EDUARDO JOSÉ FERREIRA DA ROCHA

ICARO ROBERTO MUNIZ FILHO

KAUÃ DOS SANTOS OLIVEIRA

VICTOR ALVES HIPÓLITO

O SISTEMA DE SEGURANÇA BANCÁRIO E SUA INFLUÊNCIA NA GESTÃO DE RISCO DAS EMPRESAS

São Carlos/SP 2024

O SISTEMA DE SEGURANÇA BANCÁRIO E SUA INFLUÊNCIA NA GESTÃO DE RISCO DAS EMPRESAS

São Carlos/SP

2024

EDUARDO JOSÉ FERREIRA DA ROCHA

ICARO ROBERTO MUNIZ FILHO

KAUÃ DOS SANTOS

VICTOR ALVES HIPÓLITO

O SISTEMA DE SEGURANÇA CIBERNÉTICO BANCÁRIO E SUA INFLUÊNCIA NA GESTÃO DE RISCO DAS EMPRESAS

Trabalho de Conclusão de Curso apresentado à Instituição de Ensino Técnico Etec Paulino Botelho como requisito parcial para obtenção do Título de Técnico em Administração.

Orientador (a): Prof.

São Carlos/SP 2024

FOLHA DE APROVAÇÃO

EDUARDO JOSÉ FERREIRA DA ROCHA

ICARO ROBERTO MUNIZ FILHO

KAUÃ DOS SANTOS

VICTOR ALVES HIPÓLITO

O SISTEMA DE SEGURANÇA CIBERNÉTICO BANCÁRIO E SUA INFLUÊNCIA NA GESTÃO DE RISCO DAS EMPRESAS

Trabalho de Conclusão de Curso aprovado, apresentado à Etec Paulino Botelho – Cidade: São Carlos, no Sistema de Ensino Presencial Conectado, como requisito parcial para a obtenção do título de Técnico em Administração, com nota final igual a _____, conferida pela Banca Examinadora formada pelos professores:

_____

Prof. Orientador
ETEC -

_____

Prof. Membro 2
ETEC -

_____

Prof. Membro 3
ETEC -

_____,____de_____de 2024

DEDICATÓRIA

Nós dedicamos este TCC às rosas mais belas de nosso jardim, o motivo pelo qual estamos aqui e que sempre nos incentivou a continuar estudando e a sempre cuidar de nosso futuro, nossas mães.

AGRADECIMENTOS

Agradeço a Deus que toda manhã me dá forças para alcançar meus objetivos.
Aos professores que participaram da pesquisa contida no presente trabalho.
Aos gestores do curso de "Pós-Graduação em Administração Pública", que nos proporcionaram uma grande graduação e aos professores do referido curso, sobretudo, aos que contribuíram para a realização deste trabalho.

EPÍGRAFE

“Se o dinheiro for a sua esperança de independência, você jamais a terá. A única segurança verdadeira consiste numa reserva de sabedoria, de experiência e de competência. ”

(Henry Ford)

DA ROCHA, José Eduardo Ferreira. FILHO, Icaro Roberto Muniz. HIPÓLITO, Victor Alves. OLIVEIRA, Kauã dos Santos. **O sistema de segurança bancário e sua influência na gestão de risco das empresas**. 2024. 34. Trabalho de Conclusão de Curso (Técnico em Administração) – Etec Paulino Botelho, São Carlos.

RESUMO

O presente trabalho de conclusão de curso (TCC) aborda a segurança bancária, destacando sua relevância tanto para instituições financeiras quanto para empresas e seus clientes. A segurança bancária abrange uma série de elementos físicos e digitais destinados a proteger o capital e os dados dos usuários, e seus elementos são apresentados no seguinte trabalho. Com o crescente avanço da digitalização, os bancos têm investido consideravelmente em segurança cibernética, prevendo um aumento nos gastos nesta área.

Este TCC elucida os principais setores da segurança bancária: os físicos, que incluem vigilância e dispositivos de segurança, e os digitais, que englobam cyber-segurança e aplicativos. Além disso, são discutidos os diversos tipos de fraudes e golpes que os clientes podem enfrentar, como *phishing* e clonagem de WhatsApp, assim como erros internos que podem impactar negativamente as transações financeiras.

O trabalho também explora a gestão de riscos nas empresas, enfatizando a importância de identificar e mitigar riscos para evitar perdas financeiras significativas. E por fim, o TCC ressalta a relação de cooperação entre bancos e empresas, na qual um sistema de segurança robusto e eficaz fortalece a confiança e a fidelização, beneficiando ambas as partes. A intermediação bancária é considerada fundamental para a diversificação das fontes de financiamento e a gestão de riscos, estabelecendo uma relação de longo prazo que favorece a estabilidade e o crescimento econômico.

Palavras-chave: Segurança Bancária, Riscos, Impacto, Pesquisa, Empresas, Bancos.

DA ROCHA, José Eduardo Ferreira. FILHO, Icaro Roberto Muniz. HIPÓLITO, Victor Alves. OLIVEIRA, Kauã dos Santos. **O sistema de segurança bancário e sua influência na gestão de risco das empresas**. 2024. 34. Trabalho de Conclusão de Curso (Técnico em Administração) – Etec Paulino Botelho, São Carlos.

ABSTRACT

This thesis addresses bank security, highlighting its relevance for financial institutions, businesses, and their clients. Bank security encompasses a range of physical and digital elements designed to protect users' capital and data, with these elements presented in the following work. With the increasing advancement of digitalization, banks have been investing significantly in cybersecurity, anticipating a rise in spending in this area.

This thesis elucidates the main sectors of bank security: the physical, which includes surveillance and security devices, and the digital, which encompasses cybersecurity and applications. Additionally, it discusses various types of fraud and scams that clients may encounter, such as phishing and WhatsApp cloning, as well as internal errors that can negatively impact financial transactions.

The work also explores risk management in businesses, emphasizing the importance of identifying and mitigating risks to avoid significant financial losses. Finally, the thesis highlights the cooperative relationship between banks and companies, where a robust and effective security system strengthens trust and customer loyalty, benefiting both parties. Bank intermediation is considered essential for diversifying funding sources and managing risks, establishing a long-term relationship that fosters stability and economic growth.

Keywords: Bank security, Risks, Impact, Search, Companies, Banks.

SUMÁRIO:

1 INTRODUÇÃO:.....11
1.1. Contextualização do tema.....11
1.2 Justificativa:.....18
1.3 Problema de pesquisa:.....19
1.4 Objetivos:.....19
1.4.1 Objetivo Geral.....19
1.4.2 Objetivos Específicos.....19
1.5 Delimitação do Trabalho.....19
2 Referencial Teórico.....20
3 Método de Pesquisa:.....24
4 Resultados:.....25
4.1 Estudo de caso.....28
5 CONSIDERAÇÕES FINAIS:.....30
5.1 Estudos Futuros:.....31
REFERÊNCIAS:.....32

1 INTRODUÇÃO:

Este primeiro capítulo serve como uma explicação objetiva da proposta do trabalho de pesquisa a partir da contextualização do tema, de sua justificava, objetivos e ainda, pontuando e demarcando os principais pontos analisados dentro do tema e, contudo, suas delimitações e contribuições.

1.1. Contextualização do tema

Segurança bancária é um conceito amplamente conhecido, mas, na maioria das vezes, pouco compreendido em suas diversas implicações. Muitas pessoas não têm plena noção de como esse sistema de proteção pode impactar, de maneira significativa, em suas vidas e de diversas maneiras tanto físicas em suas empresas, quanto econômicas em suas contas.

Não é de hoje que empresas e bancos andam lado a lado em um sistema de cooperatividade, e isso vem aumentando ao longo dos anos, cada vez mais empresas vão abrindo contas e cooperando com seus bancos deixando-o responsável por uma parte de seu capital.

Dentro desse sistema de segurança bancário há seus fundamentos que são compostos por diversos elementos e cada elemento tem suas características, funções e objetivos únicos que não podem ser trocados entre si, pois são extremamente importantes para a segurança do banco e de seus clientes. Os elementos da segurança bancária envolvem desde a parte física do banco, suas manutenções, procedimentos até sua parte tecnológica onde muitas pessoas preferem essa tecnologia em bancos através dos aplicativos de seus respectivos bancos. Segundo o site Blog da *idwall*: “Em 2022 houve um aumento de aberturas de contas bancárias, chegando a 1 bilhão de contas abertas, média de 5,4 por brasileiros”.

Os setores da segurança bancária são diversos e cada um com vários elementos que os compõem, tantos setores para uma prevenção de segurança para o capital quanto para a segurança de seus clientes, esses setores são:

- FÍSICOS - envolvem as portas de giratórias que detectam metais; os vigilantes armados dentro do banco; câmeras de segurança por toda a agência; vidros temperados; monitoramento vinte e quatro horas; sistema de alarme; cofre com retardo de trinta minutos muito bem protegido; e deslocamento de veículos especiais.

- DIGITAIS – Envolvem toda a parte interna do sistema bancário como; cyber segurança, aplicativos próprios dos bancos; sistema de transações; sistema de autoatendimento e responsável por movimentar o dinheiro por dentro do banco juntamente com os capitais de empresas em que ele seja responsável.

Atualmente os bancos brasileiros estão investindo muito na segurança digital por ser o meio que está sendo mais utilizado no século XXI, de acordo com a Pesquisa FEBRABAN de Tecnologia Bancária, os bancos brasileiros investem 10% do orçamento de tecnologia em segurança – cerca de R$ 3,5 bilhões por ano. Este número deve crescer aproximadamente para R$ 4,5 bilhões, segundo a entidade. As instituições estimam aumentar o orçamento de segurança cibernética para infraestrutura, prevenção às ameaças, gestão de identidade e acesso.

Com o investimento da segurança bancária as transações agora são muito mais recorrentes através dos canais de digitais, com a criação do “pix” e as senhas de transações. Segundo a FEBRABAN “73% das transações são realizadas por canais digitais”, mas há tipos de pessoas como as pessoas jurídicas que não podem realizar transações de valores muito acima do padrão por meios digitais que necessitam ir até a agência bancária para poder fazer tal transferência, elucidando que alguns atos ainda devem ser realizados propriamente em agências bancárias onde as contas estão criadas.

Desde a criação do primeiro banco do Brasil a criminalidade sempre esteve presente e ainda está até os dias de hoje só que mais forte, precisa e inovadora do que antes e conforme a segurança dos bancos evolui a criminalidade caminha junto com as constantes evoluções buscando sempre se aproveitar de pessoas mais vulneráveis como os idosos e pessoas desavisadas, se tornando um desafio constante para os bancos tendo sempre que se adaptar a esses golpes e intervir de alguma forma. Os gopes são muito variados indo desde fake news na internet até a ursurpação de pessoas que trabalham nas instituições, e a FEBRABAN decidiu listar os principais golpes que acontecem com as pessoas dentro e fora de bancos como uma forma de prevenção e pesquisa; a lista contém os 5 principais golpes mais utlizados, sendo eles:

1 - Falso Link (Phishing): O phishing, ou pescaria digital, é uma fraude eletrônica cometida pelos fraudadores (engenheiros sociais) que visa obter as senhas e dados pessoais do usuário. A forma mais comum de um ataque de phishing são as mensagens em e-mails, SMS, aplicativos de mensagens como WhatsApp, redes sociais que induzem o usuário a clicar em links maliciosos. Também existem páginas falsas na internet que induzem a pessoa a revelar as senhas e dados pessoais. Os casos mais comuns de phishing são e-mails recebidos de supostos bancos com mensagens que afirmam que a conta do cliente está irregular, ou o cartão ultrapassou

o limite, atualização de token ou ainda que existe um novo software de segurança do banco que precisa ser instalado imediatamente pelo usuário.

2 - Clonagem do WhatsApp: Os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de WhatsApp. Com essas informações em mãos, os criminosos tentam cadastrar o WhatsApp da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo WhatsApp fingindo ser do Serviço de Atendimento ao Cliente de bancos e instituições financeiras ou da empresa em que a vítima tem cadastro. Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular, tendo acesso a todo o histórico de conversas e contatos. A partir daí, os criminosos enviam mensagens para os contatos, passando-se pela pessoa, pedindo dinheiro emprestado.

3 - Falso motoboy: O golpe começa quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente. O outro golpista aparece onde a vítima está e retira o cartão. Mesmo com o cartão cortado, o chip está intacto e os fraudadores podem utilizá-lo para fazer transações e roubar o dinheiro da vítima.

4 - Falsa Central de Atendimento (o mais comum): O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema 6 e, a partir daí, solicita os dados pessoais e financeiros da vítima. Em alguns casos, os golpistas até mesmo pedem para que a vítima ligue para central do banco, no número que aparece atrás do seu cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, a senha do correntista.

5 - Golpe da troca de cartão: Golpistas que trabalham como vendedores prestam atenção quando você digita sua senha na máquina de compra e depois trocam o cartão na hora de devolvê-lo. Com seu cartão e senha, fazem compras usando o seu dinheiro. O mesmo pode acontecer com desconhecidos oferecendo ajuda no caixa eletrônico. Eles se aproveitam de alguma dificuldade sua no terminal eletrônico para pegar rapidamente o seu cartão e depois devolver um que não é seu, ao mesmo tempo que espiam sua senha.

Além dos golpes citados existem outros riscos que bancos enfrentam que são os que interferem indiretamente os clientes mas diretamente empresas, que são erros comuns de acontecerem com qualquer banco, os erros cibernéticos ou erros internos bancários, aqueles que estão presentes no sistema de segurança, para melhor entendimento será necessário a utilização de um exemplo: Empresa X fez uma transferência para outra empresa mas por algum erro do sistema isso não foi possível e o dinheiro volta para a conta ou no pior dos casos o dinheiro sai da conta da empresa mas não chega na conta do destinatário, isso é um erro do sistema bancário e a solução para isso esta em no banco que por lei segundo o Superior Tribunal de Justiça (STJ), súmula 479 (2024); "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". Ou seja, os bancos se responsabilizam 100% por erros de sistema que prejudiquem seus clientes.

Em relação a erros HUMANOS como tranferência via pix para outra pessoa ou instituição não serão de responsabilidade da instituição e sim da pessoa responsável por fazer a transação sabendo dos riscos, e o máximo que a instituição poderá fazer é entrar em contato com o dono da conta que foi realizada a transação e se possível chegar a um acordo para que devolva o dinheiro, do contrário a pessoa pode apenas recorrer a uma delegacia e fazer um Boletim de Ocorrência (B.O).

Para que sejam evitadas as práticas de golpes em instituições financeiras, a FEBRABAN publicou em seu site dicas para se prevenir de golpes tanto na internet quanto na rua; essas dicas servem como instruções para pessoas mais vulneráveis e desinformadas sendo uma boa precaução por parte das instituições financeiras. Abaixo encontra-se a lista de dicas feitas pela FEBRABAN:

1. Cuidado com as suas senhas

    Não compartilhe sua senha com amigos e parentes ou encaminhe senhas por aplicativos de mensagens, e-mails ou SMS. Nunca utilize dados pessoais como senha (ex. data de aniversário, placa de carro etc.), nem números repetidos ou sequenciais (ex. 111111 ou 123456), nem anote senhas em papel, no celular ou no computador.

2. Cuidados com seu cartão

    Nunca entregue seu cartão a ninguém. Os bancos não pedem os cartões de volta, mesmo se houver a possibilidade de fraude ou defeito. Eles também não mandam um portador buscar seu cartão.

3. Confira seu cartão após uma compra

Ao terminar de realizar uma compra na maquininha, verifique o nome no cartão para ter certeza de que realmente é o seu. Sempre confira o valor na maquininha antes de digitar a sua senha. E proteja o código de segurança.

4. Ative duplo fator de autenticação

Sempre ative a função de segurança “duplo fator de autenticação” em suas contas na internet que oferecem essa opção: e-mail, redes sociais, aplicativos, sistemas operacionais etc

5. Atenção com ligações

Se receber contato em nome do banco solicitando para ligar para sua Central de Atendimento, ligue a partir de outro aparelho, assim evita que o golpista “prenda” a sua linha telefônica e nunca informe suas senhas.

6. Nunca clique em links desconhecidos

Sempre confira a origem das mensagens ao receber promoções e e-mails que se dizem do banco. Nunca clique em links de promoções muito vantajosas ou que peçam sincronização, atualização, manutenção de token, app ou cadastro. O banco nunca envia e-mails informando que sua conta foi invadida e pede para enviar os seus dados.

7. Cuidado em compras online

Dê preferência a sites conhecidos e confira sempre se o endereço do site é o verdadeiro. Para garantir, não clique em links, digite o endereço no navegador. Sempre use o cartão virtual para realizar compras na internet.

8. Cuidado nas operações bancárias

Sempre confira o nome do recebedor ao pagar um boleto, realizar transferências ou Pix.

9. Não fotografe ou filme a tela do caixa eletrônico ao usá-lo

Nunca envie fotos, vídeos ou capturas de tela pelo celular. Se precisar de auxílio no caixa eletrônico, peça ajuda a um funcionário do banco devidamente identificado.

10. Cuidado com o que compartilha nas redes sociais

> Um simples post pode dar muitas informações sobre você para golpistas. O que você compartilha pode ajudar bandidos a conhecer seu perfil e comportamento.

Além da prática de informação com dicas de prevenção, há outras práticas que as instituições financeiras podem adotar, como procedimentos de segurança rigorosos e serviços que são realizados somente indo até o banco físico evitando assim fraudes e falsificação de documentos.

A tecnologia na segurança bancária é algo que tem que estar em constante evolução, pois conforme o banco evolui a criminalidade se aprimora, com isso a tecnologia de segurança bancária evoluiu muito com o passar do tempo e graças as pesquisas realizadas anualmente pela FEBRABAN é possível ter alguma noção dessa evolução. Mas para que essa evolução seja feita é necessário capital, por isso é importante realizar pesquisas sobre o investimento do governo na segurança tecnológica bancária, e a empresa Dados da Gartner empresa de pesquisa e consultoria em tecnologia da informação dentre outros temas, apontam que, globalmente, os bancos são o segundo setor que mais destina recursos para tecnologia, atrás apenas dos governos e muito à frente da indústria de telecomunicações (FEBRABAN, 2019). Em 2018, o governo foi responsável por 16% do total de gastos com tecnologia no mundo, seguido do setor bancário (13%) e das telecomunicações (6%).

A gestão de risco é uma ferramenta utilizada pelas empresas como forma de “oráculo ", pois é realizada uma previsão através de elementos passados da empresa como gastos, riscos que já aconteceram e que a empresa utiliza para prever os riscos que podem ocorrer futuramente. A palavra Risco tem várias definições e segundo o livro Risco Financeiro, “o termo risco pode ser entendido mais como uma escolha do que como uma fatalidade, uma sina ou um destino. ” Com uma gestão de risco eficiente, evita-se muitos e muitos problemas para a empresa, fazendo com que seja gasto pouco capital ou até mesmo dependendo do risco um prejuízo enorme ser evitado.

Os riscos que empresas podem enfrentar ou que já enfrentam são diversos e muito variados, e segundo o livro Riscos Empresariais: “Os riscos são tudo aquilo que impede de ganhar e/ou faz perder. Os riscos empresariais são todos os eventos e expectativas de eventos que impedem a empresa de ganharem dinheiro e respeito.” Mas com uma boa gestão de risco, problemas como perda de dinheiro e confiança podem ser evitados se utilizar estratégias com as ferramentas certas; e se o gestor de risco souber superar as dificuldades ele consegue, por conseguinte tirar alguma vantagem do risco ocorrido ou previsto, como citado acima utilizando os métodos e ferramentas certos.

Ao fazer uma gestão de risco em sua empresa e evitar declínios e riscos previstos, porém não evitados são utilizados Métodos e ferramentas para uma boa gestão de

previsão de riscos, e dentre métodos e ferramentas existem muitos e por isso empresários precisam ser criativos e pensarem além do seu alcance, afinal riscos podem vir a qualquer hora e a qualquer momento e uma boa gestão de riscos salvará sua empresa inúmeras vezes. Tais métodos e ferramentas se baseiam no tempo, ou seja, se a empresa já sofreu algum tipo de emergência, ou contratempo que interferiu em suas atividades, esses riscos que ela já sofreu serão utilizados como base para prever futuros riscos. Dentro da forma de prevenção de riscos existem ferramentas que servem apenas como identificação de riscos, de acordo com sites e blogs na internet, TNX Brasil, pode se utilizar 7 ferramentas para a identificação desses riscos, são elas: Brainstorming, Matriz SWOT, Análise de causa Raiz, técnica Delphi, Entrevistas, Inspeções e revisar requisitos e documentações para que não ocorra nenhum imprevisto internamente relacionado a documentações próprias da empresa. Já os métodos utilizados na gestão de risco segundo o Blog Kronos são: Análise causa e efeito utilizando o diagrama de Ishikawa, fazendo um mapeamento de riscos para melhor visualização, Mitigação de riscos para que após a identificação desses riscos utilizando as ferramentas citadas sejam feitas propostas para a prevenção desses riscos; Transferência de riscos, ou seja, ter uma seguradora é um ótimo passo para o empresário que não tenha nenhuma forma de mitigar esses riscos, e por fim se o risco não for danificar sua empresa a aceitação do risco talvez seja a melhor opção.

O impacto do sistema de segurança bancário na gestão de risco das empresas é significativo e multifacetado. Primeiramente, um sistema de segurança robusto e eficaz atua como uma linha de defesa contra fraudes e roubos, protegendo os ativos das empresas.

Além disso, a implementação de medidas eficazes ajuda a mitigar as perdas financeiras por fraudes, cyber-ataques e até mesmo erros administrativos, impactando positivamente os ativos financeiros das organizações.

E por consequência de um bom Sistema de Segurança Bancário, pode-se impactar no empresário de forma positiva, pois ao ver um bom sistema de segurança protegendo seus ativos acaba acarretando uma confiabilidade exemplar na instituição financeira favorecendo a fidelização e atraindo mais clientes. Empresas que demonstram um forte compromisso com a segurança tendem a se destacar em um mercado competitivo.

A relação entre bancos e empresas ocupa um lugar importante na literatura económica e financeira. Esta relação insere-se na atividade de intermediação dos bancos. As teorias mais recentes da intermediação desenvolvem esta relação num ambiente de informação assimétrica. Os bancos incluem nos contratos incentivos de modo a enfrentarem problemas de risco moral (Allegret e Baudry, 1996). Tal relação interfere

em sua cooperação, ou seja, para que a cooperação de bancos e empresas seja boa a sua relação terá que ser excelente e profissional e para manter essa relação de Bancos e Empresas Segundo Allegret e Baudry existem três estruturas na relação de bancos e empresas: (1) uma relação de mercado (2) uma relação hierárquica e (3) uma relação da quase-integração.

O banco diversifica a sua carteira de clientes e a empresa diversifica as suas fontes de financiamento. Neste caso, a empresa sentirá maior dificuldade em iniciar a sua atividade com investimentos que apresentam um determinado grau de risco. A estrutura do financiamento é marcada pela dependência da empresa ao banco no que concerne aos empréstimos a efetuar. Diversificando os serviços oferecidos, o banco pode seguir de perto a atividade da empresa. Os intermediários financeiros ocupam a parte central do sistema. Uma empresa mantém um relacionamento privilegiado de longo prazo com um banco (princípio de autoridade). Nesta troca de relação privilegiada o banco obtém o direito de interferência na gerência da empresa. Os bancos, neste caso, tomam em mãos a gestão de sectores importantes das empresas que controlam e podem supervisionar e recolher a informação sobre a empresa, quer como emprestadores quer como acionistas. Logo, a relação de bancos com empresas é a melhor estratégia de cooperação, pois os dois lados se beneficiam com tal relação e cooperação.

1.2 Justificativa:

Uma parte fundamental deste trabalho é auxiliar empresas e instituições financeiras na garantia de que seus sistemas de segurança cibernética realmente protejam os dados sensíveis. Também há colaboração com a gestão de riscos, com o objetivo de antecipar possíveis vulnerabilidades e prevenir problemas futuros.

No âmbito acadêmico, o foco é aprofundar o conhecimento sobre os sistemas cibernéticos bancários. Isso é realizado por meio de estudos de caso e validações que servem como referência para novos pesquisadores e estudantes.

Além disso, reconhece-se a importância de educar a população sobre o funcionamento do sistema bancário, a fim de evitar boatos e mal-entendidos. É relevante destacar que 82% da população brasileira possui conta corrente em bancos, enquanto muitos outros utilizam contas poupança. Assim, busca-se demonstrar que o sistema bancário pode ser seguro e confiável, promovendo maior confiança entre os cidadãos.

1.3 Problema de pesquisa:

Tendo em vista que algumas empresas sofrem ou já sofreram com um sistema de segurança bancário frágil, visa responder o seguinte questionamento:

Qual a importância de um sistema de segurança bancário seguro dentro da sociedade empresarial?

1.4 Objetivos:

1.4.1 Objetivo Geral

O tema deste TCC tem como objetivo geral explicar como um sistema de segurança bancário frágil pode interferir nas empresas. Serão apontados alguns cuidados e prevenções, além de ser destacada a importância de um sistema de segurança bancária eficaz.

1.4.2 Objetivos Específicos

Os seguintes objetivos específicos são considerados na pesquisa:

A) Ressaltar a importância de um sistema bancário seguro
B) Dissertar os riscos que sua empresa correr
C) Discutir de que forma o sistema bancário interfere nas empresas
D) Identificar os problemas que a cyber-segurança bancária sofre

2 Referencial Teórico

Desde a história do dinheiro até o surgimento do primeiro banco, houve mudanças drásticas na segurança e na utilização dos serviços bancários. Nos tempos modernos, é imperativo evoluir para um sistema bancário digital, mais prático e acessível tanto para pessoas jurídicas quanto físicas, para que assim seja seguro de pessoas usarem digitalmente tornando mas fácil a utilização dos serviços bancários.

> Os Bancos Centrais tem procurado se adaptar a um mundo onde cada vez mais aspectos da vida socioeconômica são permeados por processos digitais. A implementação destas moedas carrega consigo uma série de fatores a serem considerados, uma vez que questões como segurança, privacidade, estabilidade econômica, hegemonia monetária, inclusão digital, acessibilidade e desenvolvimento de novos produtos e serviços estão diretamente relacionados a como esta implementação vai ser feita, e quais serão as características da moeda digital. *(ROMODA, 2022, p. 05).*

Conforme a segurança dos bancos evolui a criminalidade caminha junto com constantes evoluções buscando sempre se aproveitar de pessoas mais vulneráveis como os idoso e isso se torno um desafio constante para os bancos tendo que sempre se adaptar a esses meio de golpes e intervir de alguma forma.

> *O setor bancário enfrenta desafios crescentes relacionados à segurança devido à evolução das ameaças cibernéticas e à crescente sofisticação dos ataques. (DARAME, 2023, p. 01).*

No contexto atual deve-se sempre contextualizar sobre cada tema e como esse tema pode interferir em outro, a gestão de risco empresarial segundo o Livro Risco Financeiro, no capítulo 1 – A gestão de Risco diz que; muitas pessoas hoje em dia utilizam o termo <<Risco>> de forma aquivocada quando falamos de Gestão de risco nas empresas, mostrando que a melhor definição tem a ver com a dupla dimensão incerteza/indesejabilidade que podemos associar a um dado resultado de um determinado acontecimento.

> A utilização generalizada, embora de forma muitas vezes ambígua, do termo «risco» conduz a alguma confusão sobre o seu verdadeiro significado. Pensamos que a melhor definição de risco tem a ver com a dupla dimensão incerteza/indesejabilidade que podemos associar a um dado resultado de um determinado acontecimento. *(Pinho, 2019, p. 16)*

Hoje em dia bancos contam com seu*s* próprios aplicati*vo*s para que isso facilite seus serviços para seus clientes sendo mais fácil utilizar os serviçoes bancários, podendo usar dentro e fora de casa, e até mesmo podendo até fazer transações de valores consideravelmente altos tornando mais fácil empresas realizarem transferências, mas com uma eficácia tão grande também há seus riscos e segundo o modelo de pesquisa realizado em por *Carlos Moraes Affonso Junio*r “Com o advento do Internet banking, por meio do qual as operações financeiras passam a ser eletrônicas, surgem implicações jurídicas decorrentes do furto de senhas dos usuários (phishing), da qual trataremos enfocando basicamente as normas brasileiras de responsabilidade civil aplicáveis em decorrência de danos.”

> *"Responsabilidade civil dos bancos virtuais brasileiros nas fraudes envolvendo o furto de senhas eletrônicas. As implicações do desenvolvimento de sistemas de segurança. (Júnior, 2008, p.05).*

Pessoas que trabalham em bancos podem cometer falhas, mas no setor bancário isso não pode ocorrer de forma alguma, por ter consequências graves e por isso muitas pessoas que são vítimas destes erros fazem processos contra as instituições bancárias por dano moral ou outro processo que procura ressarcir o erro causado pelos bancos.

> “O ordenamento jurídico conceitua dano como sendo qualquer ato ou fato humano produtor de lesões a interesses alheios juridicamente protegidos. O dano moral, portanto, é aquele que se opõe ao dano material, não afetando os bens patrimoniais propriamente ditos, mas atingindo os bens de ordem moral, de foro íntimo da pessoa, como a honra, a liberdade, a intimidade e a imagem. A história confirma, desde tempos remotos, que a preocupação com alguma forma de reparação aos danos morais sempre existiu.” (*Tossin, 2007, p. 03*)

Muitos dos gastos governamentais são com educação, sáude e entre outras coisas, mas será que esses gastos são destinados a segurança bancária? A resposta para a pergunta é sim, segundo uma pesquisa feita pela Gartner, os bancos são o segundo setor que mais destina recursos para a tecnologia. E o setor bancário é o responsável por 13% do desenvolvimento tecnológico e das telecomunicações.

> *Em 2018, o governo foi responsável por 16% do total de*
>
> *gastos com tecnologia no mundo, seguido do setor bancário (13%) e das telecomunicações*
>
> *(6%). De forma semelhante, em 2018, pela primeira vez, os gastos com tecnologia do setor*
>
> *bancário, no Brasil, atingiram o mesmo patamar do setor público, 14% dos dispêndios totais o setor bancário brasileiro é reconhecido como um ecossistema robusto, maduro e de ampla envergadura, que se encontra conectado às novas tendências nos mais diversos campos e está na vanguarda mundial da tecnologia*

(FEBRABAN, 2019)

“Para que uma pesquisa passe a ideia de concreta é necessário um estudo de caso realizado, pois com isso a perspectiva da entrevista/dados estudados mudam completamente e fazem o pesquisador enxergar por outro lado dando um novo olhar para a sua pesquisa”

> “Um estudo de caso é restrito a uma ou poucas unidades, identificadas como indivíduos, famílias, organização, sociedade, dentre outros. Caracteriza-se pela investigação e pelo detalhamento do objeto de estudo, através de uma análise sobre o ponto de vista dos participantes”. *(Vergara, 2004)*

“Ao ver um bom sistema de segurança protegendo seus ativos acaba acarretando uma confiabilidade exemplar na instituição financeira favorecendo a fidelização e atraindo mais clientes. Empresas que demonstram um forte compromisso com a segurança tendem a se destacar em um mercado competitivo”.

> Como consequência de um mercado cada vez mais competitivo e crescente valorização das necessidades dos clientes, muitas empresas têm vindo a adoptar políticas de gestão da qualidade como forma de garantir a satisfação dos seus clientes e restantes *stakeholders.* (Lopes, 2014, p. 06)

3 Método de Pesquisa:

A partir da pesquisa realizada na Instituição Financeira Caixa Econômica Federal, município de São Carlos – SP, é possível verificar como funciona a relação de bancos e empresas baseando-se em uma entrevista realizada na instituição financeira.

> “Todas as ciências caracterizam-se pela utilização de métodos científicos; em contrapartida, nem todos os ramos de estudo que empregam estes métodos são ciências. Dessas afirmações podemos concluir que a utilização de métodos científicos não é da alçada exclusiva da ciência, mas não há ciência sem o emprego de métodos científicos. ”. (Marconi; Lakatos 2003, p. 83)

Buscou-se compreender como o sistema de segurança bancário impacta na gestão de risco das empresas e até mesmo para pessoas físicas. Para a idealização desta pesquisa foi utilizado os seguintes termos: “segurança bancária”, “instituições financeiras”, “riscos” e “impacto”.

Para que se compreenda qual o impacto de um sistema de segurança bancário deplorável nas empresas, para o seguinte trabalho usou-se as seguintes abordagens: qualitativa para explicar se o sistema de segurança bancário é realmente seguro para as empresas que tem relação com as instituições financeiras, e quantidade pois foi elaborada uma análise de diversos artigos.

Para a elaboração desse artigo foram analisados dezessete artigos por intermédio da plataforma Google Acadêmico e livros relacionados a administração, através deles procurou-se entender como o sistema de segurança bancário impacta tanto na gestão de risco das empresas quanto diretamente no capital das empresas.

Após a leitura desses artigos e livros foram divididos tarefas para cada integrante. O grupo é composto por quatro pessoas e para cada integrante foi designada uma tarefa e responsabilidade dentro do trabalho levando em consideração as limitações e disponibilidades de cada um.

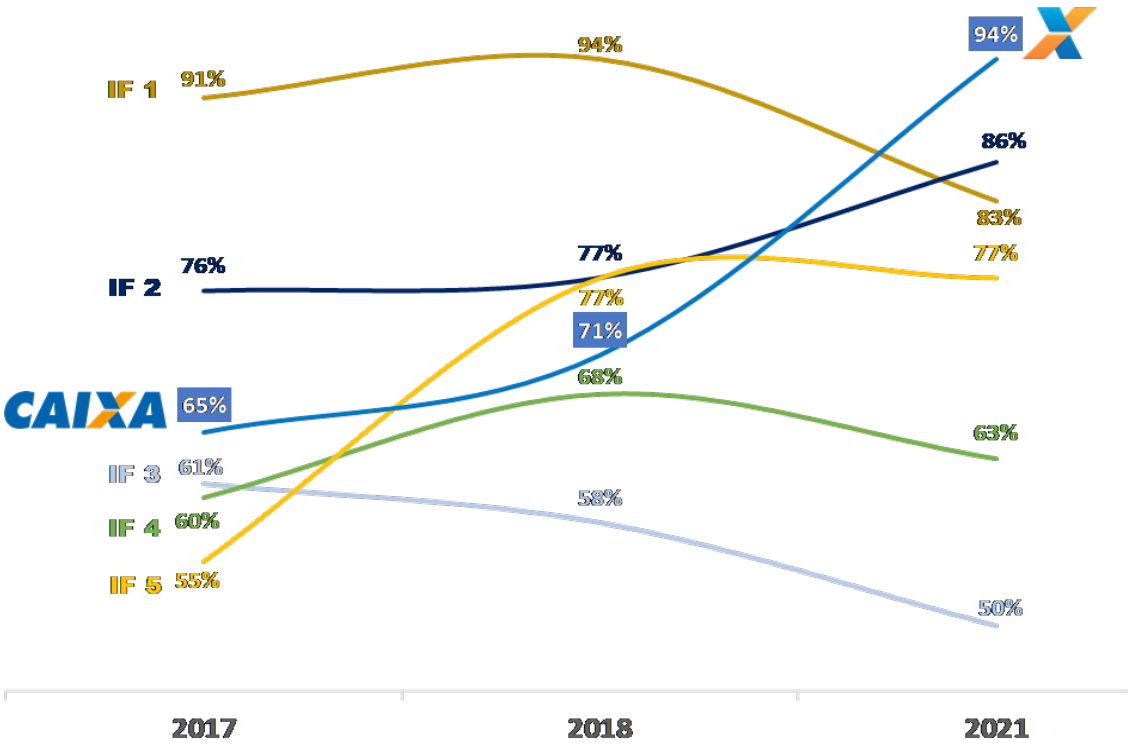
O estudo de caso foi realizado na Caixa Econômica Federal com um funcionário de alto escalão da empresa, sendo feito com perguntas específicas com o objetivo de obter

respostas mais amplas dando espaço para o entrevistado responder como quiser, para assim obter os dados e pesquisas presentes neste trabalho.

4 Resultados:

Ao fazer pesquisas sobre o tema na Instituição financeira Caixa Econômica Federal, notamos a importância de demonstrar qual a importância da Caixa Econômica Federal dentro de nosso trabalho e dentro do ramo empresarial. Abaixo encontra-se um gráfico mostrando os prêmios e reconhecimentos da Caixa Econômica Federal, reforçando a importância de ter um banco de qualidade que preza por seus clientes e que acima de tudo tenha um bom sistema de segurança.

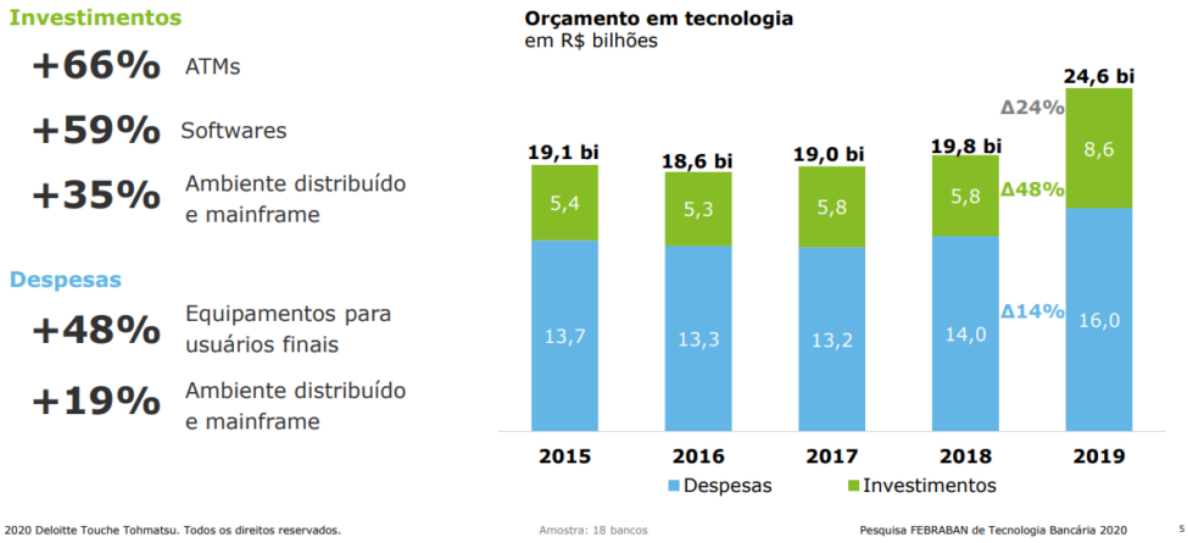
Gráfico 1 - Melhor nota em Índice de Governança e Gestão Pública (IGG), pelo TCU



Fonte: Tribunal de Contas da União (TCU) (2021).

O orçamento bancário para as suas tecnologias cresceu 24% em 2019, em comparação a 2018. Isso é um resultado extremamente positivo para o setor bancário, gerando mais credibilidade para a sua segurança.

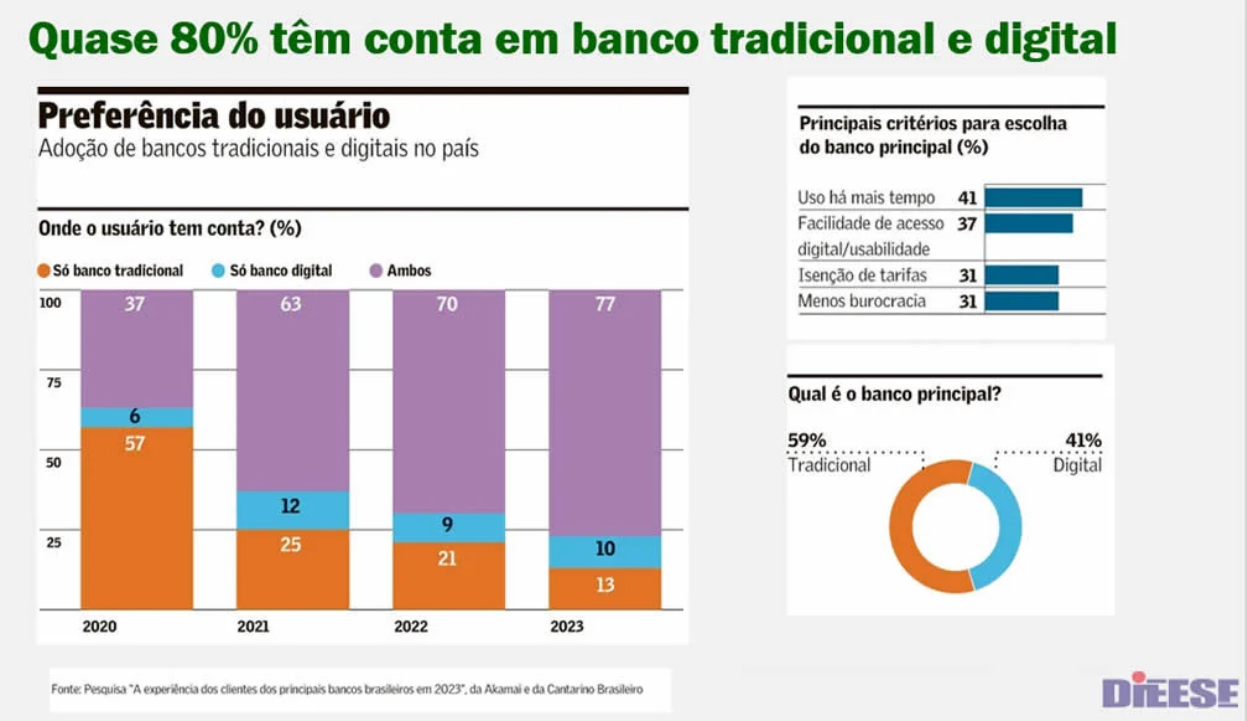
Gráfico 2 – Orçamento em tecnologia



Fonte: FEBRABAN. (2020)

Atualmente com a criação dos aplicativos bancários e bancos digitais os serviçops bancários nunca foram tão acessíevis e práticos, tanto que pessoas hoje em dia preferem muito mais criarem contas em bancos digitais do que enfrentarem filas e a burocrácia de bancos físicos, sendo assim os clientes que já tem contas me bancos físicos optam por criarem contas em bancos digitais por sua praticidade.

Gráfico 3 – Preferência do usuário



Fonte: Pesquisa ”A experiência dos clientes dos princpais bancos brasileiros em 2023”. da Akamai e da Cantarino Brasileiro. (2023)

4.1 Estudo de caso

A partir da pesquisa realizada na Instituição Financeira Caixa Econômica Federal, município de São Carlos – SP, é possível verificar como funciona a relação de bancos e empresas baseando-se em uma entrevista realizada na instituição financeira.

De acordo com Marconi e Lakatos (2001, p. 105): “a especificação da metodologia da pesquisa é a que abrange maior número de itens, pois responde, a um só tempo, às questões: Como? Com quê? Onde? Quando? ”.

Os respectivos autores realizaram essa pesquisa de duas formas: exploratório e explicativo.

Exploratório - é considerada uma pesquisa que busca por meio das suas táticas e parâmetros, uma proximidade da realidade do objeto desejado.

Explicativo – seria uma pesquisa que se aprofunda de forma mais concreta no estudo, relacionando hipótese e técnicas ao decorrer da pesquisa.

Segundo vergara (2004), “um estudo de caso é restrito a uma ou poucas unidades, identificadas como indivíduos, famílias, organização, sociedade, dentre outros. Caracteriza-se pela investigação e pelo detalhamento do objeto de estudo, através de uma análise sobre o ponto de vista dos participantes”.

A consulta foi elaborada com o método monográfico, participando apenas um funcionário da instituição financeira Caixa Econômica Federal, do município de São Carlos – SP.

A coleta de dados foi realizada através de uma entrevista com um funcionário da Caixa Econômica Federal, por conseguinte obtivemos as respostas necessárias para o desenvolvimento da pesquisa. A pesquisa deste estudo foi realizada com uma entrevista, composta por uma sequência de perguntas abertas dando espaço ao entrevistado falar à vontade e assim fazendo a coleta de dados.

Diante do estudo sondado, foi possível ver que a relação de instituições financeiras e empresas é algo confiável e com tamanhas responsabilidades, uma troca dos dois lados que beneficia ambos e se por um acaso uma das partes não cumprir com as

responsabilidades terá consequências severas, por isso tal troca necessita da colaboração dos dois lados.

Por isso deve ser levado em consideração que qualquer falha por parte do banco internamente que afete empresas em que o banco estiver liberando crédito ou esteja responsável pelo capital investido será ressarcido cem por cento, embora falhas graves ocorridas internamente que envolva algum capital empresarial segundo o entrevistado sejam extremamente difíceis de ocorrer nos dias de hoje.

E por observação os erros mais frequentes que podem ocorrer e que já são ditos aos empresários são falhas em aplicativos bancários que envolvem a queda do sistema, mas que podem voltar no mesmo dia e que por algum motivo do banco alguns atrasos podem ocorrer na categoria de empréstimos ou liberação de crédito (por estarem analisando a empresa), mas sobre isso os empresários que estiverem interessados em fazer tal troca com o banco receberá um termo de riscos que contém as falhas citadas anteriormente deixando os empresários cientes desses problemas que podem acontecer.

5 CONSIDERAÇÕES FINAIS:

Neste trabalho procurou-se entender como o sistema de segurança bancário pode impactar de forma negativa ou positiva a gestão de uma empresa ou ela por completo a fim de que empresários estejam cientes da relação de bancos e empresa e que entendam que os riscos do sistema de segurança bancário também podem ser previstos ou até mesmo evitados, visando tranquilizar e conscientizar os donos de empresas.

Após pesquisas realizadas pelo grupo pode-se compreender que as empresas como um todo e pessoas físicas têm algum receio pelo sistema de segurança bancário, levando a uma desconfiança desnecessária por parte da sociedade empresarial e pessoas em geral. Muitas vezes por medo do sistema ser falho ou de não saber o que pode ser feito com seu capital aplicado.

É de suma importância o entendimento do tema apresentado contido neste trabalho, para que empresas e pessoas passem a confiar mais nas instituições financeiras e não apenas isso, mostrar que uma boa relação entre bancos e empresas é beneficente para ambos, além de demonstrar os elementos que compõe a segurança bancária.

A partir dos dados apresentados concluímos que é de extrema importância que as instituições financeiras tenham um sistema de segurança 100% seguro ou próximo a 100% mantendo a responsabilidade de qualquer erro de sistema ocorrer, desta forma expressando sua confiabilidade a qual chegamos a observar com as pesquisas realizadas.

5.1 Estudos Futuros:

Considera-se que este estudo possa ser levado em consideração pelo ramo empresarial, para que assim, coloque em práticas os conceitos e dados apresentados neste trabalho. Desta forma os empresários terão uma visão mais ampla relacionados ao sistema de segurança bancário e assim tomar uma melhor decisão sobre a cooperação com instituições financeiras. Como planejamento para contribuir em tal ação, é necessário a colaboração de site importantes e pessoas especializadas no assunto para que a publicação deste trabalho seja realizada e por fim seja utilizada como base para trabalhos futuros de outras escolas ajudando estudantes de curso de administração e ainda poderá servir como estudo para as instituições financeiras publicarem em seus sites. Finalmente, para que seja possível uma visão abrangente, seria importante que os próximos trabalhos sobre o assunto sejam realizados a partir de estudos de caso com maior precisão de dados e mais abrangente envolvendo mais pessoas, pois há muitos estudos sobre este tema em específico a partir de uma abordagem mais prática.

REFERÊNCIAS:

ARAÚJO, Ministro Raul. **Lei do STJ de responsabilidade dos bancos em erros cibernéticos.** Supremo Tribunal de Justiça (STJ). 2024.

BARALDI, Paulo. **Gerenciamento de riscos empresariais.** 3º edição Timburi, São Paulo: Cia do eBook. 2018.

BARROSO, Liliane Cordeiro. **Evolução da tecnologia no setor de segurança bancário.** Fortaleza, Ceará. 2019.

BRASIL, Secretaria de Comunicação Social. **Desenrola Pequenas Empresas já negociou mais de R$ 800 milhões por meio dos bancos públicos.** Governo Federal, Brasília, 2024. Disponível em: https://www.gov.br/secom/pt-br/assuntos/noticias/2024/06/desenrola-pequenas-empresas-ja-negociou-mais-de-r-800-milhoes-por-meio-dos-bancos-publicos. Acesso em: 02 de setembro de 2024.

COSTA, Carlos Arriaga. **Métodos Qualitativos na Análise de Risco de Crédito– Confiança e Credibilidade na Relação entre Bancos e Empresas**. Braga, Portugal. 2003.

DARAME, Celeste Umo. **A percepção dos colaboradores do setor bancário sobre a evolução tecnológica nas suas funções-Estudo de caso do Banco Ideal, SA**. 2023. Tese de Doutorado.

FEBRABAN. **Pesquisa FEBRABAN de Tecnologia Bancária. Empresa FEBRABAN.** 2023. Disponível em: https://portal.febraban.org.br/pagina/3106/48/pt-br/pesquisa. Acesso em: 04 de setembro de 2024.

GOULART, Bruna Joana. **A influência da regulação para a governança corporativa no setor bancário e sua associação com indicadores de desempenho de risco.** Santa Catarina. 2023.

JÚNIOR, Carlos Morais Affonso. **Responsabilidade civil dos bancos virtuais brasileiros nas fraudes envolvendo o furto de senhas eletrônicas. As implicações do desenvolvimento de sistemas de segurança**. São Paulo. 2008

LOPES, Janice Correia da Costa. **Gestão da Qualidade: Decisão ou Constrangimento Estratégico**. Lisboa. 2004.

MARCONI, Maria de Andrade; Lakatos, Eva Maria**. Fundamentos de metodologia científica**. 5º edição, São Paulo: Atlas, 2003.

PEGORARO, Alexandre. **Métodos e ferramentas utilizados na gestão de risco das empresas.** Empresa Kronos**.** 2023. Disponível em: https://kronoos.com/blog/quais-s%C3%A3o-os-m%C3%A9todos-de-gerenciamento-de-risco. Acesso em: 13 de abril de 2024.

PINHO, Carlos. **Risco Financeiro-Medida e Gestão.** 2º edição. Lisboa: Edições Sílabo, 2011.

SEGURIDADE. **Segurança em bancos, confira regras e procedimentos.** Blog da empresa Seguridade. 2018. Disponível em: https://blog.seguridade.com.br/seguranca-em-bancos-confira-as-regras-e-procedimentos/. Acesso em 05 de agosto de 2024.

TOSSIN, Lessandra. **Pedido de indenização por danos morais: Problema crescente no setor bancário.** Porto Alegre. 2007.

VERGARA, Sylvia Constant. **Métodos de Pesquisa em Administração**. 1º edição, São Paulo: Atlas, 2004.

WUST, Ewellyn Fernanda Moura. **Tecnologias práticas comuns de segurança em instituições financeiras**. Naviraí, Mato Grosso do Sul. 2023.