Comunicação de Risco na Campanha Itaú e Você Contra Golpes e Fraudes[1]

Amanda Bedra Serratt[2]
Universidade Federal do Rio Grande do Sul – UFRGS

RESUMO

Este estudo, que constitui um recorte de um Trabalho de Conclusão de Curso, analisa a comunicação de risco do Itaú Unibanco no contexto da Segurança da Informação, com foco na campanha *Itaú e você contra golpes e fraudes*. Com caráter exploratório, a pesquisa combina revisão bibliográfica e estudo de caso, abordando conceitos de risco, percepção de risco e comunicação. A análise dos vídeos da campanha e dos comentários no YouTube evidenciou uma abordagem educativa e narrativa que facilita a identificação do público com o conteúdo. Os resultados indicam que o banco constrói um relacionamento contínuo com seus clientes, sendo a maioria das reações positivas, o que sugere eficácia na estratégia de comunicação adotada.

PALAVRAS-CHAVE: comunicação de risco; segurança da informação; Relações Públicas; Itaú Unibanco.

A COMUNICAÇÃO DE RISCO EM TEMPOS DE AMEAÇAS CIBERNÉTICAS

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). 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). A produção de riscos relacionados à 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

[1] Trabalho apresentado no Grupo de Trabalho Risco, crise e comunicação, evento integrante da programação do 24º Congresso de Ciências da Comunicação na Região Sul, realizado de 3 a 5 de julho de 2025.
[2] Bacharel em Relações Públicas – UFRGS, email: amandabedra1@gmail.com.

precisam estar atentos e informados sobre esses riscos, uma vez que são o elo mais fraco na tríade entre golpe, instituição e usuário. Dessa forma, é importante que as pessoas estejam informadas sobre esses riscos, para que saibam como agir ao passar por situações semelhantes. A área da tecnologia, especialmente a Segurança da Informação, abrange uma ampla variedade de setores, resultando em uma pluralidade de riscos e ameaças, como exemplos: 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.

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. Desse modo, conforme Marciano e Marques (2006) a segurança permeia as arquiteturas e modelos da informação, incorporando-se em todos os seus níveis.

Nesse cenário, a comunicação de risco tem um papel crucial em tentar abordar a percepção de riscos da Segurança da Informação para a sociedade. Assim, bancos como o Itaú Unibanco, devem ser transparentes sobre esses riscos, já que também são produtores deles. Nessa perspectiva, este trabalho apresenta alguns resultados obtidos por um Trabalho de Conclusão de Curso de Graduação em Relações Públicas, o qual buscou avaliar as características da comunicação de risco na campanha *Itaú e você contra golpes e fraudes* do Itaú Unibanco. Para tal, os métodos aplicados foram pesquisa bibliográfica (Stumpf, 2005), estudo de caso (Gil, 2002) e (Yin, 2001) a fim de focar no Itaú Unibanco, e as técnicas de análise documental (Gil, 2002) e análise de conteúdo (Bardin, 1977) para a construção das categorias analisadas ao longo do Trabalho de Conclusão de Curso. Já o referencial teórico contém autores como Ulrich Beck (2010) para a conceitualização de risco, Rovere (2006), Darley e Latané (1968) e Douglas (1966) para percepção de risco e Leandro Batista (2007) para a compreensão dos formatos das mensagens de comunicação de risco.

Para fins de análise, definiram-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 contêm 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 do público em geral de percepções compartilhadas por Andrelo (2016), Grunig (2005), Rovere (2006) e outros.

Sobre os resultados obtidos, o formato narrativo citado por Batista (2007) mostrou-se completamente presente em todos os vídeos da campanha, o que parece ser devido à necessidade de identificação em um contexto como os riscos da Segurança da Informação. Ainda assim, seria importante que a abordagem técnica aparecesse mais para informar sobre medidas de proteção, como o que aparece no último vídeo da campanha (*Fique Atento)*, já que as informações técnicas auxiliam o público leigo a compreender mais o desenvolvimento e esquemas por trás 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 contada, 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.

Além 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 no geral, acendem um alerta para o receptor, como “sempre confira seu cartão: se trocarem,

é golpe" ou então a própria mensagem geral do vídeo *Fique Atento*, em que o ator repassa por diversos golpes e a atriz segue afirmando que todos são golpe. 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 a serem 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.

Por fim, a pesquisadora concluiu que o Banco poderia criar um canal específico tanto para testar eventuais links fraudulentos, 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*, redes sociais, conteúdos em diferentes formatos, 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.

Assim sendo, 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.

REFERÊNCIAS

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.

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/BARDIN__L._1977._Analise_de_conteudo.pdf. 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. **Sociedade de risco**. São Paulo: Editora 34, 2010.

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. Acesso em: 03 ago. 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. **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.

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

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.

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.

MATTOS, F. de A. M. et al. **Métodos e técnicas de pesquisa em comunicação**. São Paulo: Atlas, 2005.

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/tde26092022160927/publico/MTR_1478_Rovere_2006.pdf. Acesso em: 14 jul. 2024.

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

WORLD ECONOMIC FORUM. **Global Risks Report 2024**: 19th edition. [s.*I.*]: 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.