UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE
CURSO DE TECNOLOGIAS
DA INFORMAÇÃO E COMUNICAÇÃO

Érica de Souza Pires

# Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso

Araranguá
2023

Érica de Souza Pires

# Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso

Trabalho de Conclusão de Curso de Graduação em Tecnologias da Informação e Comunicação do Centro de Ciência, Tecnologias e Saúde da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Tecnologias da Informação e Comunicação.

Orientador: Prof. Paulo César Leite Esteves

Araranguá

2023

Pires, Érica de Souza
Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso / Érica de Souza Pires ; orientador, Paulo César Leite Esteves, 2023.
55 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2023.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. KnowBe4. 3. segurança da informação. 4. conscientização. I. Esteves, Paulo César Leite . II. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. III. Título.

Érica de Souza Pires

**Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso**

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de "Bacharel em Tecnologias da Informação e Comunicação" e aprovado em sua forma final pelo Curso de Tecnologias da Informação e Comunicação.

Araranguá, 03 de julho de 2023.

Documento assinado digitalmente
Vilson Gruber
Data: 13/07/2023 09:56:48-0300
CPF: ***.317.788-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Vilson Gruber, Dr.

Coordenador do Curso

**Banca examinadora**

Documento assinado digitalmente
Paulo Cesar Leite Esteves
Data: 12/07/2023 10:00:15-0300
CPF: ***.412.357-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Paulo César Leite Esteves, Dr.

Orientador

Documento assinado digitalmente
Marina Carradore Sergio
Data: 12/07/2023 10:04:58-0300
CPF: ***.746.359-**
Verifique as assinaturas em https://v.ufsc.br

Profª. Marina Carradore Sérgio, Dra.

Avaliadora

Universidade Federal de Santa Catarina

Documento assinado digitalmente
Giovani Mendonca Lunardi
Data: 12/07/2023 10:05:50-0300
CPF: ***.394.559-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Giovani Mendonça Lunardi, Dr.

Avaliador

Universidade Federal de Santa Catarina

Dedico este trabalho aos meus pais, amigos e professores

## AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida, e por me dar sabedoria para trilhar essa jornada de conhecimento.

Aos meus pais, Edson e Adriana, pois foram meu alicerce em todas as dificuldades e por priorizarem uma educação de qualidade e incentivarem os meus sonhos. Ao meu irmão Felipe por fazer parte desses momentos.

A Cooperativa, que possibilitou a realização da pesquisa. Em especial ao meu chefe Michel, que me deu todo apoio e me auxiliou na realização da coleta de dados junto aos colaboradores.

Aos meus valiosos amigos, Lucas, Beatriz e Lorenzo que compartilharam comigo além da graduação, bons momentos juntos.

À Universidade de Santa Catarina (UFSC), pela oportunidade de realizar meu sonho de fazer uma graduação em uma instituição federal de tão grande valor, por sua qualidade de ensino e formação gratuita. Aos professores e profissionais que contribuíram para minha formação acadêmica.

E ao professor Paulo César Esteves pela sua dedicação e orientação durante o período de elaboração deste trabalho.

Por fim, a todos aqueles que passaram pela minha vida pessoal e acadêmica, que auxiliaram de alguma forma a ser quem sou, obrigada.

*“A segurança da informação é um processo contínuo,não um destino final”.*

*(Bruce Schneier)*

## RESUMO

A presente pesquisa tem por objetivo analisar a eficácia da plataforma KnowBe4 para promover a conscientização da segurança da informação aos colaboradores de uma Cooperativa de Crédito. No atual cenário, as instituições financeiras enfrentam constantemente ameaças de ataques cibernéticos, *phishing*, *malware* e engenharia social, para tanto, os colaboradores precisam estar preparados para se protegerem e proteger a instituição. Quanto à metodologia, a pesquisa caracteriza-se como qualitativa, descritiva, sendo desenvolvida por meio de um estudo de caso. A coleta de dados foi realizada por meio de um questionário. Os resultados obtidos revelaram que a avaliação da ferramenta pelos próprios colaboradores foi muito positiva, demonstrando que é uma boa forma de compartilhar conhecimento e mudar comportamentos usando uma ferramenta de treinamento. Observou-se também as atitudes que os colaboradores seguiam a respeito das normas de Segurança da Informação, a maior parte mostrou seguir corretamente, entretanto uma pequena parcela não seguiu de forma rigorosa. A conscientização da Segurança da Informação deve ser contínua, e com o uso de ferramentas que enfatizem e tornem mais engajado para proteger seus ativos digitais e mitigar os riscos associados às ameaças cibernéticas.



**Palavras-chave**: KnowBe4; segurança da informação; conscientização.

**ABSTRACT**

This research aims to analyze the effectiveness of the KnowBe4 platform to promote information security awareness among employees of a Credit Union. In the current scenario, financial institutions constantly face threats of cyber attacks, phishing, malware and social engineering, therefore, employees need to be prepared to protect themselves and the institution. As for the methodology, the research is characterized as qualitative, descriptive, being developed through a case study. Data collection was performed through a questionnaire. The results obtained revealed that the assessment of the tool by the employees themselves was very positive, demonstrating that it is a good way to share knowledge and change behaviors using a training tool. It was also observed the attitudes that the employees followed regarding the Information Security standards, most of them showed to follow correctly, however a small portion did not follow rigorously. Information Security awareness must be continuous, and with the use of tools that emphasize and make you more engaged to protect your digital assets and mitigate the risks associated with cyber threats.

**Keywords**: KnowBe4; information security; awareness.

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| TI | Tecnologia da informação |
| TCC | Trabalho de Conclusão de Curso |
| TICs | Tecnologias da Informação e Comunicação |
| SI | Segurança da informação |
| LGPD | Lei Geral de Proteção de Dados |
| COBIT | *Control Objectives for Information and Related Technology* |
| ISO | *International Organization for Standardization* |
| ISACA | Associação de Auditoria e Controle de Sistemas de Informação |
| ABNT | Associação Brasileira de Normas Técnicas |
| SGSI | Sistema de Gestão de Segurança da Informação |
| DDoS | *Distributed Denial of Service* |
| CEO | *Chief Executive Officer* |
| AMABio | Amigos da Mata, do Agro e da Biodiversidade |
| CERT | Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil |

**SUMÁRIO**

# 1 INTRODUÇÃO

Levando em consideração o atual cenário das instituições financeiras em relação ao uso de dados e o cuidado com a proteção de ativos de informação partindo primeiramente dos seus colaboradores, esse estudo tem por motivação os elevados índices de golpes e ataques de engenheiros sociais a instituições financeiras que tem por intuito coletar informações e dados confidenciais para práticas de crimes. Um levantamento feito pela (FEBRABAN,2021), percebeu um aumento significativo de 165% nos ataques de engenharia social no primeiro semestre de 2021, em comparação ao segundo semestre de 2020.

São identificados uma sequência de riscos que a instituição pode sofrer caso seus colaboradores não estejam bem instruídos sobre os procedimentos para assegurar o uso e manuseio correto dos dados e informações da empresa e de seus clientes. Alguns deles são: vazamento de informações sensíveis, perda de dados, ataques cibernéticos, prejuízos financeiros, reputação negativa na credibilidade e imagem da empresa e até mesmo multas e sanções judiciais.

Neste contexto, o uso de plataformas de conscientização da segurança da informação se torna uma estratégia muito bem avaliada e eficaz para melhorar a cultura sobre esse assunto entre colaboradores de uma instituição bancária. Neste tipo de plataforma, são oferecidos treinamentos, teste de conhecimento, simuladores de ataques de *phishing*, entre outras funções, que ajudam os colaboradores a compreenderem a importância de adotarem boas práticas em seu dia a dia e também auxiliar a equipe de TI da empresa a avaliar, monitorar e impulsionar os conhecimentos dos funcionários a partir da ferramenta.

Portanto, este trabalho tem como objetivo investigar os benefícios do uso da plataforma KnowBe4 de conscientização em segurança da informação para os colaboradores de uma instituição financeira. Serão avaliados aspectos como a eficácia da plataforma na melhoria da cultura de proteção de dados, a satisfação dos colaboradores com o treinamento oferecido e propor recomendações para utilizar essas ferramentas de forma que estimule o usuário a pôr em prática seus aprendizados.

Pergunta da pesquisa: O uso da ferramenta KnowBe4 contribui para a conscientização dos colaboradores sobre segurança da informação em uma instituição financeira?

Espera-se que os resultados deste estudo contribuam para a compreensão dos benefícios das plataformas de conscientização para as instituições financeiras e incentivem a adoção dessas plataformas como uma estratégia para melhorar a segurança da informação e proteger os dados sensíveis dos clientes.

## 1.1 OBJETIVOS

Com base na contextualização apresentada são definidos os objetivos da pesquisa, a seguir:

### 1.1.1 Objetivo Geral

O objetivo geral deste estudo é analisar os benefícios do uso da ferramenta KnowBe4 para conscientização dos colaboradores sobre segurança da informação em uma instituição financeira.

### 1.1.2 Objetivos Específicos

Por meio dos objetivos específicos, será definido o caminho para chegar ao objetivo geral:

- Identificar, a partir de literatura específica, os conceitos relacionados à segurança da informação, dentre outras temáticas relacionadas à pesquisa;
- Demonstrar a importância da conscientização dos colaboradores de instituições sobre a SI;
- Analisar a efetividade da plataforma KnowBe4 na conscientização dos colaboradores sobre segurança da informação em uma instituição financeira;
- Identificar os principais benefícios que os colaboradores da instituição financeira obtiveram com o uso da plataforma KnowBe4;

## 1.2 ESTRUTURAÇÃO DO TEXTO

Para facilitar a compreensão sobre a pesquisa desenvolvida o trabalho foi dividido em 4 (quatro) capítulos.

- Capítulo um: apresenta a introdução, contextualizando o trabalho e definindo objetivos;
- Capítulo dois: aborda o referencial teórico levantado sobre o tema, definindo conceitos e com especificidades da plataforma KnowBe4;
- Capítulo três: aborda a metodologia utilizada e os resultados do questionário aplicado na instituição financeira que fez uso da KnowBe4;
- Capítulo quatro: apresenta as conclusões que o trabalho alcançou, além de ações e trabalhos futuros recomendados para a replicação da metodologia de conscientização.

## 1.3 ADERÊNCIA AO CURSO DE TIC

O Quadro 1 apresenta os trabalhos identificados nas bases de dados de Trabalhos de Conclusão de Curso (TCCs) do Curso de TIC, do Campus da UFSC de Araranguá. Com base nesses três trabalhos, percebe-se que apresentam a temática de segurança da informação nas organizações, mas não abordam sobre a forma de conscientização dos colaboradores.

Quadro 1 – Aderência aos trabalhos de conclusão do curso de TIC.

| **Título** | **Autor** | **Ano** |
|---|---|---|
| Engenharia Social e Segurança da Informação no Ambiente Corporativo: um estudo de caso em uma Cooperativa de Crédito localizada no sul de Santa Catarina | Jeison Estevam Costa | 2018 |
| Gestão da Segurança da Informação: Desafios E Perspectivas | Jesiel de Oliveira Bitencourt Cittadin | 2018 |
| Análise crítica da aplicação de uma política de Segurança da Informação (PSI) em empresa do setor financeiro: um estudo de caso | Michel Bortoluzzi | 2016 |

Fonte: Elaborado pelo autor (2023).

# 2 FUNDAMENTAÇÃO TEÓRICA

O capítulo referente à fundamentação teórica tem o objetivo de apresentar a literatura, que envolve a temática. Para tanto, foram consultados livros e artigos de periódicos científicos.

## 2.1 CONCEITO DE SEGURANÇA DA INFORMAÇÃO

A internet e os meios digitais revolucionaram a forma de organização dos sistemas informacionais. São poucos os documentos que estão em papéis nas empresas, sua maioria, após a utilização de computadores e interação do usuário com sistemas, foram transferidos para servidores locais ou armazenados em nuvem, gerando uma mudança gigantesca no que diz respeito a segurança no tratamento, usabilidade, armazenamento e descarte desses ativos de informação.

As informações nas empresas não estão restritas apenas a papéis, registros, armazenados em servidores e na nuvem. Ela pode ser transmitida também em meios sociais, por meio da comunicação. Conforme Sêmola (2014, p. 69), a definição de informação é:

> [...] conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais. [...] A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvos de proteção da segurança da informação.

As empresas têm as informações como recursos essenciais para seu crescimento e geração de negócios, além de auxiliar diretamente no processo decisório, fazendo com que as organizações alcancem seus objetivos e melhorem seu desempenho no mercado. Neste sentido, Beal (2008) aponta que a informação como um ativo tão precioso para a organização que precisa ser protegida contra ameaças que podem levar à sua destruição, alteração, indisponibilidade ou compartilhamento não autorizado.

A segurança da informação pode ser definida como o conjunto de medidas técnicas, administrativas e humanas que visam proteger a informação contra acessos não autorizados, uso indevido, perda ou alteração. Essas medidas incluem desde a criptografia de dados até a definição de políticas de acesso e uso dos recursos de informática.

Segurança da informação tornou-se um pilar fundamental para as empresas. Segundo (Schwab,2016) “hoje, em vez de capital ou outros ativos tangíveis, o valor é criado cada vez mais a partir do conhecimento, informações e inovação". As informações de uma empresa podem incluir desde dados financeiros e recursos humanos até segredos comerciais e propriedade intelectual. Nesse sentido, a segurança da informação é essencial para garantir a integridade, confidencialidade e disponibilidade dessas informações.

De acordo com Beal (2008), a confidencialidade diz respeito ao acesso à informação somente aos usuários autorizados. Já a integridade garante que as informações tenham criação legítima e consistência mesmo após tempos de uso. E por fim, a disponibilidade está relacionada em assegurar que a informação e os ativos associados estarão disponíveis sempre que necessário. Isso significa que os recursos de informática devem ser capazes de garantir o acesso à informação quando demandado.

Figura 1 – Pirâmide ou tríade da Segurança da Informação


Fonte: adaptada de RAMOS, 2006, p. 21

Nesse sentido, é fundamental que as empresas invistam em medidas de segurança da informação, como a criptografia de dados, definição de políticas de acesso, uso dos recursos de informática, e principalmente na educação e conscientização de seus colaboradores a fim de garantir a continuidade dos negócios e a conformidade com as regulamentações.

Como afirma Díaz et al. (2020), "a segurança da informação é um desafio constante para as organizações, que precisam estar sempre atentas às novas ameaças e adotar uma abordagem proativa na proteção de seus sistemas e dados". Além disso, é importante lembrar que a SI é um processo contínuo, que requer atualizações constantes, avaliações de riscos e ações preventivas para garantir que as informações estejam protegidas em todos os momentos.

## 2.2 NORMAS E PADRÕES DE SEGURANÇA

Normas e padrões de segurança são conjuntos de regras, diretrizes e métricas que as organizações podem utilizar para garantir a segurança da informação e proteger seus ativos de informações contra ameaças internas e externas. Conforme Beal(2008) destaca:

> Normas e padrões técnicos representam uma referência importante para a qualidade de qualquer processo.[…] Existem diversas referências criadas para auxiliar as organizações a implementar as melhores práticas na gestão da segurança da informação e da TI.

Para garantir a proteção das informações sensíveis que circulam tanto no meio cibernético quanto no meio físico é necessário a padronização de regras que delimitam as melhores práticas de segurança. Essas normas são importantes para orientar as organizações na implementação de medidas de segurança que protejam seus ativos  minimizem os riscos de ataque cibernético ou vazamento de dados.

### 2.2.1 Marco Civil da Internet

A lei nº12.965, de 23 de abril de 2014, intitulada como Marco Civil da Internet estabelece no Brasil, direitos e deveres na utilização da internet (BRASIL,2014). Ela foi criada com o objetivo de garantir a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, além de definir regras e diretrizes para o armazenamento e compartilhamento de dados na Internet.

> O Marco Civil será importante para a sociedade da informação porque será um sistema complementar às leis já existentes e preencherá lacunas legislativas. A privacidade é um dos princípios a serem discutidos: da mesma forma que existe a proteção constitucional, ela também é garantida na Internet, e é essa proteção de dados pela guarda de logs nos provedores que o anteprojeto discute, e uma das questões mais importantes para a sua aprovação. (PINHEIRO, 2013, p. 44)

É importante ressaltar que a implementação do Marco Civil da Internet no Brasil representa um avanço significativo na regulamentação do uso da Internet e na garantia de direitos fundamentais dos usuários da rede. Como destaca Mendes (2014), "o Marco Civil da Internet é uma conquista da sociedade brasileira, que reconheceu a necessidade de estabelecer regras claras e democráticas para a utilização da rede, visando proteger a liberdade de expressão, a privacidade dos usuários e o acesso igualitário à informação".

### 2.2.2 CoBit

O CoBit (*Control Objectives for Information and Related Technology*) é um conjunto de diretrizes para gestão de processos e controles de TI desenvolvida pela Associação de Auditoria e Controle de Sistemas de Informação (ISACA). Seu objetivo é auxiliar as empresas na implementação e gerenciamento de sistemas, garantindo maior segurança das informações e o cumprimento de normas e regulamentações (ISACA, 2019).

Muitas empresas desconhecem o CoBit e suas vantagens na gestão e geração de negócios. Para tanto, surge a importância do conhecimento da abordagem que o CoBit trata. Uma das principais características é levar em consideração não apenas a segurança da informação, mas também outros aspectos importantes, como o alinhamento estratégico da Tecnologia da Informação(TI) com os objetivos de negócio da empresa, a gestão de riscos, o gerenciamento de projetos, entre outros.

O CoBit oferece às empresas a flexibilidade para otimizar riscos e gerenciar a segurança, sendo amplamente reconhecida e adotada pelas empresas por todo o mundo. Os vários elementos do CoBit incluem a estruturação e organização dos objetivos e requisitos, as descrições de processos, os objetivos de controle, os modelos de maturidade e as diretrizes de gestão (SOUZA NETO, 2020).

A utilização do CoBit traz respostas às perguntas mais complexas, entretanto precisa ter um aprofundamento nos conteúdos relacionados a essa ferramenta, para saber assim, usar e selecionar as melhores práticas que se encaixam e se adaptam na empresa, modificando e atualizando o que for necessário.

### 2.2.3 ISO 27000

A ISO (*International Organization for Standardization*) é uma organização não governamental com sede em Genebra, Suíça, criada em 1947 para desenvolver e promover padrões internacionais em diversas áreas como segurança da informação, gestão ambiental e qualidade. As normas desenvolvidas pela ISO não são obrigatórias a serem seguidas pelas organizações e não possuem força de lei, mas são utilizadas por empresas de todo o mundo como referência de boas práticas.

Dentre as normas desenvolvidas por essa organização, a família ISO/IEC 27000, se destaca por compreender um conjunto de padrões voltados para a segurança da informação (DISTERER, 2013). No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) adota os padrões desta família de normas, adaptando-as e traduzindo-as para português, que compõem, então, a família ABNT NBR ISO 27000.

Mascarenhas Neto e Araújo (2019) em sua obra, destacaram as principais normas que norteiam a implantação da segurança da informação em uma organização.

Quadro 2 - Normas da NBR/ISO fundamentais para a implementação da SI

| NORMA | ANO DE PUBLICAÇÃO | TÍTULO | OBJETIVO |
|---|---|---|---|
| 27000 | 2016 | Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão da Segurança da Informação - Descrições e vocabulários | Introduz os conceitos e a terminologia da segurança da informação, fornecendo uma visão geral dos padrões da família ABNT NBR ISO 27000. |
| 27001 | 2013 | Tecnologia da informação - Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos | Estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), incluindo a avaliação de riscos, seleção de controles e implementação do SGSI. |
| 27002 | 2013 | Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da | Fornece diretrizes e recomendações para a implementação de boas práticas de gestão e normas de segurança da informação, |

| | | | |
|---|---|---|---|
| | | informação | incluindo a seleção, a implementação e o gerenciamento de controles, considerando os ambientes de risco da segurança da informação da organização. |
| 27003 | 2011 | Tecnologia da informação - Técnicas de segurança - Diretrizes para a implantação de um sistema de gestão da segurança da informação | Fornecerá orientações para a implantação de um SGSI, visando alcançar a conformidade com a ABNT NBR ISO 27001. |
| 27004 | 2010 | Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição | Estabelece orientações para medição e avaliação da eficácia do SGSI, definindo métricas, indicadores de desempenho e o processo de análise crítica. |
| 27005 | 2011 | Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação | Estabelece diretrizes para gestão de riscos, fornecendo um processo sistemático para a identificação, avaliação e tratamento dos riscos associados à segurança da informação. |

Fonte: Adaptado de Mascarenhas Neto e Araújo (2019)

A família ABNT NBR ISO 27000 enfatiza a importância da segurança da informação para proteção de ativos de informação das mais diversificadas organizações. Sendo assim, suas normas estabelecem diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) e destacam a necessidade de avaliação e

tratamento dos riscos e incidentes , considerando o ciclo de vida da informação, gestão sistêmica e integração da segurança da informação em toda a organização.

### 2.2.4 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), lei n° 13.709/2018, é um conjunto de normas válidas no território brasileiro, que delimita como as empresas, pessoas e órgãos públicos devem guardar, proteger e utilizar informações pessoais coletadas dos usuários, tanto no meio físico quanto nos meios digitais (BRASIL,2018).

A comunicação constante entre dispositivos, sensores e pessoas cria uma quantidade significativa de dados diariamente de cada indivíduo. Com a divulgação de incidentes e a preocupação das pessoas sobre como estão sendo tratados, armazenados e protegidos seus dados cria uma concorrência na qual as empresas se veem obrigadas a investir em segurança muito além das sanções para mostrar que sua empresa é segura e que segue as regulamentações corretamente. Conforme Maciel (2019):

> A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, valor cada vez mais na pauta dos cidadãos a partir da divulgação cada vez maior de uso indevido de tais informações.

De acordo com Brasil (2018) o art. 6º da LGPD determina 10 princípios que devem ser seguidos no tratamento de dados pessoais, são eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

A implementação da LGPD nas organizações vem exigindo uma mudança cultural bem importante, envolvendo a conscientização dos colaboradores e a adoção de boas práticas de gestão de riscos.

A lei nº 13.709 representa um marco regulatório fundamental para as organizações financeiras, empresas que lidam diariamente com dados e informações sensíveis de seus clientes. A adequação às disposições da LGPD não é apenas uma obrigação legal, mas também pode gerar oportunidades de fortalecimento na confiança e aprimoramento da gestão dos dados que circulam em cada processo da organização.

## 2.2 PRINCIPAIS AMEAÇAS À SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES FINANCEIRAS

As instituições financeiras são alvos frequentes de ataques e ameaças devido à natureza sensível das informações que lidam diariamente. Por este motivo, a segurança da informação é uma prioridade no setor bancário no Brasil. Segundo estimativa da FEBRABAN, os bancos investiram cerca de 10% do orçamento de TI em segurança cibernética, valor que pode ser estimado em R$2,5 bilhões (TADEU, 2021).

Com a expansão acelerada do uso de canais digitais para monitoramento, investimentos e transações financeiras, principalmente após a pandemia, as tentativas de golpes e ataques de engenheiros sociais se intensificaram ainda mais. A pesquisa da Kaspersky mostra que, em 2022, foram detectados e impedidos 20 milhões de ataques na tentativa de roubar dados bancários de clientes que tentavam realizar compras pela internet (KASPERSKY,2021).

De acordo com Volpini (2022), os valores dos bancos em investimento em tecnologia envolvem três grandes pilares: conscientização dos clientes, monitoramento massivo transacional para detectar transações com indícios de fraude e a repressão. As ameaças à segurança da informação em instituições bancárias são diversas e podem ocorrer tanto por meio de ataques internos quanto externos, digitalmente ou fisicamente. Algumas das principais ameaças incluem:

- *Phishing*: é uma técnica usada por *hackers* que explora a engenharia social para ludibriar a vítima para obter senhas, números de cartão de crédito e até mesmo informações dos próprios colaboradores bancários. Segundo a pesquisa da APWG (2022), o *phishing* é responsável por mais de 23% dos ataques de segurança da informação em instituições financeiras;

- Engenharia social: é um termo utilizado para definição da área que estuda e pratica técnicas e estratégias de persuasão, usando da ingenuidade ou confiança para obter informações importantes ou sigilosas de pessoas ou organizações para prática de crimes (COELHO, 2023);

.

- *Malware*: é um software, *script* ou código malicioso que pode infectar sistemas financeiros para sequestrar informações confidenciais por meio de *sites* maliciosos, dispositivos USB ou e-mails (spam). De acordo com a pesquisa da Verizon (2022), o *malware* é responsável por 17% dos ataques de segurança da informação em instituições financeiras;

- *Ransomware*: é um *malware* que bloqueia o acesso dos dados da vítima, criptografando para que a instituição não consiga resgatar, exigindo pagamento para liberação. Segundo o relatório da IBM CORPORATION(2020), os ataques de *ransomware* em instituições financeiras aumentaram 350% em 2019;

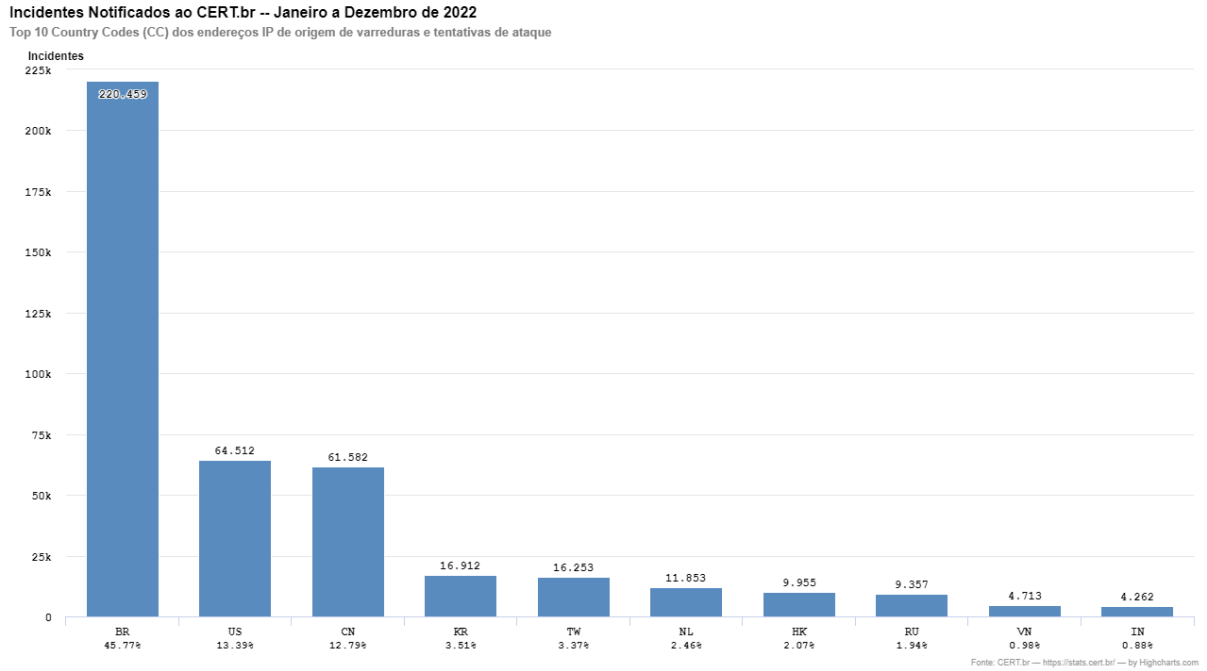
- Ataques DDoS: são ataques de negação de serviço que sobrecarregam os sistemas financeiros com tráfego falso, impedindo que clientes e funcionários acessem causando perdas financeiras. De acordo com o relatório de Inteligência de Ameaças DDoS da NETSCOUT (2023), a frequência de ataque ficou em torno de 285.529 e a média desse tipo de ataque foi um a cada 16 minutos no segundo semestre de 2022 no Brasil.

- Ataques Internos: realizados por funcionários ou ex-colaboradores das instituições bancárias, na qual obteve acesso privilegiado às informações sensíveis de sistemas, senhas, áreas restritas, entre outros fatores, onde se beneficiam para a prática de roubo, sabotagem ou espionagem. Com base na pesquisa "2022 *Cost of Insider Threats Global Reports*" da Ponemon Institute (2022) os incidentes causados por funcionários e ex-funcionários aumentaram 44% nos últimos dois anos, com um custo estimado de US$ 15,38 milhões.

Segundo análise de incidentes notificados ao CERT (2022), o Brasil fica em primeiro lugar entre países como os EUA, China, Coreia do Sul e Rússia, com 220.459 notificações. Tais notificações variam entre negação de serviço, fraudes, varreduras, *phishings* e ataques a servidores *web*. O Brasil ficou com uma porcentagem de 71% maior de incidentes que os

Estados Unidos e 73% maior que a China, mostrando como o país se encontra ainda em uma situação bem delicada no *ranking* de proteção das informações e dados de suas empresas e organizações. A Figura 2 apresenta esses dados.

Figura 2 - Incidentes e tentativas de ataques notificados a CERT




Fonte: CERT (2023)

No setor bancário, as ameaças são muitas, pessoas de má fé buscam de todas as formas, usando inclusive a tecnologia para ludibriar suas vítimas pela prática de golpes e fraudes. Desta forma é fundamental que as instituições financeiras invistam na educação e conscientização de seus colaboradores sobre as melhores práticas de segurança da informação. Treinamentos regulares e campanhas de conscientização são cruciais para garantir que os colaboradores estejam cientes dos riscos e saibam como agir diante de situações de ameaça à segurança da informação.

## 2.3 IMPORTÂNCIA DA CONSCIENTIZAÇÃO DOS COLABORADORES

Os avanços tecnológicos a partir do século XX possibilitaram o surgimento da era da informação. Nessa era, segundo Santos (2006), “o homem se vê em um mundo globalizado e inconstante, onde se intensificam os relacionamentos entre povos a nível social, político, cultural e principalmente econômico, o que facilita o intercâmbio entre eles”. Dentro deste

contexto, é notório que as organizações precisam estar em constante desenvolvimento e fortalecimento de suas estratégias visando o melhor proveito das informações e disponibilizar meios de segurança para cuidar desses ativos.

A proteção das informações é fundamental para garantir a continuidade e sobrevivência da empresa. Conforme Fontes (2006) as informações são ativos de valor, necessárias e vistas atualmente como recurso crítico para a realização de negócios e a execução de suas tarefas. Portanto, todos os envolvidos no processo de manuseio desses ativos são responsáveis por qualquer malefício feito a ela, não devendo depender de apenas recursos tecnológicos para assegurar os princípios de disponibilidade, integridade e confidencialidade da informação, mas também o aspecto humano deve ser visto como uma grande preocupação em relação a conscientização da segurança da informação.

Segundo Finkelstein et al. (2017), os colaboradores são frequentemente apontados como o elo mais fraco na cadeia da segurança de informações, pois muitas vezes não estão cientes dos riscos e não seguem as políticas de segurança da empresa. A afirmação se baseia no fato que um sistema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma única pessoa mal informada ou com más intenções dentro da empresa. Por isso, é fundamental que as organizações invistam em programas de conscientização e treinamento.

Portanto, conforme ISO 27002(2013) convém que todos os colaboradores da organização recebam treinamento e educação adequados para a segurança da empresa e de todos os ativos contidos e que circulam nela. Além disso, devem continuamente certificar-se que seus funcionários estão conscientes, realizando testes, como, por exemplo, um *e-mail* de *phishing* falso ou um questionário para assim analisar as ações.

## 2.4 KNOWBE4 E SUA PLATAFORMA DE TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um desafio cada vez mais relevante nas organizações, à medida que a tecnologia avança, as ameaças cibernéticas se aprimoram e fazem mais vítimas. Muitos ataques são bem-sucedidos devido a inexperiência, falta de conhecimento e cuidados do colaborador. Beal (2008) afirma que o treinamento aos colaboradores sobre os procedimentos de segurança é fundamental para a proteção da informação e da organização ao todo.

> A organização deve adotar estratégias diversificadas para compor um treinamento e conscientização completo e eficaz, englobando instrumentos complementares, como cursos e capacitação para as equipes técnicas, *workshops,* seminários*,* campanhas por e-mail, cartas da diretoria etc.

As violações de segurança ocorrem tanto nas grandes como também nas pequenas empresas, internacionais ou locais, de todos os segmentos possíveis. Por meio de qualquer funcionário, do estagiário até mais alto nível podem ser ludibriados por engenheiros sociais ou ainda clicar em um *phishing* colocando a empresa e todos seus dados em risco de vazamento e perdas operacionais. (CIAMPA, 2014; EMINAAOLU, UÇAR, EREN, 2009; FOWLER, 2011).

Como estratégia das empresas em preparar seus usuários para protegerem-se dessas ameaças e mitigar riscos de invasão e vazamento de dados, pode-se incluir treinamentos de conscientização de segurança para funcionários, usando teoria e prática, como simuladores de *phishing*, gerando relatórios para verificação da situação atual da empresa (SLOAN, 2020). Uma empresa que oferece esse tipo de capacitação para colaboradores de organizações é o KnowBe4, empresa fundada em 2010, com sede em Tampa Bay, Flórida.

Figura 3 - Empresa de conscientização da segurança da informação - KnowBe4


Fonte: KnowBe4 (2023)

A plataforma KnowBe4 é voltada para a realização de treinamento de funcionários sobre conscientização de segurança da informação que também combina simulações de ataques de *phishing*. A ferramenta já possui mais de 50.000 clientes e possui como fundador/CEO o Stu Sjouwerman (KNOWBE4, 2023) e tem como diretor de *hacking*, Kevin Mitnick -que em meados dos anos 90 era o *hacker* mais procurado do mundo.

O treinamento baseia-se em uma biblioteca com mais de 1300 itens de conteúdo de conscientização, incluindo módulos interativos, vídeos, jogos, pôsteres e boletins informativos. O quadro 3 demonstra as características que a plataforma KnowBe4 oferece para seus clientes.

Quadro 3 - Características da plataforma KnowBe4

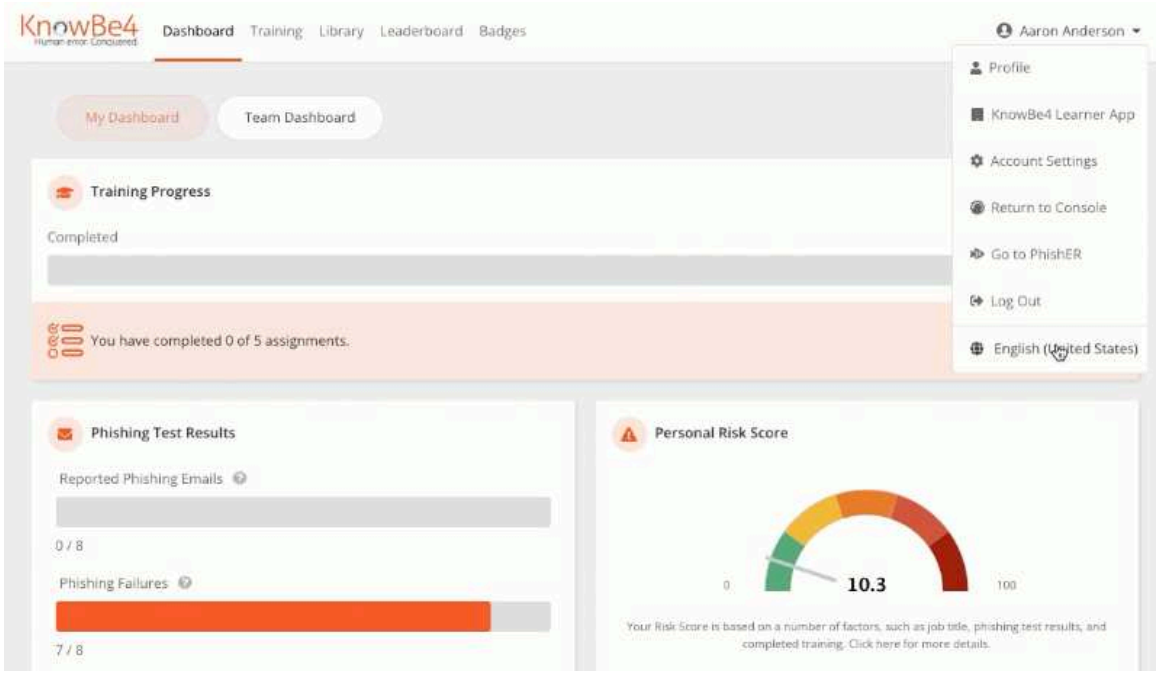
| **Tema** | **Características** |
|---|---|
| Conteúdos nativos | Conteúdo em diversas línguas. |
| | Conteúdo LGPD nacional |
| | Entregar conhecimento através de conteúdos tais como: vídeos, games, *quizzes*, artes (pôsteres), *assessments* (avaliações). |
| | Plataforma/Conteúdo em conformidade com padrão WCAG. |
| Conteúdo do Cliente | Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM |
| | Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma. |
| Implantação e Segurança | Possui integração com AD. |
| | Carga de usuários por meio de arquivos csv. |
| | Permite duplo fator de autenticação para usuários e administradores. |
| Normas de Segurança como conteúdo | Permite duplo fator de autenticação para usuários e administradores. |
| Automação | Atribuição automática de treinamento para novos usuários. |
| | Criação automatizada de um programa personalizado em segurança da informação ou recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários. |
| | APIs que permitam a exportação de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante para guarda ou integração com outros sistemas. |
| Gestão de Usuários e Cursos | Seleção de módulos de treinamento para grupo de usuários(Atribuição de treinamentos). |
| | Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos |
| | Acompanhamento online de progressão e desempenho dos usuários. |
| | Emissão de Certificados para os cursos. |
| | Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos. |
| | Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes. |
| | Inativação de usuários sem perda do histórico de dados. |
| | Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos. |
| | Provê um ambiente de gestão que possibilita a criação de grupos de usuários com base em |

| | |
|---|---|
| | comportamento frente às simulações e treinamentos realizados. |
| | Possibilita a atribuição da licença de acesso de um usuário que foi desligado da instituição para um novo usuário (neste caso não é necessário manter o histórico). |
| Campanhas de *Phishing* | Permite a criação de número ilimitado de campanhas durante a vigência do contrato. |
| | Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante. |
| | Mantém histórico por usuário e por campanha. |
| | Permite que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação. |
| Indicador de Maturidade em Segurança | Possui indicador de nível de risco em segurança da informação para cada usuário e para a instituição. O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de *phishing*. |
| Suporte Técnico | A contratada disponibiliza durante todo período contratual um gerente de contas para apoiar e orientar a contratante no uso da plataforma. |
| | Passagem de Conhecimento |
| Customização | Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários. |
| Linguagem da Plataforma | Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br). |

Fonte: adaptada de Tribunal Regional Eleitoral do Espírito Santo (2022)

Segundo KnowBe4(2023) o conteúdo da plataforma é interativo, demonstrando situações de problemas com segurança da informação, na qual inclui dicas e sugestões para proteger e desviar dos criminosos em cenários do mundo real em seus treinamentos, com o intuito principal de construir um *firewall* humano nas organizações. Na figura 4 demonstra como é apresentado o painel principal da ferramenta na qual os usuários vão utilizar para fazer seus treinamentos.

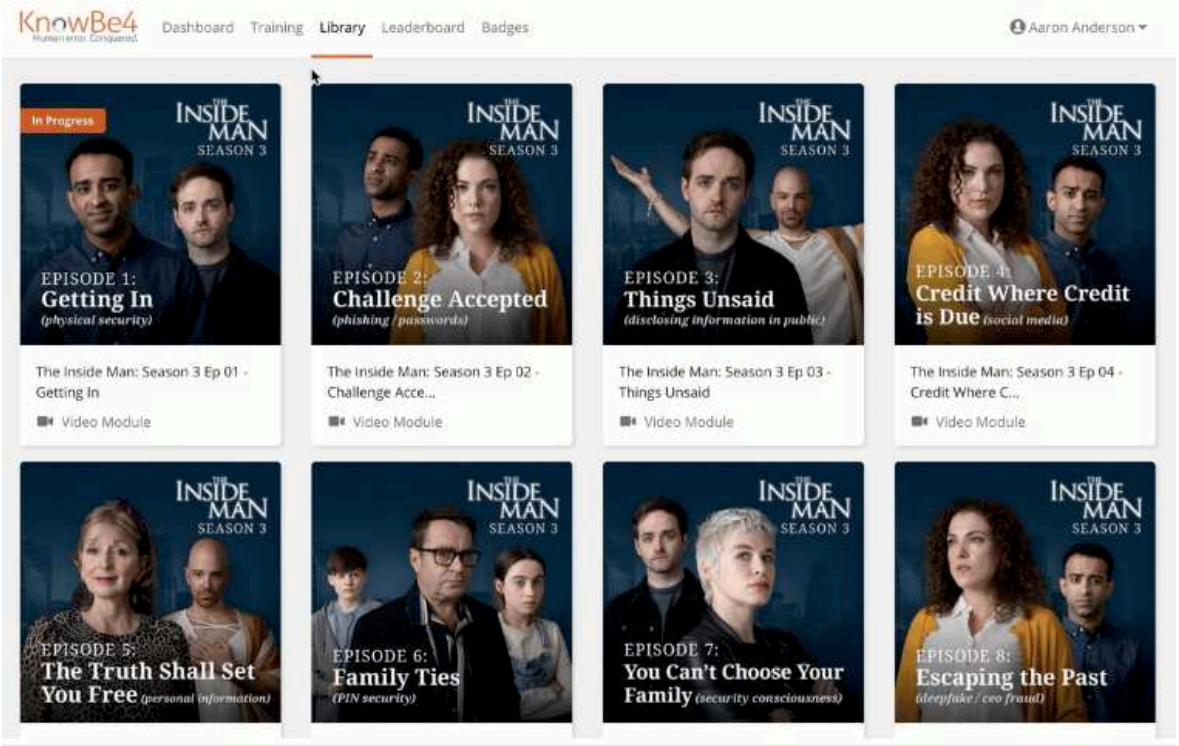
Figura 4 - Painel principal plataforma KnowBe4




Fonte: KnowBe4 (2023)

A plataforma KnowBe4 oferece treinamentos, criação de campanhas de *phishing* para teste de usuários e relatórios de todo o desenvolvimento do usuário dentro da ferramenta. Os conteúdos dos treinamentos abrangem todos os temas de segurança tanto física quanto lógica em uma organização. Um exemplo de treinamento muito famoso entre os usuários é a série *The Inside Man* (figura 5), é basicamente uma série modelo Netflix com conteúdo educativo, com episódios repletos de ensinamentos para ajudar os colaboradores a entenderem as práticas recomendadas de segurança cibernética e proteção da informação (KNOWBE4, 2023).

Figura 5 - *The Inside Man*




Fonte: KnowBe4 (2023)

O treinamento de conscientização "à moda antiga" não funciona mais. Os colaboradores precisam ser conquistados a cada curso passado, para que assim, o conteúdo seja absorvido e colocado realmente em prática. A plataforma KnowBe4 oferece treinamentos com uma didática diferente das tradicionais, e proporciona ao administrador uma maneira fácil de gerenciar as dificuldades de cada colaborador e trabalhar nelas para proteger de forma mais eficaz sua organização.

# 3 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo, inicialmente, se descreve o enquadramento metodológico do estudo. Posteriormente, são apresentados os métodos utilizados para a coleta e análise dos dados.

## 3.1 CARACTERIZAÇÃO DA COOPERATIVA DE CRÉDITO

A Cooperativa de Crédito Alfa situada no sul de Santa Catarina, atua no ramo cooperativista há cerca de 35 anos, possuindo 29 pontos de atendimento nas 26 cidades. Busca contribuir para o desenvolvimento econômico e social das regiões que trabalha e também, promover melhoria de vida a seus mais de 50.000 (cinquenta mil) associados e as comunidades que eles fazem parte.

São mais de 200 (duzentos) funcionários dedicados a oferecer as melhores opções de produtos e serviços, dentre eles: conta corrente, poupança, financiamentos, investimentos, cartões de crédito, consórcios, previdência e seguros, entre muitos outros.

A instituição investe em vários projetos para disseminar a educação financeira, o cuidado e preservação da natureza, a cooperação comunitária e também a democratização da leitura. Todos esses projetos são organizados pela equipe da Turminha do Sulca e da AMABIo, setores criados para materializar o propósito Cooperativista.

A Cooperativa dedica-se a ser reconhecida pela sociedade como a melhor opção financeira e de serviços da região. Preservando pela qualidade e satisfação de seu atendimento, além da transparência e credibilidade para conquistar cada vez mais espaço na vida das famílias.

## 3.2 O MÉTODO DA PESQUISA E O DELINEAMENTO NESTE TRABALHO

Para elaboração deste trabalho foram realizadas revisões bibliográficas em livros, artigos, relatórios, TCCs, periódicos e sites de pesquisa. Conforme Fonseca (2002), um método de pesquisa deve ser selecionado para permitir a inspeção realizar uma análise detalhada da realidade a ser investigada, a fim de resolver o problema usando procedimentos

científicos. Deste modo, foram realizados levantamento de informações no método de pesquisa quantitativa e qualitativa.

Objetivou-se, no primeiro momento, uma pesquisa exploratória e descritiva. Na qual buscou explorar a temática envolta nos conceitos principais do trabalho(GIL, 2010). A entidade analisada utiliza a plataforma KnowBe4 e motivou o desenvolvimento dessa pesquisa principalmente por estar sendo implementada recentemente na empresa usada no estudo de caso. A partir desse momento inicia-se o levantamento referencial teórico sobre os temas relacionados, dentre eles: segurança da informação, conscientização, leis e normas, ameaças e sobre a plataforma KnowBe4.

A respeito da análise dos dados coletados, se utilizou da pesquisa qualitativa, com o uso de um questionário feito no Microsoft Form, que consistiu na elaboração de 24 (vinte e quatro) perguntas abertas e fechadas.

A divulgação do questionário dentro da instituição partiu de um e-mail corporativo enviado do setor de TI e foram 174 (cento e setenta e quatro) respondentes

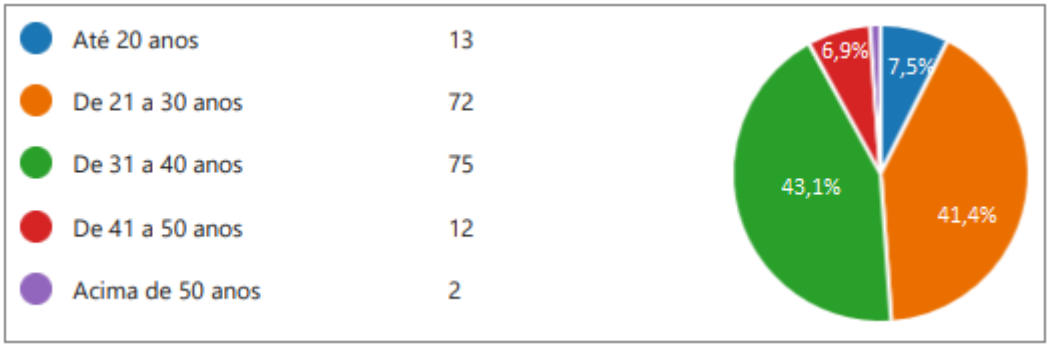
## 4 RESULTADOS E DISCUSSÃO

Após a coleta dos dados com a realização do questionário, tem-se base para analisar a efetividade do uso da plataforma KnowBe4 na conscientização dos colaboradores de uma Cooperativa de Crédito Alfa em relação a segurança da informação.

Na primeira sessão, composta por três questões, foi possível identificar o perfil médio dos colaboradores.

A figura 6 demonstra a classificação dos colaboradores por faixa etária

Figura 6 - Idade



Fonte: dados da pesquisa (2023)

A faixa etária com maior representatividade foi de 31 a 40 anos, com 43,1%, logo abaixo com uma porcentagem muito próxima, com 41,4% na faixa dos 21 a 30 anos, e a menos representada foram 1,1% acima de 50 anos. Portanto, é visto que o quadro de funcionários da organização é integrado, na sua maioria, por pessoas nas idades entre 21 a 40 anos de idade.

A figura 7 demonstra a segregação de colaboradores por gênero.

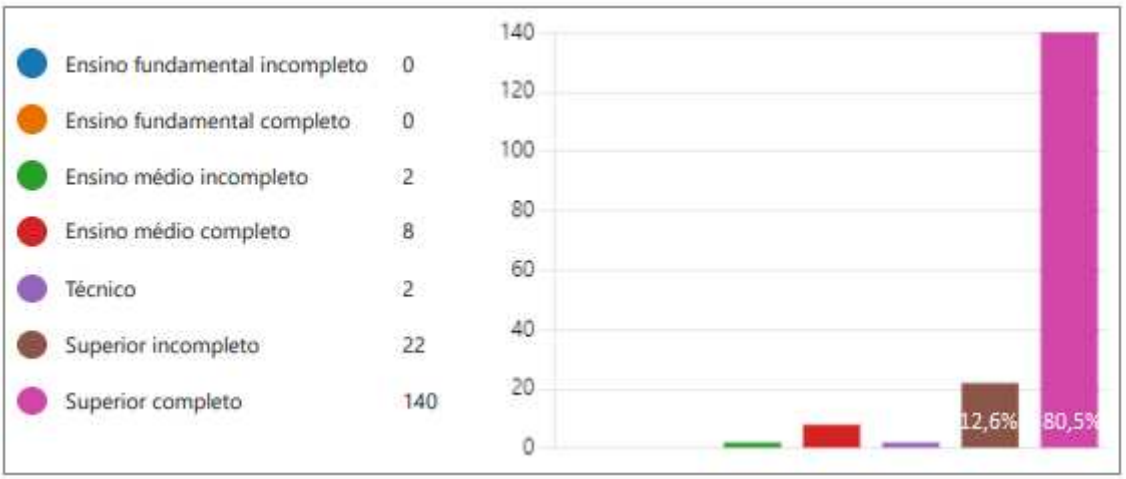
Figura 7 - Gênero


Fonte: dados da pesquisa (2023)

Na instituição, 73,6% dos colaboradores são do sexo feminino, e sendo apenas 26,4% do sexo masculino, mostrando que a presença feminina é significativa em todo quadro organizacional.

A figura 8 refere-se ao grau de escolaridade dos entrevistados.

Figura 8 - Grau escolaridade



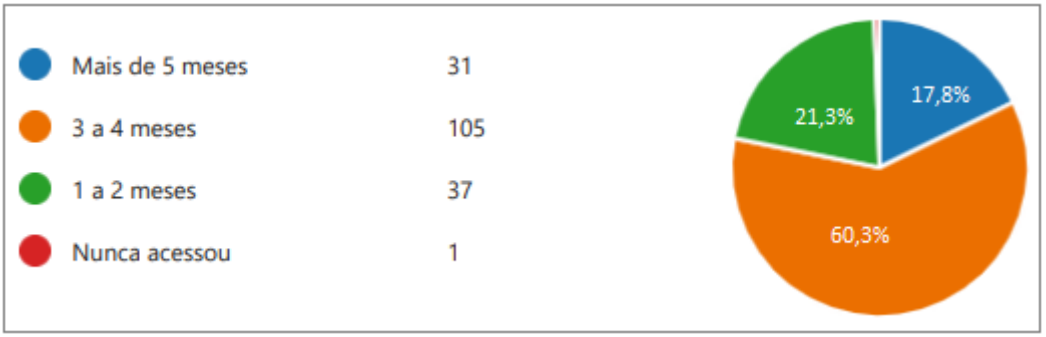

Fonte: dados da pesquisa (2023)

Conforme dados da figura 8, observa-se que a Cooperativa se empenha em ter um quadro de funcionários com um nível de conhecimento mais elevado, visto que, o índice de superior completo ultrapassa os 80%, além disso 12,6% estão cursando ensino superior e com 4,6 ensino médio completo.

A segunda sessão é composta por onze questões relacionadas à plataforma KnowBe4 e sua eficácia na conscientização da segurança da informação.

A figura 9 demonstra o período que os funcionários estão utilizando a plataforma Knowbe4 como forma de treinamento e conscientização sobre a segurança da informação.

Figura 9 - Período de uso da plataforma KnowBe4

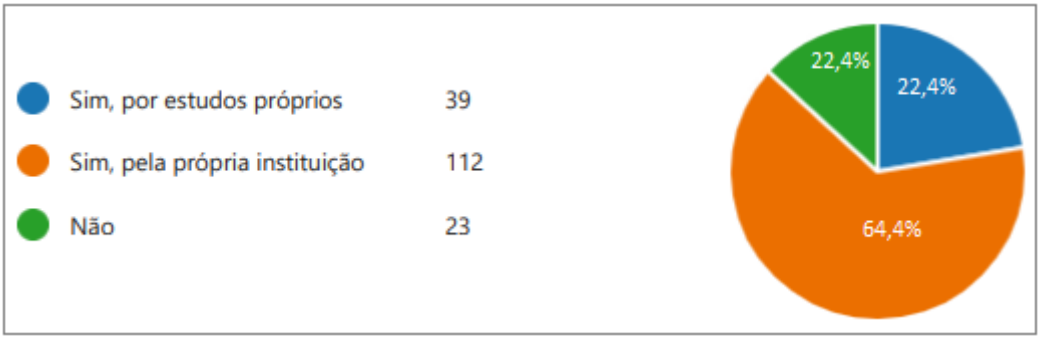



Fonte: dados da pesquisa (2023)

Referente ao período de uso da plataforma KnowBe4, dos 174 respondes, 60,3% fazem uso de 3 a 4 meses, No período de 1 a 2 meses e acima de 5 meses a porcentagem de usuários da plataforma é respectivamente 21,3% e 17,8%. Nesta pesquisa foi concluído que de todos os respondentes, apenas uma pessoa nunca teve acesso a plataforma, a maior parte acessa a plataforma no período de 3 a 4 meses.

A figura 10 explana sobre a forma de conhecimento sobre segurança da informação antes da utilização da plataforma KnowBe4.

Figura 10 - Conhecimento sobre SI



Fonte: dados da pesquisa (2023)

De acordo com a figura 10, é notório observar que a instituição já fazia um trabalho significativo na conscientização e transferência de conhecimento acerca das políticas e sobre a segurança da informação, pois 64,4% já tinham o conhecimento oferecido pela própria instituição. Também observa-se que 22,4% dos colaboradores tiveram a proatividade de se interessar no assunto e buscar conhecimento próprio e apenas 13,2% informaram na pesquisa que antes da plataforma não sabiam nenhum assunto relacionado a SI.

Na figura 11 diz respeito a compreensão sobre ameaças cibernéticas, sentimento de segurança ao manusear informações confidenciais e se a plataforma KnowBe4 seria recomendada a outras instituições.

Figura 11 - Compreensão, segurança e recomendação após uso da ferramenta


Fonte: dados da pesquisa (2023)

É evidente, através da análise da figura 11, que a KnowBe4, com seus treinamentos, passou mais segurança ao tratarem de informações de mais alto risco aos funcionários, já que 99,4% confirmaram que se sentiram mais confiantes e que recomendariam a plataforma para outras instituições. E apenas 1 pessoa respondeu “não”, entretanto, ela nunca teve acesso e neste caso não conseguiu responder com certeza.

O quadro 4 apresenta as respostas mais recorrentes à pergunta aberta relacionada à mudança de atitude após ter contato com a plataforma KnowBe4 que visou conscientizá-los sobre a segurança da informação, solicitando uma breve descrição do ato. Todos os respondentes deram retornos positivos nas suas atitudes. As respostas da questão estão organizadas numericamente abaixo:

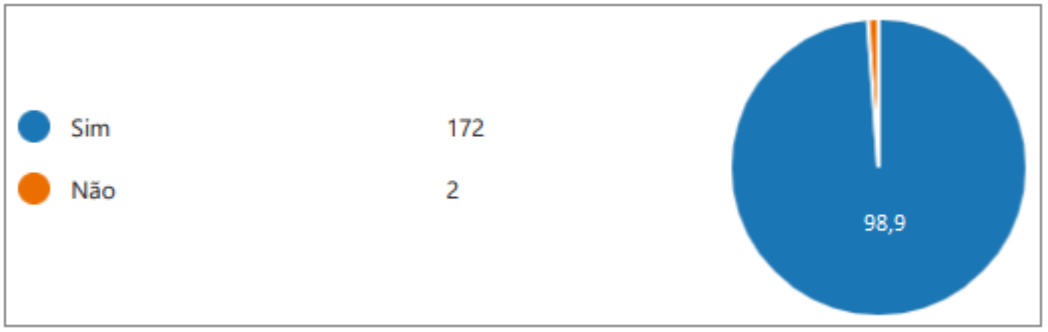
Quadro 4 - A plataforma KnowBe4 ajudou a mudar a atitude sobre SI? Como?

| | |
|---|---|
| 1 | Reforçou ainda mais os cuidados com as informações que tenho em mãos, seja ela impressa ou não. |
| 2 | Antes de repassar ou visualizar qualquer informação, ter a consciência de como tratar a mesma. |
| 3 | Sim, evitando deixar senhas anotadas em local visível, atentar a e-mail não confiáveis, etc... |
| 4 | Em relação a deixar documentos e agendas em cima da mesa de trabalho enquanto atendo. |
| 5 | Prestar atenção na utilização da internet, ficar mais atento a tudo principalmente com nosso atos |
| 6 | Sim, pois com ela foi possível de forma dinâmica entender conceitos e também que os perigos são reais. |
| 7 | Sim, certificando sobre o cuidado da estação do trabalho |
| 8 | Sim, ajuda e orienta estar atento às possíveis tentativas de golpes |
| 9 | Sim, fez com que a atenção aos detalhes a possíveis perigos a rede e confidencialidade das informações, fossem redobrados. |
| 10 | sim, atitudes simples do dia a dia que poderiam causar um transtorno enorme em caso de vazamento de dados. |

Fonte: dados da pesquisa (2023)

A figura 12 destaca que 98,9% dos colaboradores levaram o aprendizado além da vida profissional, implementando melhoramento também em suas atividades pessoais, protegendo os dados, evitando perdas e prejuízos, e apenas 1,1% não fizeram uso em suas vidas pessoais.

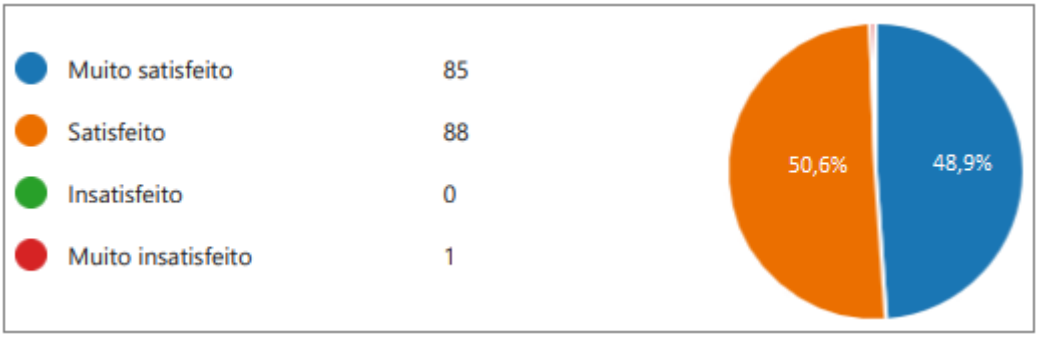
Figura 12 - Uso do aprendizado na vida pessoal




Fonte: dados da pesquisa (2023)

A figura 13 buscou avaliar a satisfação em relação a eficácia da ferramenta na conscientização, tendo 50,6% dos respondentes afirmaram estar satisfeitos; 48,9% muito satisfeitos e apenas 0,6% afirmaram estar muito insatisfeitos.

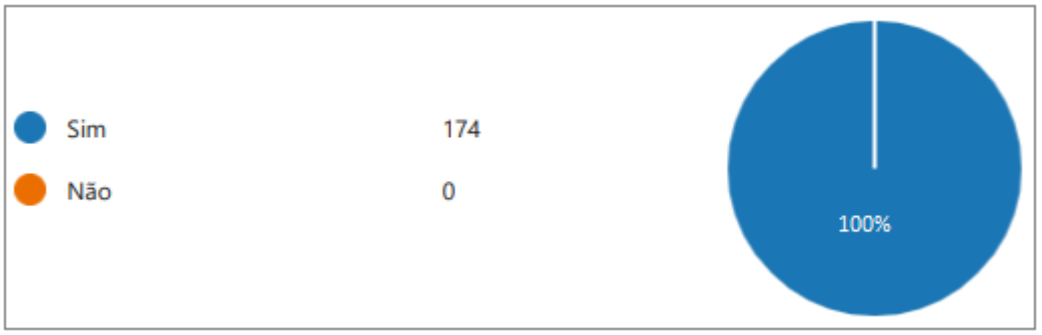
Figura 13 - Avaliação da eficácia da ferramenta na conscientização




Fonte: dados da pesquisa (2023)

A figura 14 representa que todos os respondentes acreditam que com o uso da plataforma KnowBe4 e com os conhecimentos adquiridos nela, fizeram que os incidentes de segurança tivessem uma redução.

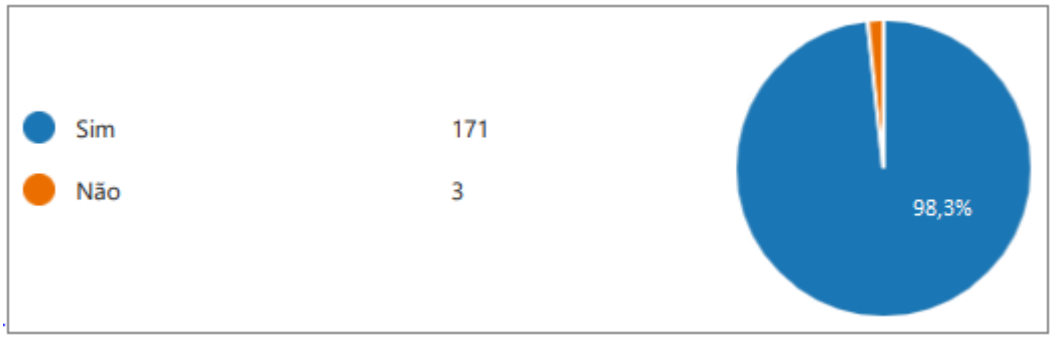
Figura 14 - Contribuição para redução de incidentes




Fonte: dados da pesquisa (2023)

A figura 15 expõe a opinião sobre a continuação da plataforma e de seus treinamentos: 98,3% incentivar e apenas 1,7% não indicam a continuação. Deste modo, é possível observar que a maioria dos funcionários compreendem a importância do conhecimento e de boas práticas no tratamento, armazenamento e circulação das informações e dados da organização, desta forma o desenvolvimento dessas competências precisa ser contínua.

Figura 15 - Opinião sobre continuação do uso da ferramenta na instituição




Fonte: dados da pesquisa (2023)

O quadro 5 apresenta as respostas mais recorrentes à pergunta aberta focada em observar a opinião dos respondentes sobre a Cooperativa investir mais em treinamentos e na conscientização dos colaboradores sobre SI. Deste modo, destacou que todos os colaboradores afirmam que é necessário, tanto para proteção dos dados dos clientes, quanto para evitar golpes, entre muitos outros motivos que são citados abaixo:

Quadro 5 - Investimento em mais treinamentos de SI

| | |
|---|---|
| 1 | sim, para ajudar na proteção dos dados de associados e colaboradores e da |

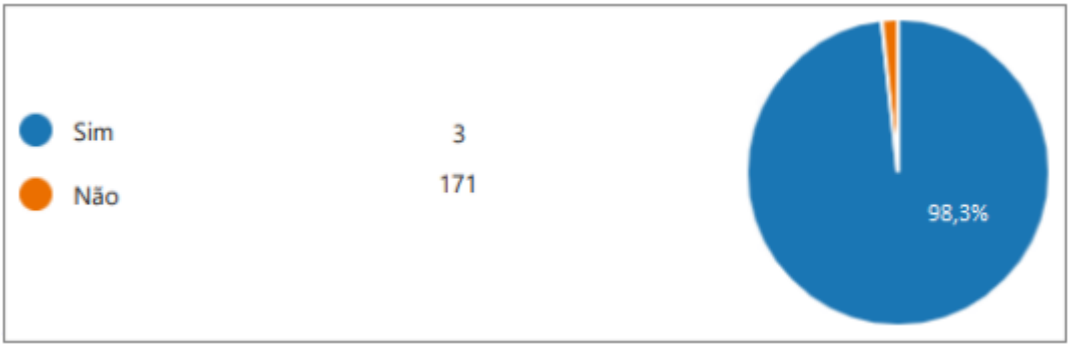
| | |
|---|---|
| | instituição. |
| 2 | sim, pois as fraudes estão cada vez mais frequentes e elaboradas |
| 3 | Sim, pois ajuda os colaboradores a prestarem mais atenção nas atitudes do dia a dia no trabalho, assim evitando certos transtornos de vazamentos de informação. |
| 4 | Sim, devido às informações sigilosas que trabalhamos. |
| 5 | Sim, devido às informações sigilosas que trabalhamos. |
| 6 | Sim. Pois acredito ser um assunto muito importante que deve ser sempre atualizado e repassado para novos colaboradores. |
| 7 | Sim, devido às inúmeras tentativas de várias formas novas de tentar invadir os dados das pessoas e das organizações. |
| 8 | Para manter a segurança e consolidar essa cultura. |
| 9 | SIm pois muitas pessoas ainda não tem conhecimento necessário até mesmo em golpe com boletos |
| 10 | sim, porque muitos cliques são feitos de forma automática, sem ao menos ler a informação apresentada. |

Fonte: dados da pesquisa (2023)

A terceira e última sessão apresentou sete perguntas quanto a utilização de senhas, repasse de informações, comportamento do usuário e incidentes ocorridos.

A figura 16 é relacionada ao compartilhamento de senhas, questionando o respondente se fazia uso de senhas de outros colegas nos sistemas do dia a dia ou ainda se compartilhava das suas. Verificou-se que 98,3% não compartilham suas senhas e nem utilizam senhas de colegas, demonstrando que os usuários estão conscientes e que prezam pela segurança da empresa. Somente 1,7% dos entrevistados fazem uso de senha de terceiros ou repassam sua própria senha a colegas.

Figura 16 - Compartilhamento ou utilização de senha de terceiros




Fonte: dados da pesquisa (2023)

Por meio da figura 17, é possível verificar que 62,6% dos colaboradores gravam suas senhas na memória sem a necessidade de armazenar em outro local físico, 25,3% guardam suas senhas em local seguro, num "container" de senhas, sendo assim visto como um ponto muito positivo para a segurança de sistemas. Por outro lado ainda a usuários que utilizam cadernos ou post it (9,2%), navegador (1,7%) ou ainda blocos de notas do computador (1,1%) para armazenamento, demonstrando assim, que ainda é necessário aplicar métodos de conscientização mais eficazes sobre as consequências, pois cada usuário é responsável pelos procedimentos realizados em seu *login*.

Figura 17 - Anotação de usuários e senhas de sistemas


Fonte: dados da pesquisa (2023)

Referente a figura 18, foi questionado sobre a atitude do respondente ao receber uma ligação solicitando informações sensíveis. Conforme a figura, 81% afirmam que não repassam informações por telefone, o que se considera muito favorável na proteção de ataques e golpes de Engenheiros Sociais, que se aproveitam do elo mais fraco das organizações, o ser humano, para conseguir dados sigilosos para cometer crimes.

Contudo, 18,4% repassam as informações após a confirmação de dados da pessoa, entretanto o método de confirmações não é mais tão eficaz. Informações, até mesmo privadas, podem ser colhidas por engenheiros sociais e usadas para falsificar a legitimidade do associado e ludibriar o atendente, desta forma é indispensável informar a pessoa do outro lado da linha que informações são repassadas somente pessoalmente para segurança da empresa e do próprio associado.

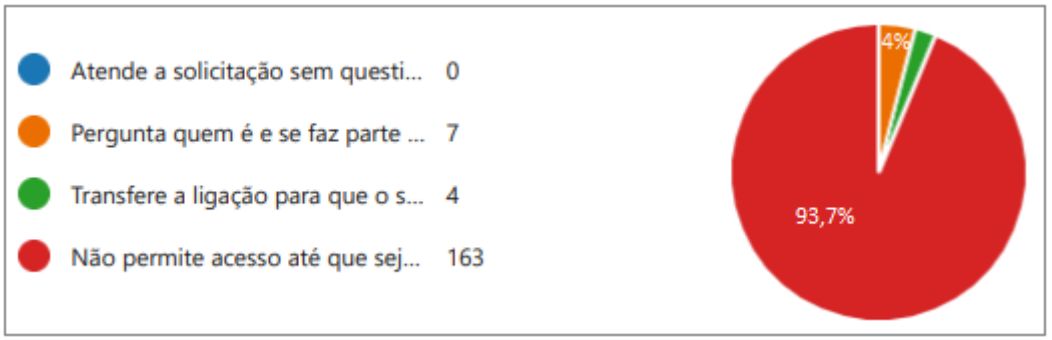
Figura 18 - Repasse de informações por telefone


Fonte: dados da pesquisa (2023)

A figura 19 diz respeito ao recebimento de telefonema do setor de TI solicitando acesso remoto para realizar atualizações em sistemas. Conforme respostas, 93,7% dos usuários não permitem o acesso sem uma confirmação do setor de tecnologia via chat ou outro meio de comunicação, no entanto, 4% permitiriam, após solicitar o nome e questionar se faz parte do TI da Cooperativa e ainda 2,3% repassam para que o supervisor resolva.

Golpes para acesso a sistemas estão cada vez mais frequentes nas agências de instituições financeiras, principalmente tentando se passar por funcionários da própria organização para tentar obter privilégios. Portanto, o uso de um código de confirmação ou ainda outro meio de comunicação para confirmar o acesso é visto como uma maneira importante para evitar que golpistas invadam a rede corporativa.

Figura 19 - Telefonema para acesso remoto




Fonte: dados da pesquisa (2023)

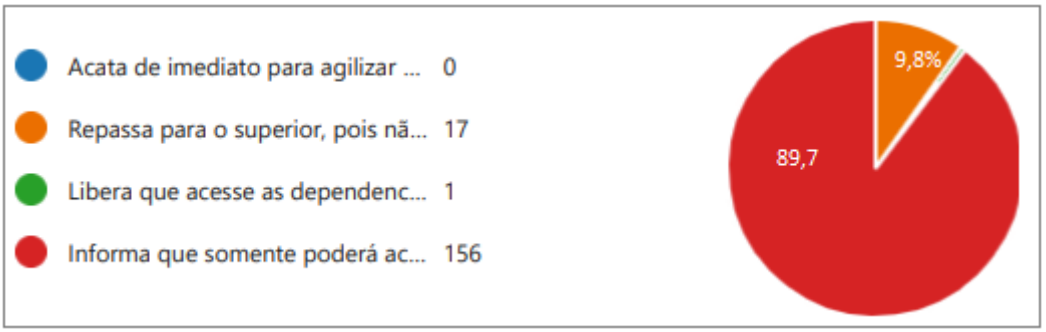
De acordo com a figura 20, a forma que o colaborador agiria ao receber um e-mail com um *link* ou um anexo estranho, neste caso, 78,2% entram em contato primeiramente com o setor de tecnologia para obter auxílio na análise do e-mail antes de abri-lo. E o restante dos 21,8% afirmam que analisam o endereço, assinatura, *link*, bem como a extensão do anexo, antes de fazer a abertura do e-mail. Mostrando dessa forma, que os colaboradores estão cientes dos perigos que podem se esconder em um possível *phishing*.

Figura 20 - Recebimento e e-mail com *link* ou anexo


Fonte: dados da pesquisa (2023)

A figura 21 se refere a segurança física, na qual a pergunta foi sobre a atitude que o pesquisado tomaria ao surgir uma solicitação de um terceiro para acesso às dependências da Cooperativa. Verificou-se que grande parte da amostra está consciente, sendo 89,7% dos pesquisados só acompanham o terceiro caso haja uma solicitação formal por e-mail, e outros 9,8% repassam ao superior, não sendo a melhor resposta, pois todos da instituição devem estar cientes das políticas e como agir nessas situações e somente 0,6% agiriam de forma totalmente errada, liberam a entrada por já conhecer o terceiro.

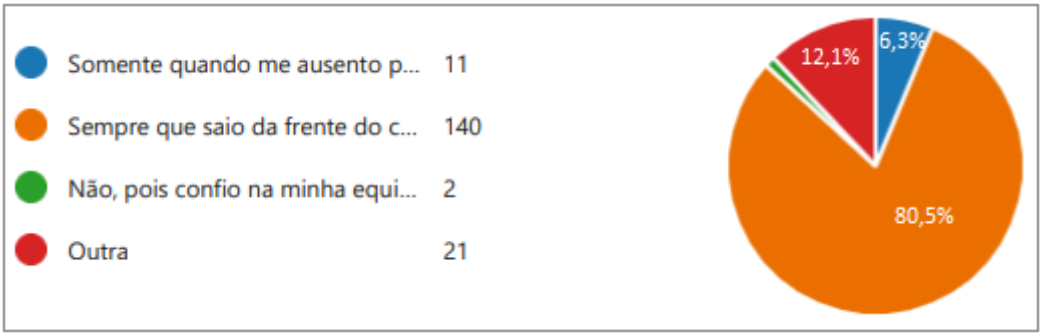
Figura 21 - Acesso externo e acompanhamento de terceiros




Fonte: dados da pesquisa (2023)

Na pesquisa da figura 22, é ilustrado que 80,5% dos usuários sempre bloqueiam suas áreas de trabalho quando saem da frente do computador, mostrando que maior parte dos colaboradores estão atentos à proteção dos dados, enquanto 6,3% bloqueiam somente quando se ausentam por horas e 12,1% não quiseram responder.

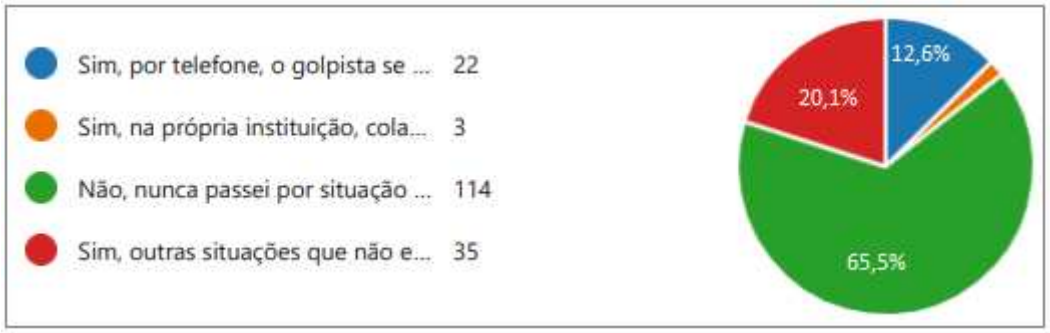
Figura 22 - Bloqueio de estação de trabalho




Fonte: dados da pesquisa (2023)

A última questão, teve como propósito, questionar os funcionários da Cooperativa se já haviam sofrido ou presenciado alguma tentativa de golpe dentro da instituição em que trabalham. Diante da amostragem, 65,5% nunca passaram por situação parecida, demonstrando que a Cooperativa está bem protegida de ataques, entretanto 20,1% afirmaram que já sofreram e 12,6% foram abordados por golpistas em ligações telefônicas se passando por pessoas da própria instituição para tentar obter privilégios e acesso a informações confidenciais.

Figura 23 - Sofreu ou presenciou tentativa de golpe dentro da instituição?




Fonte: dados da pesquisa (2023)

Em suma, pode-se averiguar que os colaboradores, em sua maioria, avaliaram positivamente a plataforma KnowBe4, e que com o conhecimento dos treinamentos, estão colocando em prática na organização e até em suas vidas pessoais.

## 5. CONSIDERAÇÕES FINAIS

O objetivo desta pesquisa, foi analisar a efetividade do uso da plataforma Knowbe4 em uma Cooperativa de Crédito situada no sul de Santa Catarina. Observou-se a avaliação dos usuários sobre os conhecimentos adquiridos, a didática apresentada e juntamente uma análise das atitudes dos colaboradores sobre situações que envolviam cuidado e manuseio de ativos de informação. Podendo-se afirmar que o propósito foi atingido por meio dos objetivos, coleta de dados e metodologia aplicada.

Primeiramente, foram apresentados alguns elementos que compõem o "universo" da segurança da informação, como conceitos, leis e normas, além de abordar as principais ameaças e a relevância significativa de possuir colaboradores bem conscientes sobre o tema.

Depois, foi abordado a plataforma KnowBe4, sua origem, estratégias de conquista do usuário para aumento da efetividade e continuação dos treinamentos, uso de relatórios e indicadores para melhor gestão dos riscos da empresa. Desta maneira, foi apresentado que as empresas precisam se adaptar à nova era da informação e inovação, e também com seus pontos positivos e negativos. E precisam saber preparar seus colaboradores para que não sejam mais vistos como o elo fraco da organização e sim elementos cruciais na proteção contra ameaças.

Com o diagnóstico da pesquisa com os usuários, foi possível constatar que a maioria dos colaboradores adotaram hábitos corretos sobre segurança de forma mais confiante após os

treinamentos da KnowBe4, entretanto é visto que ainda há pontos a serem melhorados e que a conscientização deve ser um processo contínuo.

Alguns pontos a serem melhorados se referem ao compartilhamento e utilização de senha de terceiros, anotações de senhas em locais inadequados, repasse de informações por telefone e falta de bloqueio da área de trabalho ao se ausentar da frente do computador. Essas ações tiveram percentuais pequenos de funcionários com atitudes erradas, mas com apenas um clique ou uma informação repassada sem segurança pode gerar inúmeras consequências.

Quanto às limitações da pesquisa, reforça-se a necessidade de mais estudos sobre a problemática das ações de colaboradores mal informados sobre a segurança da informação e as atitudes certas no dia a dia e sobre o impacto que isso pode gerar no ponto de vista não somente de instituições financeiras, mas também de qualquer tipo de empresa. Todos os segmentos do mercado fazem uso de informações, dados de funcionários, de clientes, produtos e de serviços e todos tem a necessidade de serem bem assegurados.

Sugere-se então, com base nessa pesquisa, que sejam aplicados estudos de forma comparativa entre outras plataformas de treinamento sobre segurança da informação disponíveis no mercado, visando identificar qual delas oferece os melhores recursos e resultados para a conscientização dos colaboradores sobre segurança da informação em instituições financeiras ou, até mesmo, em organizações de outros segmentos.

## REFERÊNCIAS


APWG. **Relatório de Tendências de Atividades de Phishing**, [s. l.], ano 3, 12 dez. 2022.

BEAL, Adriana. **Segurança Da Informação: Princípios e Melhores Práticas Para a Proteção Dos Ativos de Informação Nas Organizações**. Editora Atlas SA, 2000.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm:>. Acesso em: 05 mai. 2023

BRASIL. Presidência da República Casa Civil. Subchefia Para Assuntos Jurídicos. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 abr. 2023.

CERT. **Incidentes Notificados ao CERT.BR– Janeiro a Dezembro de 2022**. 2022. Disponível: <https://wwwhttps://stats.cert.br/incidentes>. Acesso: 29 abril 2023.

CIAMPA, M., **Conscientização sobre segurança: aplicando segurança prática em seu mundo** (4ª ed.) (2014). Boston, Massachusetts: Curso de Tecnologia.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. **Engenharia Social: uma ameaça à sociedade da informação.** Exatas & Engenharias, v. 3, n. 05, 2013.

DÍAS, J. C. R., Aragão, A. M., & Borges, M. R. S. (2020). **A importância da segurança da informação nas organizações**. Revista Conexão Eletrônica, 18(1), 52-59.

DISTERER, G. ISO/IEC 27000, **27001 and 27002 for Information Security Management.** Journal of Information Security. p. 92-100. 2013.

EMINAAOLU, M., Uçar, E., Eren, ^. (2009). **Os resultados positivos do treinamento de conscientização em segurança da informação nas empresas - Um estudo de caso.** Relatório Técnico de Segurança da Informação, I14, pp. 223-229.

FEBRABAN. **Brasil tem alta de 200% nos ataques de engenharia social em 2020**, 2021. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-tem-alta-de-200-nos-ataques-de-engenharia-social-em-2020. Acesso em: 22 abr. 2023.

FINKELSTEIN, A.; PENNATHUR, A.; RYDER, M.; O'MEARA, M. **Cybersecurity and organizational practices: An integrative review and future directions.** Journal of Business Research, v. 70, p. 233-246, 2017.

FONSECA, João J. S. **Metodologia da pesquisa científica.** Curso de Especialização de Comunidades Virtuais de Aprendizagem - InformáticaEducativa. Fortaleza: Universidade Federal do Ceará, 2002.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença**-São Paulo: Saraiva, 2006. GIL, AC Como elaborar projetos de pesquisa. 5ª Ed. São Paulo: Atlas, 2010.

FOWLER, G. (2011, 11 de setembro). **Qual é o maior risco de segurança de uma empresa?** Você. Jornal de Wall Street.

GIL, A. C. **Como elaborar projetos de pesquisa.** 5a ed. São Paulo: Atlas, 2010

IBM CORPORATION. **X-Force Threat Intelligence Index,** 2020. Disponível em: <https://www.ibm.com/security/data-breach/threat-intelligence>. Acesso em: 02 de mai. de 2023

ISACA. COBIT® **2019 Framework: Governance and Management Objectives.** ISBN 978-1-60420- 764-4

KASPESKY. **Black Friday: roubo de dados bancários dobra em 2022**, 2021. Disponível em: https://www.kaspersky.com.br/blog/black-friday-golpes-dobram/20338/. Acesso em: 22 abr 2023

KNOWBE4. **About Us | KnowBe4**. Disponível em: <https://www.knowbe4.com/about-us/>. Acesso em: 21 maio. 2023.

KNOWBE4. **Security Awareness Training Features** | KnowBe4. Disponível em:<https://www.knowbe4.com/en/security-awareness-training-feature/> Acesso em: 21 maio. 2023.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

MASCARENHAS NETO, Pedro, Tenório; ARAÚJO, Wagner Junqueira. **Segurança da Informação**: uma visão sistêmica para implantação em organizações. João Pessoa: Ufpb, 2019.

MENDES, Laura Schertel. **Marco Civil da Internet comentado.** São Paulo: Revista dos Tribunais, 2014.

NETSCOUT. **Relatório de inteligência de ameaças DDOS NETSCOUT,2023. Relatando o novo quadro de ameaças.** Disponível em: <https://www.netscout.com/threatreport/latam/brazil/>. Acesso em: 20 de maio de 2023.

PINHEIRO, Patrícia Peck, **Direito digital** — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013.

PONEMON INSTITUTE. **2022 Cost of Insider Threats Global Report.** Proofoint, 2023. Disponível em: <https://www.proofpoint.com/us/resources/threat-reports/

cost-of-insider-threats>. Acesso em: 24 de abr. 2023.

RAMOS, Anderson (org.). **Security Officer - 1: guia oficial para formação de gestores em segurança da informação.** Porto Alegre: Zouk, 2006. 460p. Módulo Security Solutions.

SANTOS, Antônio Silveira Ribeiro dos. **As Empresas e a Era da Informação.**[S. l.: s. n.],2006.Disponível em:http://www.aultimaarcadenoe.com/artigo16.htm. Acesso em: 12 out.2006.

SCHWAB, Klaus. **The Fourth Industrial Revolution**. Genebra: World Economic Forum, 2016.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva da segurança da informação.** Rio de Janeiro: Elsevier, 2014.

SLOAN, Jocelyn. **Phishing Mitigation for Small and Medium Businesses**. 2020.

SOUZA NETO, J. (2020) **Workshop de COBIT 2019**. PMP, RMP, CGEIT, CRISC, FAIR,. CSX, CLOUD, ITIL, COBIT 2019, COBIT 5 Implementation, COBIT 5 Assessor, Certified COBIT Assessor, COBIT-INCS. Instituto Brasileiro de Governança Pública.

TADEU, Erivelto. **Com R$ 2,5 bi para cibersegurança em 2020, bancos reforçam ações de conscientização digital.** [S. l.], 26 jun. 2021. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/com-r-2-5-bi-para-ciberseguranca-em-2020-bancos-reforcam-acoes-de-conscientizacao-digital. Acesso em: 22 abr. 2023.

TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO (ES). **OFÍCIO-CIRCULAR DA DIRETORIA GERAL Nº 4** - TRE-ES/PRE/DG/GAB-DG. [S. l.], 2. 2022. Disponível em: https://static.tre-al.jus.br/portal/transparencia/contratacoes/sei/sei_ct_552022.pdf. Acesso em: 25 mai. 2023.

VOLPINI, Adriano. FEBRABAN TECH 2022 | **A ciber-resiliência no setor financeiro**. YouTube, 9 ago. 2022. Disponível em: <https://www.youtube.com/watch?v=dxlcRMsOoko>. Acesso em: 28 jun. 2023

VERIZON. DBIR. **Data Breach Investigation Repost**. 2022

# APÊNDICE A – QUESTIONÁRIO

1. Qual sua idade?
   - ☐ Até 20 anos
   - ☐ De 21 a 31 anos
   - ☐ De 31 a 40 anos
   - ☐ Acima de 50 anos

2. Qual seu gênero?
   - ☐ Feminino
   - ☐ Masculino

3. Qual sua escolaridade?
   - ☐ Ensino fundamental incompleto
   - ☐ Ensino fundamental completo
   - ☐ Técnico
   - ☐ Superior incompleto
   - ☐ Superior completo

4. Período de uso da plataforma KnowBe4:
   - ☐ Mais de 5 meses
   - ☐ 3 a  4 meses
   - ☐ 1 a 2 meses
   - ☐ Nunca acessou

5. Você já tinha conhecimento sobre segurança da informação antes de utilizar a ferramenta KnowBe4?
   - ☐ Sim, por estudos próprios
   - ☐ Sim, pela própria instituição
   - ☐ Não

6. Após a utilização da ferramenta KnowBe4, você se sente mais seguro ao lidar com informações confidenciais?
   - ☐ Sim
   - ☐ Não

7. A ferramenta KnowBe4 ajudou a aumentar sua compreensão sobre ameaças cibernéticas?
   - ☐ Sim
   - ☐ Não

8. Você acredita que a ferramenta KnowBe4 contribuiu para o desenvolvimento de boas práticas de segurança da informação?
   - ☐ Sim, muito
   - ☐ Sim, mas pode melhorar
   - ☐ Não, acho o uso sem retorno a instituição

9. Você acha que a frequência e a qualidade do treinamento fornecido pela ferramenta são adequadas?
   - ☐ Sim
   - ☐ Não

10. Você aplicou o que aprendeu com a ferramenta KnowBe4 na sua vida pessoal?
    - ☐ Sim
    - ☐ Não

11. Você recomendaria a ferramenta KnowBe4 para outras instituições?
    - ☐ Sim
    - ☐ Não

12. Como você avalia a eficácia da ferramenta KnowBe4 em relação à conscientização sobre segurança da informação?

- ☐ Muito satisfeito
- ☐ Satisfeito
- ☐ Insatisfeito
- ☐ Muito satisfeito

13. Você considera que a utilização da ferramenta KnowBe4 contribui para a redução de incidentes de segurança da informação na instituição?
    - ☐ Sim
    - ☐ Não

14. A ferramenta KnowBe4 ajudou a mudar sua atitude em relação à segurança da informação? Se sim, como?

    _____

    _____

15. Você acredita que a instituição deve continuar a utilizar a ferramenta KnowBe4 para conscientização sobre segurança da informação?
    - ☐ Sim
    - ☐ Não

16. Em sua opinião, a instituição deveria investir mais em treinamento e conscientização sobre segurança da informação para seus colaboradores? Por quê?

    _____

    _____

17. Em relação às práticas. Você faz compartilhamento ou utiliza senhas de terceiros?
    - ☐ Sim
    - ☐ Não

18. Onde anota senhas e usuários de sistemas?
    - ☐ Keepass

- ☐ Bloco de notas do computador
- ☐ Salva no navegador
- ☐ Cadernos ou post it
- ☐ Não anoto, gravo na memória

19. Repasse de informações por telefone:
    - ☐ Repassa imediatamente, pois a pessoa na linha está com pressa
    - ☐ Repassa após confirmação de dados da pessoa
    - ☐ Não repassa informações por telefone

20. Telefonema para acesso remoto
    - ☐ Atende a solicitação sem questionar, pois é importante para a rapidez no atendimento e eficácia do sistema
    - ☐ Pergunta quem é e se faz parte da equipe de TI, e deixa prosseguir com os procedimentos
    - ☐ Transfere a ligação para que o superior resolva
    - ☐ Não permite acesso até que seja confirmado com a equipe via chat ou outro meio a efetividade da solicitação

21. Recebimento de e-mail com link ou anexo:
    - ☐ Clica para verificar o que se trata
    - ☐ Analisa o endereço de e-mail, a assinatura, o link, bem como a extensão do anexo, só então atende a solicitação
    - ☐ Entra em contato com setor de TI para auxílio na verificação e exclusão caso necessário

22. Acesso externo e acompanhamento de terceiros:
    - ☐ Acata de imediato para agilizar o procedimento
    - ☐ Repassa para o superior, pois não sabe como funciona nesses casos
    - ☐ Libera que acesse as dependências sem acompanhamento pois já conhece o terceiro

- ☐ Informa que somente poderá acompanhá-lo se a solicitação de acesso for formalizada via e-mail e aprovada pelo setor responsável

23. Bloqueio de estação de trabalho:

- ☐ Somente quando me ausento por horas
- ☐ Sempre que saiu da frente do computador
- ☐ Não, pois confio na minha equipe e em todos que circulam ali

24. Já sofreu ou presenciou alguma tentativa de golpe dentro da instituição?

- ☐ Sim, por telefone, o golpista se passando por alguém do setor de TI
- ☐ Sim, na própria instituição, colaborador mal intencionado
- ☐ Não, nunca passei por situação parecida
- ☐ Sim, outras situações que não estão descritas