adaptado de (FELIPE et al., 2020)

Para facilitar a avaliação do APSEA, disponibilizamos um endereço local específico, fornecendo acesso personalizado a cada usuário com seu respectivo perfil. Ao acessar esse ambiente controlado, os usuários foram direcionados por um processo de interação estruturado, adaptado às suas necessidades específicas.

Sucessivamente ao período de testes foi encaminhado aos participantes o *link* <https://forms.gle/oyHUSMbnai2PC1wc6> de acesso ao Questionário utilizando a escala *Likert* de Avaliação do Grau de Satisfação do APSEA, contendo também disponível na íntegra o TCLE (Apêndice C). O *link* foi gerado por meio do *Google Forms*.

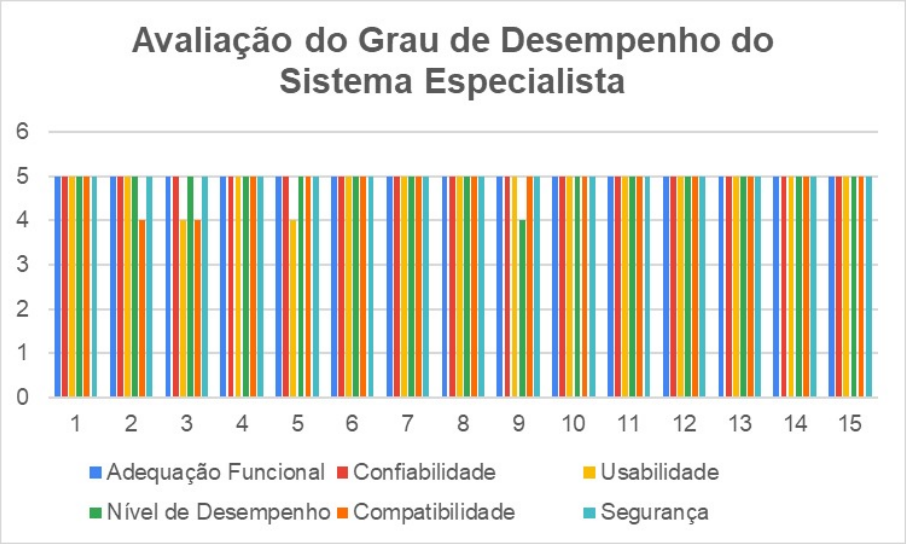
9

Resultados e Discussões

Durante o período de novembro a dezembro de 2023, conduzimos testes e avaliações do APSEA, envolvendo a participação de 15 profissionais de tecnologia da informação do DETRAN/SE. Este grupo incluiu não apenas usuários representativos, como analistas, desenvolvedores e técnicos, mas também figuras-chave como o gerente de TI e o gerente de risco.

A seguir podemos observar, na Figura 19, os resultados gerais com a média representativa de cada um dos atributos, e suas respectivas cores correspondentes, da Avaliação do Grau de Satisfação do Usuário com APSEA proposto neste estudo.

Figura 19 – Avaliação do Grau de Satisfação do Usuário com APSEA



Fonte: Elaborada pelo autor

Foi realizada uma Média das notas concedidas para cada atributo das avaliações efetuadas,

ao APSEA desenvolvido, pelos participantes deste estudo. A Média geral da avaliação referente a cada atributo (5=100%).

- Adequação Funcional 5,0 (100%)
- Confiabilidade 5,0 (100%)
- Usabilidade 4,8 (96%)
- Nível de Desempenho 4,9 (98%)
- Compatibilidade 4,8 (96%)
- Segurança 5,0 (100%)

Esses resultados indicam uma avaliação bastante positiva e refletem a eficácia do APSEA em atender às expectativas e requisitos estabelecidos durante o desenvolvimento.

A utilização do APSEA adaptado às demandas específicas do DETRAN/SE marca um significativo avanço no enfrentamento de ameaças de engenharia social (ES). O APSEA destacou-se pela sua elevada adequação funcional, confiabilidade e segurança, elementos cruciais para otimizar a eficácia e eficiência do sistema dentro do contexto organizacional em foco.

Além disso, a usabilidade e o nível de desempenho, avaliados com percentuais bastante elevados, sugerem uma interface amigável e um desempenho satisfatório, contribuindo para uma experiência positiva dos usuários no manejo do sistema.

O APSEA proposto foi avaliado no quesito **Adequação Funcional**, respondendo ao questionamento *"A Funcionalidade do software atende ao que foi proposto?"*.

As avaliações se restringiram em Completamente Apropriado. A análise da média percentual de Adequação Funcional do sistema proposto é de 100%, ou seja, 100% dos profissionais julgaram o APSEA como Adequado em relação à característica Adequação Funcional, comprovando que o *software* atende ao que foi proposto.

Essa avaliação é realizada para verificar se o *software* possui os atributos esperados. Consiste em determinar se os usuários percebem que o sistema efetivamente auxilia na solução dos problemas que se propõe a resolver e que são interessantes para os usuários.

O APSEA proposto foi avaliado no quesito **Confiabilidade**, respondendo ao questionamento *"Qual a confiabilidade do sistema em executar as funções necessárias?"*.

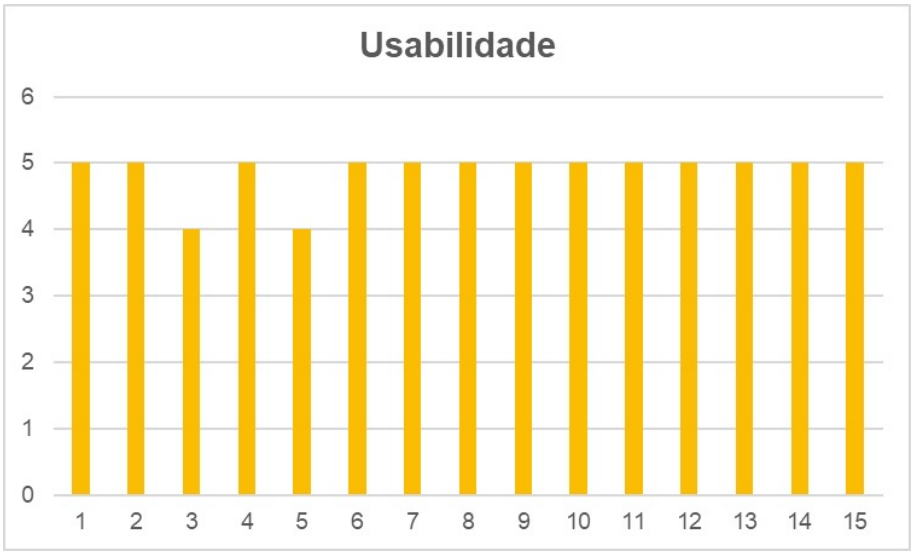
A análise da média percentual de Confiabilidade do sistema elaborado foi de 100%, revelando assim a prevalência dos profissionais que julgaram o APSEA como adequado em relação à característica Confiabilidade, indicando que, sob determinadas condições, o sistema é capaz de executar suas tarefas de forma confiável.

É imprescindível que o *software* seja confiável o bastante para que o usuário final possa aplicá-lo sem que erros de funcionamento venham a prejudicar a avaliação e classificação do risco de vulnerabilidade.

O APSEA proposto foi avaliado no quesito **Usabilidade**, respondendo ao questionamento *"Qual o esforço necessário para utilizar o APSEA?"*.

São apresentados na Figura 20, a seguir, os resultados da análise do atributo Usabilidade na Avaliação do Grau de Satisfação do Usuário com APSEA. Na base da imagem do gráfico de barras, estão listados os avaliadores, cada um representado por uma barra vertical correspondente. Cada barra se estende verticalmente até alcançar o valor atribuído na escala à esquerda, refletindo a avaliação individual feita por cada avaliador.

Figura 20 – Avaliação do Atributo Usabilidade



Fonte: Elaborada pelo autor

Considerando a análise da avaliação de Usabilidade, conforme representado na Figura 20, observamos que 86.67% dos participantes atribuíram a classificação Completamente Apropriado, enquanto 13.33% optaram por Muito Apropriado. Esses percentuais somam 100%, indicando que a totalidade das avaliações considerou o sistema produzido como adequado em relação à característica de Usabilidade, medindo o esforço necessário para utilizar o APSEA.

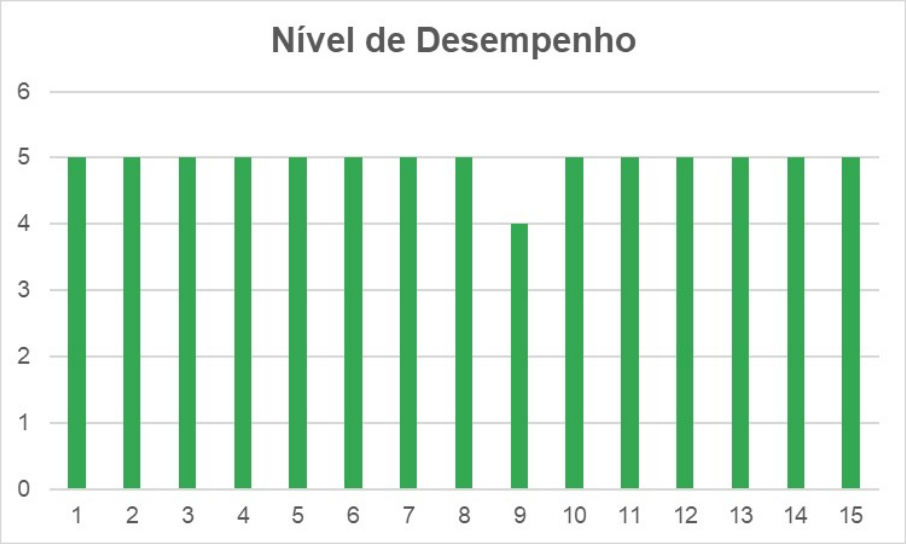
O APSEA deve dispor das informações e ferramentas necessárias que permitam sua utilização, facilitando o trabalho do usuário, sem a necessidade de recordar grande quantidade de informações para que consiga utilizar o sistema.

A avaliação da usabilidade é reconhecida como fator importante para o sucesso na elaboração de tecnologias eficazes e aceitáveis, indicando o emprego de métodos simples e de menor complexidade para sua realização.

O APSEA proposto foi avaliado no quesito **Nível de Desempenho**, respondendo ao questionamento *"Qual o Nível de Desempenho do APSEA?"*.

Podemos notar no Figura 21, a seguir, os resultados da análise do atributo Nível de Desempenho na Avaliação do Grau de Satisfação do Usuário com APSEA. Na base da imagem do gráfico de barras, estão listados os avaliadores, cada um representado por uma barra vertical correspondente. Cada barra se estende verticalmente até alcançar o valor atribuído na escala à esquerda, refletindo a avaliação individual feita por cada avaliador.

Figura 21 – Avaliação do Atributo Nível de Desempenho.



Fonte: Elaborada pelo autor

Refletindo a análise da avaliação de Eficiência de Desempenho expressa na Figura 21 constatamos que 93.33% dos participantes atribuíram a classificação Completamente Apropriado, enquanto 6.67% optaram por Muito Apropriado. Sendo que 100% do total das avaliações do sistema confeccionado indicando como Adequado o Nível de Desempenho do APSEA elaborado.

O APSEA proposto foi avaliado no quesito **Compatibilidade**, respondendo ao questionamento *"Qual a Capacidade de manter o nível de desempenho num período de tempo?"*.

Um total de 100,0% das avaliações indicou que o APSEA é Muito ou Completamente Apropriado em relação ao atributo Compatibilidade, demonstrando uma excelente capacidade do APSEA de executar suas funções durante um período de utilização.

O APSEA proposto foi avaliado no quesito **Segurança**, respondendo ao questionamento *"Qual a Proteção de informações e dados e Nível de acesso de pessoas?"*.

As avaliações se delimitam em Completamente Apropriado com 100%. O desfecho da média percentual de Adequação Funcional é que 100% dos profissionais julgaram o APSEA como Adequado em relação à característica Segurança, confirmando que a proteção dos dados e informações estão adequados e o APSEA desenvolvido atende ao que foi proposto.

O APSEA proposto foi avaliado no quesito sugestão, respondendo ao questionamento "Você tem alguma sugestão específica para melhorar o APSEA?".

Dos 15 participantes envolvidos na avaliação, a maioria (14 participantes) não apresentou sugestões adicionais, indicando, em sua maioria, satisfação com o APSEA conforme sua proposta.

No entanto, um participante expressou uma sugestão valiosa, destacando a oportunidade de aprimorar a experiência do usuário. Essa sugestão específica envolve a incorporação de *"mais informações ilustrativas e lúdicas sobre os tipos de ataques de Engenharia Social"*.

O participante que forneceu *feedback* sugeriu que a ferramenta poderia ser ainda mais eficaz ao oferecer informações adicionais por meio de elementos ilustrativos e lúdicos. Esta sugestão visa proporcionar uma abordagem mais envolvente e visual na apresentação dos tipos de ataques de ES.

Incluir elementos gráficos, infográficos ou simulações visuais pode não apenas tornar o aprendizado mais atraente, mas também facilitar a compreensão e retenção das informações. A abordagem lúdica pode transformar a experiência de aprendizado, tornando-a mais interativa e memorável para os usuários.

Os resultados indicam que o APSEA não apenas atende, mas também supera as expectativas em termos de funcionalidade, confiabilidade, usabilidade, desempenho, compatibilidade e segurança. O alto grau de satisfação dos usuários reforça a validade e a relevância do sistema no contexto do DETRAN/SE, marcando um significativo avanço no enfrentamento de ameaças de engenharia social.

A sugestão de aprimoramento, embora única, destaca a oportunidade de tornar o APSEA ainda mais eficaz e envolvente. Incorporar elementos visuais e interativos pode melhorar a experiência do usuário e facilitar a compreensão dos conceitos de segurança, ampliando a eficácia do aprendizado sobre ataques de Engenharia Social.

Em resumo, a validação confirma que o APSEA é uma solução robusta e eficiente, capaz de atender às necessidades específicas do DETRAN/SE, com potencial para futuras melhorias baseadas no *feedback* dos usuários.

10
Conclusão

Este estudo começou com uma análise abrangente sobre a engenharia social, um dos principais desafios enfrentados pelas organizações na proteção de seus dados e recursos. Através do mapeamento sistemático da literatura, identificamos os tipos mais comuns de organizações alvo de ataques de engenharia social, os principais métodos e técnicas de ataque utilizados, como *Phishing*, *Pretexting* e *Baiting*, e as estratégias de defesa adotadas por essas organizações. Os resultados revelaram que empresas são os principais alvos de ataques de engenharia social, destacando a importância de investir em programas de conscientização do usuário humano e na aplicação de políticas e processos internos para mitigar essas ameaças. As conclusões deste estudo enfatizam a importância de uma abordagem multidisciplinar na proteção contra engenharia social, que vai além das medidas tecnológicas tradicionais e inclui a conscientização dos usuários.

Em seguida, a revisão de sistemas especialistas no contexto da segurança da informação, com foco especial em conscientização e treinamento contra ameaças de engenharia social, revelou um cenário rico em abordagens inovadoras e soluções práticas. Os artigos selecionados enfatizam coletivamente o papel fundamental dos sistemas especialistas em abordar vários aspectos dos desafios de cibersegurança. Desde aumentar a conscientização sobre ataques cibernéticos até mitigar ameaças internas e desenvolver modelos eficazes de treinamento em cibersegurança, esses artigos fornecem *insights* valiosos sobre as diversas aplicações de sistemas especialistas. A eficácia dos sistemas especialistas não está apenas em suas capacidades técnicas, mas também em sua integração em estratégias mais amplas que consideram o fator humano na cibersegurança.

Com base nesses estudos, desenvolvemos o sistema especialista APSEA, voltado para a conscientização e prevenção contra ataques de engenharia social (ES). O sistema foi criado para oferecer recursos de treinamento interativo, apresentação de conteúdo e avaliação da conscientização dos usuários. Através de exercícios interativos e questionários, os usuários têm a oportunidade de aprender sobre os riscos associados à ES, as táticas utilizadas pelos atacantes e as melhores práticas para prevenir esses ataques. A capacidade de personalizar o conteúdo

e os questionários permite ao Gerente de TI adaptar o sistema às necessidades específicas da organização.

A análise das respostas dos usuários e a aplicação do método de encadeamento para frente permitem a identificação de vulnerabilidades específicas. O sistema gera relatórios detalhados que destacam áreas onde os usuários demonstram falta de conscientização ou práticas de segurança inadequadas. Esses relatórios são disponibilizados para o Gerente de Risco, possibilitando a tomada de medidas corretivas e o aprimoramento contínuo da conscientização em segurança da informação. A utilização do APSEA promove a segurança da informação e previne ataques de ES, preparando os usuários para reconhecer e responder de forma eficaz às ameaças, reduzindo os riscos de exposição a ataques e mitigando impactos severos nos dados sensíveis. Através deste sistema, a conscientização em segurança da informação é aprimorada, os usuários são capacitados e as vulnerabilidades são identificadas, promovendo um ambiente mais seguro para as organizações.

Em suma, este estudo contribui para um entendimento mais profundo da engenharia social e suas implicações para a segurança da informação, fornecendo *insights* valiosos para profissionais de segurança cibernética, gestores de TI e pesquisadores interessados em proteger as organizações contra ameaças cada vez mais sofisticadas.

10.1 Trabalhos Futuros

Como sugestão para trabalhos futuros, consideramos o seguinte:

1. **Expansão para Plataformas Móveis**:
    - Considerar a adaptação e implementação do APSEA em plataformas móveis, como *Android e iOS*, para garantir maior acessibilidade e alcance;
2. **Integração de Recursos Complementares de IA:**:
    - Exploração da integração de recursos complementares de Inteligência Artificial (IA), como Aprendizado de Máquina (*Machine Learning*) e Redes Neurais, para enriquecer e aprimorar as capacidades do APSEA;
    - Investigação de como essas abordagens podem ser incorporadas de maneira sinérgica para oferecer uma solução mais abrangente na conscientização e prevenção contra ataques de ES.
    - Implementação de um *chatbot* integrado ao APSEA, que utiliza IA para análise de emoções e intenções em comunicações digitais, permitindo uma interação mais intuitiva e proativa com os usuários, além de detectar sinais de tentativas de engenharia social e alertar os usuários e administradores sobre possíveis ameaças.

10.2 Limitações

Algumas limitações econtradas neste trabalho incluem:

- Tamanho da Amostra: O número de participantes foi limitado a 15 pessoas, devido ao âmbito no setor de Tecnologia da Informação e às restrições logísticas e temporais do projeto. Embora uma amostra maior pudesse oferecer uma visão mais abrangente, as limitações de recursos e a necessidade de manter a eficiência no processo de coleta de dados levaram à decisão de focar em um grupo mais restrito. É importante considerar essa limitação ao interpretar e generalizar os resultados. Em estudos futuros, a expansão da amostra pode ser explorada para uma compreensão mais abrangente e representativa, a exemplo de outros setores e órgãos públicos para uma analogia mais condizente.
- Viés: O estudo apresenta uma limitação significativa devido à sua realização exclusiva no setor de tecnologia, resultando em um viés específico para as características e desafios desse ambiente. Embora essa abordagem tenha permitido uma análise aprofundada das ameaças de ES relevantes para profissionais de tecnologia da informação do setor público, as conclusões podem não ser diretamente aplicáveis a outros setores.
- Recursos Disponíveis: A restrição de recursos, notadamente no que diz respeito ao tempo, interesse e disponibilidade dos participantes em utilizar o *software* e dedicar-se à avaliação do desempenho, emerge como uma limitação substancial do estudo. O envolvimento ativo dos participantes é crucial para obter *insights* significativos, e fatores como a carga de trabalho, prioridades operacionais e o grau de disposição individual para se engajar no processo podem influenciar diretamente os resultados. A qualidade das avaliações depende não apenas da ferramenta em si, mas também do comprometimento e da disponibilidade dos usuários.

10.3 Produções Relacionadas

Nesta seção são apresentadas as produções relacionadas à dissertação

1. Artigos Publicados:
    - Cardoso, Waldson Rodrigues, João Marco Cardoso Silva and Admilson de Ribamar Lima Ribeiro. *"An Expert System as an Awareness Tool to Prevent Social Engineering Attacks in Public Organizations."International Journal on Cybernetics & Informatics (IJCI) Vol 12 (2023). Qualis A3.*
    - Cardoso, Waldson Rodrigues, Admilson de Ribamar Lima Ribeiro and João Marco Cardoso Silva. *"Expert Systems in Information Security: A Comprehensive Exploration of Awareness Strategies Against Social Engineering Attacks."Springer, Qualis A2.*

Referências

ADANE, K. Development of advisory knowledge-based expert system to identify and mitigate unintentional insider threats in financial institutions of ethiopia. *IUP Journal of Computer Sciences*, IUP Publications, v. 14, n. 3, p. 7–23, 2020. Citado 3 vezes nas páginas 53, 54 e 57.

ALASSAF, M.; ALKHALIFAH, A. Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access*, v. 9, p. 162687–162705, 2021. Citado na página 21.

ALDAWOOD, H.; SKINNER, G. Challenges of implementing training and awareness programs targeting cyber security social engineering. In: *2019 Cybersecurity and Cyberforensics Conference (CCC)*. [S.l.: s.n.], 2019. p. 111–117. Citado 2 vezes nas páginas 41 e 45.

ALDAWOOD, H.; SKINNER, G. Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions. *IEEE Access*, v. 8, p. 67321–67329, 2020. Citado 3 vezes nas páginas 42, 45 e 46.

ALGHENAIM, M. F. et al. Employee awareness model to enhance awareness of social engineering threats in the saudi public sector. In: *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*. [S.l.: s.n.], 2021. p. 1–6. Citado 3 vezes nas páginas 42, 45 e 46.

ARABIA-OBEDOZA, M. R. et al. Social engineering attacks: A reconnaissance synthesis analysis. In: *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. New York, NY, USA: [s.n.], 2020. p. 0843–0848. Citado na página 30.

ARABIA-OBEDOZA, M. R. et al. Social engineering attacks a reconnaissance synthesis analysis. In: *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*. [S.l.: s.n.], 2020. p. 0843–0848. Citado na página 46.

ARAMUNI, J. P. C.; MAIA, L. C. The impact of social engineering on information security: A management-oriented approach. *AtoZ: New Practices in Information and Knowledge*, v. 7, n. 1, p. 31–37, 2020. Citado na página 50.

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 24.

ASTAKHOVA, L.; MEDVEDEV, I. Scanning the resilience of an organization employees to social engineering attacks using machine learning technologies. In: *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*. [S.l.: s.n.], 2020. p. 606–610. Citado 5 vezes nas páginas 15, 24, 42, 45 e 46.

AZEVEDO, M. S. de; AL. et. Desenvolvimento de protótipo de sistema especialista para o auxílio no diagnóstico de esquizofrenia. *Revista Brasileira Educação e Saúde*, v. 9, p. 8, 2019. Citado na página 62.

BECKERS, K.; PAPE, S. A serious game for eliciting social engineering security requirements. In: *2016 IEEE 24th International Requirements Engineering Conference (RE)*. [S.l.: s.n.], 2016. p. 16–25. Citado 3 vezes nas páginas 43, 45 e 46.

BOAVENTURA, E. M. *Metodologia da pesquisa: monografia, dissertação, tese*. [S.l.]: Atlas, 2004. Citado na página 32.

CARRICO, M. A.; GIRARD, J. E.; JONES, J. P. *Building knowledge systems: developing and managing rule-based applications*. [S.l.]: McGraw-Hill, Inc., 1989. Citado na página 31.

CASTRO, E. T. V. de; SILVA, G. R. S.; CANEDO, E. D. Ensuring privacy in the application of the brazilian general data protection law (lgpd). In: *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2022. (SAC '22), p. 1228–1235. ISBN 9781450387132. Disponível em: <https://doi-org.ez20.periodicos.capes.gov.br/10.1145/3477314.3507023>. Citado 2 vezes nas páginas 22 e 23.

COELHO, C. F.; RASMA, E. T.; MORALES, G. Social engineering: A threat to the information society. *Exatas & Engenharias, Higher Education Institutes of Censa*, v. 3, n. 05, 2013. Citado na página 50.

COELHO, F.; RASMA, E.; MORALES, G. Engenharia social: Uma ameaça à sociedade da informação. *Revista Perspectivas Online*, 2013. Disponível em: <https://goo.gl/74kwCq>. Citado na página 24.

CULLEN, A.; ARMITAGE, L. A human vulnerability assessment methodology. In: *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. [S.l.: s.n.], 2018. p. 1–2. Citado na página 24.

DANTAS, A. R. P. Cyrm: Cyber range to support the teaching of defense for students in the information security discipline. 2022. Master's Thesis (se aplicável). Citado na página 51.

DASH, B.; ANSARI, M. F. An effective cybersecurity awareness training model: First defense of an organizational security strategy. 2022. Citado 3 vezes nas páginas 53, 54 e 57.

ELMASRI, R.; NAVATHE, S. B. *Sistemas de Banco de Dados*. [S.l.]: Pearson Brasil, 2011. ISBN 9788579360855. Citado na página 67.

FELIPE, G. F. et al. Avaliação de software para acolhimento com classificação de risco em pediatria. *Revista Brasileira de Enfermagem*, SciELO Brasil, v. 73, 2020. Citado 2 vezes nas páginas 89 e 90.

FERREIRA, M. M. G.; AL. et. Aplicação do software expert sinta objetivando o auxílio da tomada de decisão em situação de acidente de trabalho em uma madeireira. *Brazilian Journal of Development*, v. 6, n. 3, p. 14704–14715, 2020. Acesso em: 20 jun. 2022. Disponível em: <https://www.brazilianjournals.com/index.php/BRJD/article/view/7996>. Citado na página 65.

FERREIRA, M. M. G. et al. Aplicação do software expert sinta objetivando o auxílio da tomada de decisão em situação de acidente de trabalho em uma madeireira. *Brazilian Journal of Development*, v. 6, n. 3, p. 14704–14715, 2020. Citado na página 60.

FOWLER, M. *Patterns of Enterprise Application Architecture*. Boston, MA: Addison-Wesley, 2002. Citado na página 71.

GAMMA, E. et al. *Design Patterns: Elements of Reusable Object-Oriented Software*. Reading, MA: Addison-Wesley, 1994. Citado na página 70.

GIARRATANO, J. C.; RILEY, G. *Expert systems: principles and programming*. [S.l.]: Brooks/Cole Publishing Co., 1989. Citado na página 31.

GIL, A. C. *Métodos e técnicas de pesquisa social*. [S.l.]: 6. ed. Ediitora Atlas SA, 2008. Citado na página 32.

GRASSEGGER, T.; NEDBAL, D. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, v. 181, p. 59–66, 2021. ISSN 1877-0509. CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050921001381>. Citado 4 vezes nas páginas 15, 41, 45 e 46.

HADNAGY, C. *Social Engineering: The Art of Human Hacking*. [S.l.]: John Wiley & Sons, 2010. Citado na página 50.

HAMMOUR, R. A. et al. The status of information security systems in banking sector from social engineering perspective. In: *Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems*. New York, NY, USA: Association for Computing Machinery, 2019. (DATA '19). ISBN 9781450372848. Disponível em: <https://doi-org.ez20.periodicos.capes.gov.br/10.1145/3368691.3368705>. Citado 3 vezes nas páginas 41, 45 e 46.

HIJJI, M.; ALAM, G. Cybersecurity awareness and training (cat) framework for remote working employees. *Sensors (Basel)*, MDPI AG, v. 22, n. 22, p. 8663, 2022. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/22/22/8663>. Citado na página 49.

HONORIO, T. J. The use of cyberattacks in elections and international relations. *Mural Internacional*, v. 9, n. 1, p. 85–98, 2018. Citado na página 51.

JACKSON, P. Introduction to expert systems. Addison-Wesley Pub. Co., Reading, MA, 1986. Citado na página 31.

JANSEN, P.; FISCHBACH, F. The social engineer: An immersive virtual reality educational game to raise social engineering awareness. In: ____. *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play*. New York, NY, USA: Association for Computing Machinery, 2020. p. 59–63. ISBN 9781450375870. Disponível em: <https://doi.org/10.1145/3383668.3419917>. Citado 3 vezes nas páginas 42, 45 e 46.

JUNIOR, J. V. C. Threat analysis environment for threat intelligence generation using open sources. 2018. Mestrado Thesis. Citado na página 51.

KHLOBYSTOVA, A.; ABRAMOV, M. Time-based model of the success of a malefactor's multistep social engineering attack on a user. In: SPRINGER. *International Conference on Intelligent Information Technologies for Industry*. [S.l.], 2021. p. 216–223. Citado na página 41.

KOYUN, A.; JANABI, E. A. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, v. 4, n. 6, p. 7533–7538, 2017. Citado 2 vezes nas páginas 25 e 26.

KROMBHOLZ, K. et al. Advanced social engineering attacks. *Journal of Information Security and Applications*, v. 22, p. 113–122, 2015. ISSN 2214-2126. Special Issue on Security of Information and Networks. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214212614001343>. Citado 8 vezes nas páginas 23, 25, 26, 28, 29, 30, 40 e 45.

LEONOV, P. Y. et al. The main social engineering techniques aimed at hacking information systems. In: *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*. [S.l.: s.n.], 2021. p. 0471–0473. Citado 2 vezes nas páginas 15 e 16.

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 22.

MANDRAKOV, E. S.; VASILIEV, V. A.; DUDINA, D. A. Application of expert systems in quality management. In: *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies*. [S.l.: s.n.], 2021. p. 516–518. Citado na página 30.

MAXIM, B.; PRESSMAN, R. S. *Engenharia de software: uma abordagem profissional*. [S.l.]: Porto Alegre:[sn], 2021. Citado na página 68.

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 50.

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 22.

MOUTON, F.; LEENEN, L.; VENTER, H. S. Social engineering attack examples, templates and scenarios. *Computers & Security*, Elsevier, v. 59, p. 186–209, 2016. Citado 2 vezes nas páginas 41 e 45.

MOUTON, F.; TEIXEIRA, M.; MEYER, T. Benchmarking a mobile implementation of the social engineering prevention training tool. In: *2017 Information Security for South Africa (ISSA)*. [S.l.: s.n.], 2017. p. 106–116. Citado 3 vezes nas páginas 42, 45 e 46.

NAIR, A. S. V.; ACHARY, R. Social engineering defender (se.def): Human emotion factor based classification and defense against social engineering attacks. *2023 International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1)*, Bangalore, India, p. 1–5, 2023. Citado na página 51.

NILSSON, N. J. *Principles of artificial intelligence*. [S.l.]: Springer Science & Business Media, 1982. Citado na página 31.

NORMATOV, S.; RAKHMATULLAEV, M. Expert system with fuzzy logic for protecting scientific information resources. In: *2020 International Conference on Information Science and Communications Technologies (ICISCT)*. [S.l.: s.n.], 2020. p. 1–4. Citado 3 vezes nas páginas 53, 55 e 57.

OBUHUMA, J.; ZIVUKU, S. Social engineering based cyber-attacks in kenya. In: *2020 IST-Africa Conference (IST-Africa)*. [S.l.: s.n.], 2020. p. 1–9. Citado 6 vezes nas páginas 43, 45, 46, 53, 54 e 57.

OSUAGWU, E. U. et al. Mitigating social engineering for improved cybersecurity. In: *2015 International Conference on Cyberspace (CYBER-Abuja)*. [S.l.: s.n.], 2015. p. 91–100. Citado 7 vezes nas páginas 20, 25, 28, 29, 40, 45 e 46.

OTWELL, T. Laravel. 2016. Disponível em: <https://github.com/laravel/laravel>. Citado na página 34.

PASCHOAL, D. A. C.; PEREIRA, G. F. Information security in industry 4.0: Nist framework. 2019. Bachelor Thesis. Citado na página 51.

PETERSEN, K.; VAKKALANKA, S.; KUZNIARZ, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, v. 64, p. 1–18, 2015. ISSN 0950-5849. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0950584915000646>. Citado na página 37.

PINZON, J. J. S. et al. Social engineering, the before and now of a global problem. *National Open and Distance University UNAD*, 2015. Citado na página 50.

RANI, C.; GOEL, S. Csaaes: An expert system for cyber security attack awareness. In: *International Conference on Computing, Communication Automation*. [S.l.: s.n.], 2015. p. 242–245. Citado 4 vezes nas páginas 31, 53, 54 e 56.

RITA, M. da N. B.; AL. et. Proposta de um sistema especialista para identificação de transtornos alimentares. *Revista Brasileira Educação e Saúde*, v. 10, n. 2, p. 117–126, 2020. Acesso em: 20 jun. 2022. Disponível em: <https://doi.org/10.18378/rebes.v10i2.7842>. Citado 3 vezes nas páginas 60, 62 e 65.

Rocha Flores, W.; EKSTEDT, M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, v. 59, p. 26–44, 2016. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404816000067>. Citado 2 vezes nas páginas 23 e 45.

ROSA, R. R.; AL. et. Reflexão sobre a classificação de risco como tendência para o pronto-socorro infantil/reflection on risk classification as a trend for the infant emergency room/la reflexión sobre la calificación de riesgo como una tendencia para la emergencia del niño. *JOURNAL HEALTH NPEPS*, v. 4, n. 1, p. 330–340, 2019. Acesso em: 20 jun. 2022. Disponível em: <https://periodicos.unemat.br/index.php/jhnpeps/article/view/3327>. Citado na página 64.

ROSSO, M.; SILVA, S. H. da; SCALABRIN, E. E. Sistema baseado em conhecimento para apoio à identificação dos focos do processo corporal da cipe®. *Texto & Contexto-Enfermagem*, v. 18, p. 523–531, 2009. Acesso em: 25 jul. 2022. Disponível em: <https://www.scielo.br/j/tce/a/VHtRYGncx3FYXV8GzgzxwCy/abstract/?format=html&lang=pt>. Citado na página 60.

RUSSELL, S. J.; NORVIG, P. *Artificial Intelligence: A Modern Approach*. 3rd. ed. Upper Saddle River, NJ: Prentice Hall, 2010. Citado na página 16.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. *Future internet*, MDPI, v. 11, n. 4, p. 89, 2019. Citado 3 vezes nas páginas 25, 26 e 28.

SIHWI, S. W.; ANDRIYANTO, F.; ANGGRAININGSIH, R. An expert system for risk assessment of information system security based on iso 27002. In: *2016 IEEE International Conference on Knowledge Engineering and Applications (ICKEA)*. [S.l.: s.n.], 2016. p. 56–61. Citado 3 vezes nas páginas 30, 31 e 60.

SILVA, N. B. X.; ARAúJO, W. J. d.; AZEVEDO, P. M. d. Social engineering in online social networks: A case study on the exposure of personal information and the need for information security strategies. *Ibero-American Journal of Information Science*, v. 6, n. 2, 2013. Citado na página 50.

SILVEIRA, D. T.; CÓRDOVA, F. P. A pesquisa científica. *Métodos de pesquisa. Porto Alegre: Editora da UFRGS, 2009. p. 33-44*, 2009. Citado 2 vezes nas páginas 32 e 87.

Sohrabi Safa, N.; Von Solms, R.; FURNELL, S. Information security policy compliance model in organizations. *Computers & Security*, v. 56, p. 70–82, 2016. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404815001583>. Citado 3 vezes nas páginas 21, 41 e 46.

SOMMERVILLE, I. *Engenharia de Software*. 8. ed. São Paulo: Pearson Addison Wesley, 2007. ISBN 9788588639287. Citado na página 66.

SOMMERVILLE, I. *Engenharia de Software*. 9. ed. [S.l.]: Pearson Prentice Hall, 2011. ISBN 9788579361081. Citado na página 34.

STALLINGS, W.; BROWN, L. *Computer security: principles and practice*. [S.l.]: Pearson, 2015. Citado na página 21.

TIOH, J.-N.; MINA, M.; JACOBSON, D. W. Cyber security social engineers an extensible teaching tool for social engineering education and awareness. In: *2019 IEEE Frontiers in Education Conference (FIE)*. [S.l.: s.n.], 2019. p. 1–5. Citado 3 vezes nas páginas 43, 45 e 46.

WERLINGER, R. et al. Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, Elsevier, v. 67, n. 7, p. 584–606, 2009. Citado na página 20.

WHITMAN, M. E.; MATTORD, H. J. *Management of information security*. [S.l.]: Cengage Learning, 2019. Citado na página 21.

WILCOX, H.; BHATTACHARYA, M. A human dimension of hacking: Social engineering through social media. *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, v. 790, n. 1, p. 012040, mar 2020. Disponível em: <https://doi.org/10.1088/1757-899x/790/1/012040>. Citado 2 vezes nas páginas 24 e 45.

WILSON, B. Introducing cyber security by designing social engineering attacks. Consortium for Computing Sciences in Faculdades, Evansville, IN, EUA, v. 34, n. 1, p. 235–241, out 2018. ISSN 1937-4771. Citado 4 vezes nas páginas 15, 41, 45 e 46.

YANASE, J.; TRIANTAPHYLLOU, E. A systematic survey of computer-aided diagnosis in medicine: Past and present developments. *Expert Systems with Applications*, v. 138, p. 112821, 2019. Acesso em: 20 jun. 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417419305238>. Citado 3 vezes nas páginas 60, 64 e 65.

YU, J. et al. Research and design of subway bas intrusion detection expert system. In: *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. [S.l.: s.n.], 2018. p. 152–156. Citado na página 30.

ZADEH, L. A. Fuzzy sets. *Information and control*, Elsevier, v. 8, n. 3, p. 338–353, 1965. Citado na página 31.

Apêndices

APÊNDICE A – Definição de Perguntas e Regras

Definição Inicial das Perguntas e Regras do Sistema Especialista APSEA

Pergunta 1 (*Phishing*):

- Pergunta: Você verifica cuidadosamente os remetentes de *e-mails* antes de abrir anexos ou clicar em *links*?

Regra 1:

Se Resposta = "Sempre" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Ótimo! Verificar cuidadosamente os remetentes é crucial para evitar *Phishing*."
Senão Se Resposta = "Às vezes" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Fique atento! Melhorar a verificação pode reduzir riscos de *Phishing.*"
Senão Resposta = "Nunca" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Verificar remetentes é fundamental para evitar *Phishing*."

Pergunta 2 (*Vishing*):

- Pergunta: Você desconfia de chamadas telefônicas inesperadas que solicitam informações sensíveis?

Regra 2:

Se Resposta = "Sempre" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Ótimo! Desconfiar de chamadas inesperadas ajuda a evitar *Vishing*."
Senão Se Resposta = "Às vezes" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Fique atento! Melhorar a desconfiança pode reduzir riscos de *Vishing*."
Senão Resposta = "Nunca" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Desconfiar de chamadas é essencial para evitar *Vishing*."

Pergunta 3 (*Pretexting*):

- Pergunta: Você verifica a legitimidade de solicitações de informações pessoais, mesmo que pareçam oficiais?

Regra 3:

Se Resposta = "Sempre" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Excelente! Verificar a legitimidade é fundamental para evitar *Pretexting*."
Senão Se Resposta = "Às vezes" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Fique atento! Melhorar a verificação pode reduzir riscos de *Pretexting*."
Senão Resposta = "Nunca" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Verificar legitimidade é essencial para evitar *Pretexting*."

Pergunta 4 (*Quid Pro Quo*):

- Pergunta: Você recusa ofertas de benefícios em troca de informações confidenciais, mesmo que pareçam vantajosas?

Regra 4:

Se Resposta = "Sempre" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Parabéns! Recusar ofertas em troca de informações é essencial para evitar *Quid Pro Quo*."
Senão Se Resposta = "Às vezes" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Fique atento! Recusar ofertas suspeitas pode reduzir riscos de *Quid Pro Quo*."
Senão Resposta = "Nunca" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Recusar ofertas suspeitas é crucial para evitar situações de *Quid Pro Quo*."

Pergunta 5 (*Baiting*):

- Pergunta: Ao encontrar dispositivos USB ou mídias deixadas propositalmente, como você reage?

Regra 5 :

Se Resposta = "Conecto ao computador" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Conectar dispositivos desconhecidos pode expor seu sistema a riscos de *Baiting*."
Senão Resposta = "Ignoro" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Atenção! Ignorar mídias desconhecidas é um primeiro passo, mas avaliar o risco é fundamental."

Pergunta 6 (*Tailgating*):

- Pergunta: Você permite que pessoas desconhecidas entrem em áreas restritas sem verificar suas credenciais?

Regra 6:

Se Resposta = "Permito entrada" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Permitir acesso sem verificar credenciais pode resultar em vulnerabilidades de *Tailgating*."
Senão Resposta = "Verifico credenciais" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Bom trabalho! Verificar as credenciais ajuda a prevenir situações de *Tailgating*."

Pergunta 7 (*Dumpster Diving*):

- Pergunta: Ao descartar documentos ou dispositivos, você adota precauções para evitar o Dumpster Diving, como a destruição segura de informações sensíveis?

Regra 7:

Se Resposta = "Descarto sem precauções" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Descartar informações sem precauções pode resultar em riscos de *Dumpster Diving*. Adote práticas seguras de descarte."
Senão Resposta = "Adoto precauções de destruição" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Ótimo! Adotar precauções na destruição de informações ajuda a proteger contra ataques de *Dumpster Diving*."

Pergunta 8 (*Shoulder Surfing*):

- Pergunta: Ao digitar informações confidenciais em seu dispositivo, você toma medidas para proteger contra Shoulder Surfing, como ajustar sua posição para evitar olhares indiscretos?

Regra 8:

Se Resposta = "Não tomo precauções" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Não tomar precauções contra *Shoulder Surfing* pode expor informações sensíveis. Proteja sua privacidade adotando medidas preventivas."
Senão Resposta = "Adoto medidas de proteção" => Nível de Vulnerabilidade = "Baixo", Feedback = "Parabéns! Adotar medidas para proteger contra Shoulder Surfing é fundamental para garantir a segurança de suas informações confidenciais."

Pergunta 9 (*Scareware*):

- Pergunta: Ao encontrar pop-ups ou mensagens assustadoras em seu dispositivo, você mantém a calma e verifica a autenticidade, evitando ações impulsivas?

Regra 9:

Se Resposta = "Reajo impulsivamente" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Reações impulsivas diante de mensagens assustadoras podem expor você a Scareware. Mantenha a calma e verifique a autenticidade antes de agir."
Senão Resposta = "Verifico a autenticidade" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Ótimo! Verificar a autenticidade diante de mensagens alarmantes é uma prática segura para evitar *Scareware*. Continue mantendo a calma e agindo com cautela."

Pergunta 10 (*Phishing*):

- Pergunta: Diante de uma oferta inesperada por e-mail, como você decide compartilhar ou não suas informações?

Regra 10:

Se Resposta = "Compartilho" => Nível de Vulnerabilidade = "Alto", *Feedback* = "Cuidado! Compartilhar informações sem avaliar pode ser arriscado."
Senão Se Resposta = "Peço mais informações" => Nível de Vulnerabilidade = "Médio", *Feedback* = "Boa abordagem! Pedir mais informações ajuda a tomar decisões conscientes."
Senão Resposta = "Recuso imediatamente" => Nível de Vulnerabilidade = "Baixo", *Feedback* = "Ótimo! Recusar ofertas inesperadas é uma prática segura."

APÊNDICE B – Exemplo de um Resultado Individual da Avaliação no APSEA

Resultados da Avaliação de Segurança

Voltar

Aqui estão os resultados da sua avaliação de segurança. Estes resultados fornecem uma análise personalizada com base nas suas respostas.

Informações da Avaliação

Nome: **********

Data da Avaliação: 27/11/2023

Percentual do Nível de Vulnerabilidade de sua Avaliação:

Percentual Alta: 10.00%

Percentual Média: 20.00%

Percentual Baixa: 70.00%

Resultado 1

Pergunta: Você verifica cuidadosamente os remetentes de e-mails antes de abrir anexos ou clicar em links?

Tipo de Ataque: Phishing

Detalhe: O termo "phishing" deriva da palavra em inglês "fishing" (pescaria) e representa um tipo de ataque cibernético no qual os criminosos buscam obter informações confidenciais, como senhas e dados financeiros, ao se passarem por entidades confiáveis. Utilizando e-mails, mensagens de texto e outros meios eletrônicos, os golpistas enganam as vítimas para clicarem em links maliciosos ou divulgarem informações pessoais. A prática envolve manipulação psicológica para explorar a confiança das vítimas, com o objetivo final de obter acesso não autorizado a contas online, realizar fraudes financeiras ou roubar identidades.

Recomendações: Para evitar golpes de phishing, adote práticas sólidas de segurança cibernética, como desconfiar de e-mails e mensagens não solicitados. Nunca forneça informações pessoais em resposta a solicitações suspeitas. Verifique cuidadosamente a legitimidade do remetente, evite clicar em links suspeitos e acesse sites oficiais digitando manualmente os URLs. Mantenha senhas seguras, evite reutilizá-las e ative a autenticação de dois fatores para maior segurança. Fique atualizado sobre as técnicas de phishing, compartilhando informações com colegas e familiares. Mantenha dispositivos e softwares atualizados, incluindo antivírus e firewalls, para reduzir significativamente o risco de cair em armadilhas de phishing, protegendo suas informações online.

Resposta: Sempre

Vulnerabilidade: Baixa

Feedback: Ótimo! Verificar cuidadosamente os remetentes é crucial para evitar Phishing.

Resultado 2

Pergunta: Você desconfia de chamadas telefônicas inesperadas que solicitam informações sensíveis?

Tipo de Ataque: Vishing

Detalhe: O termo vishing é uma combinação das palavras voice (voz) e phishing. Trata-se de uma forma de ataque de phishing que ocorre por meio de chamadas telefônicas. Os criminosos que praticam vishing geralmente se passam por instituições legítimas, como bancos, empresas de cartão de crédito ou agências governamentais, com o objetivo de obter informações pessoais, como números de cartão de crédito, senhas ou detalhes de contas bancárias.

Recomendações: Para evitar ataques de vishing, é essencial adotar práticas específicas durante chamadas telefônicas. Ao receber chamadas não solicitadas, mantenha uma postura cautelosa, evitando fornecer informações pessoais ou financeiras. Em situações em que um solicitante, mesmo aparentando ser de uma instituição legítima, pede dados confidenciais, confirme a identidade ligando diretamente para a empresa através de um número confiável, não o fornecido na chamada. Além disso, ao lidar com chamadas de números desconhecidos, é recomendável não compartilhar informações imediatamente. Peça detalhes de contato e verifique a legitimidade da chamada antes de fornecer qualquer dado. Caso uma mensagem de voz ou chamada exija ação imediata, evite retornar a chamada usando o número fornecido na mensagem, optando por utilizar um número oficial da empresa. A utilização de um identificador de chamadas confiável pode ser uma ferramenta valiosa para verificar a origem das chamadas recebidas. É crucial investir na educação própria e de outros membros da equipe sobre os perigos do vishing, proporcionando treinamento regular para identificação e prevenção desse tipo de ataque. Para um registro eficiente, anote detalhes de chamadas suspeitas, como números de telefone, horários e informações fornecidas. Esses registros podem ser úteis para referência futura ou para relatar atividades suspeitas às autoridades. Ao seguir essas práticas, você estará protegendo suas informações pessoais e financeiras durante interações telefônicas, reduzindo significativamente o risco de cair em golpes de vishing.

Resposta: Sempre

Vulnerabilidade: Baixa

Feedback: Ótimo! Desconfiar de chamadas inesperadas ajuda a evitar Vishing.

Resultado 3

Pergunta: Você verifica a legitimidade de solicitações de informações pessoais, mesmo que pareçam oficiais?

Tipo de Ataque: Pretexting

Detalhe: Pretexting é uma técnica de engenharia social em que um indivíduo cria um cenário fictício ou uma história falsa (pretexto) para obter informações confidenciais de outra pessoa. O pretexto é projetado para parecer legítimo e persuadir a vítima a revelar detalhes pessoais, financeiros ou outros dados sensíveis. Essa forma de manipulação visa explorar a confiança da vítima na aparente autenticidade da situação apresentada.

Recomendações: Para fortalecer sua resistência contra ataques de pretexting, é crucial adotar práticas de segurança específicas. Mantenha cautela ao compartilhar informações pessoais, questionando a necessidade e autenticidade das solicitações, e, em caso de dúvida, verificando diretamente a legitimidade com a empresa envolvida. Conheça os processos internos da sua organização para identificar solicitações suspeitas e estabeleça uma política de verificação que encoraje a checagem de informações sensíveis. Seja cauteloso com chamadas não solicitadas, encerrando-as e contatando diretamente a empresa em questão. Proteja suas informações confidenciais, como números de conta bancária, evitando compartilhá-las desnecessariamente. Eduque-se sobre as táticas de pretexting, participe de treinamentos regulares de conscientização como este e promova uma cultura organizacional que valorize a segurança da informação. Implemente um processo claro

para relatar atividades suspeitas, incentivando a vigilância e prontidão para identificar e responder eficazmente a tentativas de manipulação baseadas em histórias fictícias. Essas práticas fortalecem sua postura contra ataques de pretexting.

Resposta: Sempre

Vulnerabilidade: Baixa

Feedback: Excelente! Verificar a legitimidade é fundamental para evitar Pretexting.

Resultado 4

Pergunta: Você recusa ofertas de benefícios em troca de informações confidenciais, mesmo que pareçam vantajosas?

Tipo de Ataque: Quid Pro Quo

Detalhe: Quid pro quo é uma expressão em latim que significa algo por algo. No contexto da segurança da informação e da engenharia social, o termo é utilizado para descrever uma técnica em que um atacante oferece algo de valor ou vantajoso em troca de informações sensíveis ou acesso não autorizado a sistemas.

Recomendações: Ao enfrentar situações de quid pro quo, é essencial adotar práticas preventivas para fortalecer sua resiliência contra tentativas de manipulação. Isso inclui cultivar ceticismo em relação a ofertas inesperadas e evitar trocar informações sensíveis por benefícios. Confirme a legitimidade das propostas, conheça os procedimentos internos da organização e participe de treinamentos de conscientização, como os proporcionados pela ferramenta APSEA. Promova uma cultura organizacional que valorize a segurança da informação, implemente políticas claras e estabeleça um processo para relatar atividades suspeitas. Essas medidas ajudam a fortalecer sua capacidade de resistir a tentativas de manipulação baseadas em trocas de informações.

Resposta: Sempre

Vulnerabilidade: Baixa

Feedback: Parabéns! Recusar ofertas em troca de informações é essencial para evitar Quid Pro Quo.

Resultado 5

Pergunta: Ao encontrar dispositivos USB ou mídias deixadas propositalmente, como você reage?

Tipo de Ataque: Baiting

Detalhe: Baiting é uma técnica de engenharia social que envolve oferecer algo atrativo ou irresistível para atrair pessoas e induzi-las a realizar ações específicas, muitas vezes prejudiciais. O termo é derivado da palavra em inglês bait, que significa isca. Esse tipo de ataque visa explorar a curiosidade ou a ganância das vítimas para obter informações confidenciais ou instalar malware em seus dispositivos.

Recomendações: Para evitar ataques de "baiting", é fundamental adotar medidas preventivas. Nunca conecte dispositivos USB ou outros meios de armazenamento encontrados em locais desconhecidos ou públicos. Evite a tentação de utilizar objetos aparentemente abandonados, como USBs, que podem servir como isca para ataques. Mantenha seu software de segurança sempre atualizado, garantindo a detecção eficaz de possíveis

ameaças. Ao adotar uma postura de precaução e evitar a curiosidade desnecessária em relação a dispositivos encontrados, você reduz significativamente o risco de cair em armadilhas de "baiting".

Resposta: Conecto ao computador

Vulnerabilidade: Alta

Feedback: Cuidado! Conectar dispositivos desconhecidos pode expor seu sistema a riscos de Baiting.

Resultado 6

Pergunta: Você permite que pessoas desconhecidas entrem em áreas restritas sem verificar suas credenciais?

Tipo de Ataque: Tailgating

Detalhe: Tailgating, também conhecido como "piggybacking" ou carona, é uma forma de ataque de engenharia social que ocorre quando um indivíduo não autorizado segue de perto um indivíduo autorizado para ganhar acesso a áreas restritas sem a devida autenticação. Este tipo de ataque explora a cortesia ou a falta de vigilância por parte dos funcionários para infiltrar-se em instalações protegidas.

Recomendações: Para evitar o tailgating, é essencial reforçar a segurança física instruindo os funcionários a não permitir a entrada de desconhecidos em áreas restritas. A implementação de controles de acesso, como cartões e câmeras, é crucial para garantir acesso autorizado. Promova uma cultura de segurança, incentivando relatórios de comportamentos suspeitos, e realize treinamentos regulares para sensibilizar os funcionários sobre os riscos associados ao tailgating. Essas práticas, integradas, reduzem significativamente o risco de acesso não autorizado por meio dessa técnica.

Resposta: Verifico credenciais

Vulnerabilidade: Média

Feedback: Bom trabalho! Verificar as credenciais ajuda a prevenir situações de Tailgating.

Resultado 7

Pergunta: Ao descartar documentos ou dispositivos, você adota precauções para evitar o Dumpster Diving, como a destruição segura de informações sensíveis?

Tipo de Ataque: Dumpster Diving

Detalhe: Dumpster diving é uma prática em que indivíduos procuram informações sensíveis ou materiais valiosos em lixeiras, contêineres de lixo ou descarte de documentos. Essa atividade é uma ameaça à segurança da informação e privacidade, pois informações confidenciais podem ser recuperadas indevidamente.

Recomendações: Para evitar o dumpster diving e proteger informações importantes, certifique-se de destruir documentos e dispositivos antes de descartá-los, utilizando trituradoras para documentos físicos e métodos seguros para eletrônicos. Promova a cultura de segurança, evitando descartar informações confidenciais em lixeiras comuns e esteja ciente dos riscos do dumpster diving. Utilize recipientes designados para descarte seguro de documentos confidenciais. Considere marcar ou destruir dispositivos eletrônicos antes do descarte. Participe de treinamentos como este e esteja ciente das políticas de segurança. Seguindo essas diretrizes, você contribui para evitar o dumpster diving e protege as informações sensíveis da organização.

Resposta: Adoto precauções de destruição

Vulnerabilidade: Baixa

Feedback: Ótimo! Adotar precauções na destruição de informações ajuda a proteger contra ataques de Dumpster Diving.

Resultado 8

Pergunta: Ao digitar informações confidenciais em seu dispositivo, você toma medidas para proteger contra Shoulder Surfing, como ajustar sua posição para evitar olhares indiscretos?

Tipo de Ataque: Shoulder Surfing

Detalhe: Shoulder surfing é uma técnica de engenharia social em que um indivíduo observa as informações confidenciais, como senhas, PINs ou dados pessoais, de uma pessoa sem o seu conhecimento, geralmente olhando por cima do ombro da vítima.

Recomendações: Ao evitar o shoulder surfing, mantenha a segurança em mente durante atividades cotidianas. Ao digitar senhas, faça isso em locais privados, bloqueando a visão de curiosos. Esteja ciente dos riscos, protegendo suas informações em caixas eletrônicos e teclados públicos. Considere o uso de protetores de tela de privacidade para limitar a visão lateral. Escolha ambientes isolados para tarefas sensíveis e adote a troca regular de senhas para aumentar a segurança. Essas práticas simples reduzem efetivamente o risco de exposição de informações durante suas atividades diárias.

Resposta: Adoto medidas de proteção

Vulnerabilidade: Baixa

Feedback: Parabéns! Adotar medidas para proteger contra Shoulder Surfing é fundamental para garantir a segurança de suas informações confidenciais.

Resultado 9

Pergunta: Ao encontrar pop-ups ou mensagens assustadoras em seu dispositivo, você mantém a calma e verifica a autenticidade, evitando ações impulsivas?

Tipo de Ataque: Scareware

Detalhe: Scareware é uma forma de software malicioso que tenta assustar os usuários, geralmente exibindo mensagens falsas de alerta de segurança, na esperança de persuadi-los a tomar ações prejudiciais, como comprar software falso ou fornecer informações pessoais.

Recomendações: Para se prevenir do scareware, comece educando-se sobre essas ameaças. Evite clicar em pop-ups suspeitos que usam táticas de urgência para pressionar ações rápidas. Mantenha seu software antivírus atualizado e faça o download apenas de fontes confiáveis. Desconfie de ofertas online muito vantajosas e verifique a legitimidade de alertas pesquisando online. Faça backups regulares de dados importantes e verifique a autenticidade de mensagens diretamente das fontes oficiais. Participe de programas de conscientização para fortalecer sua resiliência contra ameaças online. Ao adotar essas medidas, você reduz consideravelmente o risco de cair em táticas enganosas de scareware.

Resposta: Verifico a autenticidade

Vulnerabilidade: Baixa

Feedback: Ótimo! Verificar a autenticidade diante de mensagens alarmantes é uma prática segura para evitar Scareware. Continue mantendo a calma e agindo com cautela.

Resultado 10

Pergunta: Diante de uma oferta inesperada por e-mail, como você decide compartilhar ou não suas informações?

Tipo de Ataque: Phishing

Detalhe: O termo "phishing" deriva da palavra em inglês "fishing" (pescaria) e representa um tipo de ataque cibernético no qual os criminosos buscam obter informações confidenciais, como senhas e dados financeiros, ao se passarem por entidades confiáveis. Utilizando e-mails, mensagens de texto e outros meios eletrônicos, os golpistas enganam as vítimas para clicarem em links maliciosos ou divulgarem informações pessoais. A prática envolve manipulação psicológica para explorar a confiança das vítimas, com o objetivo final de obter acesso não autorizado a contas online, realizar fraudes financeiras ou roubar identidades.

Recomendações: Para evitar golpes de phishing, adote práticas sólidas de segurança cibernética, como desconfiar de e-mails e mensagens não solicitados. Nunca forneça informações pessoais em resposta a solicitações suspeitas. Verifique cuidadosamente a legitimidade do remetente, evite clicar em links suspeitos e acesse sites oficiais digitando manualmente os URLs. Mantenha senhas seguras, evite reutilizá-las e ative a autenticação de dois fatores para maior segurança. Fique atualizado sobre as técnicas de phishing, compartilhando informações com colegas e familiares. Mantenha dispositivos e softwares atualizados, incluindo antivírus e firewalls, para reduzir significativamente o risco de cair em armadilhas de phishing, protegendo suas informações online.

Resposta: Peço mais informações

Vulnerabilidade: Média

Feedback: Boa abordagem! Pedir mais informações ajuda a tomar decisões conscientes.

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

Este formulário tem como objetivo, coletar informações para validar o uso do APSEA (Sistema Especialista de Conscientização e Prevenção contra Ataques de Engenharia Social), que foi desenvolvido durante uma pesquisa de mestrado do programa de Pós Graduação em Ciência 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 da ferramenta APSEA (Sistema Especialista de Conscientização e Prevenção contra Ataques de Engenharia Social). Ao participar deste estudo a(o) sra. (sr.) irá colaborar com os orientadores Prof. Dr. Admilson de Ribamar Lima Ribeiro, Prof. Dr. João Marco Cardoso Silva e aluno Waldson Rodrigues Cardoso na validação do material desenvolvido durante uma pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação - PROCC/UFS para aplicação em pesquisas futuras. O presente formulário tomará um tempo médio entre 5 e 10 minutos para ser respondida. Ao responder às questões a seguir, a (o) sra (sr.) tem a liberdade de recusar a participação a qualquer momento, sem sofrer qualquer prejuízo. Além disso, se decidir continuar participando em qualquer fase da pesquisa, não haverá impacto negativo para a(o) sra. (sr.). Para obter mais informações sobre a pesquisa, sinta-se à vontade para entrar em contato através do e-mail waldson.cardoso@dcomp.ufs.br. Salientamos que todas as informações coletadas neste estudo serão tratadas com total confidencialidade, sendo que somente o mestrando e os orientadores terão acesso aos dados. Ao participar desta pesquisa, a sra. (sr.) não receberá benefícios diretos nem sofrerá prejuízos. No entanto, esperamos que este estudo forneça informações valiosas para validar o uso do APSEA como ferramenta eficaz contra esses ataques, contribuindo assim para aprimorar a segurança e a proteção das informações no âmbito do DETRAN/SE.

APÊNDICE D – Questionário de Avaliação

Avaliação do Sistema - APSEA

Este formulário tem como objetivo, coletar informações para validar o uso do APSEA (Sistema Especialista de Conscientização e Prevenção contra Ataques de Engenharia Social), que foi desenvolvido durante uma pesquisa de mestrado do programa de Pós Graduação em Ciência da Computação da Universidade Federal de Sergipe (DCOMP/UFS) como requisito parcial para a obtenção do título de Mestrado em Ciência da Computação.

* Indica uma pergunta obrigatória

1. A(O) sra. (sr.) está sendo convidado(a) a participar desta pesquisa que tem como finalidade validar o uso da ferramenta APSEA (Sistema Especialista de Conscientização e Prevenção contra Ataques de Engenharia Social). Ao participar deste estudo a(o) sra. (sr.) irá colaborar com os orientadores Prof. Dr. Admilson de Ribamar Lima Ribeiro, Prof. Dr. João Marco Cardoso Silva e aluno Waldson Rodrigues Cardoso na validação do material desenvolvido durante uma pesquisa de mestrado do Programa de Pós-Graduação em Ciência da Computação - PROCC/UFS para aplicação em pesquisas futuras. O presente formulário tomará um tempo médio entre 5 e 10 minutos para ser respondida. Ao responder às questões a seguir, a (o) sra (sr.) tem a liberdade de recusar a participação a qualquer momento, sem sofrer qualquer prejuízo. Além disso, se decidir continuar participando em qualquer fase da pesquisa, não haverá impacto negativo para a(o) sra. (sr.). Para obter mais informações sobre a pesquisa, sinta-se à vontade para entrar em contato através do e-mail waldson.cardoso@dcomp.ufs.br. Salientamos que todas as informações coletadas neste estudo serão tratadas com total confidencialidade, sendo que somente o mestrando e os orientadores terão acesso aos dados. Ao participar desta pesquisa, a sra. (sr.) não receberá benefícios diretos nem sofrerá prejuízos. No entanto, esperamos que este estudo forneça informações valiosas para validar o uso do APSEA como ferramenta eficaz contra esses ataques, contribuindo assim para aprimorar a segurança e a proteção das informações no âmbito do DETRAN/SE. *

Marcar apenas uma oval.

- ◯ sim
- ◯ não

2. Nome *

3. e-mail *

4. Função *

5. idade (faixa etária)

Marcar apenas uma oval.

- 18 a 25
- 26 a 33
- 34 a 41
- 42 ou mais

6. A funcionalidade do software atende ao que foi proposto? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

7. Qual a confiabilidade do sistema em executar as funções necessárias? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

8. Qual o esforço necessário para utilizar o APSEA? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

9. Qual o Nível de Desempenho do APSEA? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

10. Qual a Capacidade de manter o nível de desempenho num período de tempo? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

11. Qual a Proteção de informações e dados e Nível de acesso de pessoas? *

Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Completamente Apropriado

12. Você tem alguma sugestão específica para melhorar o APSEA? *