UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO
CURSO DE RELAÇÕES PÚBLICAS

AMANDA BEDRA SERRATT

"JUNTOS, NÓS PROTEGEMOS EM DOBRO": COMUNICAÇÃO DE RISCO NA CAMPANHA AUDIOVISUAL DO ITAÚ UNIBANCO

Porto Alegre
2024

AMANDA BEDRA SERRATT

“JUNTOS, NÓS PROTEGEMOS EM DOBRO”: COMUNICAÇÃO DE RISCO NA CAMPANHA AUDIOVISUAL DO ITAÚ UNIBANCO

Trabalho de Conclusão do Curso de Relações Públicas, a ser apresentado à Faculdade de Biblioteconomia e comunicação da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharela em Relações Públicas.

Orientadora: Prof. Dra. Ana Karin Nunes

Porto Alegre

2024

Amanda Bedra Serratt

“JUNTOS, NÓS PROTEGEMOS EM DOBRO”: COMUNICAÇÃO DE RISCO NA CAMPANHA AUDIOVISUAL DO ITAÚ UNIBANCO

Trabalho de Conclusão do Curso de Relações Públicas, a ser apresentado à Faculdade de Biblioteconomia e comunicação da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharela em Relações Públicas.

BANCA EXAMINADORA:

_____

Prof. Dra. Ana Karin Nunes (Orientadora)

_____

Prof. Dr. Diego Wander Montagner (UFRGS)

_____

Prof. Dra. Denise Avancini Alves (UFRGS)

Porto Alegre, 22 de agosto de 2024.

AGRADECIMENTOS

Aos meus pais, Ivete e João Gilberto, se não fosse pelo incentivo, participação e cobrança, eu não estaria escrevendo esses agradecimentos hoje. Mãe, pela confiança em todas as etapas da minha vida e pelas palavras de afirmação do meu potencial durante esse processo. Como diria Miley Cyrus: “My mama always told me that I'd make it, so I made it". Pai, por ser sempre me incentivar a buscar respostas nos estudos, através principalmente da educação pública e de qualidade.

Ao meu irmão Eduardo, minha madrasta Silvana, minha prima Carol, minha avó Clementina: obrigada por todo apoio e carinho. À minha vó Felomena, que de alguma forma sempre esteve comigo nessa jornada. À minha gatinha Phoebe, meu grude. Ao meu melhor amigo e amor, Arthur, por ter ouvido tanto sobre esse TCC e ter sido obrigado a trabalhar ao meu lado para que eu focasse hahaha. Obrigada por ser você.

Ao meu ciclo de amizades femininas, meu muito obrigada. Tenho orgulho de manter e contar a cada novo ano nosso tempo de amizade: Lilian, Wi, Dani, Mari, Gabs, Isa, Suellen, Nathany. Obrigada por serem essas amigas extraordinárias na minha vida.

Aos profissionais da comunicação com quem compartilhei minha trajetória ao longo da graduação: Bruno, meu primeiro chefe querido e compreensivo; Dani, minha parceira ligeirinha da firma; Renata, meu exemplo de Relações Públicas na prática; Anna, minha dupla de trabalhos e fofocas; Amanda e Vitória, pessoas que tive a sorte de encontrar no começo de tudo.

A todos os meus colegas de trabalho da Axur, que me aproximam da cibersegurança diariamente, mas especialmente à minha chefe Isa: vocês fizeram essa temática ser possível e principalmente, me ensinaram a confiar em mim como uma profissional da área.

À Ana Karin, lembro das primeiras aulas e do desejo de finalizar a graduação como tua orientanda. Você é uma inspiração. Também agradeço a elas que me acolheram e sempre acreditaram no meu potencial: Ana, Denise, Enoí e Helenice.

RESUMO

Este estudo busca analisar a comunicação de risco do Itaú Unibanco no contexto da Segurança da Informação. Os objetivos específicos são: a. compreender as perspectivas teóricas de risco, em especial no ambiente da Segurança da Informação; b. avaliar as características da comunicação de risco usada pelo Itaú Unibanco por meio da campanha audiovisual *Itaú e você contra golpes e fraudes*; e c. discutir as reações à comunicação de risco da campanha. A pesquisa tem carácter exploratório. Quanto aos métodos, utiliza-se de pesquisa bibliográfica e estudo de caso. Na pesquisa bibliográfica foram abordados conceitos e ideias a respeito de risco, percepção de risco, assim como a gestão e comunicação de risco no contexto da Segurança da Informação. O estudo de caso baseia-se no Itaú Unibanco, sendo a campanha *Itaú e você contra golpes e fraudes* o objeto de estudo. A análise se concentrou em identificar as características da comunicação de risco dos seis vídeos bases da campanha no Youtube, bem como as reações através dos comentários. Em relação aos resultados obtidos, observou-se que em sua maioria os conteúdos informam e educam o público quanto aos golpes e fraudes. O formato narrativo se sobressai, justamente porque os riscos que envolvem a Segurança da Informação são relativamente novos e nesse cenário é importante que o público se identifique com o conteúdo. Da mesma forma, o Itaú Unibanco constrói um relacionamento contínuo com seus públicos, visto que os comentários positivos se sobressaem comparação com os negativos.

Palavras-chave: comunicação de risco; segurança da informação; Relações Públicas; Itaú Unibanco.

ABSTRACT

This study seeks to analyze Itaú Unibanco's risk communication in the context of Information Security. The specific objectives are: a. to understand the theoretical perspectives of risk, especially in the Information Security environment; b. to evaluate the characteristics of the risk communication used by Itaú Unibanco through the audiovisual campaign Itaú and you against scams and fraud; and c. to discuss the reactions to the risk communication of the campaign. The research has an exploratory character. In terms of methods, it uses bibliographical research and a case study. The bibliographical research covered concepts and ideas about risk, risk perception and risk management and communication in the context of Information Security. The case study is based on Itaú Unibanco, with the Itaú and you campaign against scams and fraud being the object of study. The analysis focused on identifying the risk communication characteristics of the six base videos of the YouTube campaign, as well as the reaction of the public through the comments. The results showed that most of the content informs and educates the audience about scams and fraud. The narrative format stands out, precisely because the risks involving Information Security are relatively new and in this scenario, it is important that the public identifies with the content. In the same way, Itaú Unibanco builds an ongoing relationship with its audiences, as positive comments outweigh negative ones.

Key words: risk communication; information security; Public Relations; Itaú Unibanco.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O *Global Risks Report 2024* cita ataques cibernéticos em quinto lugar na lista das maiores preocupações e com maiores chances de gerarem crises globais (World Economic Forum, 2024). No que tange aos riscos globais por gravidade no curto prazo, insegurança cibernética encontra-se em quinto lugar (World Economic Forum, 2024). Ainda, projeta-se que o custo global do crime cibernético alcance US$ 9,5 trilhões em 2024. Se fosse considerado um país, o crime cibernético ocuparia a terceira posição entre as maiores economias do mundo, atrás apenas dos Estados Unidos e da China (Cybersecurity [...], 2023).

Com a tecnologia ocupando um espaço crescente na vida dos indivíduos, fraudadores aproveitam para aplicar golpes por meio de compras online, falsas centrais de atendimento, aplicativos de mensagens e outros. Muitas pessoas que antes não utilizavam serviços digitais começaram a fazê-lo por necessidade (alguns processos de atendimentos foram extintos do presencial, por exemplo) ou por preferência (o atendimento e solicitações tende a ser mais rápido no digital), aumentando assim, os acessos e o compartilhamento de dados pessoais, abrindo margem para a ocorrência de fraudes e golpes. Nesse contexto, na cadeia de Segurança da Informação, a parte mais vulnerável é o usuário. Além disso, o uso da inteligência artificial também se mostra um desafio para usuários e organizações, uma vez que ela tende a viabilizar novas formas de fraudes e ataques (Axur, 2023).

O cenário não é diferente no Brasil, onde 80% dos consumidos brasileiros disse ter sido alvo de algum tipo de fraude digital ao menos uma vez (Gonçalves, 2024). Para além, no ano de 2023, os golpes digitais aumentaram em 35% no país, quando comparado ao ano anterior. Os golpes bancários lideram a lista, através principalmente do roubo ou furto de celulares, para posterior acesso aos dados bancários da vítima ou o acesso da conta por meio de ligação telefônica, links fraudulentos (Golpes [...], 2023). Segundo a Federação Brasileira de Bancos (A Febraban, [2024]), existem 155 instituições financeiras em operação no país, enquanto dados do Instituto Brasileiro de Geografia e Estatística (IBGE), em junho de 2022, revelavam que a quantidade de cartões de crédito (190,8 milhões cartões) representava quase o dobro da população economicamente ativa no Brasil (107,4 milhões de pessoas). Para o cenário da Segurança da Informação, essa relação de menos instituições e muitas pessoas economicamente ativas facilita a criação e

proliferação de golpes e fraudes digitais, o que pressupõem certa vulnerabilidade e aumento na produção de riscos. Ainda, conforme pesquisa anual da Proofpoint, 78% das empresas brasileiras tiveram, ao menos, uma experiência de ataque de roubo de dados por e-mail bem-sucedido em 2022, e 23% delas sofreram perdas financeiras como resultado (Hackers [...], 2023).

A justificativa desse estudo se encontra na crescente quantidade de golpes e no fato do Brasil ser o segundo país que mais sofre crimes cibernéticos na América Latina, segundo pesquisa realizada pela SAS Institute (Gonçalves, 2024). Nesse cenário, a comunicação de risco tem um papel crucial em tentar abordar a percepção de um risco para a sociedade. Assim, no meio digital, onde é possível comprar, guardar dinheiro, acessar bancos e armazenar senhas e credenciais na palma da mão, os riscos são vastos e igualmente vulneráveis, uma vez que os potenciais golpes podem vir de ligações, SMS, redes sociais, links patrocinados e e-mails. Para além, os bancos precisam possuir uma relação de transparência e responsabilidade em relação a esses riscos, uma vez que também são produtores deles.

Quanto às motivações pessoais que levaram a esse estudo, a autora, como estudante de Relações Públicas, desenvolveu interesse pelo processo de gestão de risco e crise. Nos últimos anos da graduação, inseriu-se na área da Segurança da Informação, mais especificamente na cibersegurança. Assim, pode entender a dimensão dos riscos referentes a Segurança da Informação no ambiente digital, a relação de conteúdos fraudulentos, tentativas de golpes, páginas de *phishing*[1], demandas de pagamentos para *ransomware*[2]: práticas em que os fraudadores usam normalmente o nome da marca para conseguir algo em troca. Junto disso, o Itaú Unibanco exibiu vídeos da sua campanha relacionada a golpes e fraudes em rede nacional e, depois dele, outros bancos iniciaram um movimento de campanhas sobre golpes ou fraudes. Ao compreender que o setor financeiro é um dos mais atingidos como alvos de fraudadores, por ser cliente do Itaú, e admirar a construção de uma marca brasileira de 100 anos, que é uma referência no setor financeiro privado, é que o Banco foi escolhido pela autora como objeto de estudo.

---

[1] *Phishing* é um tipo ataque que visa roubar dinheiro e/ou identidade, induzindo a revelação de informações pessoais, como números de cartão de crédito, dados bancários ou senhas, em sites que se apresentam como legítimos (O que é [...], c2024).

[2] *Ransomware* é um software de extorsão que pode bloquear computadores e depois exigir um resgate para desbloqueá-lo (Ransomware [...], c2024).

Diante desse contexto, o estudo tem como motivação o problema de pesquisa: quais são os aspectos da comunicação de risco utilizada pelo Itaú Unibanco na campanha *Itaú e você contra golpes e fraudes*?

Para responder a essa questão, foi definido como objetivo geral: analisar a comunicação de risco utilizada pelo Itaú Unibanco, no contexto da Segurança da Informação. Além disso, três objetivos específicos foram estabelecidos: a. compreender as perspectivas teóricas de risco, em especial no ambiente da Segurança da Informação; b. avaliar as características da comunicação de risco usada pelo Itaú Unibanco por meio da campanha audiovisual *Itaú e você contra golpes e fraudes*; e c. discutir as reações à comunicação de risco da campanha *Itaú e você contra golpes e fraudes*.

Para o desenvolvimento do estudo, foram utilizados dois métodos de pesquisa: a pesquisa bibliográfica e o estudo de caso. O primeiro, com base em Stumpf (2005) compreende uma revisão teórica sobre risco e sua gestão, percepção de risco, riscos da Segurança da Informação e comunicação de risco. Já o estudo de caso, a partir de Gil (2002) e Yin (2001), foi aplicado para aprofundar a comunicação de risco no cenário da campanha *Itaú e você contra golpes e fraudes*.

O estudo está dividido em cinco capítulos, constituído primeiramente pela Introdução. O segundo capítulo, apresenta especificamente a construção de risco, sua percepção e os riscos da Segurança da Informação na perspectiva organizacional. Já no terceiro capítulo, o processo de gestão de riscos, comunicação de risco e relacionamento na perspectiva de Relações Públicas são abordados. O quarto capítulo diz respeito à análise do conteúdo, que foi dividido em cinco subcapítulos. Primeiro contempla a metodologia, depois apresenta o objeto de pesquisa, finalizando com a análise e resultados percebidos. Por fim, o quinto capítulo contempla as considerações finais do estudo.

2 RISCO NA PERSPECTIVA ORGANIZACIONAL

Ao longo deste capítulo são apresentados aspectos e contexto histórico do termo risco, suas conceituações no âmbito social e organizacional. Também se aborda a percepção de risco e suas perspectivas teóricas para tratar dos tipos de risco, com foco nos riscos da Segurança da Informação, o qual dá início às discussões sobre a importância desta temática na era digital.

2.1 RISCO

Risco pode ser conceituado como "[...] o potencial de realização de consequências negativas e indesejadas de um evento"[3] (Rowe, 1977, p. 24, tradução nossa). O conceito de risco desde seu surgimento fora atribuído a diferentes áreas do conhecimento. Um dos primeiros registros do uso do termo é da Idade Média, Século XIII, encontrado em um documento italiano, no qual risco estava vinculado a aspectos de navegação em locais rochosos (Villain Gandossi, 1990 apud Rebelo, 2014). Bernstein (1996, p. 08) endossa esse ponto de vista ao revelar que a palavra risco teve origem há cerca de sete ou oito séculos, derivada do termo italiano risicare:

> A palavra 'risco' deriva do italiano antigo risicare, que significa "ousar". Nesse sentido, o risco é uma escolha e não um destino. As ações que ousamos tomar, que dependem da liberdade que temos para fazer escolhas, são a história do risco.

Todavia, até o período que precedia à Revolução Industrial, a ideia de risco era compreendida e gerenciada dentro das manifestações dos deuses, visto que incêndios, inundações, furacões, avalanches, fome e epidemias eram reflexos de manifestação divina, sendo necessário interpretar os sinais sagrados para revelar e prever tais situações (Theys, 1987).

Em contrapartida, a compreensão contemporânea do conceito de risco é derivada da Teoria das Probabilidades, que teve origem na Teoria dos Jogos na França do Século XVII (Douglas, 1987), que significa levar em conta a possibilidade de prever certas situações ou eventos por meio do conhecimento dos parâmetros de uma distribuição de probabilidades dos acontecimentos futuros através do cálculo das expectativas matemáticas (FGV, 1987 *apud* Freitas; Gomez, 1996). Sendo assim,

[3] "The potencial for realization of unwated, negative consequences of an event".

Douglas (1992) considera isso o modelo probabilístico, em que é frequente o desdobramento do risco somente a partir de dois fatores principais: suas probabilidades e consequências.

Posteriormente, a conceituação começou a ser mais utilizada com o fim do feudalismo e início da Revolução Industrial. Naquele momento, os valores sociais começaram a serem considerados para o conceito de risco, e durante esse período houve uma mudança significativa na conversa e na análise sobre risco com a ascensão da perspectiva social, que revela uma visão crítica das ciências sociais em relação à conceituação anterior do risco (Tierney, 1999). Nesse sentido, risco tornou-se um conceito bastante discutido após a Revolução Industrial, já que trata também de um termo relacionado às novas profissões, adventos tecnológicos e produção de riquezas. Nesta perspectiva, Teixeira (2019, p. 24) caracteriza os riscos como "[...] ameaças, cuja consequências são incertas, geradas pelo próprio capitalismo, no desejo de produzir mais e mais, sem ter controle ou não de quais problemas podem decorrer para o mundo". Corroborando teoricamente com esta visão de risco atrelada às riquezas, o sociólogo alemão Ulrich Beck (2010, p. 361) criou o termo sociedade de risco: "[...] o conceito de sociedade de risco expressa a acumulação de riscos – ecológicos, financeiros, militares, terroristas, bioquímicos, informacionais –, que tem uma presença esmagadora hoje em nosso mundo". Sendo assim, segundo Beck (2010), tem-se a sociedade de risco, em que ameaças e riscos em potencial são diminuídos e considerados aceitáveis dentro de um contexto de grandes riquezas, e que a produção dessas riquezas está intrinsecamente relacionada à produção social de riscos, os quais desencadeiam na sociedade moderna ameaças em uma frequência desconhecida. Embora os riscos individuais tenham sido uma constante, a modernidade deu origem a formas inéditas de riscos, completamente diferentes das anteriores; alguns destes novos riscos tornaram-se cada vez mais globais (Areosa, 2010).

Para Beck (1999) a compreensão dos riscos está ligada à história e aos símbolos da cultura em questão. Por esse motivo, a percepção pública e a gestão política dos riscos variam de forma tão distinta em diferentes regiões do mundo. "O conceito de sociedade de risco se cruza diretamente com o de globalização: os riscos são democráticos, afetando nações e classes sociais sem respeitar fronteiras de nenhum tipo" (Guivant, 2013, p. 95). Teixeira (2019) também cita a globalização e os avanços da comunicação – principalmente o advento da internet – como resultados

da produção de novos riscos não mensuráveis. Um exemplo do risco enquanto global e relaciona as nações, refere-se à ameaça de bomba nuclear; e ainda que os riscos estejam mais democráticos, a distribuição social dos riscos permanece desigual. Nesta ótica, segundo Beck (2010), as organizações tornaram-se produtoras e consumidoras das diferentes formas e fontes de risco, as quais é inviável exercer o controle.

Neste viés, as organizações exercem um papel fundamental sob os indivíduos na sociedade atual capitalista e em suas percepções de risco:

> As organizações sonharam com a globalização, aumentaram a escala de produção, estimularam o consumo, multiplicaram seus lucros, e agora, se deparam com a sociedade de risco. Não calcularam que sua produção poderia poluir o meio ambiente e que os recursos naturais ficariam escassos. Não compreenderam que a falta de controle de qualidade afetaria seus lucros e que as crises ecológicas seriam cada vez mais preocupantes aos negócios. Não significa que as empresas agiram maleficamente, mas poucas contemplaram os riscos em seus negócios por se tratar de um assunto novo, que requer atenção (Teixeira, 2019, p. 34).

Uma vez que o risco se tornou um fenômeno socialmente construído e representado, ele pode ser influenciado e moldado por diversas formas de transmissão de informação na sociedade, bem como por diferentes fontes de poder e conhecimento. No que tange à transmissão de informações e conhecimento; acidentes como o de Chernobyl[4] começaram a ter grandes impactos nas mídias, e a partir disso:

> Diferentes partes interessadas passaram a exigir novas regulamentações por parte dos poderes públicos e, das organizações, maior transparência na maneira como os riscos decorrentes de suas atividades deveriam ser gerenciados (Rinaldi; Barreiros, 2007, p. 140).

Dessa forma, a mídia também exerce um papel de influência no que tange ao risco, exercendo poder em cima de organizações e o mesmo acontece ao contrário; por esses motivos, as organizações auxiliam na definição e nas percepções de risco. Rayner e Cantor (1987, p. 8) propõem um "[...] modelo cultural de comportamento de risco institucional", no qual os interesses organizacionais moldam as estimativas de risco e dão origem a conflitos entre os diversos grupos envolvidos no gerenciamento

[4] Um dos maiores desastres nucleares da história. Se trata de uma explosão em um reator em uma usina da cidade de Pripyat em 1986, que gerou diversas consequências para a população e para região. Essa explosão aconteceu devido a desconsideração de algumas normas de segurança que eram essenciais para o bom funcionamento do reator (Siqueira *et al*., 2016).

de riscos. Além do envolvimento em discussões, Johnson e Covello (1987) destacam a importância que os riscos não são apenas determinados por eventos isolados, mas são moldados por uma interação complexa de diversos atores sociais, como grupos emergentes, movimentos sociais, organizações e órgãos governamentais. Esses atores desempenham um papel significativo na caracterização do risco e na seleção de estratégias de gerenciamento. Além disso, como apontado por Fischhoff e Kadvany (2011), os riscos são influenciados pelas instituições sociais, que têm o poder de definir sua natureza e influenciar o processo decisório tanto em nível individual quanto coletivo.

Neste contexto, para além da delimitação, as organizações exercem influência e estabelecem suas vulnerabilidades e ameaças, ou seja, situações viáveis de ocorrerem no âmbito organizacional, como problemas no controle de processos, falhas em sistemas e contaminação de alimentos, por exemplo. A materialização dessas vulnerabilidades pode resultar em crises institucionais, e no contexto organizacional atual, a propagação de uma crise adquire uma dimensão global em questão de minutos (Teixeira, 2019). Além disso, conforme Areosa (2010, p. 68): “No mundo do trabalho não existem organizações ou empresas imunes aos riscos laborais. Em muitas situações os riscos organizacionais são quase inevitáveis”. Sendo assim, fica evidente a importância da relação e definição dos riscos de uma organização, para que ela não passe por crises, já que as mesmas podem ser evitadas ou mitigadas a partir da gestão de riscos. Por vezes, os indivíduos e as organizações selecionam determinados tipos de riscos dentro das suas preocupações e rejeitam outros com magnitude semelhante (Douglas; Wildavsky, 1982); ao não perceber determinados riscos como magnitude semelhante as organizações se põem em risco.

Por outro lado, essa seleção de riscos está também ligada ao fato de os riscos fazerem parte da construção social. Areosa (2010) argumenta que o risco é entendido como um algo carregado de significados, fortemente influenciado por valores e crenças sociais, ou seja, o risco é culturalmente construído. Ele é moldado pelos atores sociais, como as organizações, que desempenham um papel importante na rotina diária dos indivíduos em sociedade e auxiliam na construção e relação com riscos que podem estar relacionados diretamente ao trabalho laboral ou não.

Na percepção de risco individual, Clarke e James (1993) sugerem que as organizações também usam a heurística quando desenvolvem suas posições sobre o risco. Os planos de contingência para eventos de desastre, como grandes

derramamentos de óleo, por exemplo, baseiam-se em cenários de acidentes, que, por sua vez, baseiam-se em análises de risco quantitativas e objetivas. No entanto, ao decidir os tipos de eventos a serem modelados, as organizações preferem cenários fáceis de gerenciar e estimativas de baixo risco, que são usados para justificar as avaliações otimistas correspondentes de sua capacidade de resposta. Isso pode influenciar na compreensão de riscos dos indivíduos eventualmente relacionados à concretização dessas ameaças. De acordo com Beck (1997) a responsabilidade pelos riscos futuros recai sobre os agentes causadores, não sobre aqueles prejudicados e afetados. “Cabe aos causadores apontar os prejuízos que suas empresas podem infligir ao mundo como também as soluções e respostas para tais riscos” (Teixeira, 2019, p. 34). Também é responsabilidade das organizações apontar, direcionar e estudar as ameaças e riscos resultantes de sua atividade; como também informar e instruir seus funcionários quanto a esses riscos.

Portanto, a percepção e gestão de riscos são influenciadas por uma interação dinâmica entre atores sociais e organizações, destacando a importância de uma abordagem integrada no entendimento e enfrentamento dos desafios relacionados aos riscos. Visto que, buscar soluções relacionadas aos riscos tem sido o dever de todos os envolvidos, tanto de empresas, governos, associações e organizações de influência (Teixeira, 2019). Ademais, as organizações são cada vez mais pressionadas a integrar iniciativas que demonstrem sua ética e responsabilidade social em relação a riscos. Conforme Rinaldi e Barreiros (2007) elas precisam integrar em suas estratégias projetos voluntários que demandam uma maior adesão a princípios, os quais possam demonstrar às diversas partes interessadas que sua atuação é ética e socialmente responsável ao enfrentar e lidar com riscos.

Portanto, as conceituações do risco e suas ramificações trazem à tona a influência externa e social na compreensão e gestão dos potenciais ameaças e riscos na sociedade atual após as mudanças na conceituação de risco com a Revolução Industrial, a implementação do sistema capitalismo e das organizações contemporâneas. Nessa perspectiva, destaca-se o papel das organizações na definição de riscos, poder de relações, escolhas e prioridades. Todos esses elementos são fundamentais para abordar a percepção de risco no próximo subcapítulo, destacando também sua influência no social.

2.2 PERCEPÇÃO DE RISCO

A percepção de risco pode ser conceituada como: “[...] conjunto de crenças, atitudes, avaliações e sentimentos das pessoas acerca das situações de perigo e dos riscos a elas associadas” (Pidgeon *et al*., 1992 *apud* Lima, M. L., 1999, p. 381). Quando se trata dos riscos associados, as pessoas precisam ter certa proximidade ou algum conhecimento de determinado risco, para que essa ameaça exista no imaginário.

No que tange à percepção de risco, Renn (2008) evidencia três principais correntes: a psicológica, a cultural e a social. A abordagem psicológica é definida por: “[...] foca nas imagens semânticas, partindo da ideia de que os indivíduos constroem sua própria realidade e avaliam o risco de acordo com suas percepções subjetivas” (Giulio et al., 2015, p. 1220), ou seja, a realidade e instrumentos que se tem no momento de passar por uma situação de risco são os conhecimentos naquela dada ocasião. Portanto, a compreensão de um risco é um processo subjetivo, que também é influenciado por fatores externos, mais especificamente a comunicação referente aquele risco; focando nos métodos pessoais para lidar com incertezas e o contexto em que se encontra. Assim, nessa corrente, ter controle pessoal sobre um risco ou ter mais familiaridade com ele pode diminuir a percepção de risco dos indivíduos (Slovic, 1987; Lupton, 1999). Dessa forma, para Renn (2008), os estudos psicológicos fundamentados em algumas teorias do campo, apesar de suas vantagens, deixam de lado questões sobre quais estímulos sociais ou culturais provocam certos padrões ou porque atributos específicos estão ligados a diferentes tipos de risco.

Por outro lado, a corrente sociológica e cultural, caracteriza-se pelo valor cultural e social nas definições e trocas relacionadas à risco. Essa vertente investiga como os valores orientam julgamentos e comportamentos na percepção do risco. A abordagem também mostra que os riscos refletem valores tradicionais e éticos, influenciando percepções, atuando como filtros de atenção e adicionando um viés emocional no processamento de informações conflitantes sobre o risco (Renn, 2008). Sendo assim, os valores culturais influenciam percepções e comportamentos em relação ao risco, além da dimensão emocional ter uma função crucial no processo de tomada de decisão. Nesta linha, segundo Darley e Latané (1968), mesmo que seja detectado sinalizações de perigo em um local de trabalho, a importância que é concedido depende de fatores sociais; como exemplo, a presença de outras pessoas

realizando um trabalho semelhante leva os indivíduos a categorizarem determinada situação como não perigosa, justamente pela influência do externo.

Um outro ponto relacionado diretamente a essa corrente, trata do saber de peritos e leigos e suas eventuais construções de percepções de riscos. Rovere (2006, p. 29) relaciona os saberes de peritos e leigos:

> O risco pode ser percebido pelos peritos e tecnocratas de forma divergente dos leigos. Os peritos e tecnocratas avaliam e gerenciam os riscos como processos objetivos e racionais, já para os leigos a percepção é obtida nas evidências disponíveis. A percepção social do risco é de suma importância, pois é fundamental que se estude qual a percepção da sociedade a respeito do risco que está exposta, pois nem sempre a percepção da sociedade corresponde com o que ocorre de fato.

Ou seja, ambos conhecimentos acerca dos riscos precisam ser considerados em uma análise. Ainda assim, não é necessário considerar o saber perito superior ao leigo são construções diferentes, mas relacionados ao mesmo objetivo de estudo. Por outro lado, é importante ser crítico na diferença dessas percepções:

> A antropóloga Mary Douglas, maior expressão dessa abordagem, ao apontar que as análises de risco, conduzidas pelos peritos e usadas para estipular os limites daquilo que seriam ou não riscos aceitáveis, não eram racionais não só mostrou que não existiam elementos lógicos nessas técnicas de avaliação, como também trouxe à tona o relativismo cultural, questionando a razão moderna e a fé cega na autonomia dos cientistas e dos peritos na tomada de decisões sobre os riscos que as pessoas poderiam ou não correr (Douglas, 1966; Lupton, 1999 apud Giulio *et al*., 2015, p. 1221).

Em síntese, Mary Douglas (1966) introduziu a dimensão cultural no discurso sobre risco, demonstrando que a percepção e as respostas aos riscos são moldadas pela organização sociocultural de um grupo. Sendo assim, relativo aos riscos vale concentrar-se no papel da cultura como intermediária entre ação e conhecimento, examinar a construção simbólica do significado do discurso e das narrativas, e entender os riscos como experiências pessoais concretas, enfatizando, desse modo, as questões morais e as dinâmicas de poder relacionadas a esses riscos e a construção de suas percepções. A percepção de risco do leigo e dos cientistas tende a divergir, pois este último tem como julgar tomando como base técnicas e estatísticas, enquanto o leigo não subjugado a estes parâmetros toma como base uma variedade de aspectos díspares da visão matemática, portanto valendo-se de outros valores como os aspectos subjetivos (Fischhoff *et al*., 1978). Um exemplo disto é a percepção de risco ao comparar uma pessoa que anda de avião mensalmente e outra que anda

diariamente de ônibus e a possibilidade de acontecer um acidente. Muitos tendem a perceber o risco com base na possibilidade de um evento catastrófico, por isso afirmam que quem utiliza o ônibus diariamente está menos exposto nessa situação, mas a probabilidade de um acidente aéreo é menor do que a de um acidente rodoviário. Dessa forma, para o público leigo cabe a informação acerca do risco para que a percepção da sociedade seja correspondem com o que de fato acontece, como reforça Rovere (2006, p. 32): “Quanto mais se obtém conhecimento de determinada informação, mais se desfaz dos preconceitos e crenças obtidos ao decorrer da vida e se aproxima mais do risco real que se está exposto”.

Neste viés, as organizações têm um papel fundamental, já que “[...] as percepções de risco constroem em função do grau de confiança que o público tem nas instituições responsáveis pela administração e gestão do risco” (Giulio *et al*., 2015, p. 1220). Sabe-se que, ao informar, as organizações lidam como emissores da percepção de risco e diretamente constroem direcionamentos sobre riscos relacionados a sua atuação:

> A relação entre emissor e receptor [...] passa pela percepção de risco e, portanto, depende da percepção do receptor quanto ao grau de risco representado por uma ameaça, seja ela diretamente ligada aos atos da empresa (emissão de poluentes, barulho etc.) ou uma consequência de tais atos (novas pessoas na comunidade, desvalorização de imóveis etc.). O mesmo vale para se salientar fatores de risco relacionados a doenças. (Batista, 2007, p. 103)

Na elaboração e disseminação de informações, os indivíduos atuam como receptores, variando em seu nível de criticidade ao receber a informação. No entanto, o processo de percepção de risco e essa criticidade são influenciados pela relação entre o indivíduo e o emissor, onde as organizações atuam como emissores e interagem com seus públicos, os receptores. Relacionado a isto, Douglas e Wildavsky (1982, p. 79-80, tradução nossa) comentam sobre a função das organizações na construção destas percepções:

> Na percepção de risco, os humanos agem menos como indivíduos e mais como seres sociais que internalizaram pressões sociais e delegaram seus processos de tomada de decisão às instituições. Eles lidam tão bem quanto o fazem, sem conhecer os riscos que enfrentam, seguindo regras sociais

> sobre o que ignorar: as instituições são seus dispositivos de simplificação de problemas[5].

Os julgamentos do público sobre risco e segurança não se desenvolvem no vazio: pelo contrário, o público é influenciado por estratégias organizacionais que buscam enquadrar os riscos de maneiras que beneficiam os atores corporativos e institucionais (Heimer, 1988 *apud* Tierney, 1999). Portanto, a percepção do público sobre os riscos e eventuais ameaças muitas vezes reflete não apenas a realidade objetiva dos riscos, mas também as narrativas e molduras fornecidas pelas organizações interessadas e envolvidas.

Ademais, Carochinho (2011) estabelece sob estudos da percepção de risco três dimensões multidimensionais de análise: o grau de informação acerca do risco, o grau de controle possível sobre o risco e o grau de envolvimento pessoal com o risco. Na linha de informações compartilhadas sobre riscos, a abordagem da Amplificação Social do Risco (SAR – Social Amplification of Risk), cujos principais enfoques são a percepção e a comunicação de risco, pressupõe que a percepção de risco é principalmente influenciada pela forma como é transmitida pela mídia e outras fontes. Examinar como essas informações são passadas poderia elucidar a amplificação ou redução das preocupações relacionadas a um determinado risco (Pidgeon; Kasperson; Slovic, 2003).

Além disso, "[...] é importante ressaltar que é a partir da percepção que vai se dar a comunicação de risco, por isso é necessário saber qual a percepção social do risco para que se possa ter maior efetividade na comunicação de risco" (Rovere, 2006, p. 30).

Em suma, as construções das percepções de riscos passam por muitos filtros sociais. Dentre eles, ressalta-se o papel das organizações nessa percepção, as quais são influentes e possuem interesses particulares nessa estrutura junto aos seus públicos. Para que essa construção ocorra, a comunicação de risco precisa ser pautada pelos responsáveis, de forma planejada e responsável. Por outro lado, são diferentes os tipos de riscos e este também é um fator que influência em sua

---

[5] "In risk perception, humans act less as individuals and more as social beings who have internalized social pressures and delegated their decision-making processes to institutions. They manage as well as they do without knowing the risks they face, by following social rules on what to ignore: institutions are their problem-simplifying devices".

percepção e construção. Por esse motivo, os riscos referentes a Segurança da Informação serão abordados a seguir.

2.3 RISCOS DE SEGURANÇA DA INFORMAÇÃO

Os riscos relacionados à Segurança da informação são diversos e a cada ano a importância de abordá-los fica mais evidente. Anualmente, o World Economic Forum lança o *Global Risks Report*[6], no qual são apresentados cenários e percepções de risco no contexto global. Nos últimos três relatórios (World Economic Forum, 2022, 2023, 2024), riscos relacionados à Segurança da Informação aparecem no ranking entre os dez primeiros. Em 2022, falha na segurança cibernética apareceu em sétimo lugar dentro do ranking dos riscos que pioraram desde a crise da Covid-19. Ainda, quanto a Riscos globais classificados por gravidade no curto prazo (2 anos) no relatório de 2022, falha na segurança cibernética também está em sétimo. Já no *Global Risks Report 2023*, na classificação dos riscos considerados mais graves e que poderiam impactar a nível global, ataques cibernéticos em infraestrutura crítica consta em quinto lugar, e relacionado aos riscos por gravidade em curto prazo, crimes cibernéticos e insegurança cibernética está em oitavo lugar.

Por outro lado, o *Global Risks Report 2024* cita ataques cibernéticos em quinto lugar quando relacionado como uma das maiores preocupações e com maiores chances de estarem ligados a crises globais ainda neste ano. No que tange aos riscos globais por gravidade no curto prazo, no primeiro lugar está desinformação e no quinto insegurança cibernética. Cabe citar que, nos relatórios anteriores, riscos relacionados a tecnologia também aparecerem, mas foram nos últimos anos que a incidência relacionada a diferentes riscos da tecnologia foi mais evidenciada, principalmente após o contexto e resultados da pandemia de Covid-19. A partir do ano de 2020 notou-se um aceleramento do uso de muitos recursos digitais e, por consequência, o digital está cada dia mais presente na vida das pessoas.

Outro aspecto destacado pelo *Global Risks Report 2024* abrange as preocupações quanto às notícias falsas e inteligência artificial. Mesmo sendo um risco separado do conceito de risco dos ataques cibernéticos, é um tópico interligado ao

[6] A principal fonte de dados do *Global Risks Report* é originada da Pesquisa de Percepção de Riscos Globais (GRPS) do World Economic Forum. Em 2024, o GRPS reuniu as principais percepções sobre o cenário de riscos globais de 1.490 especialistas do meio acadêmico, empresarial, governamental, comunidade internacional e da sociedade civil (World Economic Forum, 2024).

contexto da tecnologia, já que também pressupõe a utilização de ferramentas de inteligência artificial para articular novas formas de ataques e fraudes no ambiente digital (Axur, 2024). Nesta linha, os riscos relativos ao ramo da tecnologia são vários. A Segurança da Informação abrange uma ampla variedade de áreas, resultando em uma pluralidade de riscos e ameaças, como exemplos os mencionados anteriormente: falhas na segurança cibernética, ataques cibernéticos à infraestrutura crítica, crimes cibernéticos e insegurança cibernética. Essa diversificação também se reflete nos diversos desdobramentos decorrentes da materialização desses riscos, o que ocorre devido à amplitude da gestão da Segurança da Informação. Segundo a norma da ABNT NBR ISO/IEC 27002:2013:

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos (ABNT, 2005).

Sendo assim, o escopo da Segurança da Informação passa pela segurança digital (armazenamento de informações, criptografia de dados, proteção digital, sistemas operacionais etc.), mas também a segurança física responsável por sistemas para acessos a locais físicos (catracas, serviços de biometria e captura de faces, transferência física de mídias, segurança de recursos humanos), por exemplo. Deste modo, conforme Marciano e Marques (2006) a segurança permeia as arquiteturas e modelos da informação, incorporando-se em todos os seus níveis. Além disso, com o uso e dependência da tecnologia, o número de ocorrências de incidentes relativos à segurança da informação cresce: 1) fraudes digitais: vazamentos de senhas e dados; 2) malwares como ataques de ransomware: forma de ciberataque em que os invasores infectam os sistemas de computadores ou redes e bloqueiam o acesso aos dados ou sistemas; e outras formas de ameaças. Todas essas se encontram na abrangência da segurança cibernética ou cibersegurança. Neste viés, cabe trazer a conceituação de insegurança cibernética do *Global Risks Report* (2024, p. 98, tradução nossa):

> Uso de armas e ferramentas cibernéticas para conduzir guerra cibernética, ciberespionagem e crime cibernético para obter controle sobre uma presença

> digital e/ou causar interrupção operacional. Inclui: ransomware, fraude ou roubo de dados[7].

Atualmente, devido a todos os agentes envolvidos tanto na gestão quanto na produção de riscos, a incerteza e o surgimento de novas formas de riscos são constantes. Segundo Areosa (2010), estas novas formas de risco apresentam-se como dificuldades acrescidas ao entendimento humano, quer pelo desconhecimento sobre elas, quer pela falta de experiência em lidar com essas situações. Determinados tipos de risco constituem-se como um território inexplorado ou desconhecido para a humanidade. Logo, os riscos da área da Segurança da Informação podem ser percebidos e enquadrados neste novo território para indivíduos e organizações, pois são riscos novos, bastante técnicos e com resultados não tão claros junto aos públicos. Com relação à área da Segurança da informação, Marcos Sêmola (2013, p. 18) a classifica relacionando-a com a gestão de riscos: "[...] E para gerir riscos é preciso conjugar vários verbos: conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar são apenas alguns deles". A partir deste ponto, o autor compara e traz apontamentos quanto aos riscos organizacionais. Segundo ele, na figura de um correntista, há pouco tempo era necessário se dirigir a uma instituição financeira para realizar eventuais movimentações em conta, visto que as informações estavam centralizadas e acessíveis apenas no local de atendimento. Esta centralização traz maior controle e segurança, ou seja, menos risco. Por outro lado, atualmente as movimentações bancárias podem ser realizadas sem necessidade de deslocamento físico, através de smartphones ou computadores. Sendo assim, para Sêmola (2013, p. 7) o grau de risco dessas alterações trata de algo jamais visto:

> Notadamente, essas novas e modernas condições elevam o risco das empresas a níveis nunca antes vividos, fazendo-as perceber a necessidade de ações corporativas integradas em busca de mecanismos de controle que permitam reduzi-lo e torná-lo administrável e viável.

Em suma, trata-se de mudanças consideráveis na rotina de indivíduos e das organizações, as quais ocorrem de forma bastante rápida e constante, sendo necessário organização e planejamento para lidar com os novos riscos que são resultados das novas tecnologias e suas aplicações. Sêmola (2013) reforça que é

---

[7] "Use of cyber weapons and tools to conduct cyberwarfare, cyberespionage and cybercrime to gain control over a digital presence and/or cause operational disruption. Includes: ransomware, data fraud or theft".

impossível uma organização operar com risco zero, mas que é importante considerar as variáveis internas e externas para viabilizar a operação, entre as quais a cibersegurança. Nesta perspectiva, segundo relatório da Axur (2024) existe um movimento de integrar os riscos cibernéticos ao risco das organizações. Essa movimentação aparecia brevemente em ações passadas, mas atualmente reforça ainda mais a importância na dimensão econômica organizacional, especificamente quando um eventual ataque para uma organização por um grande período ou gera multas por vazamento de dados, além dos danos e prejuízos relacionados à reputação e confiança dos públicos.

Os crescentes riscos de tópicos da tecnologia, mais especificamente da Segurança da Informação dos últimos anos, reforçam a necessidade de identificar esses riscos, gerir e comunicá-los. Assim sendo, na gestão e comunicação de riscos relacionados à Segurança da Informação são concebidas e percebidos de forma diferente devido a recente introdução deles na sociedade moderna, principalmente no que tange aos riscos de cibersegurança, os quais resultam da ampliação da tecnologia no dia a dia dos indivíduos. Por esses motivos, gestão de risco e comunicação de risco serão tópicos abordados ao longo do próximo capítulo neste viés da Segurança da Informação.

3 GESTÃO E COMUNICAÇÃO DE RISCO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo, o conceito de gestão de risco organizacional, bem como seu processo serão apresentados. Além disso, regras e normas da International Organization for Standardization (ISO) e toda relação de gestão de riscos e a Segurança da Informação pertinentes para o processo da comunicação de risco nessa área.

3.1 GESTÃO DE RISCO: PROCESSO E NORMATIVAS

A gestão de risco tem um papel crucial principalmente no cenário organizacional. Ao observar riscos, o gerenciamento precisa ser organizado e previsto:

> O processo de gerenciamento de riscos gera informações que permitem ao tomador de decisão melhor compreender os riscos existentes e seus possíveis impactos, possibilitando às organizações alternativas para minimizar perdas e identificar oportunidades (Rinaldi; Barreiros, 2007, p. 140).

Relativo à reputação das organizações, o gerenciamento de riscos é mais do que uma prática técnica. Ele também incorpora valores e ideais, entre eles responsabilidade e prestação de contas (Power, 2004). Todavia, a junção e relação direta entre gerenciamento de riscos e organizações como tem-se atualmente, é algo relativamente novo em termos científicos e profissionais. Segundo Otway (1985) é apenas na década de 1980, do Século XX, que a análise e a gestão de riscos surgem enquanto campo científico e profissional. Por outro lado, para Power (2004) é no ano de 1995 (o ano do colapso do banco Barings[8] e da crise da instalação de Brent Spar para a Shell[9]), que ser uma organização competente e qualificada tornou-se sinônimo de ter um programa de gerenciamento de riscos. A análise de riscos foi incluída dentro de uma estrutura maior de responsabilidade e controle a partir daquela época. Desde

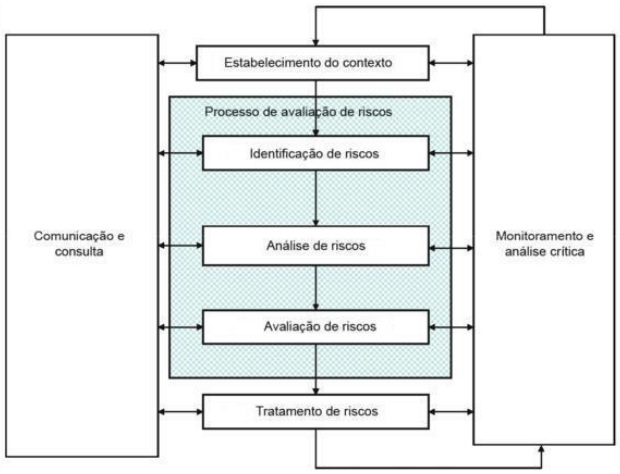
[8] Barings Bank (1762-1995) foi a companhia de banco de investimento mais antiga de Londres, Inglaterra, até seu colapso em 1995, quando um dos empregados do banco, Nick Leeson, perdeu US$ 1,4 bilhão em especulação primariamente em contrato de futuros (Barings [...], 2019).

[9] Brent Spar era uma instalação de reserva de petróleo operada pela Shell UK. O reservatório foi retirado de utilização em 1991. O fato teve grande repercussão junto ao público em 1995, quando o governo britânico anunciou o seu apoio aos planos da Shell, de inutilizar o equipamento, afundando-o a 2,5km de profundidade no oceano Atlântico (Brent [...], 2023).

então, existe a percepção de que uma organização considerada competente precisa estar alinhada com a adoção dessas práticas de gestão.

Ademais, as normas da International Organization for Standardization (ISO10) são bases importantes no processo de gerenciamento de riscos. Cabe citar quatro delas, as quais são norteadoras na área da Gestão de Riscos e da Segurança da Informação: 1) a ISO 31000, norma que estabelece princípios e orientações em relação ao gerenciamento de riscos; 2) a ISO 27001, padrão para sistemas de gerenciamento de Segurança da Informação; 3) a ISO 27002, norma para estabelecer, implementar e melhorar um Sistema de Gestão de Segurança da Informação focado em segurança cibernética; e 4) a ISO 27005, padrão que orienta sobre gerenciamento de riscos de Segurança da Informação. Cabe destacar que a ISO/IEC 27005:2023 deriva de várias normas, sendo uma delas a própria ISO 31000:2018, tendo inclusive passado por uma atualização no ano de 2023 para alterar e seguir o padrão de terminologia e o conteúdo da norma ISO 31000:2018 (ISO, 2018a). Nesse viés, o gerenciamento de riscos na perspectiva da ISO 31000 se dá conforme a Figura 1. Vale citar que o mesmo fluxograma também faz parte do processo da ISO 27005 (ISO, 2018b) focada na Gestão de Riscos da Segurança da informação.

Figura 1 - Processo de gestão de riscos ABNT



Fonte: ABNT NBR ISO 31000:2009 (ABNT, 2009).

[10] A ISO, International Organization for Standardization (Organização Internacional de Padronização), reúne especialistas globais para chegar a um acordo sobre a melhor maneira de fazer as coisas, desde a fabricação de um produto até o gerenciamento de um processo. Como uma das mais antigas organizações internacionais não governamentais, a ISO tem possibilitado o comércio e a cooperação entre pessoas e empresas em todo o mundo desde 1946 (ISO, [2024]).

Sendo assim, o processo de gerenciamento de riscos na conjuntura da ISO 31000 compreende:

1. A comunicação e consulta de riscos;
2. Estabelecimento do contexto;
3. Identificação de riscos;
4. Análise de riscos;
5. Avaliação de riscos;
6. Tratamento de riscos; e
7. Monitoramento e análise crítica de riscos.

O processo conforme a ABNT (2009) inicia e continuamente retorna para a etapa de comunicação e consulta durante as fases da gestão de riscos. Ela precisa estar disponível para as pessoas interessadas, sejam elas internas ou externas. Os planos de comunicação e consulta necessitam abordar as causas dos riscos, suas consequências e quais ações tomar para tratá-los. A comunicação e consulta compreendem os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas. Por isso, faz parte de todo o processo e continuamente é necessário voltar para essa etapa, além de reforçar que as partes interessadas estejam inteiradas sobre esses fundamentos e decisões. Sendo assim, durante todo fluxo e processo da etapa, é necessário para além dos pontos já citados: 1) assegurar que os riscos sejam identificados adequadamente; 2) agrupar diferentes especialistas para análise dos riscos e assegurar que diferentes pontos de vistas sejam considerados na definição dos critérios de riscos e na avaliação dos mesmos; e 3) desenvolver um plano para comunicação e consulta interna e externa. Por fim, esse fluxo também se mostra contínuo justamente pelas diferentes percepções de riscos das distintas pessoas envolvidas no processo de gestão de riscos. Dessa forma, as partes interessadas participam do processo de tomada de decisão e continuamente retomam para essa fase.

Posteriormente, cabe estabelecer a etapa de contexto, assim a organização relaciona seus objetivos de negócio e define parâmetros externos e internos que precisam ser considerados ao gerenciar os riscos, como ambiente cultural, social, legal, regulatório, financeiro e o ambiente cultural, sistemas de informação, fluxos de informação e tomada de decisão, dentre outros. Convém que a gestão de riscos seja realizada com plena consciência de sua necessidade e dessa forma, participação das partes interessadas, para participar de atividades como definição dos responsáveis

pelo processo de gestão de riscos, definição de metodologias de processos para a avaliação dos riscos, especificação de ações e decisões a serem tomadas. Considerar esses e outros fatores relevantes pode ajudar a garantir que a abordagem escolhida para a gestão de riscos seja adequada às circunstâncias, à organização e aos riscos que impactam o alcance de seus objetivos.

Já na etapa de identificação dos riscos, as organizações precisam definir as fontes de riscos, áreas de impactos, eventos, ativos, suas causas e consequências em potencial, a fim de gerar uma lista com todos os eventuais riscos que possam reduzir, aumentar, acelerar ou atrasar a realização dos objetivos do negócio. Nessa etapa é preciso que todos os riscos, de forma bastante abrangente, sejam listados.

Na análise de riscos cabe verificar as estratégias e métodos mais adequados para o tratamento de riscos. Esta é uma espécie de entrada para as próximas fases e para a tomada de decisão, sendo necessário identificar causas, fontes e consequência dos riscos. A análise dos riscos pode ser qualitativa, quantitativa, semi qualitativa ou quantitativa, ou até mesmo uma combinação das duas. Por outro lado, a avaliação de riscos é a continuidade da análise dos riscos, a partir dela, avalia-se os riscos, que precisam ser tratados imediatamente, quais as escalas de prioridade de cada risco, e toda a definição de priorização para um processo de tratamento ser implementado, vale aqui reforçar que as decisões tomadas precisam seguir requisitos legais.

A partir da avaliação, a fase de tratamento de riscos inicia-se e, nela, as escolhas de quais riscos serão modificados e quais as implementações para as devidas modificações. No processo de modificação dos riscos também há alteração dos controles de riscos. Todavia, o processo de tratamento em si consiste na avaliação do tratamento de riscos que já são realizados, avaliação e decisão se os riscos residuais são toleráveis, caso não sejam, é necessário definir e implementar um novo tratamento e por fim, avaliar a eficácia desse tratamento escolhido. Escolher a alternativa mais apropriada para o tratamento de riscos requer equilibrar os custos e os esforços de implementação com os benefícios resultantes, considerando requisitos legais, regulatórios, além de considerar fatores externos, como a responsabilidade social.

Ademais, como última etapa tem-se o monitoramento e análise crítica. É recomendado que eles sejam integrados ao processo de gestão de riscos, incluindo verificações ou auditorias regulares a esses processos e etapas, mas também cabe a esta etapa garantir que os controles sejam eficazes no projeto e na operação da

gestão de riscos. Assim, o ciclo e as etapas da gestão de riscos são todos abordados e concretizados, tratando-se de um fluxo contínuo.

Já na perspectiva da Segurança da Informação, a gestão dos riscos tem um papel relacionado aos acessos físicos e digitais. Conforme citado por Sêmola (2008, p. 55): “[...] a gestão de riscos é uma extensão natural da responsabilidade da gestão da segurança da informação nas organizações”. Isto reforça o fato de a conceituação de gestão de risco comumente ser vinculada à área de Segurança da Informação. Além disso, a gestão de riscos nessa área tem o impacto de fortalecer a segurança de um sistema. Um sistema seguro é aquele que tem a segurança de continuar operando conforme suas especificações, mesmo diante de eventos adversos resultantes da interação com agentes mal-intencionados ou de ocorrências naturais ou ambientais. Para uma organização, segurança implica manter a realização de seus objetivos de negócio, mesmo diante de situações adversas (Fernandes, 2011). Dessa forma, cabe gerir os diferentes acessos físicos, como portões eletrônicos e acessos virtuais, quais pessoas podem acessar a plataformas de dados de uma empresa e até mesmo quais programas são baixados por funcionários, visto que alguns podem conter vírus. Esses são exemplos de alguns ativos que precisam ser considerados na gestão de riscos. Por isso, as organizações ou indivíduos precisam compreender os riscos presentes em seu ambiente de ativos de informação e como esses riscos podem ser reduzidos ou até eliminados. A gestão de risco deve ser um processo contínuo e proativo, visando estabelecer e manter um nível aceitável de segurança para o sistema de informação. Após atingir um nível adequado de segurança, o processo de gestão de risco monitora os riscos nas atividades diárias, seguindo os resultados da análise de risco de segurança e são os resultados da gestão de risco que constituem a base para descrever o estado atual da segurança de uma organização (Gouveia, 2016).

Após a análise de abordagens do processo de gestão, avança-se para uma discussão mais específica sobre comunicação de risco, uma das etapas da gestão que necessariamente é constante e demanda de estratégias para ser efetiva. Além disso, a implementação de técnicas adequadas de comunicação pode melhorar significativamente a capacidade da organização de responder e lidar com os riscos, a fim de minimizar os impactos negativos. Portanto, entender e aplicar práticas eficazes de comunicação de risco é um componente importante para o sucesso da gestão de riscos como um todo.

3.2 COMUNICAÇÃO DE RISCO

A comunicação de risco pode ser conceituada no contexto da Segurança da Informação como: “Um processo interativo de troca de informações e opiniões com as diferentes partes interessadas, compreendendo múltiplas mensagens sobre a natureza dos riscos e a maneira como são identificados, analisados e gerenciados” (Série Risk Management, 2005, p. 14).

O processo de gestão de risco, como comentado é contínuo, e por ele perpassa a comunicação. Isso é reforçado por Rinaldi e Barreiros (2007), quando defendem que a comunicação de risco possui um aspecto técnico e precisa ser considerada dentro do conjunto de ações e decisões das organizações. Segundo os autores, a comunicação de risco é um instrumento que pode ajudar o gestor a fornecer às partes interessadas mais transparência sobre como as organizações lidam com os diversos riscos decorrentes de suas atividades. Neste contexto, a comunicação de risco se entrelaça com as percepções de risco dos públicos, tornando essencial promover a interação com as diversas partes interessadas para evitar que divergências na percepção desses riscos compliquem a gestão organizacional. Batista (2007) afirma que a etapa da comunicação de risco se refere a um campo onde os estudos começaram devido ao interesse em transmitir informações técnicas para públicos leigos, destacando o papel da mídia nessa transmissão de conhecimento. Portanto, a comunicação deve estar sempre alinhada com os públicos para evitar percepções divergentes dentro da organização, pois em momentos de crise, o repasse incorreto de informações pode agravar a situação. Todavia, através do processo de comunicação de risco, os gestores conseguem evidenciar diferentes vulnerabilidades, facilitando a gestão eficaz dos riscos e assim as crises podem ser amenizadas, e principalmente, compreendidas dentro de um fluxo intenso como os de crise.

A comunicação de risco também pode ser compreendida pelo seu conteúdo, formato e objetivos. Dessa forma, para Covello, Slovic e Winterfeldt (1986) os objetivos da comunicação de risco são quatro e, baseado em uma reinterpretação da autora, eles podem ser relacionados com a Segurança da Informação:

1. Informação e educação. Informar e educar as pessoas em relação a um risco e a sua avaliação. Exemplos podem ser informativos sobre a existência de golpes, como o golpe do WhatsApp [11] ou o golpe da maquininha[12];
2. Mudança de comportamento e ações de proteção. Encorajar menos exposição a um risco, como as mensagens de alertas dos programas de antivírus, os quais sinalizam download suspeitos. Outro exemplo são os informativos visuais da força de senhas ao cadastrar uma nova senha de acesso (sendo normalmente vermelha para informar que a senha está fraca, amarela ou laranja intermediária e verde a senha é considerada forte para determinado sistema);
3. Alertas de desastres e informações emergenciais. Fornecer orientação em desastres e emergências; como os alertas de exposição e vazamentos de credenciais, que reforçam a necessidade de alterar uma senha que foi exposta em um grande vazamento de dados;
4. Resolução conjunta de problemas e conflitos. Envolver o público na tomada de decisões sobre gerenciamento de riscos e o envolver em discussões sobre saúde, segurança e meio ambiente. Por fim, este objetivo está relacionado a postura de uma organização em relação a gestão de seus riscos de Segurança da Informações e eventuais ações junto aos públicos, como espaços para troca de conhecimento virtuais ou presenciais sobre o tópico da cibersegurança, bem como alertas e informações sobre mudanças em políticas de privacidades de aplicativos.

Por outro lado, quando a finalidade da comunicação de risco é gerar atenção a um problema, Batista (2007) cita que comunicação de risco pode ser usada para as seguintes situações:

1. Alerta de um perigo presente com o objetivo de proteção imediata. Um exemplo seria os avisos e bloqueios sobre a eventual presença de vírus quando um novo programa é instalado em um computador;

---

[11] Nesse golpe, o criminoso cria um perfil falso no WhatsApp com fotos roubadas e finge ser o usuário, pedindo que amigos e parentes apaguem o número antigo. Depois, começa a pedir dinheiro com desculpas para as transferências (Golpe [...], c2024).

[12] O golpe da maquininha envolve o golpista usando a máquina de cartão de crédito para cobrar valores excessivos ou clonar o cartão do consumidor, sem que ele perceba (Golpe [...], 2024).

2. Alerta de problemas contínuos, como casos de sites falsos, com o objetivo de phishing[13]. Bastante comum com marcas do varejo, por exemplo, as marcas deste segmento tendem a alertar continuamente sobre;
3. Prevenção de problemas a fim de aumentar a percepção de risco. Um exemplo pode ser relacionado a importância de atribuir diferentes senhas a diferentes acessos virtuais.

Quando o objetivo principal é gerar atenção, não basta somente informar, "[...] a informação tem que ser acessível, isto é, entendida e aplicável ao processo de decisão ao mesmo tempo em que está presente na mente do receptor" (Batista, 2007. p. 106). Sendo assim, é crucial ativar a preocupação no público através do conteúdo da comunicação, uma das formas é gerando identificação com a mensagem exposta. Relativo ao conteúdo e ao formato da comunicação, a informação técnica aumenta a confiabilidade de uma informação e é considera útil no inicial, quando é necessário chamar atenção para um problema (Golding; Krimsky; Plough, 1992). Por outro lado, conforme Batista (2007), o formato narrativo aproxima o leitor e o traz para o processo da representação, mantendo a atenção ao problema. Sendo assim, cabe utilizar dados e estatísticas um em processo informativo técnico quando a informação for comunicada pela primeira vez, por outro lado, para reforçar a comunicação o formato narrativo se mostra mais eficaz. No que tange a mudanças no comportamento frente aos riscos, o indicado é focar em perdas, já para comportamentos em que o risco não está presente, o foco em ganhos pode ser mais assertivo.

Portanto, a comunicação de risco precisa ser pensada e planejada após o devido conhecimento dos públicos e de suas percepções em relação aos riscos de determinada organização. Nesse sentido, o relacionamento com as organizações e as trocas que elas criam com seus públicos são estratégias complexas que agregam na facilitação e no fluxo da própria comunicação de risco entre emissor e receptor. Assim sendo, a perspectiva de Relações Públicas auxilia na construção desses relacionamentos e em suas interações.

[13] Phishing é um tipo ataque que visa roubar dinheiro e/ou identidade, induzindo a revelação de informações pessoais, como números de cartão de crédito, dados bancários ou senhas, em sites que se apresentam como legítimos (O que é [...], c2024).

3.3 COMUNICAÇÃO DE RISCO E RELACIONAMENTO NA PERSPECTIVA DE RELAÇÕES PÚBLICAS

A comunicação de risco, para ser efetiva, necessita de um processo apurado tanto para seu planejamento, quanto para sua divulgação, e tudo isso passa pelo conhecimento quanto ao público-alvo dessa comunicação. Consequentemente, torna-se necessário a realização de uma boa gestão do relacionamento entre os públicos. A atividade de Relações Públicas desempenha um papel específico nesse processo:

> As organizações mais eficazes confiavam nas relações públicas para auxiliar e estabelecer quais públicos de interesse lhes eram estratégicos e então auxiliar a desenvolver relacionamentos estáveis e dignos de crédito com esses públicos. [...] Relacionamentos com tanta qualidade apenas existem quando a organização reconhece a legitimidade dos públicos, ouve suas preocupações e lida com as consequências negativas que possam causar a esses públicos (Grunig, 2009, p. 45).

Atender, ouvir e acompanhar os públicos de uma organização são algumas das tarefas das Relações Públicas que fortalecem os relacionamentos, e justamente junto às percepções de riscos que uma organização pode gerar, esses pilares da profissão se tornam ainda mais relevantes. Ao construir um relacionamento de troca entre os públicos de interesse de uma organização, como os clientes, por exemplo, pode-se gerar confiança e priorização, tanto do lado da organização quanto do público. Por sua vez, a comunicação de risco quando criada pelo emissor (organização) e transmitida para o receptor (cliente), na perspectiva da construção de relacionamentos em Relações Públicas, pode ser mais assertiva, visto que o emissor conhece qual mensagem (e como) essa mensagem deve ser transmitida, assim o receptor tem mais chances de a captar, visto que há confiança na organização devido ao relacionamento.

Neste viés, para Andrelo (2016) o relacionamento entre organização e públicos deve ser sólido e por isso, constantemente gerido, já que o advento da Internet trouxe rapidez na circulação de mensagens e um maior número de interações. Visto que antes do surgimento da Internet, no contexto organizacional, predominava a comunicação de massa e a linguagem publicitária. Clientes, comunidade, fornecedores e outros públicos, conheciam a organização pelo que ela desejava que fosse conhecido através desses recursos. Por outro lado, devido às mudanças que o acesso à Internet trouxe, as pessoas comuns ampliaram o acesso à informação e a possibilidade de expressão dentro das diferentes redes sociais e canais. Os públicos

se expressam diretamente com as marcas, sem a necessidade de mediadores ou sem se tratar de um fluxo amplamente conhecido e planejado, como o da comunicação de massas. Sendo assim, os relacionamentos são expandidos com a Internet, tanto em número de canais quanto em número de assuntos que uma organização pode e deve gerir junto aos seus públicos.

Reforça-se que a prática das Relações Públicas também precisa ser uma via de mão-dupla, ou simétrico de duas mãos, conforme conceituado por Grunig (2005), que representa um dos possíveis modelos das Relações Públicas, em que se busca um equilíbrio entre os interesses da organização e os de seus públicos. Nele, se utiliza a comunicação para administrar conflitos, e assim melhorar o entendimento com públicos estratégicos. Há um engajamento nas trocas entre a organização (emissora ou fonte) e os públicos (receptores) (Andrelo, 2016). Nessa perspectiva, os efeitos e mudanças esperadas quando da implementação de uma via de mão-dupla são:

- A exposição torna-se consciência mútua. A gestão e o público estão cientes do impacto que exercem um sobre o outro, estando cientes da influência recíproca que exercem. Uma campanha de cibersegurança pode ser pega como exemplo. Essa campanha foca na comunicação de risco e alerta clientes sobre alguns riscos digitais, especialmente os riscos de usar a mesma senha para diferentes contas bancárias e serviços financeiros. A organização (nesse caso um banco) realiza alguns eventos, em que os clientes escutam sobre os perigos, mas também compartilham suas experiências com a reutilização de senhas e outros problemas que enfrentaram no meio digital. Isso cria uma consciência mútua onde tanto o banco, quanto os clientes estão cientes da influência recíproca que suas ações e comportamentos têm sobre a segurança das contas bancárias e financeiras;
- A retenção da mensagem torna-se precisão. Ambos conseguem lembrar exatamente o que o outro disse. Seguindo com o exemplo mencionado, durante a campanha, o banco envia e-mails com resumos e dicas de segurança para seus clientes. Através de um formulário sobre o evento, a organização analisa se os clientes se lembram das recomendações específicas sobre segurança de senhas. A precisão é alcançada quando ambos (banco e clientes) se recordam dos pontos discutidos e as ações recomendadas para proteger seus acessos financeiros;

- O efeito do conhecimento transforma-se em entendimento. Ambos possuem conhecimentos semelhantes sobre um problema, questão ou propósito da organização. A campanha termina e após todas as trocas de conhecimentos, os clientes de fato criam senhas distintas para diferentes acessos a serviços financeiros. Ambos os lados, banco e clientes, compartilham um conhecimento semelhante sobre a importância das práticas de segurança cibernética;
- O efeito na atitude transforma-se em concordância. Ambos possuem avaliações semelhantes sobre o que a organização ou o público desejam e pretendem agir de modo a fortalecer o relacionamento. Após participar do evento, os clientes expressam que compreende a necessidade de usar senhas diferentes como uma prioridade. O banco e os clientes estão de acordo sobre a importância desta prática para melhorar a segurança das contas e informações financeiras;
- O efeito no comportamento transforma-se em comportamento simbiótico. Ambos agem de forma a atender aos interesses do outro, bem como aos seus próprios. O banco implementa uma ferramenta gratuita que ajuda os clientes a criar e gerenciar senhas únicas para cada conta. Os clientes adotam essa ferramenta e começam a aplicá-la em seu cotidiano, enquanto o banco continua a fornecer suporte e atualizações para melhorar a experiência do usuário. Além disso, durante as atividades da campanha, a organização encontra outros tópicos a serem trabalhados a partir de problemas que os clientes compartilharam e dessa forma, a organização planeja e segue promovendo novas práticas de segurança com seus públicos de interesse.

Sendo assim, os relacionamentos gerenciados pelas Relações Públicas podem ter como objetivo essa construção de engajamento mútuo entre os públicos. Além disso, nessa definição de Grunig (2005) a ética também é citada e precisa ser considerada como parte do papel de Relações Públicas, inclusive a proximidade com a responsabilidade social que se dá ao longo da avaliação e análise dos riscos de uma organização:

> Sabe-se que os cidadãos estão cada vez mais conscientes de seus direitos e que movimentos sociais exigem mais transparência, visando uma comunidade sustentável, apoiada no relacionamento ético. Além de bons preços e prazos, é preciso ter valores agregados para ganhar espaço em um mercado cada vez mais competitivo. É preciso ter credibilidade e, para obtê-

> la, conceitos como responsabilidade e transparência são fundamentais (Ferrari, 2009 *apud* Andrelo, 2016, p. 24).

Para além do fluxo de comunicar acerca de um risco em específico, a profissão de Relações Públicas ao construir esses relacionamentos pode trazer os públicos para debate a fim de identificar o que é mais assertivo em determinado contexto, até mesmo durante a etapa de monitoramento e análise crítica dos riscos ao longo do processo de gestão de risco. Inclusive, a ISO 31000 (ISO, 2018a) pode ser também uma das fontes para conferência no que tange as ações de comunicação no contexto de riscos organizacionais. Ainda assim, a certificação é apenas uma das referências para checagem de informações e eventuais direcionamentos, cabe citar que a certificação não é comum no Brasil, visto que apenas seis empresas brasileiras são certificadas com a ISO 31000[14]. Em contraste, a ISO 27001, padrão para sistemas de gerenciamento de Segurança da Informação**,** é relativamente mais comum, contando com 110 empresas brasileiras certificadas[15].

Já quanto ao correto seguimento em termos legais e responsáveis de uma organização, também é uma possibilidade para o profissional de Relações Públicas tentar construir uma postura de responsabilidade e transparência no contexto organizacional:

> A comunicação se torna um fator fundamental nesse processo, pois o risco, ao se transformar em tema de discussão e reflexão na organização, abre a possibilidade para o debate, o diálogo, a negociação e, por fim, para a busca de soluções, ou ao menos para tentativa de se elaborar medidas de precaução (Texeira, 2019, p. 31).

Sendo assim, ao longo do fluxo apresentado de gestão de riscos, e por toda contextualização da importância da comunicação nele, o Relações Públicas é um dos profissionais que pode criar os laços entre os públicos de uma organização, além de manter e fortalecê-los. Para além do contexto da comunicação em termos gerais de uma organização, Fernandes (2011) reforça sobre o papel da profissão no campo da Segurança da Informação:

---

[14] As organizações são a Biocor Instituto (Hospital), a UPA de Imbiribeira (Unidade de Pronto Atendimento), a Oncomed (Clínica hospitalar), a Faelba (Previdência complementar), a Forluz (Previdência complementar) e a Petros (Previdência complementar) (ISO, 2018a).

[15] Destaque para alguns bancos brasileiros que possuem a certificação citada em seus sites, sendo eles o Itaú Unibanco, Bradesco, Banco do Brasil e BTG Pactual (D'Addario, 2020).

> Diferentes planos de comunicação do risco devem ser desenvolvidos para os casos de operação da organização sob condições normais e quando a mesma está operando em modo de emergência ou crise. É importante, sobretudo, estabelecer um canal de informações sobre riscos com a área de relações públicas da organização, especialmente durante emergências ou crises (Fernandes, 2011, p. 50).

Dessa forma, o próprio fluxo da gestão de riscos e todas suas especificidades mostra-se multidisciplinar, mas com eventuais saldos positivos quando com uma comunicação bem administrada pelas Relações Públicas, visto que essa é uma das profissões responsáveis por informar os públicos de interesse sobre os riscos que uma organização pode gerar, além de manter a comunicação direcionada e próxima, a fim de realizar constantes trocas e interações e, nesse ambiente pode-se estabelecer um relacionamento sólido entre públicos e organização.

4 SEGURANÇA DA INFORMAÇÃO, COMUNICAÇÃO DE RISCO E ITAÚ UNIBANCO

Ao longo desse capítulo são apresentados os procedimentos metodológicos, os quais serviram de base para este estudo. Além disso, nessa seção, são realizadas as análises relacionadas ao objeto de pesquisa, com vistas a responder aos objetivos propostos para o estudo.

4.1 METODOLOGIA

Este estudo é caracterizado como descritivo e exploratório. Segundo Gil (2002), as pesquisas descritivas visam principalmente descrever as características de um fenômeno específico ou estabelecer relações entre variáveis. Já as pesquisas exploratórias, de acordo com Gil (2002, p. 41): "[...] têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses". Esta pesquisa é considerada exploratória na medida em que releva os aspectos da relação da comunicação de risco, da Segurança da Informação e da instituição financeira brasileira Itaú Unibanco.

Os métodos de pesquisa aplicados são a pesquisa bibliográfica, com base em Stumpf (2005), e estudo de caso, na perspectiva de Gil (2002) e Yin (2001). Além das técnicas de análise documental (Gil, 2002) e análise de conteúdo (Bardin, 1977).

Primeiramente, a fim de conceituar risco e seus desdobramentos na perspectiva organizacional, realizou-se a pesquisa bibliográfica a partir de livros e artigos científicos. Ela foi necessária para aprofundar mais os conhecimentos sobre risco na perspectiva da Segurança da Informação, o contexto da percepção de risco, o processo de gestão de riscos e a comunicação de risco. A pesquisa bibliográfica, segundo Stumpf (2006), é o passo inicial de todo e qualquer trabalho acadêmico a fim de planejar, organizar, para identificação, localização e exploração de uma bibliografia referente ao assunto abordado, passando pela seleção das informações mais relevantes e finalizando com o objetivo de evidenciar, em um texto estruturado, entendimento e ideias da literatura pesquisada, juntamente com as ideias e opiniões dos autores.

Quanto ao objeto de pesquisa, a organização Itaú Unibanco e o seu processo de comunicação de risco no contexto da Segurança da Informação foram escolhidos

para o estudo de caso. Para Yin (2001 *apud* Gil 2002, p. 54), o estudo de caso é “[...] o delineamento mais adequado para a investigação de um fenômeno contemporâneo dentro de seu contexto real, onde os limites entre o fenômeno e o contexto não são claramente percebidos”. Dessa forma, o estudo de caso, no contexto dessa pesquisa, é utilizado a fim de resolver os objetivos do estudo, os quais cabe serem citados novamente: a. compreender as perspectivas teóricas de risco, em especial no ambiente da Segurança da Informação; b. avaliar as características da comunicação de risco usada pelo Itaú Unibanco por meio da campanha audiovisual *Itaú e você contra golpes e fraudes*; e c. Discutir as reações à comunicação de risco da campanha *Itaú e você contra golpes e fraudes*.

Para a coleta de dados sobre o objeto de estudo, realizar a pesquisa foi utilizada a técnica de pesquisa de análise documental, que a qual, para Gil (2002, p. 45), “[...] vale-se de materiais que não receberam ainda um tratamento analítico ou que ainda podem ser reelaborados conforme os objetivos da pesquisa”. A análise documental se concentrou em informações oriundas do fez parte da etapa de conferência do site do Banco brasileiro, de suas redes sociais (Facebook e Instagram). Além disso, também foram coletadas informações a partir de vídeos no Youtube do Itaú Unibanco.

Por fim, adota-se, como técnica de análise dos dados coletados, a análise de conteúdo. Bardin (1977, p.31) explica que esta consiste em “um conjunto de técnicas de análise das comunicações, que utiliza procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens”. Além disso, a autora salienta que essa técnica permite, através de uma leitura atenta, descobrir

> [...] conteúdos e de estruturas que confirmam (ou informam) o que se procura demonstrar a propósito das mensagens, ou pelo esclarecimento de elementos de significações susceptíveis de conduzir a uma descrição de mecanismos de que a priori não tínhamos a compreensão (Bardin, 1977, p. 29, grifo do autor).

Sendo assim, a análise de conteúdo lida com mensagens com o objetivo de encontrar indicadores e apontamentos que através do enriquecimento de uma leitura (e análise) atenta, aumenta a produtividade e pertinência dessa compreensão. Essa técnica é utilizada para categorizar e analisar seis vídeos da campanha audiovisual *Itaú e você contra golpes e fraudes*, os quais foram vinculados ao canal no Youtube do Itaú Unibanco ao longo dos anos de 2022 e 2023. Os comentários e curtidas

também serão considerados. Além das informações apresentadas na página intitulada *Segurança* do site do Banco.

Para fins de análise, definiu-se três categorias para classificação do conteúdo, em consonância com o que foi produzido durante a pesquisa bibliográfica. São elas: 1) objetivos da comunicação de risco: a fim de identificar qual a principal estratégia de cada conteúdo segundo classificações de Covello, Slovic e Winterfeldt (1986); 2) características da mensagem de comunicação de risco: compreender se os conteúdos contém um viés mais narrativo ou técnico conforme conceituação de Batista (2007); e 3) engajamento e relacionamento com os públicos: analisar a relação entre o conteúdo apresentado e os comentários de percepções compartilhadas por Andrelo (2016), Grunig (2005), Rovere (2006), Teixeira (2019) e outros.

4.2 ITAÚ UNIBANCO

A história do Itaú Unibanco é resultado de uma série de aquisições de instituições financeiras e fusões, segundo informações de seu site institucional. Fundado em 1924 por Alfredo Egydio de Souza Aranha, o Banco Itaú iniciou na cidade de Poço de Caldas no estado de Minas Gerais. Inicialmente, era chamado de Casa Moreira Salles. Em 2008, o Itaú e o Unibanco anunciam sua fusão, criando o Itaú Unibanco Holding S.A., o maior conglomerado financeiro do hemisfério sul (Kodic, 2023). Com a fusão, a marca Unibanco foi extinta gradativamente e a instituição passou a utilizar exclusivamente a marca Itaú. Atualmente o Banco está presente em 32 países (Perdil [...], 2024), emprega 85 mil funcionários no Brasil (Sindicato dos Bancários, 2023) e conta com cerca de 3.000 agências brasileiras (Itaú [...], 2022). Referente ao público externo, o Itaú Unibanco é o terceiro maior banco do Brasil em número de clientes com 99 milhões (Nubank [...], 2023) e o segundo maior em valor de mercado – US$ 56 bilhões – (Nubank [...], 2024). Ademais, cabe citar que ao longo dos últimos anos o número de agências e funcionários estão diminuindo frente a digitalização da instituição, que estima que 80% das transações de seus clientes sejam realizadas no ambiente digital e pretende implementar um plano de modernização de atendimento até 2025 (O Globo, 2023).

Assim sendo, e considerando os objetivos deste trabalho, vale mencionar a apresentação do Banco no ambiente digital, principalmente no que tange a Segurança da Informação. A organização possui um site e rede sociais (Instagram, Facebook,

Twitter ou X e Youtube) com diferentes estratégias comunicacionais. No final de 2023 passou por uma mudança de marca, com destaque para o logotipo e *slogan*, que passaram de três cores (laranja, azul e amarelo) para duas (laranja e branco) e mudou de *Itaú feito para você* para *O Itaú é feito de futuro*, conforme Figura 2, demostrando aspectos relacionados aos objetivos de modernização citados.

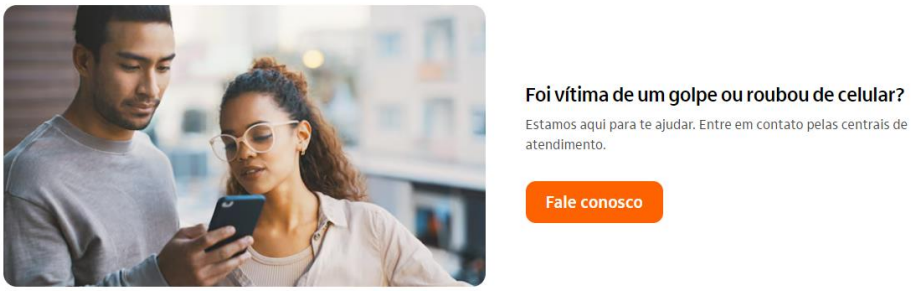
Figura 2 - Logotipo e *slogan* antigos (à esquerda) e atual (à direita) do Itaú Unibanco

Fonte: Logotipo [...] ([2024]).

O ambiente digital com mais conteúdos relativos à Segurança da Informação trata-se do site. Nele, o Itaú Unibanco apresenta que seu propósito é estimular o poder de transformação das pessoas e a visão é ser o banco líder em performance sustentável e em satisfação dos clientes. No rodapé do site do Itaú existe o subtítulo *Ajuda*, com direcionamento para página de título *Segurança*.

A página *Segurança* possui uma série de conteúdos e direcionamentos focados na Segurança da Informação, a primeira e maior delas é em relação ao auxílio para vítimas de golpes ou roubo de dispositivos móveis (Figura 3). Conforme mencionado por Marciano e Marques (2006) a segurança permeia todos as possibilidades e níveis de um Sistema da Informação, e com cada vez mais pessoas utilizando esses recursos, existem mais indivíduos expostos, logo o correto direcionamento para os devidos canais de atendimento da organização é um passo para garantir as possíveis ações de bloqueio de processos virtuais e físicos.

Figura 3 - Direcionamento para página de atendimento em caso de golpe ou roubo de celular



Fonte: Itaú [...] (c2023).

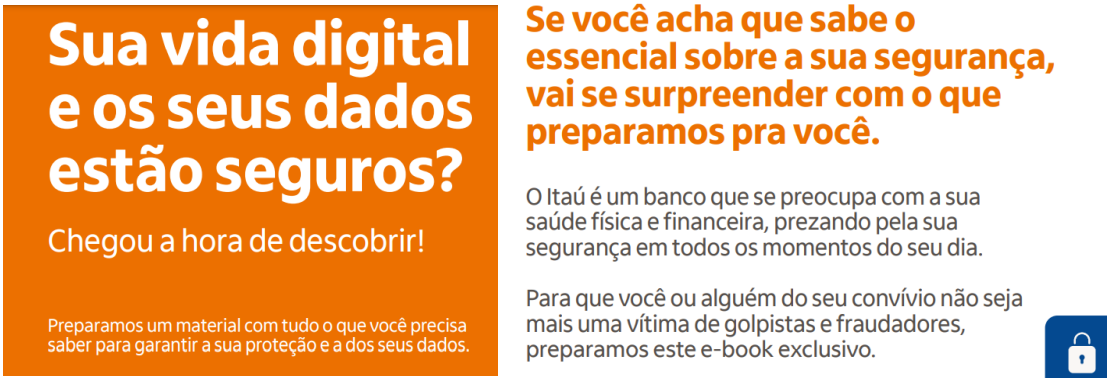
Além disso, a página tem uma série de conteúdos sobre funcionalidades para aumentar a segurança no ambiente digital e como se proteger e identificar tentativas de golpes (golpes com cartões, golpes com falsos funcionários, golpes no WhatsApp, golpes em rede sociais, golpes na internet). Conforme mostra a Figura 4, as capas são estruturadas de forma semelhante, assim como os conteúdos que contam com breves explicações sobre os tipos de golpes e dicas de segurança. No caso dos golpes com cartões, por exemplo, tem-se a citação dos diversos golpes que envolvem cartões físicos, a explicação de um golpe específico, como o do motoboy em formato de vídeos por fim, formas de proteção são citadas. A insegurança cibernética reportada no *Global Risks Report 2024* pode ser relacionada com a quantidade de informações acerca dos diferentes golpes e formas de proteção, já que a aplicação de cada um e as formas de se proteger são diferentes. Do ponto de vista da gestão de riscos, a responsabilidade da gestão de Segurança da Informação fazer parte e ser uma extensão natural da responsabilidade das organizações (Sêmola, 2013).

Figura 4 - Conteúdos sobre diferentes tipos de golpes

Fonte: Itaú [...] (c2023).

Dentre as informações apresentadas, destaque para o conteúdo com o título *Saiba como se proteger* que direciona para um *e-book* de quarenta e duas páginas focado em dicas para proteção de dados (Figura 5). Os assuntos e informações abordados no *e-book* são um aglomerado de diferentes instruções, as quais também são apresentadas na página *Segurança*, como o que fazer caso seja vítima de um golpe, o que o banco nunca faz, o uso de senhas, informativos sobre golpes. Essa integração de conteúdo pode ser considerada como ação para controlar e administrar riscos, conforme mencionado por Marcos Sêmola (2013). Sêmola (2013) cita que os graus de risco da Segurança da Informação são inéditos, elevando os riscos das organizações a níveis nunca vistos, o que exige organização para torná-los administráveis.

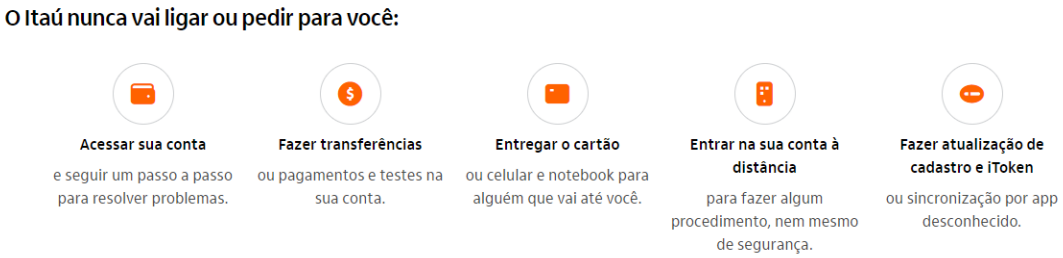
Figura 5 - *E-book* dicas de segurança Itaú Unibanco



Fonte: Itaú ([2024]).

Já para o fim da página, o Banco faz o uso do imperativo com o termo “nunca” deixando claro que tais ações não serão realizadas pelo Itaú Unibanco (Figura 6). Como Areosa (2010) afirma que as novas formas de risco são difíceis de entender devido ao desconhecimento e à falta de experiência, sendo um território inexplorado para a humanidade. Sendo assim, conteúdos e termos no imperativo e, portanto, mais diretos, facilitam a compreensão de ações e atitudes que o Banco não vai realizar. Inclusive, as ações descritas na Figura também são tópicos abordados na campanha audiovisual *Itaú e você contra golpes e fraudes* analisada posteriormente nessa seção.

Figura 6 - Página *Segurança* do site do Itaú Unibanco



Fonte: Itaú [...] (c2023)

Para além dos conteúdos, no fim da página, o Banco direciona o contato para o endereço emailsuspeito@itau-unibanco.com.br, caso alguém identifique uma página ou e-mail suspeito fazendo o uso de marca do Itaú Unibanco, reforçando a importância do controle e administração pelas organizações mencionado por Sêmola (2013). Ademais, o Itaú Unibanco no final da página *Segurança* de seu site (Itaú [...], c2023) com o subtítulo *Mantemos seus dados seguros*, apresenta a certificação ISO 27001:2022: reforçando o compromisso com a Segurança e Privacidade da Informação de seus clientes. Assegura, através das normas ISO 27001:2022 e da ISO 27701:2019, que seus processos de governança de Segurança da Informação e seus processos de governança de tratamento de dados pessoais, estão em conformidade com os requisitos das normas e certifica esse escopo conforme atestado pela Fundação Vanzolini (Itaú [...], c2023). É relevante relacionar a exposição das certificações com o que é reforçado por Otway (1985), que destaca a percepção de que uma organização considerada competente precisa estar alinhada com as práticas de gestão, como as práticas e normas da ISO. O site, ao abordar os certificados ISO, também direciona para versão em pdf de ambos, os quais foram emitidos em janeiro de 2024.Todas essas ações e conteúdos produzidos pelo Itaú Unibanco acerca de golpes e fraudes reforçam que a produção de riquezas está relacionada à produção social de riscos, os quais desencadeiam na sociedade atual ameaças em uma frequência desconhecida (Beck, 2010).

Além disso, conforme citado, o Banco realiza produções audiovisuais a fim apresentar conteúdos sobre Segurança da Informação em subpáginas de Segurança, mas também na rede social Youtube, a qual está fixada no rodapé do site do Itaú Unibanco. Portanto, este estudo analisará seis vídeos da campanha *Itaú e você contra*

golpes e fraudes[16] publicada na rede social Youtube ao longo de 2022 e 2023. A campanha está dentro da playlist no Youtube chamada Juntos, nós protegemos em dobro e conta com trinta vídeos. Sendo vinte e dois vídeos da campanha *Itaú e você contra golpes e fraudes* produzida pela Agência África. O conteúdo dos vídeos menciona golpes e fraudes bancárias e retratam situações cotidianas sobre o tema em um contexto casual retratado por três diferentes atores. Cabe citar que as produções audiovisuais dessa campanha também foram vinculadas na televisão em canais abertos (Lima, K., 2022).

A campanha totaliza 22 vídeos. Deste total, 06 deles são os vídeos originais (versão estendida) e 16 vídeos são versões reduzidas dos originais (versão com conteúdo acessível e divisão do vídeo original em dois – um que apresenta o golpe e outro que explica o golpe). Ou seja, foram selecionados os seis vídeos originais (versão estendida), pois são as bases da campanha. Esses 06 vídeos foram analisados ao longo dos meses de junho e julho de 2024, nas seguintes categorias: 1) objetivos da comunicação de risco; 2) características da mensagem de comunicação de risco; e 3) engajamento e relacionamento com os públicos. A seguir, apresenta-se a análise de cada categoria.

4.3 OBJETIVOS DA COMUNICAÇÃO DE RISCO

A fim de atingir os objetivos dessa pesquisa foram definidas três categorias de análise, com base na bibliografia desenvolvida. A primeira corresponde aos objetivos da comunicação de risco em cada um dos seis vídeos da *campanha Itaú e você contra golpes e fraudes*. São observados os aspectos comunicacionais no que tange ao geral de cada produção audiovisual, a fim de classificar seus objetivos e características.

O primeiro vídeo lançado em agosto de 2022 tem de título *Como se Proteger do Golpe da Troca de Cartão*. Nele, a atriz explica sobre como funciona o golpe da troca de cartão, comentando sobre o risco e o passo a passo de funcionamento desse golpe. Cita, principalmente, o porquê cortar o cartão ao meio não é suficiente:

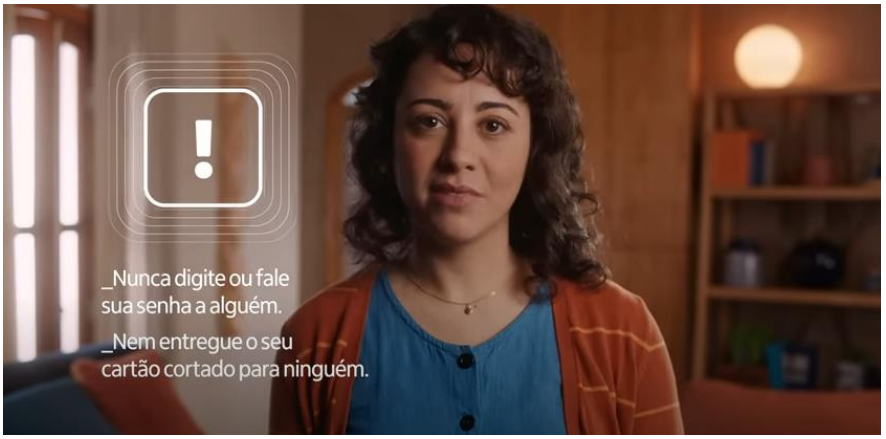
> Primeiro o golpista liga se apresentando como funcionário do banco ou do cartão de crédito. [...] Então ele pede para que você corte o cartão ao meio e diz que em breve um portador vai até a sua residência para retirar esse cartão cortado. O detalhe é que mesmo cortando o cartão, o *chip* segue intacto e é

[16] A nomeação *Itaú e você contra golpes e fraudes* trata-se da campanha, enquanto Itaú Unibanco e Banco são utilizados para se referir a instituição financeira comumente conhecida como Itaú.

> justamente com o *chip* mais a senha que eles fazem compra com o cartão (Itaú, 2022a).

Sendo assim, os fraudadores conseguem utilizá-lo em compras junto com a informação de senha digitada no teclado. Por isso, conforme a Figura 7, o vídeo atenta o receptor da mensagem para que o cartão cortado não seja entregue para ninguém. Assim, o conteúdo resume um assunto mais técnico (a função dos *chips* em cartões) na explicação do porquê cortar o cartão ao meio não é suficiente. Vale destacar que, conforme Rovere (2006), a percepção de risco para pessoas leigas é obtida através das evidências disponíveis. Nesse caso, a evidência é que mantendo o *chip* os fraudadores ainda poderão fazer o uso do cartão. Dessa forma, o vídeo classifica-se em um dos quatro objetivos da comunicação de risco citados por Covello, Slovic e Winterfeldt (1986), o de informar e educar, visto que educa principalmente sobre o não compartilhamento de senhas, sobre o processo de não entregar para ninguém cartões cortados ao meio. Além disso, informa as etapas comuns relativas a esse golpe.

Figura 7 - Como se proteger do golpe da troca de cartão



Fonte: Itaú (2022a).

Na mesma linha, o segundo vídeo, intitulado *Como se Proteger do Golpe da Falsa Central*, também de agosto de 2022, menciona o passo a passo do golpe da falsa central e quais itens normalmente os fraudadores solicitam:

> [...] E que para bloquear o seu cartão imediatamente ele precisa do seu número do cartão, do seu código de segurança, sua senha e seu *itoken*. Se você repassar esses dados, ele sim é que vai fazer compras usando seu cartão (Itaú, 2022b, grifo nosso).

O texto deste vídeo e os itens que o autor menciona estão diretamente ligados aos apontamentos da página *Segurança* no site do Itaú Unibanco, que informa o que o Banco nunca vai pedir: “Por isso, nunca fale ou digite os números do seu cartão nem a sua senha para ninguém que ligue falando que é do Itaú, isso daí é golpe! Nenhum funcionário do Banco ou do cartão vai pedir isso para você.

A mensagem principal está nos itens que os fraudadores podem solicitar, e logo após a frase informativa de que nenhum funcionário do Banco ou do cartão vai pedir tais informações para o cliente. O uso do imperativo reforça a mensagem principal do vídeo que está dentro do objetivo de informar e educar quanto os riscos dessas solicitações de prováveis golpistas. Inclusive, as instituições, como o Itaú Unibanco, têm o poder de definir a natureza e importância de um risco, influenciando no processo decisório (Fischhoff; Kadvany, 2011) e o uso do termo nunca, bem como a construção da narrativa, a qual reforça para o receptor (cliente do Banco) que o Itaú Unibanco não liga ou manda mensagem solicitando número de cartão e senha, demonstra que no processo de gestão de riscos, a instituição Itaú Unibanco constrói esse ambiente a fim de influenciar os receptores no processo decisório.

A terceira produção audiovisual da campanha tem como título *Como se Proteger do Golpe do WhatsApp*, de agosto de 2022. Mostra um passo a passo de como acontece o golpe e o que fazer caso um cenário semelhante esteja acontecendo, conforme a Figura 8. Assim, além de explicar como é abordagem, informa sobre situação em torno do golpe do WhatsApp:

> Aí ele cria uma conta no aplicativo de mensagens com a foto de uma pessoa conhecida, mas com um número diferente de celular. Ele avisa os contatos que trocou de número e aborda alguns deles dizendo que está com problema financeiro ou com a conta bloqueada e que precisa de uma transferência com urgência (Itaú, 2022c).

Diferente dos outros golpes e conteúdos, nesse caso pode ser que de fato algum conhecido realmente tenha mudado de número e esteja solicitando dinheiro. Por esse motivo, o contato síncrono com a pessoa via ligação aparece como uma ação de proteção, a fim de identificar o risco antes de tomar uma ação (Figura 8). Aliás, essa chamada para ação vai ao encontro com a percepção de risco de Renn (2008), quando argumenta que os valores culturais influenciam nas percepções e comportamentos frente ao risco, inclusive a dimensão emocional tem uma função crucial no processo de tomada de decisão. Nessa linha, a solicitação e necessidade

de dinheiro de uma pessoa conhecida ou próxima se relaciona com a dimensão emocional e eventual urgência em tomar uma ação (transferir dinheiro) para ajudar o outro. Todavia, o conteúdo direciona e sugere que o contato com a pessoa que está solicitando dinheiro seja feito por ligação.

Por fim, o vídeo termina com a frase “desconfie: pediu dinheiro emprestado no WhatsApp pode ser golpe”, ou seja, diferente dos outros vídeos já analisados, o verbo “desconfiar” prevê as ações de proteção citadas. Desta forma, essa produção audiovisual possui dois objetivos ao longo da comunicação de risco dos quatro propostos por Covello, Slovic e Winterfeldt (1986): informar e educar quanto às mudanças no comportamento e ações de proteção.

Figura 8 - Como se proteger do golpe do WhatsApp

Fonte: Itaú (2022c).

O vídeo chamado *Golpe da Troca do Cartão*[17] foi publicado em fevereiro de 2023. O ator comenta uma conversa durante uma ligação sobre como é o *modus operandi* do golpe: “Você vai pagar alguma coisa na rua, dá o cartão, bota a senha. Daí te devolvem outro cartão parecido, sem você perceber e usam o seu cartão para fazer compras com a sua senha” (Itaú, 2023a).

Assim sendo, o ator explica como funciona o golpe em etapas. Em poucos segundos, também explica o que o salvou do golpe:

> Ator 1: Você sabe quem me salvou?
> Ator 2: Quem?
> Ator 1: A princesa do cabelo azul.
> Ator 2: *Hã?*

[17] O terceiro vídeo da campanha se chama Golpe da Troca do Cartão e o primeiro Como se Proteger do Golpe da Troca de Cartão. Nomeações similares, mas cada vídeo traz um golpe diferente.

> Ator 1: É o adesivo que a minha filha colou no cartão. É inconfundível (Itaú, 2023a).

Depois da conversa telefônica, o vídeo traz uma condicional que chama a atenção “[...] sempre confira o seu cartão depois de pagar. Se trocarem, é golpe” (Itaú, 2023a). Essa frase reforça o papel das organizações na construção da percepção de risco dos clientes, já que é uma simplificação do problema (se trocarem o cartão, possivelmente trata-se de um golpe). Isso relaciona-se com o que Douglas e Wildavsky (1982) citam sobre os indivíduos que delegam processos de tomada de decisão às instituições.

Em suma, o vídeo informa sobre o funcionamento desse golpe, e inclusive também sugere o uso de um adesivo especial, como uma forma de proteção (Figura 9). Encaixa-se, assim, nos objetivos de informação e educação e mudanças de comportamento e ações de proteção (Covello; Slovic; Winterfeldt, 1986).

Figura 9 - Sugestão de uso de adesivo especial no cartão

Fonte: Itaú (2023a).

Já no início vídeo de título *Golpe do Falso Funcionário*, de fevereiro de 2023, fica exposto a abordagem para a aplicação do golpe:

> Ator: Aqui é do banco e vimos o agendamento de uma transação suspeita no valor de 4 mil reais. Ele é seu?
> Atriz: 4 mil reais?
> Ator: Para que essa transação seja cancelada é necessário que você entre no aplicativo do banco e siga o caminho que eu vou te falar agora (Itaú, 2023b).

Logo, em seguida, a atriz traz uma metalinguagem do Itaú Unibanco, quando menciona que o comercial do Banco informou ela e o golpista não terá sucesso com

o golpe: “Atriz: *Ah*, justo agora? No intervalo do jornal? [risos]. Você não tá com sorte, acabou de passar o comercial do Itaú contra golpes e fraudes” (Itaú, 2023b).

Nessa perspectiva, o uso da metalinguagem pode ser enquadrado em um processo que busca beneficiar os atores corporativos e institucionais no processo de gerenciamento de riscos (Heimer, 1988 apud Tierney, 1999). Visto que, o julgamento quanto aos riscos dos públicos e as suas percepções não se desenvolvem sozinhos, instituições como o Itaú Unibanco auxiliam nessa construção e podem inclusive se beneficiar dela. Ao abordar assuntos de golpes como o indicado nesse vídeo, outros indivíduos o podem lembrar do Banco em oposição a outras instituições financeiras.

Em seguida no conteúdo, o aviso da Figura 10 reforça que nenhum banco solicita transferências. Outro item que reforça e simplifica a ação frente ao risco, para que o processo de percepção e de decisão sejam mais diretos, já que nenhum banco vai pedir ***transferências***, o que aproxima de determinado risco e faz com que a ameaça exista no imaginário dos clientes (Pidgeon *et al*., 1992 *apud* Lima, M. L., 1999).

Figura 10 - Nenhum banco vai te pedir transferências

Fonte: Itaú (2023b).

Os objetivos da comunicação de risco desse vídeo são dois. Primeiramente, possui aspectos informativos e educativos relacionados ao fato de os bancos em geral nunca solicitarem transferências para seus clientes. Também supõe uma resolução conjunta de problemas (Covello; Slovic; Winterfeldt, 1986), entre o cliente Itaú Unibanco e a instituição, quando faz referência ao comercial do Itaú Unibanco. A correlação da metalinguagem também acontece porque outros vídeos da campanha

já tinham sido publicados, assim é possível que já se pressuponha a proximidade do público com os outros conteúdos sobre golpes e fraudes do Itaú Unibanco.

Vale mencionar o uso do imperativo, conforme a Figura 11, o qual aparece em repetição: “Atenção hein, o banco nunca liga pedindo para você realizar procedimentos como esse. Nunca”. Isso reforça alguns tópicos também compartilhados na página de *Segurança* do site do Itaú Unibanco.

Figura 11 - Golpe do falso funcionário e ações do Banco

Fonte: Itaú (2023b).

O último vídeo da campanha, e o mais recente, possui um título diferente e diferente do padrão dos outros. O título é *Fique Atento* e foi publicado em setembro de 2023. Ele narra uma situação na qual a atriz traz contextos e cita que todos são golpes:

> Atriz: O banco nunca liga para relatar problema com a conta e nem pede para seguir passo a passo no aplicativo. É golpe.
> Ator: Ta, masss..
> Atriz: Também nunca liga pedindo senha nem código de segurança. Isso aí é golpe.
> Ator: Mas...
> Atriz: Nem manda SMS com número 0800 para reconhecer compra. É golpe (Itaú, 2023c).

Ao longo do vídeo, a atriz segue com outras situações e explica que todas se tratam de golpes. Portanto, o vídeo como um todo é para acender um alerta geral, do que possivelmente é golpe. Cabe relacionar esse alerta com a construção social e relação dos riscos com as organizações, as quais auxiliam no próprio relacionamento dos indivíduos com os riscos (Areosa, 2010). Nesse caso, o Itaú Unibanco reforça a importância da desconfiança para auxiliar na tomada de decisão.

Posteriormente, o conteúdo direciona para um processo de segurança dentro do aplicativo do Itaú: “No *app* Itaú você pode habilitar ou desabilitar seu cartão físico para compras quando quiser. Assim, os seus dados não ficam expostos em caso de perda ou roubo do cartão” (Itaú, 2023c, grifo nosso).

Esse processo de segurança está ligado ao que Rinaldi e Barreiros (2007) citam quanto ao fluxo de gerenciamento de riscos, já que se trata de uma funcionalidade que a organização Itaú Unibanco identificou como oportunidade para minimizar perdas. Dado que ao sofrer a perda ou roubo de cartões, muitas vezes os indivíduos podem abrir processos contra o Banco para provar que valores não foram gastos por eles, o que também pode ferir a imagem da organização. Assim, ao reforçar essa funcionalidade, o Banco identifica, comunica e potencialmente minimiza perdas.

No que tange aos objetivos, o vídeo encaminha para dois objetivos específicos durante a sua comunicação. O primeiro é educar e informar acerca de diferentes golpes, incentiva a desconfiança nos contextos mencionados e reforça pontos de mudança de comportamento e ações de proteção dentro do aplicativo do Itaú Unibanco. Ademais, depois do passo de como habilitar ou desabilitar o cartão físico no aplicativo, o vídeo direciona para outras funcionalidades de *Segurança* no site do Itaú Unibanco (Figura 12), refletindo como as ações de gestão de risco precisam ser integradas através de diferentes mecanismos para reduzi-los e torná-los administráveis (Sêmola, 2013).

Figura 12 - Funcionalidades de segurança do Itaú Unibanco

Fonte: Itaú (2023c).

Todos os seis vídeos têm como objetivo informar e educar, o que segundo Covello, Slovic e Winterfeldt (1986) é o tipo de conteúdo na comunicação de risco que

esclarece sobre diferentes tópicos e auxilia em informar sobre novos riscos e em tópicos mais gerais. O cenário de Segurança da Informação é bastante novo, assim como os riscos relacionados aos acessos e etapas no digital, principalmente em contextos financeiros e que podem influenciar muitas pessoas, que incluem o terceiro Banco brasileiro com mais clientes. Por esse motivo, em algum grau, todos os vídeos da campanha *Itaú e você contra golpes e fraudes* informam e/ou educam. Há também destaque para três vídeos que dão dicas de mudanças de comportamento e ações de proteção, os quais passam sugestões de proteção para acessos físicos (como o adesivo no cartão), mudança de comportamento quando abordado por um conhecido solicitando uma transferência (ligar para a pessoa) e como habilitar o uso do cartão físico no aplicativo do Banco. Por fim, um dos vídeos também conta com aspectos da resolução conjunta de problemas e conflitos, quando cita através de metalinguagem que o comercial da campanha *Itaú e você contra golpes e fraudes* auxiliou na identificação do golpe.

4.4 CARACTERÍSTICAS DA MENSAGEM DE COMUNICAÇÃO DE RISCO

Essa categoria de análise compreende as características da mensagem de comunicação de risco na campanha do Itaú Unibanco. Esses pontos são analisados ao longo dos vídeos selecionados da campanha *Itaú e você contra golpes e fraudes*. Entende-se que a forma como o conteúdo é apresentado influencia na percepção do receptor. Por isso, conforme Batista (2007), a informação precisa ser acessível e aplicável no processo de decisão desse receptor. Os elementos que caracterizam as mensagens podem ser na forma da fala, no uso de ícones para chamar a atenção e em texto escrito. Sendo assim, esses elementos e seus formatos são analisados no contexto da produção audiovisual.

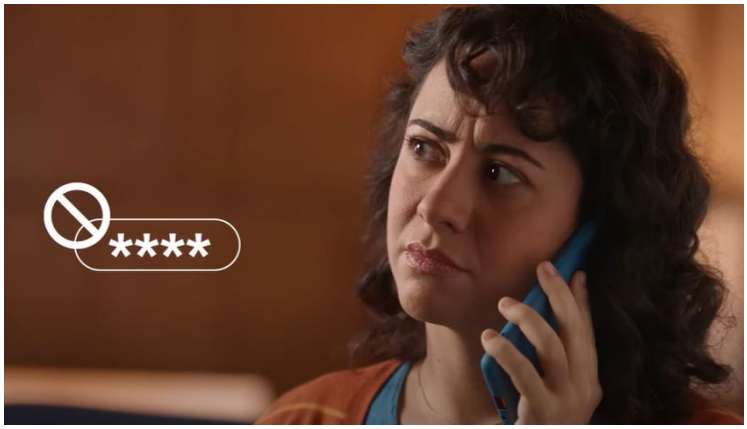
No primeiro vídeo da campanha, o passo a passo da aplicação do golpe da troca de cartão é apresentado:

> Primeiro o golpista liga se apresentando como funcionário do banco ou do cartão de crédito. [...] Então, ele pede para que você corte o cartão ao meio e diz que em breve um portador vai até a sua residência para retirar esse cartão cortado. O detalhe é que mesmo cortando o cartão, o *chip* segue intacto e é justamente com o *chip* mais a senha que eles fazem compra com o cartão (Itaú, 2022a, grifo nosso).

Termos normalmente usados para contar uma história considerando uma linha do tempo são utilizadas pela atriz, como: “primeiro”, “então”, “em breve”, “o detalhe”. Essa aproximação com o *modus operandi* do golpe relaciona-se com Rovere (2006), que cita que à medida que uma pessoa adquire mais conhecimento sobre uma determinada informação, ela tende a se livrar dos preconceitos e crenças acumulados ao longo da vida e a se conscientizar mais sobre os riscos reais aos quais está exposta.

Além disso, ícones gráficos são mostrados ao longo do vídeo, como os da Figura 13, ao se referir à solicitação de digitar a senha no teclado do telefone. Também ícones de cartão cortado ao meio e tesoura aparecem juntos do ícone de bloqueio, sinalizando o que não deve ser feito.

Figura 13 - Ícone para não compartilhar a senha



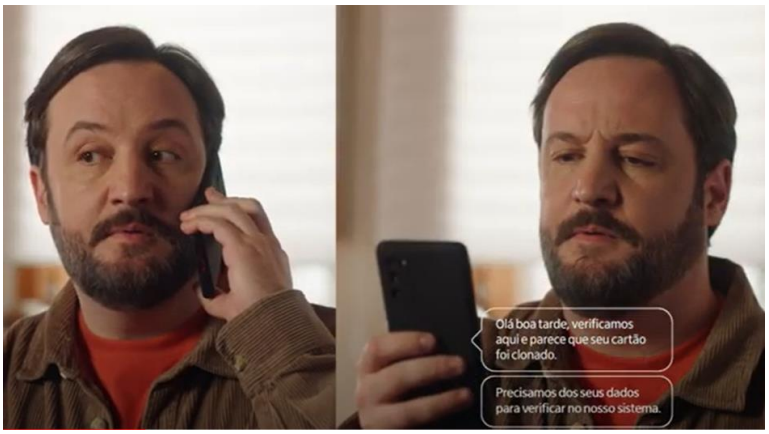
Fonte: Itaú (2022a).

Dessa forma, esse conteúdo se encaixa no formato narrativo, visto que narra como o golpe normalmente é aplicado, mostrando as expressões de estranhamento da atriz frente às solicitações do fraudador (digitar senha, cortar o cartão ao meio, etc.), narrando o motivo do golpe funcionar. Segundo Batista (2007), o conteúdo narrado aproxima o leitor e o traz para o processo da representação, mantendo a atenção ao problema.

Na segunda produção audiovisual, o ator começa explicando o funcionamento do Golpe da Falsa Central de Atendimento, nos momentos iniciais do vídeo:

> O golpista liga ou manda mensagem fingindo ser um funcionário do banco ou do cartão. Daí ele avisa que alguém clonou seu cartão e ta fazendo compras com ele. E que para bloquear o seu cartão imediatamente ele precisa do seu número do cartão [...] (Itaú, 2022b).

Figura 14 - Solicitações dos fraudadores



Fonte: Itaú (2022b).

Assim como no vídeo anterior, as expressões faciais do autor também aproximam o receptor a história que está sendo explicada. Esses pontos sutis da apresentação e encenação dos atores auxiliam na percepção de risco, o que reforça que a percepção de risco é influenciada pela forma como a mensagem é transmitida pela mídia e outras fontes (Pidgeon; Kasperson; Slovic, 2003).

A Figura 14 sinaliza a possível ligação do fraudador do lado esquerdo. No lado direito, o uso da caixa de diálogos demonstra como normalmente os SMS são enviados para as vítimas. Ao longo do vídeo, ícones demonstram o que o fraudador solicita (número de cartão, senha e *itoken* do aplicativo) e eles são apresentados por ícones. Por conter essas estruturas, de início, meio e fim, referente a explicação do funcionamento do golpe, o segundo vídeo da campanha se encaixa no formato narrativo.

A terceira produção audiovisual retrata o Golpe do WhatsApp, conforme a narração:

> O fraudador descobre o número de contato de alguém que você conhece. Aí ele cria uma conta no aplicativo de mensagens com a foto de uma pessoa conhecida, mas com um número diferente de celular. Ele avisa os contatos que trocou de número e aborda alguns deles dizendo que está com problema financeiro ou com a conta bloqueada e que precisa de uma transferência com urgência. Achando que realmente se trata de um amigo, a pessoa faz a transferência (Itaú, 2022c).

O uso de caixas de diálogo, mostra, conforme a Figura 15, quais as etapas da abordagem (número novo, problema, necessidade de dinheiro). A expressão facial de estranhamento da atriz também aproxima, e traz preocupação no receptor através do conteúdo da comunicação (Batista, 2007).

Figura 15 - Abordagem feita pelos fraudadores

Fonte: Itaú (2022c).

Nesse vídeo, a atriz reforça a importância de manter a calma caso um cenário semelhante esteja acontecendo: “Portanto, se você receber uma mensagem pedindo dinheiro, tente manter a calma, entre em contato com a pessoa e descubra se foi ela quem te mandou mensagem pedindo dinheiro emprestado ou se é golpe” (Itaú, 2022c).

Assim, a informação torna-se mais acessível, principalmente com o objetivo de se tornar parte do processo de decisão do receptor. Nesse caso, antes de realizar uma transferência, orienta que a pessoa ligue e confirme se realmente esse amigo ou conhecido está pedindo o dinheiro informado por mensagem. Isto é, neste caso, o formato narrativo (Batista, 2007) pode gerar identificação com a mensagem exposta já que descreve o padrão desse golpe.

No quarto vídeo, intitulado *Como se Proteger do Golpe da Troca do Cartão*, o ator está em uma ligação telefônica e acha atenção para uma situação:

> Ator 1: Olha isso, golpe da troca do cartão
> Ator 2: Troca do cartão?
> Ator 1: É, *cê* vai pagar alguma coisa na rua, dá o cartão, bota a senha, daí te devolvem outro cartão parecido sem você perceber, e usam o seu cartão para fazer compras com a sua senha, entendeu?
> Ator 1: Que isso?!
> Ator 1: Você sabe quem me salvou?
> Ator 2: Quem?
> Ator 1: A princesa do cabelo azul.
> Ator 2: *Hã?*
> Ator 1: É o adesivo que a minha filha colou no cartão. É inconfundível (Itaú, 2023a).

A própria forma de construção do diálogo já demonstra alguns itens que vão gerar curiosidade, como as perguntas, o apontamento sobre o “sabe quem me

salvou?”, além de estar contando uma situação casual para um amigo. Depois, o ator retorna e narra como é feito o golpe pelos fraudadores:

> Você paga alguma coisa na rua com o seu cartão, aí você dá o cartão, digita sua senha. Só que sem você perceber, o fraudador devolve outro cartão, que não é o seu. E tá feito o golpe. Com a sua senha e seu cartão em mãos, ele faz compras indevidas. Por isso. Atenção. Sempre confira o seu nome no cartão (Itaú, 2023a, grifo nosso).

Os ícones também aparecem no vídeo, conforme o autor cita os passos (digitar a senha, a troca dos cartões, conferir o cartão). A Figura 16 demostra, por um ícone de rosto triste que “tá feito o golpe”.

Figura 16 - Feito o golpe

Fonte: Itaú (2023a).

Esse vídeo também se encaixa no formato narrativo proposto por Batista (2007), visto que não traz as informações técnicas por trás do golpe, mas como ele acontece em uma situação mais casual. Aqui a referência é à época do Carnaval, indicada pelo período de publicação do vídeo, o mês de fevereiro, e pelos adereços usados pelo ator. Renn (2008) destaca que valores culturais e sociais influenciam a percepção do risco. No vídeo, o uso de trajes de carnaval pelo ator exemplifica como elementos culturais moldam a maneira como entendemos e nos aproximamos dos riscos.

Da mesma forma, o vídeo do *Golpe do Falso Funcionário* inicia com uma ligação de voz ao celular:

> Atriz: Alô?
> Ator: Aqui é do banco e vimos o agendamento de uma transação suspeita no valor de 4 mil reais. Ele é seu?
> Atriz: 4 mil reais?

> Ator: Para que essa transação seja cancelada é necessário que você entre no aplicativo do banco e siga o caminho que eu vou te falar agora.
> Atriz: *Ah*, justo agora? No intervalo do jornal? [risos]. Você não tá com sorte, acabou de passar o comercial do Itaú contra golpes e fraudes (Itaú, 2023b, grifo nosso).

De acordo com Teixeira (2019), a percepção e gestão de riscos são moldadas por uma interação dinâmica entre atores sociais e organizações, destacando a necessidade de uma abordagem integrada para enfrentar os desafios relacionados aos riscos. No vídeo, a metalinguagem é utilizada para ilustrar um golpe comumente aplicado em clientes do Banco. A atriz destaca como o Itaú Unibanco a ajudou a evitar o golpe, de certa forma exemplificando a responsabilidade social e ética que as organizações são cada vez mais pressionadas a demonstrar em relação aos riscos.

Posteriormente, a atriz inicia a explicação da aplicação do golpe:

> O fraudador liga ou manda SMS se passando por um funcionário do banco e diz que identificaram um agendamento de uma transação suspeita na sua conta. Aí ele diz que para cancelar tal transação você precisa fazer um procedimento, que nada mais é do que fazer uma transferência ou pagamento. Se você fizer, caiu num golpe (Itaú, 2023b).

Conforme a Figura 17, os ícones demonstrando a aplicação do golpe também chamam a atenção ao problema e ao fluxo de acontecimentos para o objetivo dos fraudadores – dar o golpe.

Figura 17 - Ícone solicitação de transferência

Fonte: Itaú (2023b).

Portanto, para reforçar que o Banco pede transferências ou pagamentos, esse vídeo também possui o formato narrativo, que em situações como essa se mostra mais eficaz (Batista, 2007).

Por fim, no sexto vídeo nomeado *Fique Atento*, novamente em uma ligação telefônica dois atores dialogam sobre golpes:

> Atriz: O banco nunca liga para relatar problema com a conta e nem pede para seguir passo a passo no aplicativo. É golpe.
> Ator: Ta, masss..
> Atriz: Também nunca liga pedindo senha nem código de segurança. Isso aí é golpe.
> Ator: Mas...
> Atriz: Nem manda SMS com número 0800 para reconhecer compra. É golpe.
> Ator: Ok, mas..
> Atriz: É golpe!
> Ator: Ta, mas oh
> Atriz: Golpe também
> Ator: E...
> Atriz: Outro golpe
> Ator: É que...
> Atriz: Golpe!
> Ator: E...
> Atriz: Outro golpe [cantarolando] (Itaú, 2023c).

Depois dessa parte inicial, o último e mais recente vídeo da campanha, diferentemente dos demais, os quais explicam algum golpe em especial, reforça uma dica de segurança (Figura 18):

> Quer uma camada extra de proteção para o seu cartão físico? No *app* Itaú você pode habilitar ou desabilitar seu cartão físico para compras quando quiser. Assim, os seus dados não ficam expostos em caso de perda ou roubo do cartão. E mesmo com o bloqueio do cartão físico você ainda poderá usar o cartão virtual ou a carteira digital. Vai em minhas proteções no seu *app* (Itaú, 2023c, grifo nosso).

Figura 18 - Minhas proteções no seu *App*

Fonte: Itaú (2023c).

De acordo com Darley e Latané (1968), mesmo que sinais de perigo sejam identificados em um ambiente, a importância atribuída a eles depende de fatores sociais. Por exemplo, a presença de outras pessoas realizando tarefas semelhantes

pode levar os indivíduos a considerar a situação como não perigosa, devido à influência do comportamento dos outros. Uma pessoa ter passado pessoalmente por uma situação de risco também altera a vivência dela em relação a esse risco. Por esses motivos, juntamente com o fato de que a percepção de risco é também uma construção individual, que considera a proximidade ou não a um determinado risco, o diálogo entre os atores e a constante contestação reforçam a tentativa de instaurar uma desconfiança em todos os cenários em que o Banco solicite algo ao cliente. Assim, há centralização desse comportamento frente aos riscos.

A primeira parte do vídeo gera identificação e atenção ao problema, visto que são diversos os tipos de golpes e de uma forma mais humorística narra uma situação e traz luz para desconfiança no cenário de golpes e fraudes. Por outro lado, a segunda parte do vídeo explica como ter uma camada extra de segurança. Nesse caso, como habilitar e desabilitar o cartão físico. Aqui também aparecem ícones que facilitam a visualização, como cadeado para demonstrar o habilitar e desabilitar. A atriz explica para qual situação é importante conhecer a funcionalidade de roubo ou perda do cartão. Demonstra outras soluções de uso, como cartão virtual ou carteira digital, e o que fazer para habilitar. Informações mais técnicas são expostas, indo na direção do que argumenta Batista (2007) sobre o processo informativo técnico fazer sentido quando a comunicação acontece pela primeira vez.

É nesse último vídeo da campanha, o qual funciona como um alerta geral, incentivando que o público sempre desconfie de abordagens suspeitas, pois possivelmente é golpe, acontece o direcionamento para a página de *Segurança* do site do Itaú Unibanco, onde há mais conteúdos sobre golpes e fraudes. Inclusive, além da proximidade com o processo de gestão de riscos, a estratégia do Itaú Unibanco de trabalhar esses conteúdos vai na linha do plano de modernização de atendimento do Banco, bem como da centralização de funções dentro do aplicativo, de forma *online*, distanciando o cliente da agência física aos poucos. Isso pode ser interligado com Sêmola (2013), já que as movimentações bancárias podem ser realizadas no próprio celular ou computador, o que amplia e aumenta os tipos de riscos.

Por fim, quanto às características da mensagem de comunicação de risco, cinco dos vídeos têm o formato narrativo como base, em comparação com apenas um que apresenta um conteúdo técnico (Batista, 2007). A explicação pelas escolhas frente ao formato narrativo parece ser pela necessidade de identificação dos públicos. Visto que os conteúdos e tipos de golpes aumentam a cada dia, os conteúdos

narrativos são uma possibilidade para aproximar o cliente dos riscos, chamar a atenção, apresentar propostas de resolução de problemas ou exclusivamente alertar quanto a ameaça. Além disso, o menor uso do conteúdo técnico possivelmente ocorre porque a página de *Segurança* do site do Itaú Unibanco fornece e apresenta informações em outros formatos. Considerando que essa página foi lançada antes da campanha, e que a própria campanha, em seu último vídeo, direciona os usuários para ela, a representação e a identificação tornam-se mais relevantes em um contexto de produção audiovisual curta, como na campanha *Itaú e você contra golpes e fraudes*.

Nessa linha, as produções de conteúdos e direcionamentos realizados pelo Itaú Unibanco demonstram o movimentado citado pelo relatório da Axur (2024) de integração dos riscos das organizações com os riscos cibernéticos, já que ao direcionar sobre os riscos junto ao público existe uma chance de menos danos e prejuízos à reputação do Banco.

4.4 ENGAJAMENTO E RELACIONAMENTO COM OS PÚBLICOS

Por fim, a categoria de engajamento e relacionamentos com os públicos compreende a análise dos comentários dos seis vídeos da campanha *Itaú e você contra golpes e fraudes*. Entende-se o espaço dos comentários da rede social *Youtube* como um espaço aberto, em que os públicos podem se expressar sem necessariamente mediações, mas que também, pode ser gerido pelo Itaú Unibanco em prol de um engajamento e troca entre a organização e seus públicos (Andrelo, 2016). Esses elementos são analisados a partir dos comentários e da resposta dos comentários principais nos vídeos da campanha.

O vídeo *Como se Proteger do Golpe da Troca de Cartão* em termos de engajamento e números conta com 637 mil visualizações, 5,3 mil curtidas e 80 comentários. Possivelmente, devido à quantidade de visualizações em comparação com a quantidade de curtidas e comentários, o vídeo tenha sido patrocinado. O conteúdo audiovisual tem a seguinte descrição: “Nunca compartilhe seus dados bancários, a senha ou entregue o seu cartão de crédito para um portador. Fique atento: é golpe. Juntos nós protegemos em dobro. #feitocomvocê”. Percebe-se que faz relação com a essência do conteúdo e seu objetivo principal, informar sobre os riscos de entregar o cartão.

Em relação a dados quantitativos, a fim de centralizar a análise dos 80 comentários, eles foram classificados em positivo, indiferente ou negativo. Cabe citar que as respostas aos comentários principais foram todos consideradas indiferentes, visto que se trata de respostas do próprio Banco ou de pessoas mencionando outros assuntos, e por isso estão numa subcategoria separada, chamada respostas aos comentários principais. Além disso, os comentários positivos foram considerados aqueles que citam pontos positivos sobre o conteúdo ou sobre o Banco.

Conforme o Quadro 1, os comentários positivos são a maioria com 35%, os comentários indiferentes aparecem logo atrás com 32,50% e os comentários negativos são minoria (3,75%). Das 23 respostas aos comentários principais, 11 delas foram dadas pelo Itaú Unibanco.

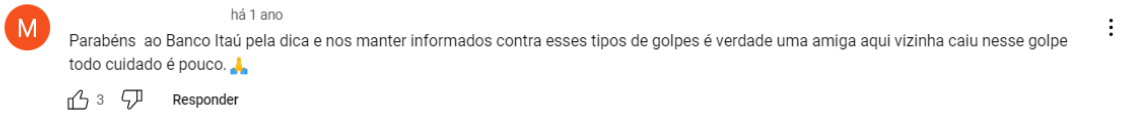
Quadro 1 - Comentários *Como se Proteger do Golpe da Troca de Cartão*

Como se Proteger do Golpe da Troca de Cartão		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	28	35%
Comentários indiferentes	26	32,50%
Comentários negativos	3	3,75%
Respostas aos comentários principais	23	28,75%
Total de comentários	80	100%

Elaborado pela autora (2024).

Alguns dos comentários positivos parabenizam o Banco pela construção do conteúdo. Também mencionam pontos da percepção de risco. Conforme Latané e Darley (1968), fatores externos influenciam nessa percepção e em como cada indivíduo lida com o mesmo risco. O comentário da Figura 19 se relaciona com a construção da relação com o risco dos golpes, já que uma pessoa próxima caiu nesse golpe.

Figura 19 - Comentário sobre amiga que caiu no golpe

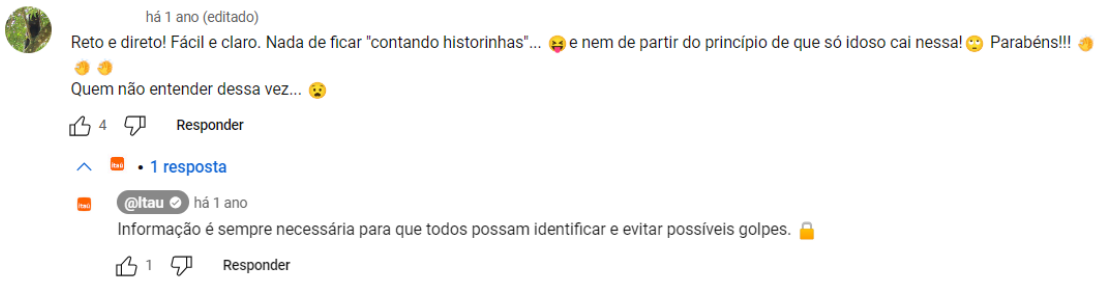


Fonte: Itaú (2022a).

Por outro lado, outro comentário positivo, esse respondido pelo Banco (Figura 20), demonstra o relacionamento e a importância que as organizações têm na

definição da perspectiva dos riscos para seus públicos, já que quanto mais informações sobre um risco, mais conscientização sobre esses riscos (Rovere, 2006).

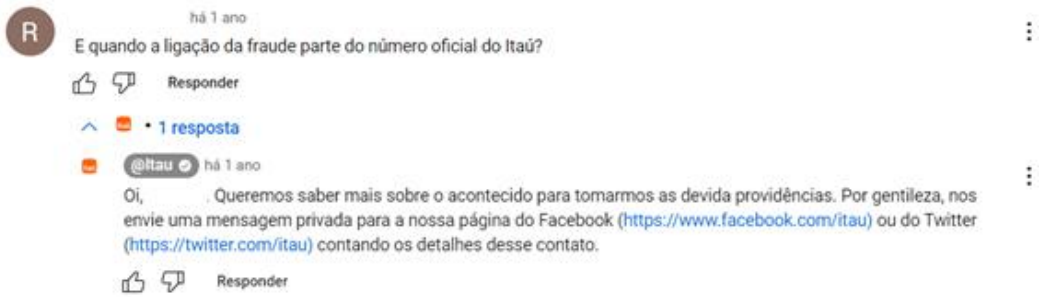
Figura 20 - Comentário sobre o conteúdo ser compreensível



Fonte: Itaú (2022a).

Em contrapartida, um comentário com viés mais negativo, como o da Figura 21 também foi respondido pelo Banco. A resposta do Itaú Unibanco direcionamento para um atendimento em que eles possam tomar as devidas providências, o que demonstra certa preocupação da organização em causar consequências negativas para seus clientes. Segundo Grunig (2009), relacionamentos de alta qualidade ocorrem quando a organização reconhece a legitimidade de seus públicos, ouve suas preocupações e trata das consequências negativas que possam afetá-los.

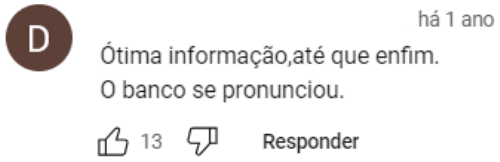
Figura 21 - Comentário sobre fraude do Itaú



Fonte: Itaú (2022a).

Por fim, outro comentário considerado positivo, pois elogia o conteúdo, cita a demora do Banco se pronunciar, como mostra a Figura 22. Comentários como esse salientam o que Douglas e Wildavsky (1982) definem sobre a percepção de risco, já que segundo os autores, as instituições sociais são atualmente responsáveis por delegar e apontar riscos para os indivíduos. Nesse caso, também conversa com a responsabilidade e transparência que os bancos precisam ter para lidar com a sociedade de risco (Teixeira, 2019).

Figura 22 - Comentário citando demora para o pronunciamento



Fonte: Itaú (2022a).

A produção audiovisual intitulada *Como se Proteger do Golpe da Falsa Central* conta com 127 mil visualizações, 1,5 mil curtidas e 50 comentários. O vídeo conta como uma definição: “Fique atento! Não compartilhe dados bancários e senha por telefone ou nenhum outro meio. Junte-se ao Itaú contra golpes e fraudes. #feitocomvocê”. Da mesma forma, a quantidade de visualizações em comparação com o número de curtidas indica que possivelmente o vídeo foi patrocinado. Das 20 respostas a comentários – conforme Quadro 2 – 14 foram dadas pelo Itaú Unibanco.

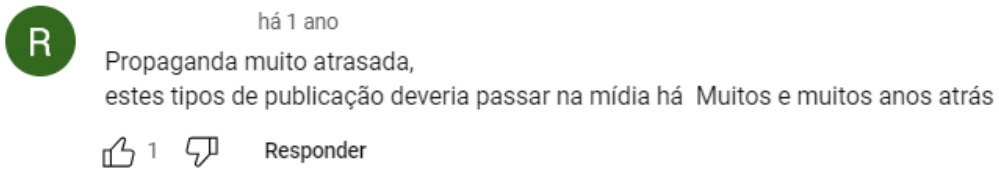
Quadro 2 - Comentários *Como se Proteger do Golpe da Falsa Central*

Como se Proteger do Golpe da Falsa Central		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	21	42%
Comentários indiferentes	8	16%
Comentários negativos	1	2%
Respostas aos comentários principais	20	40%
Total de comentários	50	100%

Elaborado pela autora (2024).

O único comentário negativo em questão mostra na Figura 23 uma crítica em relação a demora na divulgação de conteúdos sobre golpes e fraudes. Conforme destacado por Rovere (2006), é essencial compreender como a sociedade enxerga os riscos aos quais está exposta. Muitas vezes, a percepção do risco pela sociedade não corresponde à realidade dos fatos. Esse descompasso pode ser especialmente problemático quando se trata de golpes e fraudes, que têm se tornado cada vez mais sofisticados e constantes. Como destacado pelo próprio comentário, as organizações têm um papel de responsabilidade social para conscientizar seus públicos sobre os riscos do seu negócio. Sem uma percepção clara e correta dos riscos, a sociedade permanece vulnerável a ações fraudulentas.

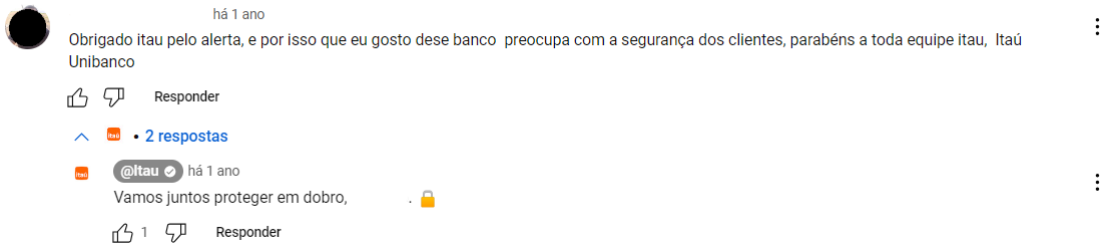
Figura 23 - Comentário sobre atraso do conteúdo



Fonte: Itaú (2022b).

Um dos comentários positivos parabeniza o Banco pela preocupação com o cliente e pela construção do alerta. Além disso, esse comentário (Figura 24) chama a atenção pelo uso de termos relacionados a comunicação de risco, como “alerta”, “preocupação” e “segurança”. O Banco também responde ao comentário utilizando o *slogan* da campanha:

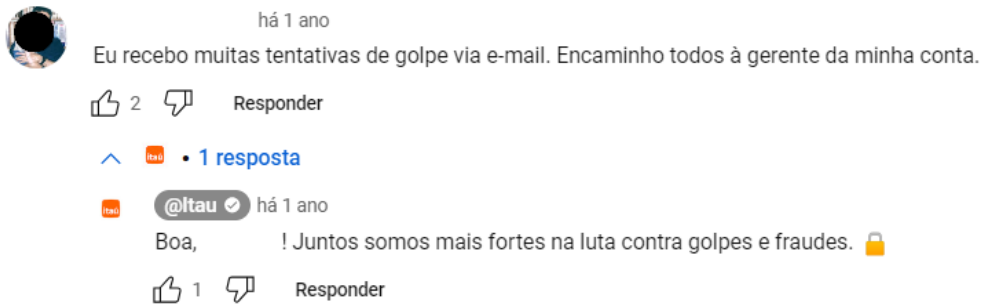
Figura 24 - Comentário que fala sobre a preocupação do Banco



Fonte: Itaú (2022b).

A Figura 25 mostra um dos oito comentários considerados indiferentes, visto que não fala necessariamente pontos positivos sobre o conteúdo ou sobre o Itaú Unibanco, mas que ainda assim, reforça a postura de relacionamento com a organização. Possivelmente o cliente compreende os interesses do Banco e os seus próprios, auxiliando a organização ao compartilhar e encaminhar tentativas de golpes de casos que ele próprio poderia cair. Além disso, a resposta positiva do Banco demonstra a preocupação e reforça esse comportamento.

Figura 25 - Comentário sobre encaminhar tentativas de golpe para gerente



Fonte: Itaú (2022b).

Quanto ao vídeo *Como se Proteger do Golpe do WhatsApp*, foram registradas 320 mil visualizações, 1,7 mil curtidas e 55 comentários. O vídeo conta com descrição:

> Se você receber uma mensagem pedindo dinheiro, tente manter a calma e, antes de fazer qualquer transferência, entre em contato por outro meio com a pessoa e descubra se ela realmente trocou de número ou se isso é um golpe. #feitocomvocê (Itaú, 2022c).

Dos 55 comentários, 21 são respostas aos comentários principais (38,2%) e desse total, 13 respostas foram dadas pelo Itaú Unibanco. Conforme o Quadro 3, são quatro comentários negativos (7,2% do total).

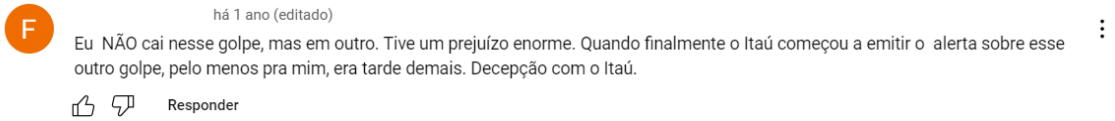
Quadro 3 - Comentários *Como se Proteger do Golpe do WhatsApp*

Como se Proteger do Golpe do WhatsApp		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	12	21,8%
Comentários indiferentes	17	30,9%
Comentários negativos	4	7,2%
Respostas aos comentários principais	21	38,2%
Total de comentários	55	100%

Elaborado pela autora (2024).

Assim como em outros vídeos, um dos comentários negativos é relacionado a demora para divulgações de conteúdos como esse (Figura 26), em que há o alerta quanto aos golpes. Cabe reforçar que esse, assim como outros 20 comentários, não foi respondido pelo Banco.

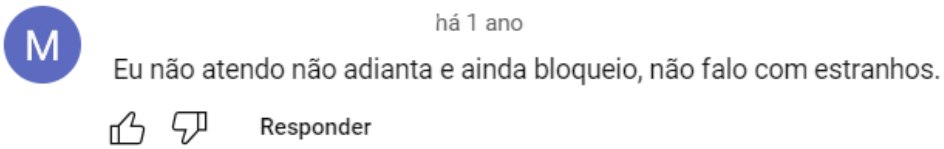
Figura 26 - Comentário sobre decepção com o Banco



Fonte: Itaú (2022c).

Os comentários indiferentes nesse vídeo são a maioria (38,2%), depois das respostas aos comentários principais, e são principalmente sobre apontamentos de ações ou situações que aconteceram com as pessoas. Como da Figura 27, em que não parabeniza necessariamente o conteúdo, também não traz termos negativos, apenas fala de uma ação da pessoa frente a situação. Ainda assim, reforça algumas ações de proteção que os indivíduos preferem tomar e, igualmente, compartilha sua percepção do risco, demonstrando ações de segurança e práticas que prefere ter.

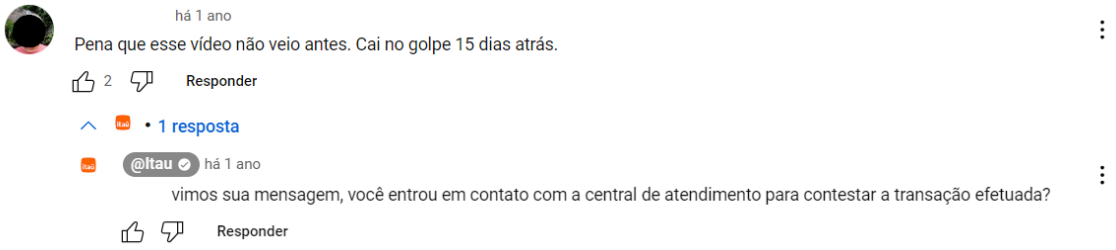
Figura 27 - Comentário sobre ações frente a situação



Fonte: Itaú (2022c).

O comentário a seguir (Figura 28), considerado indiferente – tendo em vista que não fala mal do conteúdo ou do Banco necessariamente –, apenas reforça o ponto citado em um dos comentários negativos, já que menciona a demora para o conteúdo ser divulgado, o que resultou em a pessoa cair no golpe. Por outro lado, esse foi um dos 13 comentários respondidos pelo Banco, em que o mesmo, menciona a possibilidade de contestar transações efetuadas para o fraudador. Essa menção do Itaú Unibanco demonstra pontos de relacionamento, citados por Grunig (2009), em que a organização reconhece e legitima os pontos trazidos por seus públicos, lidando e acompanhando as consequências da produção de seus riscos.

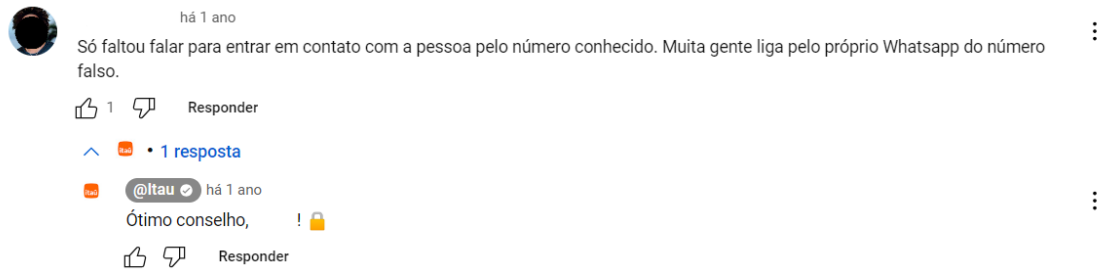
Figura 28 - Comentário sobre demora para divulgar o conteúdo



Fonte: Itaú (2022c).

Da mesma forma, o comentário da Figura 29, também considerado indiferente, conta com uma sugestão de ajuste no conteúdo. Já que no vídeo, a atriz apenas comenta para ligar para o conhecido e confirmar a necessidade da transferência, e não necessariamente sugere o número dele. Teixeira (2019) cita esse ponto no processo de gestão de risco, visto que ao criar espaços de discussões sobre riscos, o debate e o diálogo são caminhos para elaborar medidas de precaução, o que pode ser compreendido como o caso desse comentário, juntamente com a resposta do Banco, elogiando o conselho.

Figura 29 - Comentário com dica de ação



Fonte: Itaú (2022c).

Alguns dos comentários positivos também incluem pessoas citando que passaram por esse golpe (Figura 30), o que se interliga com as organizações auxiliarem na percepção de risco dos seus públicos (Giulio *et al.,* 2015). Inclusive, também auxiliam na compreensão de que os riscos são experiências pessoais concretas (Douglas, 1966), dado que, aqueles que não necessariamente caíram em golpes, terão acesso a esses comentários e suas eventuais percepções sobre esse risco, podem mudar.

Figura 30 - Comentários positivos sobre o conteúdo

Fonte: Itaú (2022c).

O vídeo *Golpe da Troca do Cartão* conta com 620 mil visualizações, 194 curtidas e oito comentários. Esse é o terceiro vídeo com mais visualizações dentro dos seis analisados. Porém, trata-se da produção com menos comentários, o que também sugere que o conteúdo tenha sido patrocinado. Dos oito comentários, três são respostas aos comentários principais. O conteúdo tem a seguinte descrição: “Sempre confira seu nome no cartão depois das compras. Fique atento: se trocarem seu cartão é golpe”. Conforme mostra o Quadro 4, não há comentários negativos nessa produção audiovisual. Além disso, das três respostas aos comentários, duas foram dadas pelo Itaú Unibanco:

Quadro 4 - Comentários *Golpe da Troca do Cartão*

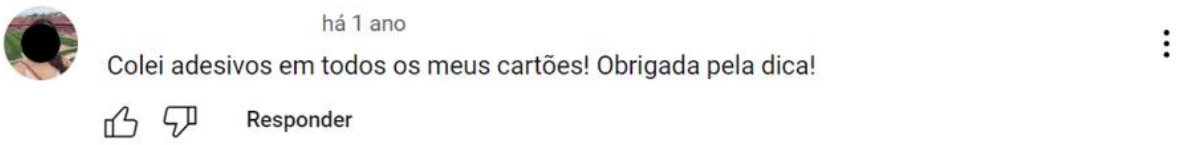
Golpe da Troca do Cartão		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	2	25%
Comentários indiferentes	3	37,50%
Comentários negativos	0	0%
Respostas aos comentários principais	3	37,50%
Total de comentários	8	100%

Fonte: Elaborado pela autora (2024).

Como reforçado pela própria descrição do conteúdo, o principal objetivo da comunicação de risco é a informação sobre a importância da conferência do cartão.

Além disso, conforme analisado, o vídeo também apresenta uma forma e dica de proteção (Covello; Slovic; Winterfeldt, 1986), a qual, conforme a Figura 31, demonstra em um dos comentários positivos, que a pessoa seguiu a indicação. Reflete que um dos objetivos dessa comunicação de risco foi atingido pelo público do Itaú Unibanco. Isso é, emissor e receptor estão cientes dessa prática para garantir a segurança dos cartões físicos. Para além, demonstra como os riscos são construídos cultamente e moldados por atores sociais, como o Itaú Unibanco (Areosa, 2010).

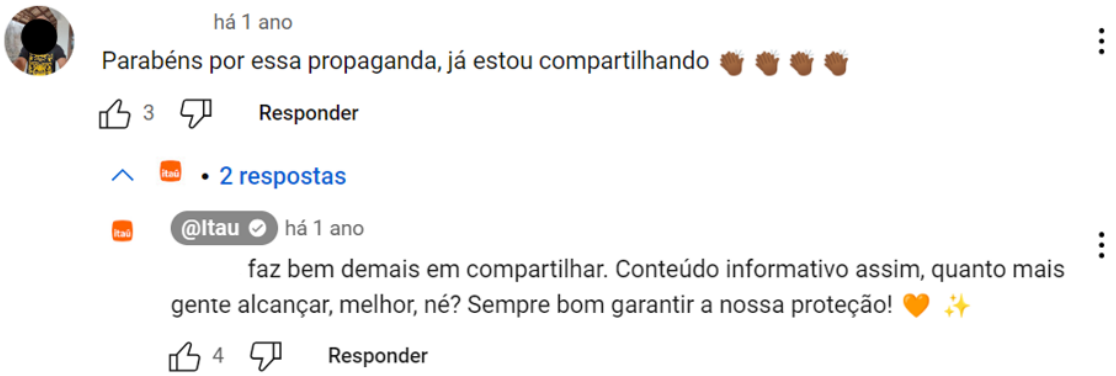
Figura 31 - Comentário relacionado a dica de proteção



Fonte: Itaú (2023a).

O segundo e último comentário positivo do vídeo menciona que a pessoa está compartilhando o conteúdo, o que é respondido pelo Banco com a citação da importância do conteúdo informativo, conforme a Figura 32.

Figura 32 - Comentário elogiando o conteúdo



Fonte: Itaú (2023a).

A produção audiovisual *Golpe do Falso Funcionário* conta com 120 mil visualizações, 477 curtidas e 33 comentários (destes, 20 são respostas aos comentários principais, quatro deles do Itaú Unibanco). A definição do vídeo é “Itaú e você contra o golpe do falso funcionário. O banco nunca liga pedindo transferências. É golpe. #FeitoComVocê”. Como mostra o Quadro 5, esse vídeo é o que

proporcionalmente tem mais comentários negativos considerando o número geral de comentários (quatro comentários e 12,12% do total):

Quadro 5 - Comentários *Golpe do Falso Funcionário*

Golpe do Falso Funcionário		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	6	18,18%
Comentários indiferentes	3	9,09%
Comentários negativos	4	12,12%
Respostas aos comentários principais	20	60,61%
Total de comentários	33	100%

Fonte: Elaborado pela autora (2024).

Por outro lado, os comentários positivos não são tão expressivos. Sendo então, as respostas aos comentários principais a maioria (60,6%) e nesse vídeo em questão, muitos desses comentários trata-se de *spam* ou somente de *emojis*.

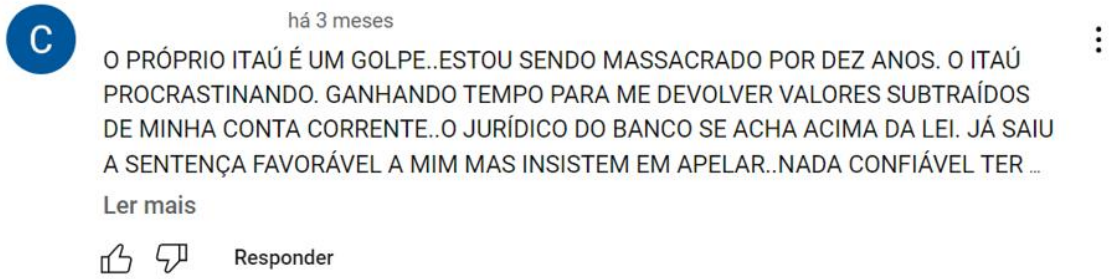
Os comentários indiferentes se direcionam também, além de alguns *emojis*, para casos de depoimento de pessoas que conhecem alguém que caiu no golpe, como o da Figura 33. Reforça-se o papel da percepção de risco individual, mas a qual igualmente auxilia na construção da percepção de risco da sociedade (Fischhoff, Kadvany, 2011).

Figura 33 - Comentário sobre o golpe

Fonte: Itaú (2023b).

Metade dos comentários negativos (dois deles) citam a mesma prática do Banco (retirar saldo de correntistas). Esses também são resultados do acesso à Internet, pois os espaços de interação sem mediação, como as redes sociais, incluindo o YouTube, demonstram que as instituições precisam saber lidar com os apontamentos negativos feitos por seus públicos (Andrelo, 2016). No comentário em questão (Figura 34), postado há três meses, o Itaú Unibanco não respondeu.

Figura 34 - Comentário negativo sobre golpe do próprio Banco



Fonte: Itaú (2023b).

Contudo, o outro comentário semelhante, postado há mais de um ano, foi respondido pelo Banco. Como mostra a Figura 35, foi mais de uma resposta dada pelo Itaú Unibanco, mas que acabou sem uma resposta final, não auxiliando em uma resolução concreta para a cliente. O que confirma a falta de resposta comentada pelo usuário. Assim, mesmo que conteúdo do comentário não tenha relação com golpes e fraudes feitos por terceiros, como um espaço aberto e sem a devida mediação, pode gerar uma imagem não tão positiva ao Banco ao deixar a cliente sem uma resposta e resolução para seu problema.

Figura 35 - Comentário sobre golpe do próprio Banco

Fonte: Itaú (2023b).

O vídeo *Fique Atento* tem 23 milhões de visualizações, 497 curtidas e 50 comentários. A quantidade de visualizações pressupõe que o conteúdo tenha sido patrocinado. O vídeo conta com a seguinte descrição: “O banco não liga para relatar problemas na sua conta. Fique atento: é golpe. Juntos, nós protegemos em dobro. #feitocomvocê”. Da mesma forma, a descrição é usada como um espaço para resumir o principal objetivo do conteúdo divulgado pelo Banco. Como mostra o Quadro 6, não há comentários negativos nesse vídeo, as respostas aos comentários principais são a maioria com 40% (sendo 10 respostas dadas pelo Itaú Unibanco) e, em seguida, os comentários positivos com 34%.

Quadro 6 - Comentários *Fique Atento*

Fique Atento		
Classificação de comentários	Quantidade	Porcentagem
Comentários positivos	17	34%
Comentários indiferentes	13	26%
Comentários negativos	0	0%
Respostas aos comentários principais	20	40%
Total de comentários	50	100%

Fonte: Elaborado pela autora (2024).

Mesmo não sendo o vídeo com mais comentários positivos, ainda assim trata-se de um dos vídeos da campanha em que fica evidente que o Banco alcançou o objetivo de citado por Covello, Slovic e Winterfeldt (1986) de informar e educar. Também funciona como um alerta geral, uma vez que os comentários positivos citam isso, conforme a Figura 36. Como reforçado por Batista (2007), uma das formas de ativar a preocupação de seus públicos é gerar identificação com mensagens expostas e as citações como “tudo é golpe”, “além de um alerta”, “entenderem direitinho” e “instrutivo e eficiente” enfatizam que o vídeo da campanha foi bem recebido pelo público. Nos comentários, também mencionam públicos e pessoas de diferentes idades, não somente quem está comentando (Figura 36).

Figura 36 - Comentários com identificações em relação ao alerta

Fonte: Itaú (2023c).

De forma semelhante, a Figura 37 evidencia os elogios ao conteúdo. Dentre os vídeos da campanha, como já citado, mesmo esse não sendo o com mais comentários positivos, é o que contém mais comentários sobre a autenticidade e criatividade do conteúdo. Ao longo do mesmo, nenhum golpe específico é mencionado, porém acontece uma advertência sobre golpes de modo geral.

Figura 37 - Comentários sobre a qualidade do conteúdo

Fonte: Itaú (2023c).

Ademais, esses são os pontos relativos ao engajamento e relacionamento com os públicos nos vídeos base da campanha *Itaú e você contra golpes e fraudes*. De modo geral, o Itaú Unibanco não necessariamente respondeu a todos os comentários nas produções audiovisuais (o Quadro 7 mostra a quantidade de interações do Banco). Entretanto, também não respondeu apenas comentários positivos, como também indiferentes e negativos. Inclusive, os números de comentários são relativamente menores do que a quantidade de visualizações, o que traz à tona a possibilidade de os conteúdos terem sido patrocinados no Youtube. Cabe citar que em vídeos patrocinados não é possível interagir (comentar ou curtidas), somente se o indivíduo optar por acessar o vídeo na íntegra para o fazer.

Quadro 7 - Engajamento dos vídeos da *campanha Itaú e você contra golpes e fraudes*

Vídeo	Visualizações	Curtidas	Total de comentários	Total de comentários positivos	Total de comentários negativos	Respostas do Itaú Unibanco
Como se Proteger do Golpe da Troca de Cartão	637.000	5.400	80	28	3	11
Como se Proteger do Golpe da Falsa Central	127.000	1.500	50	21	1	14
Como se Proteger do Golpe do WhatsApp	320.000	1.700	55	12	4	13
Golpe da Troca do Cartão	620.000	194	8	2	0	2
Golpe do Falso Funcionário	120.000	477	33	6	4	4
Fique Atento	23.000.000	496	50	17	0	10

Fonte: Elaborado pela autora (2024).

Ainda assim, vale frisar que os números de comentários negativos são baixos e alguns deles não são direcionados ao conteúdo em si, mas a postura do Itaú Unibanco em outras frentes. Inclusive, como mostra o Quadro 7, dois dos vídeos não possuem menções negativas, o que na percepção da autora, demonstra aceitação do conteúdo.

Quanto ao modelo simétrico de duas mãos de Grunig (2005) são diferentes as trocas entre público e organização que salientam a prática, como o recorte dos comentários acaba por ser limitado, não há elementos suficientes para avaliar se o modelo é implementado pelo Itaú Unibanco junto a seus públicos. Entretanto, pode-se observar algumas das práticas de forma mais recortada em algumas palavras do público nos comentários da campanha. Principalmente, no que se refere ao processo de consciência, entendimento e compartilhamento do conteúdo, como no vídeo *Fique Atento*. Nesse sentido, ficou evidente a confiança no conteúdo do Banco enquanto marca junto com seus públicos.

De forma geral, existe um relacionamento entre o Itaú Unibanco e o público que relatou suas opiniões ao longo dos comentários, igualmente há trocas e construções na percepção dos riscos comentados. Ainda assim, na visão da autora, a organização poderia fortalecer mais essa aproximação. Ademais, as considerações gerais sobre esse subcapítulo, assim como os outros dois serão abordados a seguir.

4.5 CONSIDERAÇÕES GERAIS SOBRE A COMUNICAÇÃO DE RISCO DO ITAÚ UNIBANCO

Sobre a categoria dos objetivos da comunicação de risco, a construção por trás do informar e educar é bastante abrangente e interessante no cenário de riscos novos, tanto para os públicos como para as organizações. Visto que, como Areosa (2010) afirma, essas novas formas de risco são difíceis de entender devido à falta de experiência, sendo um território pouco explorado pela sociedade. Apesar disso, na compreensão da autora, os objetivos de mudança de comportamento e dicas de proteção poderiam ser mais utilizados pela organização Itaú Unibanco, sendo inclusive possível que em todas as produções da campanha tivesse alguma dica de proteção de segurança no contexto da Segurança da Informação. Todavia, na opinião da pesquisadora, o Banco soube criar frases curtas de efeito que acendem um alerta para o receptor, como “sempre confira seu cartão: se trocarem, é golpe” ou então a própria mensagem geral do último vídeo, *Fique Atento*, em que o ator repassa por diversos golpes e a atriz segue afirmando que todos são golpe.

Referente as características da mensagem, o formato narrativo mostrou-se completamente presente, o que parece ser devido a necessidade de identificação em um contexto como os riscos da Segurança da Informação. Ainda assim, seria

importante a abordagem técnica para informar sobre medidas de proteção, como o que aparece no fim do vídeo *Fique Atento*, já que, as informações técnicas auxiliam o público leigo a compreender mais o desenvolvimento e esquemas por traz das definições de golpes e fraudes. Com relação às características da mensagem, o Banco e a campanha produzida pela Agência África souberam selecionar atores que fizeram o uso de expressões faciais constantes de dúvida, inquietação, questionamento, o que também chama atenção para o problema. O uso dos ícones também é interessante durante a abordagem narrativa, uma vez que a história do golpe vai sendo contado, aquilo que não deve ser feito é relembrado através dos ícones.

Além disso, os comentários do público mostram que há uma compreensão crescente de que os golpes e fraudes atuais podem afetar pessoas de todas as idades, e não grupos específicos, como os idosos, por exemplo. Isso reforça os apontamentos de Batista (2007) sobre representação e alerta para o problema. Por isso, caberia ao Banco selecionar atores e atrizes de outras idades para serem representados na campanha, assim seria possível gerar mais identificação durante os tópicos abordados.

Sobre engajamento e relacionamento, a postura do Itaú Unibanco, na visão da autora, poderia ser ajustada para que os objetivos da organização, incluso sua visão de ser o banco líder em performance sustentável e em satisfação dos clientes, sejam atingidos. Uma vez que a comunicação de mão-dupla de Grunig (2005) tem como um de seus sinais o engajamento nas interações entre a organização (emissora ou fonte) e os públicos (receptores), o Banco precisaria estar atento para responder aos comentários. Porém, muitos não tiveram resposta do Banco, inclusive alguns comentários negativos não tiveram uma resposta final da organização. Para a pesquisadora, o Itaú Unibanco também perdeu a oportunidade de divulgar outros meios em que compartilha informações sobre golpes e fraudes, como a página de *Segurança* no site e o próprio e-mail em que se pode compartilhar páginas suspeitas que se passam pelo Itaú Unibanco. Da mesma forma, a ISO 31000:2019 reforça as etapas da comunicação e consulta, e monitoramento e análise crítica. Na percepção da autora, a falta de resposta e a seleção aleatória de comentários respondidos (não necessariamente os comentários mais antigos foram respondidos, nem somente os positivos, por exemplo) demonstram que o Banco pode trabalhar mais em sua comunicação e relacionamento com os públicos.

Além disso, vale ressaltar os comentários que criticam a demora do Itaú Unibanco em divulgar conteúdos sobre golpes e fraudes. Considerando que o Banco, na opinião da autora, é um dos responsáveis pela produção desses riscos, é essencial que ele esteja à frente de iniciativas que rapidamente lidem com esses casos, educando seus clientes e adotando medidas proativas para minimizar os impactos e proteger os usuários.

Assim sendo, a pesquisadora concluiu que o Banco poderia criar um canal específico tanto para testar eventuais links fraudulentos, como para ter discussões abertas sobre golpes e fraudes, não somente se limitar a um e-mail para denúncia dos clientes de eventuais fraudes, e a espaços específicos como em comentários do Youtube. Informações como país do registro do domínio verificado, data de registro desse domínio, dentre outras informações nebulosas podem rapidamente ser analisadas. Isto porque os golpes e fraudes no meio digital tem sofrido transformações constantemente, alterando estratégias e formas de aplicação.

Ainda assim, para a autora, o Itaú Unibanco investe na construção de conteúdos não somente em páginas do site, mas em formatos diferentes, como *e-books*, rede sociais, o que também aproxima e gera confiança. Para além, o fato de a instituição financeira possuir a ISO 27001:2022 e ISO 27701:2019 evidencia a atenção nos pontos que tangem a gestão de riscos de Segurança da Informação e a preocupação do Itaú Unibanco em manter boas práticas em seu negócio.

Os vídeos da campanha foram patrocinados no Youtube, mas também alguns dos conteúdos foram reproduzidos em canais abertos da televisão brasileira (Terra, 2022). Ao considerar esse ponto, bem como a quantidade de visualização total dos vídeos, percebe-se a importância do papel da mídia na transmissão de conhecimentos considerados técnicos para públicos leigos (Batista, 2007). No que se refere aos comentários nas produções da campanha, um dos vídeos com mais comentários e relatos sobre pessoas que caíram no golpe, é do *Como se Proteger do Golpe do WhatsApp*. O Brasil é o terceiro país do mundo que mais usa o aplicativo (Terra, 2023), o que reforça a proximidade do nome da produção audiovisual, e a própria existência de um golpe, com um *modus operandi* aplicado para que as pessoas sejam vítimas. Isso demonstra o processo social dos riscos. Nesse sentido, é possível que por esses pontos o conteúdo gere ainda mais espaço para o compartilhamento de opiniões e percepções de risco. Relativo aos comentários que citavam a demora para o Itaú Unibanco produzir e divulgar campanhas como essa (relacionados aos tópicos de

golpes e fraudes), pode-se perceber como as organizações têm sido pressionadas para integrar iniciativas que demonstre ética e responsabilidade social quanto aos riscos que gera (Teixeira, 2019).

Assim, na sociedade de riscos, os públicos têm concedido para as organizações a definição de quais são riscos críticos e precisam ser observados, além de auxiliar na construção da percepção dos riscos para a sociedade. Dessa forma, nada mais justo, na opinião da pesquisadora, que o Banco esteja com iniciativas que demonstram responsabilidade social em relação aos riscos que ele mesmo produz.

Com o objetivo de centralizar as comparações feitas ao longo da análise, o Quadro 8 foi produzido pela autora e traz as principais inferências de cada vídeo da campanha do Itaú Unibanco.

Quadro 8 - As categorias analisadas e suas definições

	Como se Proteger do Golpe da Troca de Cartão	***Como se Proteger do Golpe da Falsa Central***	***Como se Proteger do Golpe do WhatsApp***	***Golpe da Troca do Cartão***	***Golpe do Falso Funcionário***	***Fique Atento***
Objetivos da comunicação de risco	Informar e educar	Informar e educar	Informar e educar Mudanças no comportamento e ações de proteção	Informar e educar Mudanças no comportamento e ações de proteção	Informar e educar Resolução conjunta de problemas	Informar e educar Mudanças no comportamento e ações de proteção
Características da mensagem de comunicação de risco	Formato narrativo	Formato narrativo	Formato narrativo	Formato narrativo	Formato narrativo	Formato narrativo e formato técnico
Engajamento e relacionamento com os públicos	Quanto mais informações sobre um risco, maior conscientização	A percepção da sociedade sobre o risco	Os riscos são experiências pessoas concretas	Riscos são socialmente construídos e moldados por atores sociais	O papel da percepção de risco individual na sociedade	A preocupação com os riscos gerada através da identificação com o conteúdo

Fonte: Elaborado pela autora (2024).

A partir da análise percebe-se que no cenário dos riscos de Segurança da Informação, o Itaú Unibanco tem saldos positivos em relação a sua postura. Ainda assim, existem melhorias de relacionamento e divulgações que podem aproximar seus públicos tanto da organização, como das percepções reais dos riscos que ela produz.

5 CONSIDERAÇÕES FINAIS

A produção de riscos relacionados a área da tecnologia é imensa e, com as novas funcionalidades digitais, tende a crescer constantemente. As organizações, especialmente do setor financeiro, são grandes produtoras de riscos desse tipo, afinal muitas delas estão buscando a centralização em atendimento e funcionalidades para o meio digital. Os indivíduos precisam estar atentos e informados sobre esses riscos, uma vez que são o elo mais fraco na tríade entre golpe, instituição e usuário. Assim, é importante que as pessoas estejam informadas sobre esses riscos, para que saibam como agir ao passar por situação semelhante. No cenário brasileiro, o Itaú Unibanco se destaca por se tratar de um dos bancos mais antigos e que segue sendo um dos líderes em número de clientes e em faturamento. Por esse motivo, o Banco produz também riscos relacionados à Segurança da Informação e constantemente precisa geri-los.

Este estudo teve como problema de pesquisa a questão: quais são os aspectos da comunicação de risco utilizada pelo Itaú Unibanco na campanha *Itaú e você contra golpes e fraudes*? Compreende-se que o problema foi respondido, já que foram estabelecidas três categorias de análise relacionadas aos aspectos da comunicação de risco utilizada pelo Banco. Isso, juntamente com os comentários positivos, demonstram que o Itaú Unibanco conseguiu criar uma sequência de conteúdos com aspectos da comunicação de risco, considerando as especificidades de cada um dos golpes e fraudes abordados.

O objetivo geral foi analisar a comunicação de risco utilizada pelo Itaú Unibanco no contexto específico da Segurança da Informação. Compreende-se que dentre os objetos analisados foi possível classificar os principais elementos utilizados pelo Banco em seu processo de comunicação de risco junto aos públicos considerando-os em sua maioria informativos e educativos, e em formato narrativo. Assim, acredita-se que o objetivo foi atingido, na medida em que classificou e apontou as construções feitas nos vídeos da campanha *Itaú e você contra golpes e fraudes*, e na página de *Segurança* do site do Itaú Unibanco.

Em relação aos objetivos específicos, ao longo do estudo tornou-se viável compreender as perspectivas teóricas de risco no ambiente da Segurança da Informação. Autores de diferentes áreas foram apresentados nas conceituações, possibilitando a compreensão do risco sob a visão da área da Segurança da

Informação. Além disso, após os enfoques teóricos, também se tornou viável a caracterização da comunicação de risco usada pelo Itaú Unibanco em sua campanha, através da classificação do objetivo dos conteúdos, as características das mensagens, o uso de expressões faciais e de ícones que concentram no problema apresentado em cada um dos vídeos.

Quanto às limitações da pesquisa, o estudo identificou o engajamento e relacionamento através dos comentários nos vídeos, o que de certa forma restringe a identificação da percepção dos públicos, bem como as discussões em relação às suas reações em geral quanto a comunicação de risco da campanha. Uma vez que o espaço dos comentários é um recorte, caso entrevistas tivessem sido realizadas para comparar a recepção do conteúdo, os comentários, assim como material de entrevistados, possivelmente poderiam reforçar pontos de relacionamento entre o Banco e seus públicos.

Entretanto, acredita-se que a pesquisa contribui com a área de Relações Públicas, principalmente ao aproximar questões da comunicação em uma área como a da Segurança da Informação, que produz muitos riscos e precisa gerenciá-los ao longo de fluxos de comunicação bem definidos.

Incentiva-se que outros profissionais da área pesquisem os riscos da tecnologia e seus processos comunicacionais. Tendo em vista que o trabalho de Relações Públicas também envolve o ambiente digital, onde estamos constantemente suscetíveis a fraudes e golpes, também nos compete a produção de estudos nessa área tão multidisciplinar como a comunicação de riscos.

REFERÊNCIAS

A FEBRABAN. *In*: FEBRABAN. São Paulo, [2024]. Disponível em: https://portal.febraban.org.br/pagina/3031/9/pt-br/institucional#:~:text=O%20quadro%20associativo%20da%20entidade,l%C3%ADquido%20das%20institui%C3%A7%C3%B5es%20banc%C3%A1rias%20brasileiras. Acesso em: 03 ago. 2024.

ANDRELO, R. Relações públicas sob o prisma da estratégia. *In*: ANDRELO, R. **As relações públicas e a educação corporativa**: uma interface possível. São Paulo: Editora, 2016. p. 21-36. *E-book*. Disponível em: https://books.scielo.org/id/hwgqy/pdf/andrelo-9788568334775-03.pdf. Acesso em: 14 jul. 2024.

AREOSA, J. **Riscos e sinistralidade laboral**: um estudo de caso em contexto organizacional. Tese (Doutor em Sociologia) – Instituto Universitário de Lisboa, Lisboa, 2010. Disponível em: https://repositorio.iscte-iul.pt/handle/10071/4422. Acesso em: 14 jul. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR 31000**: gestão de riscos - princípios e diretrizes. Rio de Janeiro: ABNT, 2009. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4656830/mod_resource/content/1/ISO31000.pdf. Acesso em: 03 ago. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação Rio de Janeiro: ABNT, 2005. Disponível em: http://www.professordiovani.com.br/AdmRedes/NBRISO-IEC27002.pdf. Acesso em: 14 jul. 2024.

AXUR. Relatório Axur: threat landscape 2023/2024. *In*: AXUR. [*S. l.*], 24 jan. 2024. Disponível em: https://www.axur.com/pt-br/report-axur-2023. Acesso em: 14 jul. 2024.

BARDIN, L. Definição e relação com as outras ciências. *In*: BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1977. p. 27-46. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7684991/mod_resource/content/1/BARDlN__L._1977._Analise_de_conteudo._Lisboa__edicoes__70__225.20191102-5693-11evk0e-with-cover-page-v2.pdf. Acesso em: 14 jul. 2024.

BARINGS bank. *In*: WIKIPÉDIA: a enciclopédia livre. [San Francisco: Wikimedia Foundation], 07 maio 2019. Disponível em: https://pt.wikipedia.org/wiki/Barings_Bank. Acesso em: 14 jul. 2024.

BATISTA, L. L. A comunicação de riscos no mundo corporativo e o conteúdo da mensagem. **Organicom**, São Paulo, v. 4, n. 6, p. 1-14, jan./jun. 2007. Disponível em: https://www.revistas.usp.br/organicom/article/view/138928. Acesso em: 14 set. 2024.

BECK, U. A vida em uma sociedade pós-industrial. *In*: GIDDENS, A.; BECK, U.; LASH, S. (org.). **Modernização reflexiva**: política, tradição e estética na ordem social moderna. São Paulo: Unesp, 1997. p. 73-133.

BECK, U. **Sociedade de risco**. São Paulo: 34, 2010.

BECK, U. **World risk society**. Cambridge: Polity Press, 1999.

BERNSTEIN, P. Introduction. *In*: BERNSTEIN, P. **Against the gods**: the remarkable story of risk. New York: John Wiley & Sons, Inc, 1996. p. 1-8. Disponível em: https://matrixtrainings.files.wordpress.com/2014/09/against-the-gods-the-remarkable-story-of-risk-1996-peter-l-bernstein.pdf. Acesso em: 14 jul. 2024.

BRENT spar. *In*: WIKIPÉDIA: a enciclopédia livre. [San Francisco: Wikimedia Foundation], 04 ago. 2023. Disponível em: https://pt.wikipedia.org/wiki/Brent_Spar. Acesso em: 14 jul. 2024.

CAROCHINHO, J. A. O conceito de “perceção do risco”: contributo da psicologia social. **ResPublica**: revista lusófona de ciência política, segurança e relações internacionais, Lisboa, p. 77-87, 17 mar. 2011. Disponível em: https://recil.ulusofona.pt.handle/10437/4296. Acesso em: 14 jul. 2024.

CLARKE, L.; JAMES, F. Social organization and risk: some current controversies. **Annual review of sociology**, [*s. l.*], v. 19, p. 375-399, ago. 1993. Disponível em: https://www.annualreviews.org/content/journals/10.1146/annurev.so.19.080193.002111. Acesso em: 14 jul. 2024.

COVELLO, V. T.; WINTERFELDT, D. von; SLOVIC, P. Risk communication: a review of the literature. **Risk abstracts**, [*s. l.*], v. 3, n. 4, p. 171-182, jan. 1986. Disponível em: https://www.researchgate.net/publication/285817518_Risk_communication_A_review_of_the_literature. Acesso em: 14 jul. 2024.

CYBERSECURITY ventures report on cybercrime. *In*: ESENTIRE, [*S. l.*], 2023. Disponível em: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime#:~:text=The%202023%20Cybersecurity%20Ventures%20Cybercrime%20Report%20predicts%20a%20rapid%20increase,%243%20trillion%20recorded%20in%202015. Acesso em: 03 ago. 2024.

D'ADDARIO, J. Brasil engatinha quando o assunto é Segurança da Informação e Continuidade de Negócios. *In*: BLOG Dayrus. [*S. l.*], 15 abr. 2020. Disponível em: https://blog.daryus.com.br/brasil-engatinha-quando-o-assunto-e-seguranca-da-informacao-e-continuidade-de-negocios/. Acesso em: 14 jul. 2024.

DARLEY, J. M.; LATANÉ, B. Bystander intervention in emergencies: diffusion of responsibility. **Journal of personality and social psychology**, [*s. l.*], v. 8. p. 377-383, 1968. Disponível em: https://psycnet.apa.org/record/1968-08862-001. Acesso em: 14 jul. 2024.

DOUGLAS, M. **How institutions think**. Syracuse: SyracuseUniversity Press, 1987.

DOUGLAS, M. **Pureza e perigo**: Ensaio sobre a noção de poluição e tabu. Rio de janeiro: Edições 70, 1966. Disponível em: https://edisciplinas.usp.br/pluginfile.php/1861113/mod_resource/content/1/pureza-e-perigo-mary-douglas.pdf. Acesso em: 03 ago. 2024.

DOUGLAS, M. **Risk and blame**: essays in cultural theory. London: Routledge, 1992.

DOUGLAS, M.; WILDAVSKY, A. **Risk and culture**: an essay on the selection of technological and environmental dangers. Berkeley: University of California Press, 1982.

FERNANDES, J. H. C**. Introdução à gestão de riscos em segurança da informação**. Brasília: EdUnB, 2011. *E-book*. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf. Acesso em: 14 jul. 2024.

FISCHHOFF, B.; KADVANY, J. **Risk**: a very short introduction. New York: Oxford University Press, 2011.

FISCHHOFF, B.; SLOVIC, P.; LICHTENSTEIN, S.; READ, S.; COMBS, B. How safe is safe enough? A psychometric study of towards technological risks and benefits. **Policy sciences**, [*s. l.*], v. 9, p. 127-152, 1978. Disponível em: https://www.cmu.edu/epp/people/faculty/research/PS%20FSLRC%20HowSafe.pdf. Acesso em: 14 jul. 2024.

FREITAS, C. M de; GOMEZ, C. M. Análise de riscos tecnológicos na perspectiva das ciências sociais. **História, ciências, saúde**: Manguinhos, Rio de Janeiro, v. III, n. 3, p. 485-504, 1996. Disponível em: https://www.scielo.br/j/hcsm/a/t9YRgDSmJwQs7rgNPWkXXPB/?format=pdf&lang=pt. Acesso em: 14 jul. 2024.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIULIO, G. M. Di; VASCONCELLOS, M. da P.; GÜNTHER, V. M. R.; RIBEIRO, H.; ASSUNÇÃO, J. V. de. Percepção de risco: um campo de interesse para a interface ambiente, saúde e sustentabilidade. **Saúde e Sociedade**, São Paulo, v. 24, n. 4, p. 1217-1231, 7 out. 2015. Disponível em: https://www.scielo.br/j/sausoc/a/jCwXwbpCHsYcCZJDgHHfJgy/#. Acesso em: 14 jul. 2024.

GOLDING, D.; KRIMSKY, S.; PLOUGH, A. Evaluating risk communication: narrative vs. technical presentations of information about Radon. **Risk Analysis**, [*s. l.*], v. 12, n. 1, p. 27-35, 1992. Disponível em: https://pubmed.ncbi.nlm.nih.gov/1574615/. Acesso em: 03 ago. 2024.

GOLPE da maquininha de cartão: o que fazer? Consigo uma indenização? *In*: JUSBRASIL. [*S. l.*], jan. 2024. Disponível em: https://www.jusbrasil.com.br/artigos/golpe-da-maquininha-de-cartao-o-que-fazer-consigo-uma-indenizacao/2081892422. Acesso em: 26 ago. 2024.

GOLPE do WhatsApp: saiba como se proteger e o que fazer se for vítima. *In*: SERASA. [*S. l.*], c2024. Disponível em: https://www.serasa.com.br/premium/blog/golpe-do-whatsapp-o-que-fazer/. Acesso em: 26 ago. 2024.

GOLPES digitais crescem 35% em 2023. *In*: TI INSIDE. [*S. l.*], 29 dez. 2023. Newsletter. Disponível em: https://tiinside.com.br/29/12/2023/golpes-digitais-crescem-35-em-2023/. Acesso em: 03 ago. 2024.

GONÇALVES, R. Crimes cibernéticos avançam no Brasil e aceleram com a tecnologia: País ocupa a vice-liderança em ranking global de casos, e especialistas alertam sobre os golpes mais frequentes na internet. *In*: Correio Braziliense, Brasília, DF, 24 mar. 2024. Disponível em: https://www.correiobraziliense.com.br/economia/2024/03/6824212-crimes-ciberneticos-avancam-no-brasil-e-aceleram-com-a-tecnologia.html. Disponível em: https://www.correiobraziliense.com.br/economia/2024/03/6824212-crimes-ciberneticos-avancam-no-brasil-e-aceleram-com-a-tecnologia.html. Acesso em: 03 ago. 2024.

GOUVEIA, L. **Gestão de segurança da informação**. Porto: Universidade Técnica do Porto, 2016. *E-book*. Disponível em: https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 14 jul. 2024.

GRUNIG, J. Guia de pesquisa e medição para elaborar e avaliar uma função excelente de Relações Públicas. **Organicom**, São Paulo, v. 2, n. 2, p. 46–69, 2005. Disponível em: https://www.revistas.usp.br/organicom/article/view/138881. Acesso em: 14 jul. 2024.

GRUNIG, J.; FERRARI, M. A.; FRANÇA, F. **Relações Públicas**: teoria, contexto e relacionamentos. São Paulo: Difusão, 2009.

GUIVANT, J. A teoria da sociedade de risco de Ulrich Beck: entre o diagnóstico e a profecia. **Estudos sociedade e agricultura**, Rio de Janeiro, p. 95-112, 16 abr. 2001. Disponível em: https://revistaesa.com/ojs/index.php/esa/article/view/188/184. Acesso em: 14 jul. 2024.

HACKERS causaram prejuízos a 23% das empresas brasileiras em 2022: Apenas sete em cada dez companhias recuperaram o acesso aos seus dados após pagarem o resgate em ataques digitais. *In*: FORBES [*S. l.*], 06 mar. 2023. Disponível em: https://forbes.com.br/forbes-money/2023/03/hackers-causaram-prejuizos-a-23-das-empresas-brasileiras-em-2022/. Acesso em: 03 ago. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **About ISO**. Geneva, [2024]. Disponível em: https://www.iso.org/about. Acesso em: 14 jul. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 31000:2018**: risk management. Geneva: ISO, 2018a. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en. Acesso em: 14 jul. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27005:2018**: information technology – Security techniques – Information security risk management. Geneva: ISO, 2018b. Disponível em: https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027005-2018.pdf. Acesso em: 14 jul. 2024.

ITAÚ Unibanco reforça quadro em 3,1 mil colaboradores e fecha 2021 com 99,6 mil. *In*: MONEYTIMES. [*S. l*.], 10 fev. 2022. Disponível em: https://moneytimes.com.br/itau-unibanco-reforca-quadro-em-31-mil-colaboradores-e-fecha-2021-com-996-mil/. Acesso em: 14 jul. 2024.

ITAÚ, o seu banco seguro. *In*: ITAÚ. [*S. l*.], c2023. Disponível em: https://www.itau.com.br/seguranca. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: como se proteger do Golpe da troca de cartão. [*S. l*.: *s. n*.], 19 ago. 2022a. 1 vídeo (45 s). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=sUeBXQpDWC4. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: como se proteger do Golpe da falsa central. [*S. l*.: *s. n*.], 23 ago. 2022b. 1 vídeo (45 s). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=A6Gsg_VHgnY. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: como se proteger do Golpe no WhatsApp. [*S. l*.: *s. n*.], 25 ago. 2022c. 1 vídeo (45 s). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=vs27aeCECXc. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: fique atento. [*S. l*.: *s. n*.], 21 set. 2023c. 1 vídeo (1 min). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=LphT3OYAOZM. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: golpe da Troca do Cartão. [*S. l*.: *s. n*.], 15 fev. 2023a. 1 vídeo (1 min). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=EWePhygyFG8. Acesso em: 03 ago. 2024.

ITAÚ. **Itaú e você contra golpes e fraudes**: golpe do Falso Funcionário. [*S. l*.: *s. n*.], 16 fev. 2023b. 1 vídeo (1 min). Publicado pelo Itaú. Disponível em: https://www.youtube.com/watch?app=desktop&v=jIB7eE6sqWE&t=1s. Acesso em: 03 ago. 2024.

ITAÚ. Sua vida digital e os seus dados estão seguros? São Paulo: Itaú, [2024]. Acesso em: 03 jul. 2024. Disponível em: https://www.itau.com.br/assets/dam/publisher/01_itau/11_fraudes/02_seg_ebook_pdf/finais/EBK_00_SEGURANCA.pdf. Acesso em: 03 ago. 2024.

JOHNSON, B. B.; COVELLO, V. T. Introduction: the social and cultural construction of risk: issues, methods, and case studies. *In*: JOHNSON, B. B.; COVELLO, V. T. (ed.). **The Social and cultural construction of risk**: essays on risk selection and perception. Dordrecht: D. Reidel Publishing Company, 1987.

KODIC, M. CEO do Itaú prioriza cultura centrada no cliente em cenário ultracompetitivo. *In*: FORBES Money. [*S. l*.], 30 dez. 2023. Disponível em: https://forbes.com.br/forbes-money/2023/12/ceo-do-itau-prioriza-cultura-centrada-no-cliente-em-cenario-ultracompetitivo/. Acesso em: 14 jul. 2024.

LIMA, K. Itaú divulga campanha de prevenção contra fraudes bancárias. *In*: TERRA. [*S. l*.], 06 set. 2022. Disponível em: https://www.terra.com.br/byte/itau-divulga-campanha-de-prevencao-contra-fraudesbancarias,c54dc14a39e98542f79bfacd543078f94u3drgqu.html. Acesso em: 14 jul. 2024.

LIMA, M. L. Percepção de riscos e culturas de segurança nas organizações. **Psicologia**, Lisboa, v. 12, n. 2, p. 379-386, 1999. Disponível em: https://revista.appsicologia.org/index.php/rpsicologia/article/view/584. Acesso em: 14 jul. 2024.

LOGOTIPO Itaú. *In*: GOOGLE imagens. Mountain View: Google, [2024]. Disponível em: https://www.google.com/search?sca_esv=5be91180a9a77bb4&sca_upv=1&rlz=1C1GCEU_pt-BRBR1027BR1027&sxsrf=ADLYWILr7s93yZWOmb_6ldPAY-ho2Omogw:1720994615023&q=logotipo+ita%C3%BA&udm=2&fbs=AEQNm0AuaLfhdrtx2b9ODfK0pnmi046uB92frSWoVskpBryHTpm4Flwlr5cHTE9P1oWvlAb4U7NWllknKnQGkVtXHmLHAzXNmIZSfbj7jBG9Zz8MlQPotq4j2_jY0XYatL80sHhnNhUFQ6gHIK-y_uhG4CIgi-UUDXkPZirzaM49E1XyyTpbTgnjUwz6YghxhIN1sIEqQWkzbNK9TvHLhZnZbIaF4tIJJw&sa=X&ved=2ahUKEwjjisHFxKeHAxXer5UCHdPhD1IQtKgLegQIERAB&biw=1920&bih=919&dpr=1. Acesso em: 14 jul. 2024

LUPTON, D. **Risk**. London: Routledge, 1999.

MARCIANO, J. L.; MARQUES, M. L. O enfoque social da segurança da informação. **Ciência da informação**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. Disponível em: https://www.scielo.br/j/ci/a/L8CqcznptmQK3jyqGqNpWMQ/?lang=pt&format=pdf. Acesso em: 14 jul. 2024.

NUBANK passa o Banco do Brasil em número de clientes e se torna o 4º maior do Brasil. *In*: G1. [*S. l*.], 16 jul. 2023. Disponível em: https://g1.globo.com/economia/negocios/noticia/2023/07/26/nubank-passa-o-banco-do-brasil-em-numero-de-clientes-e-se-torna-o-4o-maior-do-brasil.ghtml. Acesso em: 14 jul. 2024.

NUBANK supera Itaú e é (de novo) banco mais valioso da AL: qual ação é mais atrativa?. *In*: INFOMONEY. [*S. l*.], 29 maio. 2024. Disponível em: https://www.infomoney.com.br/mercados/nubank-roxo34-supera-itau-itub4-e-e-de-novo-banco-mais-valioso-da-america-latina-qual-acao-e-mais-atrativa/. Acesso em: 14 jul. 2024.

O QUE É phishing? *In*: MICROSOFT. [*S. l*.], c2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-phishing. Acesso em: 14 jul. 2024.

OTWAY, H. Regulation and Risk Analysis. *In*: OTWAY, H.; PELTU, M. (org.), **Regulating industrial risks**: science, hazards and public protection. London: Butterworths, 1985.

PERFIL corporativo. Muito prazer, nós somos o Itaú Unibanco! *In*: ITAÚ. [*S. l.*], 2024. Disponível em: https://www.itau.com.br/relacoes-com-investidores/itau-unibanco/perfil-corporativo/. Acesso em: 03 ago. 2024.

PIDGEON, N.; KASPERSON, R. E.; SLOVIC, P. **The social amplification of risk**. Cambridge: Cambridge University Press, 2003.

POWER, M. **Risk management of everything**: rethinking the politics of uncertainty. Londres: Demos, 2004. *E-book*. Disponível em: https://demos.co.uk/wp-content/uploads/files/riskmanagementofeverything.pdf. Acesso em: 14 jul. 2024.

RANSOMWARE: definição, prevenção e remoção. *In*: KASPERSKY. [*S. l.*], c2024. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 03 ago. 2024.

RAYNER, S.; CANTOR, R. How fair is safe enough? The cultural approach to societal technology choice. **Risk analysis journal**, [*s. l.*], v. 7, n. 1, p. 3-9, mar. 1987. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1987.tb00963.x. Acesso em: 14 jul. 2024.

REBELO, F. Terminologia do risco: origens, dificuldades de tradução e bom senso. In: REBELO, F. **Realidades e desafios na gestão dos riscos**: diálogo entre ciência e utilizadores. Coimbra: [*s. n*.], 2014. p. 7-17. Disponível em: https://www.uc.pt/fluc/nicif/Publicacoes/livros/dialogos/Artg01.pdf. Acesso em: 14 jul. 2024.

RENN, O. **Risk governance**: coping with uncertainty in a complex world. London: Earthscan, 2008.

RINALDI, A.; BARREIROS, D. A importância da comunicação de riscos para as organizações. **Organicom**, São Paulo, ano 4, n. 6, p. 137-147, jan./jun. 2007. Disponível em: https://revistas.usp.br/organicom/article/view/138930/134278. Acesso em: 14 jul. 2024.

ROVERE, L. **Comunicação e percepção de risco em áreas contaminadas**. 2007. Dissertação (Mestrado em Saúde Pública) – Faculdade de Saúde Pública, Universidade de São Paulo, São Paulo, 2006. Disponível em: https://www.teses.usp.br/teses/disponiveis/6/6134/tde-26092022-160927/publico/MTR_1478_Rovere_2006.pdf. Acesso em: 14 jul. 2024.

ROWE, A. **An anatomy of risk**. New York: Willey, 1977.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2013.

SÉRIE RISK MANAGEMENT. **Gestão de riscos**: diretrizes para a implementação da AS/NZS 4360. São Paulo: Risk Tecnologia Editora, 2005.

SIQUEIRA, A.; UMGELTER, B.; LIMA E.; AMORIM, G. Chernobyl. *In*: MOSTRA DE CIÊNCIAS, 03., 2016, Canoas. **Anais eletrônicos** [...]. Canoas: Ulbra, 2016. Disponível em:

http://www.conferencias.ulbra.br/index.php/sicjr/iv/paper/viewFile/4793/2477. Acesso em: 03 ago. 2024.

SLOVIC, P. Perception of risk. **Science**, [*s. l.*], v. 236, n. 4799, p. 280-285, 1987.

STUMPF, I. R. C. Pesquisa bibliográfica. *In*: DUARTE, J.; BARROS A. (org.). **Métodos e técnicas de pesquisa em comunicação.** São Paulo: Atlas, 2005.

TEIXEIRA, P. B. **Caiu na rede**: e agora? Gestão e gerenciamento de crises nas redes sociais. 2. ed. São Paulo: Évora, 2019.

THEYS, J. La société vulnérable. *In*: FABIANI, J-L.; THEYS, J. (org.) **la société vulnérable**: évaluer et maftriser les risques. Paris: Presses de L'École Normale Supérieure, 1987. p. 3-35.

TIERNEY, K. J. Toward a critical sociology of risk. **Sociological forum**, [*s. l.*], v. 14, n. 2, p. 215- 242, 1999.

WORLD ECONOMIC FORUM. **Global risks report 2022**: 17th edition. [*S. l.*]: World Economic Forum, 2022. Disponível em: https://www.weforum.org/publications/global-risks-report-2022/. Acesso em: 14 jul. 2024.

WORLD ECONOMIC FORUM. **Global risks report 2023**: 18th edition. [*S. l.*]: World Economic Forum, 2023. Disponível em: https://www.weforum.org/publications/global-risks-report-2023/. Acesso em: 14 jul. 2024.

WORLD ECONOMIC FORUM. Global Risks Report 2024: 19th edition. [*S. l.*]: World Economic Forum, 2024. Disponível em: https://www.weforum.org/publications/global-risks-report-2024/. Acesso em: 14 jul. 2024.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.