Universidade Federal de Alagoas – UFAL

Curso de Relações Públicas

CRISES DE COMUNICAÇÃO NO CONTEXTO DIGITAL: ANÁLISE DA INFLUÊNCIA DE CRIMES CIBERNÉTICOS NA IMAGEM DA EQUATORIAL ALAGOAS, BANCO ITAÚ E SERASA EXPERIAN

Bruno do Nascimento Gonzaga

Maceió
2025

Universidade Federal de Alagoas – UFAL

Curso de Relações Públicas

CRISES DE COMUNICAÇÃO NO CONTEXTO DIGITAL: ANÁLISE DA INFLUÊNCIA DE CRIMES CIBERNÉTICOS NA IMAGEM DA EQUATORIAL ALAGOAS, BANCO ITAÚ E SERASA EXPERIAN

Bruno do Nascimento Gonzaga

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de bacharel no curso de Relações Públicas da Universidade Federal de Alagoas.

Orientador(a): Profa. Janaína Alves Pereira Almeida dos Santos

Maceió
2025

Catalogação na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

G642c Gonzaga, Bruno do Nascimento.
Crises de comunicação no contexto digital : análise da influência de crimes cibernéticos na imagem da Equatorial Alagoas, Banco Itaú e Serasa Experian / Bruno do Nascimento Gonzaga. - 2025.
84 f. : il. color.

Orientadora: Janaína Alves Pereira Almeida dos Santos.
Monografia (Trabalho de Conclusão do Curso em Relações Públicas) – Universidade Federal de Alagoas. Instituto de Ciências, História, Comunicação e Artes. Maceió, 2025.

Bibliografia: f. 79-84.

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. Relações Públicas. 3. Ambiente cibernético. 4. Administração de crises. 5. Imagem corporativa. 6. Estratégia da comunicação. I. Título.

CDU: 659.4:34:004.738.5

BRUNO DO NASCIMENTO GONZAGA

CRISES DE COMUNICAÇÃO NO CONTEXTO DIGITAL: ANÁLISE DA INFLUÊNCIA DE CRIMES CIBERNÉTICOS NA IMAGEM DA EQUATORIAL ALAGOAS, BANCO ITAÚ E SERASA EXPERIAN

Trabalho de Conclusão de Curso apresentado ao Instituto de Ciências Humanas, Comunicação e Artes, como requisito parcial para obtenção do grau de Bacharel em Relações Públicas pela Universidade Federal de Alagoas.

Data de Aprovação: 31/03/2025

Banca Examinadora:

Documento assinado digitalmente
gov.br
JANAINA ALVES PEREIRA ALMEIDA DOS SANTOS
Data: 02/04/2025 18:54:38-0300
Verifique em https://validar.iti.gov.br

Profª Msc. Janaina Alves Pereira Almeida dos Santos
(Orientadora)

Documento assinado digitalmente
gov.br
MANOELLA MARIA PINTO MOREIRA DAS NEVES
Data: 31/03/2025 19:50:06-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Manoella Maria Pinto Moreira das Neves
(1ª Examinadora)

Documento assinado digitalmente
gov.br
MANUELA RAU DE ALMEIDA CALLOU
Data: 02/04/2025 15:39:35-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Manuela Rau de Almeida Callou
(2ª Examinadora)

Dedico este trabalho, com todo o meu amor e saudade, ao meu querido irmão Adelson.

Agradecimentos

Agradeço a mim mesmo pelo empenho, dedicação e persistência na produção deste trabalho.

Agradeço a minha professora e orientadora, Janaina Alves, sou profundamente grato pelo esforço, tempo, valiosas sugestões de melhoria e, acima de tudo, pela confiança depositada em mim ao longo da produção deste humilde trabalho.

Agradeço a todos que fizeram parte e contribuíram de alguma forma para que eu pudesse chegar até este momento ímpar de minha jornada acadêmica, especialmente aos meus pais, à Stéphany e aos meus professores durante a graduação.

"Just wake up
Can't you wake up?
(You do know this is just a simulation, don't you?)
Who is the crowd that peers through the cage
As we perform here upon the stage?
Tell me a lie in a beautiful way
I believe in answers, just not today"

— Avenged Sevenfold, *The Stage*

Resumo

Este Trabalho de Conclusão de Curso (TCC) investiga os procedimentos metodológicos e as práticas regulatórias empregadas no enfrentamento de crises cibernéticas em organizações, com ênfase nas implicações para a reputação corporativa e a confiança do público. Fundamenta-se teoricamente em autores como Margarida Kunsch, José Forni, Jorge Duarte e Carolina Frazon Terra, que abordam a importância da comunicação organizacional estratégica, da gestão da reputação e do relacionamento com stakeholders em contextos de crise. Em um cenário de intensa digitalização e crescente incidência de crimes digitais, a segurança cibernética surge como um pilar indispensável para a sustentabilidade organizacional, especialmente à luz da Lei Geral de Proteção de Dados (LGPD), com base em autores do campo jurídico como Gabriela Bandeira, Vitelino Brustolin, Siderly Almeida, que discutem os marcos legais da proteção de dados e os desafios trazidos pelas leis de crimes cibernéticos. Utilizando uma abordagem qualitativa, o estudo analisa casos práticos de gestão de crises digitais, visando compreender as estratégias comunicacionais e identificar aspectos críticos das políticas de segurança da informação no contexto organizacional contemporâneo.

Palavras-chave: Relações Públicas; Crises cibernéticas; Gestão de crises; Reputação corporativa; LGPD; Comunicação estratégica.

Abstract

This undergraduate thesis investigates the methodological procedures and regulatory practices employed in addressing cyber crises within organizations, with an emphasis on the implications for corporate reputation and public trust. The theoretical framework is based on authors such as Margarida Kunsch, José Forni, Jorge Duarte, and Carolina Frazon Terra, who highlight the importance of strategic organizational communication, reputation management, and stakeholder engagement in crisis contexts. In a scenario marked by intense digitalization and a growing incidence of cybercrimes, cybersecurity emerges as an essential pillar for organizational sustainability, especially in light of the General Data Protection Law (LGPD). The study also draws on legal scholars such as Gabriela Bandeira, Vitelino Brustolin, and Siderly Almeida, who discuss the legal frameworks of data protection and the challenges posed by cybercrime legislation. Using a qualitative approach, the study analyzes practical cases of digital crisis management, aiming to understand communication strategies and identify critical aspects of information security policies in the contemporary organizational context.

Keywords: Public Relations; Cyber crises; Crisis management; Corporate reputation; LGPD; Strategic communication.

LISTA DE FIGURAS

LISTA DE IMAGENS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O presente Trabalho de Conclusão de Curso (TCC) tem como objetivo central analisar os procedimentos metodológicos e as práticas regulatórias adotadas no enfrentamento de crises cibernéticas em organizações, com foco específico nas implicações para a reputação corporativa e a confiança do público. Em um cenário de intensa digitalização, a segurança cibernética configura-se como um alicerce indispensável para a sustentabilidade organizacional, particularmente em função do aumento expressivo de crimes digitais, que desafiam as fronteiras tecnológicas, e das rigorosas exigências impostas pela Lei Geral de Proteção de Dados (LGPD).

A evolução das tecnologias digitais e a crescente popularidade dos serviços online trouxeram benefícios significativos, como maior acessibilidade, conectividade e inovação nos processos organizacionais. Contudo, essas transformações também expuseram vulnerabilidades, tornando as organizações alvo de ataques cibernéticos, que vão desde vazamentos de dados, *ransomwares*[1] a golpes de *phishing*[2]. Esses crimes não apenas podem causar prejuízos financeiros, como também geram impactos profundos na credibilidade e na imagem das empresas perante seus públicos de interesse. A necessidade de estratégias robustas e integradas para prevenir e mitigar esses riscos nunca foi tão evidente.

Neste sentido, a escolha metodológica recai sobre uma abordagem qualitativa, com foco na análise de casos práticos que permitam evidenciar lacunas e oportunidades nas políticas e práticas de segurança cibernética. Como sugere Gil (2008), pesquisas exploratórias desempenham papel crucial na delimitação de problemas e no aprofundamento analítico, proporcionando uma base sólida para a construção de hipóteses e interpretações mais complexas.

Além de examinar os desafios técnicos e regulatórios enfrentados pelas organizações, este estudo enfatiza a relevância da comunicação corporativa como uma ferramenta estratégica no contexto de crises. A literatura aponta que uma gestão comunicativa proativa e transparente é determinante não apenas para mitigar os danos reputacionais, mas também para reconstruir a confiança do público. Nesse aspecto, Duarte (2018) destaca a necessidade de uma abordagem integradora, que

[1] Tipo de malware que sequestra dados ou sistemas, criptografando arquivos e exigindo um pagamento de resgate, geralmente em criptomoedas, para restaurar o acesso.
[2] Técnica de ataque cibernético que busca enganar usuários para que forneçam informações sensíveis, como senhas, dados bancários ou informações pessoais, por meio de comunicações fraudulentas, geralmente e-mails, mensagens ou sites falsos que se passam por entidades confiáveis.

combine clareza, agilidade e empatia na interação com os públicos.

A fim de construir um arcabouço teórico consistente, o primeiro capítulo aprofunda a definição de crimes cibernéticos e seus impactos na imagem organizacional. São abordadas as diferentes tipologias de crimes digitais e os principais desafios enfrentados pelas organizações na prevenção e mitigação desses ataques. Além disso, discute-se o papel da legislação brasileira no combate aos crimes cibernéticos e a relação entre segurança digital, reputação corporativa e a confiança perante os stakeholders.

O segundo capítulo explora as estratégias de comunicação aplicadas à gestão de crises, destacando como a transparência e a proatividade influenciam a mitigação de danos à imagem corporativa. São analisadas abordagens teóricas sobre planejamento estratégico e gestão da reputação em cenários de crise, além da importância das tecnologias digitais no monitoramento de riscos e no engajamento dos stakeholders. A literatura evidencia que uma comunicação eficiente pode ser determinante para a recuperação da confiança do público após um incidente cibernético.

O terceiro capítulo apresenta a análise de três estudos de caso envolvendo crises cibernéticas enfrentadas por organizações de grande porte: Equatorial Alagoas, Banco Itaú e Serasa Experian. A partir da investigação das respostas institucionais, são identificadas práticas eficazes e pontos de vulnerabilidade que impactaram a reputação dessas empresas. A comparação entre as diferentes abordagens adotadas evidencia padrões comuns e lições valiosas para a gestão de crises digitais.

Estas três organizações — Equatorial Alagoas, Itaú Unibanco e Serasa Experian — foram escolhidas por representarem setores distintos e essenciais à vida cotidiana da população brasileira: energia elétrica, serviços bancários e análise de crédito. Apesar de atuarem em segmentos diferentes, todas possuem operações fortemente digitalizadas e são alvos constantes de ataques cibernéticos. A seleção dessas organizações permite analisar, sob diferentes perspectivas, como a transformação digital tem ampliado a exposição a riscos cibernéticos e exigido novos modelos de resposta a crises digitais.

Por fim, o trabalho busca compreender como as crises digitais podem se transformar em oportunidades de aprendizado e inovação, contribuindo para o

fortalecimento da resiliência organizacional e para o aprimoramento das estratégias comunicacionais relacionadas a crises cibernéticas, reputação corporativa, e a manutenção da confiança do público. Para tanto, adota-se uma análise sistemática de fontes primárias e secundárias, aliada a critérios rigorosos de inclusão e exclusão, com o objetivo de assegurar a relevância e a consistência metodológica dos resultados apresentados. Acredita-se que as conclusões deste estudo poderão subsidiar tanto o avanço das discussões acadêmicas quanto a prática empresarial, apontando caminhos viáveis e efetivos para a gestão de crises no ambiente digital contemporâneo.

2 METODOLOGIA

Este capítulo apresenta os procedimentos metodológicos adotados no presente Trabalho de Conclusão de Curso (TCC), detalhando o tipo de pesquisa realizada, sua classificação e a justificativa para as escolhas metodológicas efetuadas.

2.1 Tipo de estudo

A pesquisa caracteriza-se como exploratória e descritiva. Segundo Gil (2008), a pesquisa exploratória tem como principal finalidade proporcionar maior familiaridade com o problema, tornando-o mais explícito ou possibilitando a formulação de hipóteses. Geralmente, envolve levantamento bibliográfico e entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado. Já a pesquisa descritiva tem como objetivo descrever características de determinada população ou fenômeno, utilizando técnicas padronizadas de coleta de dados, como questionários e observação sistemática.

> As pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Geralmente envolvem levantamento bibliográfico e entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado (Gil, 2008, p. 41).

A opção por uma abordagem exploratória justifica-se pela necessidade de aprofundar o conhecimento sobre o tema em questão, permitindo identificar aspectos ainda pouco explorados na literatura existente. A pesquisa descritiva complementa essa abordagem ao possibilitar a caracterização detalhada dos elementos estudados, fornecendo uma compreensão mais ampla e precisa do objeto de estudo.

2.2 Delineamento da Pesquisa

2.2.1 Natureza da Pesquisa

A presente pesquisa adota uma abordagem qualitativa, estruturada na análise de estudos de caso e na repercussão de notícias divulgadas por veículos de comunicação. Essa escolha metodológica oferece as ferramentas necessárias para interpretar a dinâmica de práticas e regulamentações, explorando os significados atribuídos pelos sujeitos em seus contextos específicos.

Para Minayo (2012, p. 623): “O verbo principal da análise qualitativa é compreender. Compreender é exercer a capacidade de colocar-se no lugar do outro,

tendo em vista que, como seres humanos, temos condições de exercitar esse entendimento". A abordagem qualitativa, nesse sentido, destaca-se por sua capacidade de captar a subjetividade dos envolvidos e a complexidade das situações estudadas. A análise busca ir além da superfície dos dados, favorecendo uma compreensão profunda dos fenômenos e permitindo insights que contribuem para o campo investigado.

2.2.2 Método de Coleta de Dados

O método de coleta de dados adotado nesta pesquisa foi estruturado para integrar fontes primárias e secundárias, garantindo uma abordagem abrangente e consistente, de modo a atender aos objetivos estabelecidos. A combinação dessas fontes permitiu construir uma base sólida para a análise qualitativa, considerando o contexto e as especificidades do tema investigado.

As fontes primárias incluem documentos, materiais institucionais e diretrizes relevantes ao campo de estudo, proporcionando uma visão direta e detalhada sobre os aspectos centrais analisados. Esses dados primários são indispensáveis para compreender as práticas, desafios e especificidades do contexto pesquisado.

As fontes secundárias foram selecionadas por meio de uma revisão de literatura, abrangendo artigos científicos, livros e legislações relacionadas. Essa etapa fornece o suporte teórico necessário, contextualizando as práticas observadas e fundamentando as análises desenvolvidas ao longo do estudo.

A coleta e organização dos dados foram realizadas com o auxílio de ferramentas acadêmicas reconhecidas, como Scielo, Google Scholar e a Biblioteca Virtual em Saúde (BVS). Essas plataformas foram escolhidas pela relevância de seu acervo e pela oferta de conteúdos atualizados e confiáveis, garantindo a qualidade das informações utilizadas na pesquisa.

2.2.3 Critérios de Inclusão e Exclusão

Os critérios de inclusão e exclusão adotados nesta pesquisa foram definidos para garantir a relevância e a qualidade das informações analisadas. Nessa etapa delimita-se o escopo do estudo e assegura que os dados selecionados estejam diretamente relacionados aos objetivos propostos.

Entre os critérios de inclusão, foram selecionados materiais que apresentassem aplicabilidade direta ao tema investigado, como documentos oficiais, estudos acadêmicos e publicações que oferecessem uma base sólida para a análise

qualitativa. Os textos e fontes escolhidos deveriam abordar aspectos centrais do objeto de estudo, contribuindo para uma compreensão ampla e fundamentada.

Por outro lado, os critérios de exclusão eliminaram materiais que não apresentassem relevância direta ou que fossem excessivamente genéricos em relação ao tema principal. Também foram excluídos documentos que não estivessem disponíveis em fontes confiáveis ou que apresentassem informações desatualizadas, a fim de manter a consistência e o rigor metodológico.

Conforme Severino (2007), a definição clara de critérios de inclusão e exclusão é essencial para qualquer revisão sistemática, pois contribui para a seleção de fontes confiáveis e pertinentes, assegurando a consistência e a qualidade do processo analítico.

De acordo com Bardin (2011), a utilização de múltiplas fontes e a aplicação de critérios rigorosos de análise são essenciais para garantir a validade e a profundidade dos resultados. Assim, a coleta de dados estruturada com base em diferentes perspectivas e instrumentos busca proporcionar uma compreensão mais completa do objeto de estudo.

2.3 Procedimentos de Análise de Dados

2.3.1 Análise Comparativa

A análise comparativa constitui uma abordagem central para identificar discrepâncias entre as regulamentações legais e as práticas adotadas por organizações na prevenção e enfrentamento de crimes cibernéticos. Este método permite verificar como as normativas, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet, são incorporadas às estratégias de proteção digital e comunicação organizacional.

De acordo com Severino (2007, p. 143), a análise comparativa em estudos científicos “possibilita estabelecer relações entre diferentes elementos investigados, identificando tanto semelhanças quanto divergências que ampliem o entendimento sobre os fenômenos analisados”. Essa perspectiva orienta o presente trabalho a confrontar práticas de gestão de crises digitais com as normas regulamentadoras aplicáveis, destacando boas práticas e lacunas críticas.

Aspectos analisados:

- Conformidade Regulatória: examinar o alinhamento das ações organizacionais com as exigências legais, como o uso ético de dados pessoais conforme a LGPD;

- Práticas Organizacionais: analisar como empresas estruturam sistemas de proteção digital e respondem a crises cibernéticas;
- Impactos na Imagem: avaliar a efetividade das estratégias de comunicação e sua influência na percepção pública.

A comparação entre práticas observadas e critérios normativos revelou desafios frequentes, como a ausência de políticas de proteção de dados e a demora na comunicação de incidentes; além de apontar iniciativas bem-sucedidas, como programas de educação digital para colaboradores e investimento em sistemas automatizados de segurança.

3 O QUE SÃO CRIMES CIBERNÉTICOS E COMO ELES INTERFEREM NA IMAGEM DAS ORGANIZAÇÕES

A era digital trouxe avanços significativos para pessoas e organizações, mas também aumentou a vulnerabilidade a crimes, que podem comprometer profundamente não só a imagem corporativa, como também a confiança do público.

De acordo com Rossini (2004), pode ser considerado crime cibernético qualquer conduta ilícita, seja dolosa ou culposa, praticada por pessoa física ou jurídica, com uso da informática, em ambiente de rede ou fora dele. Esses crimes vão desde ataques de *phishing* e invasão de sistemas até o roubo de dados sensíveis, colocando em risco não apenas informações sigilosas, mas também a própria reputação das organizações envolvidas.

Conforme destacam estudos da Secretaria de Assuntos Estratégicos da Presidência da República, o espaço cibernético constitui um novo cenário para ilícitos, o que exige das organizações uma postura proativa e robusta em segurança cibernética para manter a confiança de seus públicos de interesse.

Diante desse contexto, Martins (2024) explica que as organizações se veem pressionadas a investir em sistemas de proteção digital e na educação contínua de seus usuários, garantindo que estejam preparados para responder a ameaças virtuais com eficiência e agilidade. Sem essas medidas, correm o risco de enfrentar danos significativos, não só financeiros, mas também reputacionais, que podem levar anos para serem reparados e minar a confiança do público.

As organizações que não investem em segurança cibernética estão mais propensas a sofrer ataques que podem resultar em perdas financeiras significativas e danos irreparáveis à sua reputação. Esse cenário, em que a segurança digital se torna essencial para a manutenção da confiança do público, levou o sistema jurídico brasileiro a estabelecer legislações específicas para combater e penalizar práticas de crimes cibernéticos.

3.1 A legislação brasileira sobre crimes cibernéticos

O aumento significativo no uso da internet e das tecnologias de comunicação nos últimos anos não apenas expandiu o acesso à informação e aos serviços digitais, mas também propiciou um terreno fértil para o desenvolvimento de novos tipos de crimes, denominados crimes cibernéticos. No Brasil, essa transformação obrigou o

sistema jurídico a se adaptar para enfrentar ameaças à segurança digital que se tornam mais sofisticadas a cada dia (Silva e Vieira, 2021).

De acordo com Schmidt (2015) o sistema jurídico brasileiro classifica os crimes cibernéticos de diferentes formas, a partir de sua natureza. São considerados crimes puros aqueles cujo objetivo seja atingir o sistema de um computador, *hardware* ou *software*, geralmente praticado por *hackers*[33]. São classificados como crimes mistos aqueles em que o computador e a internet são usados apenas como meio para a obtenção de bens da vítima, como nos casos de transferências ilícitas de bens ou valores. Já os crimes comuns são aqueles que já foram tipificados pelo Código Penal Brasileiro e se dão em ambiente digital ou por meio de dispositivos informáticos, como no caso da pornografia infantil, por exemplo, que está previsto no Estatuto da Criança e do Adolescente (ECA).

Existem, ainda, os crimes classificados como próprios, uma vez que são praticados exclusivamente por meio de computadores, aqueles que têm o sistema computacional como fim da conduta ilícita. Nesses casos, muitas vezes a legislação brasileira ainda não consegue dar conta, pois não existe previsão legal para o tratamento desses crimes, sendo necessário, portanto, uma atualização legislativa. E por fim, há os crimes impróprios, que atingem o bem comum sendo o meio virtual apenas uma das formas de execução do crime, podendo ser praticado por outros meios. Nesses casos os ilícitos já estão previstos na legislação penal tradicional brasileira, sendo, portanto, necessário apenas a alteração instrumental, sem a exigência de legislação específica.

Essa expansão do ciberespaço como um campo fértil para atividades ilícitas pressiona o sistema jurídico brasileiro a se adaptar constantemente para lidar com crimes que, em muitos casos, superam os limites territoriais e exigem abordagens inovadoras. As autoridades enfrentam desafios crescentes na tentativa de proteger a segurança digital e a privacidade dos cidadãos, num cenário que demanda esforços contínuos para acompanhar o ritmo acelerado das inovações tecnológicas e suas implicações legais.

> A cada inovação tecnológica, o ambiente jurídico brasileiro precisa evoluir para proteger a segurança e a privacidade dos cidadãos, combatendo crimes

[3] O termo hacker é popularmente usado para definir especialistas em computação que utilizam o alto conhecimento para cometer crimes cibernéticos.

> cibernéticos que se tornam mais sofisticados e desafiadores de investigar e punir (ALEXANDRE; ARAÚJO; RABELO, 2024, p. 2).

Em resposta, o país promulgou uma série de legislações, incluindo a Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, que criminaliza a invasão de dispositivos informáticos, e o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios e diretrizes para o uso seguro da rede (Salles, 2022). Essas normas demonstram uma tentativa de proteger a privacidade dos cidadãos e de controlar o uso da tecnologia para fins ilegais.

No entanto, é evidente que as iniciativas legislativas enfrentam limitações quando confrontadas com a natureza fluida e transnacional dos crimes digitais. De acordo com Domingos et al. (2018), os crimes cibernéticos não respeitam fronteiras geográficas, o que complica sobremaneira a tarefa dos agentes de aplicação da lei em investigar e punir tais delitos. Para que haja uma eficácia real, a legislação não apenas deve evoluir continuamente, mas também precisa de uma implementação que inclua recursos humanos e tecnológicos adequados (Domingos et al., 2018). A ausência de infraestrutura tecnológica e de especialistas capacitados impede uma resposta adequada, refletindo uma carência estrutural que dificulta a punição e a prevenção desses crimes.

Assim, para enfrentar as especificidades dos crimes digitais, que desafiam fronteiras e demandam recursos humanos e tecnológicos, é necessário que a legislação evolua de forma a acompanhar essas ameaças. Nesse sentido, iniciativas como o Projeto de Lei 1.515/2022 buscam preencher lacunas de regulação e estabelecer bases legais mais específicas. O referido projeto, conforme apresentado na Câmara dos Deputados, propõe uma Lei de Proteção de Dados Pessoais voltada para fins de segurança do Estado e defesa nacional. Como exposto no estudo:

> Há, na Câmara de Deputados, o Projeto de Lei 1.515/2022 (Brasil, 2022), que reconhece a lacuna legal que ainda existe no Brasil e propõe estabelecer uma Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Este projeto de lei foi objeto de análise pelo IRIS – Instituto de Referência em Internet e Sociedade (Azevedo et al., 2022).

Por outro lado, a legislação sozinha não é suficiente para conter a crescente complexidade dos crimes digitais. Silva e Vieira (2021) argumentam que, para enfrentar de maneira eficaz as ameaças cibernéticas, é essencial ir além de investimentos em tecnologia. Os autores ressaltam que a segurança digital depende igualmente da educação e conscientização dos usuários, promovendo um uso mais

seguro e consciente dos recursos tecnológicos. Essa abordagem equilibrada entre tecnologia e capacitação torna-se indispensável para construir um ambiente digital mais seguro e confiável.

> Não existe um ambiente totalmente seguro. Porém, a partir do equilíbrio entre o investimento em tecnologia e a educação dos usuários, será possível utilizar os recursos tecnológicos disponíveis com maior confiança e, por conseguinte, serão todos eles melhor aproveitados para fins benéficos à sociedade (Silva e Vieira, 2021, p. 15).

Além das questões de segurança, surgem desafios éticos e legais relacionados à vigilância e ao monitoramento no ambiente digital. Diversos especialistas em direito digital alertam que o monitoramento constante das atividades online, mesmo quando justificado por razões de segurança pública, levanta preocupações sobre privacidade e o risco de um “estado de vigilância permanente”. A Lei Geral de Proteção de Dados (LGPD), como observa Maldonado (2022), tenta mediar esses conflitos ao estabelecer regras claras sobre a coleta e o tratamento de dados pessoais, exigindo o consentimento do titular e atribuindo responsabilidades a organizações e instituições. No entanto, a implementação prática da LGPD ainda enfrenta desafios, especialmente em relação à fiscalização, expondo lacunas que precisam ser preenchidas para garantir uma proteção de dados realmente eficaz.

Nesse mesmo pensamento, a LGPD também busca equilibrar o direito à privacidade com a transparência e a responsabilidade, impondo rigorosas obrigações para as organizações no tratamento de dados sensíveis. Esse equilíbrio é fundamental para estabelecer a confiança do público e garantir que a proteção dos dados seja uma prioridade contínua. Como Almeida e Soares (2022) ressaltam:

> A LGPD representa uma tentativa de equilibrar a proteção dos dados pessoais com o direito à informação e à transparência, impondo às organizações e instituições a responsabilidade de cumprir rigorosamente as normas de coleta e tratamento de dados, sob pena de sanções administrativas. (Almeida e Soares, 2022, p. 34).

Num contexto global, o combate ao cibercrime exige cooperação entre países, dado que muitos dos ataques têm origem fora das fronteiras nacionais. Cunha e Cortizo (2019) defendem uma abordagem colaborativa e integrada, na qual a criação de políticas eficazes envolva não apenas legislações nacionais, como também a cooperação entre governos, setor privado e sociedade civil: “Para enfrentar esses desafios, é crucial uma abordagem multifacetada que inclua não apenas a implementação de leis e regulamentações adequadas, mas também a colaboração entre governos, setor privado e sociedade civil” (Cunha e Cortizo, 2019, p. 32). Essa

visão dos autores ressalta a interdependência global no enfrentamento do crime cibernético e a complexidade de coordenar ações eficazes entre diferentes jurisdições.

Outro aspecto essencial da legislação brasileira é a tentativa de proteger vítimas particularmente vulneráveis, como crianças e adolescentes, diante de crimes de exploração infantil online. O Ministério Público Federal (2018) destaca a importância de um sistema judicial ágil e eficiente para identificar e processar esses casos, considerados dos mais difíceis e prejudiciais no ambiente digital. Nesse sentido, a criação de delegacias especializadas e a capacitação de profissionais para lidar com provas digitais representam passos importantes, embora limitados, para enfrentar esses crimes.

Esse comprometimento da legislação brasileira em proteger os mais vulneráveis no ambiente digital é reforçado pelo Estatuto da Criança e do Adolescente (ECA), que define punições rigorosas para casos de exploração online envolvendo menores:

> Art. 241-B do Estatuto da Criança e do Adolescente (ECA): Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa. (ECA, Art. 241-B).

Apesar dos avanços na legislação sobre crimes cibernéticos no Brasil, ainda há uma lacuna significativa em termos de tipificação detalhada para certos tipos de delitos no ambiente digital. De acordo com Salles (2022), o ordenamento jurídico brasileiro frequentemente recorre a interpretações adaptativas de leis tradicionais para julgar crimes virtuais, o que pode ser insuficiente para lidar com a complexidade dos crimes modernos. Esse contexto exige, conforme o autor aponta, a criação de legislações específicas que facilitem o enquadramento de práticas que ocorrem exclusivamente no ciberespaço, especialmente em casos de anonimato e uso de tecnologias de ocultação, como a criptografia

Outrossim, a adesão do Brasil à Convenção sobre o Cibercrime (Convenção de Budapeste) reflete um esforço de alinhamento com diretrizes internacionais para combater crimes digitais, especialmente aqueles de caráter transnacional. No entanto, a efetividade dessa política criminal comum tem sido limitada na prática, destacando a necessidade de aprimoramento nas leis internas. De acordo com o autor:

> Muitos países têm leis projetadas para proteger a privacidade, e toda

> organização que coleta e armazena informações sobre indivíduos é legalmente obrigada a adotar políticas que estejam em conformidade com a legislação de privacidade local (Salles, 2022, p. 17).

A necessidade de cooperação internacional torna-se evidente, especialmente diante da complexidade e da abrangência dos crimes cibernéticos, que ultrapassam fronteiras e exigem esforços conjuntos entre diferentes nações. Sem uma colaboração eficaz, as ações para mitigar esses crimes permanecem limitadas, favorecendo aqueles que operam em rede para atividades ilícitas.

> A falta de instrumentos efetivos de cooperação entre os países corre a favor da cibercriminalidade, considerando que, dadas as características da rede, nenhum país pode atualmente combater o cibercrime sozinho; a conduta criminosa pode se originar de qualquer lugar e atingir qualquer lugar do mundo (Ministério Público Federal, 2018, p. 168).

Dessa forma, a falta de uma colaboração internacional torna-se uma barreira na luta contra o cibercrime, que se aproveita das limitações de jurisdição e da complexidade do ambiente digital global. Conforme indicado pelo Ministério Público Federal, sem uma rede de cooperação entre nações, as iniciativas de segurança cibernética permanecem fragmentadas e limitadas, o que enfraquece a capacidade de cada país de enfrentar essas ameaças de forma independente. Para uma abordagem realmente eficaz, é indispensável que os esforços nacionais sejam somados a compromissos globais, permitindo uma resposta coordenada e abrangente que possa acompanhar a sofisticação e o alcance transnacional das atividades criminosas no ciberespaço.

3.2 Imagem e reputação das organizações no contexto digital

No contexto digital contemporâneo, a imagem e reputação das organizações são ativos indispensáveis para a sua sustentabilidade e competitividade. Em um ambiente hiperconectado, no qual a comunicação se propaga em tempo real, as organizações ficam sob constante vigilância pública, o que exige uma abordagem estratégica para a preservação da imagem corporativa. Como apontam Silva e Vieira (2021), o avanço da tecnologia amplia a vulnerabilidade das organizações, tornando-as mais expostas a riscos de ataques cibernéticos, o que ressalta a necessidade de uma gestão cuidadosa para proteger a reputação e responder a incidentes com agilidade. Sobre isso, Silva e Vieira, (2021) afirmam que:

> A evolução das tecnologias da informação e comunicação, que alcançou a sociedade moderna, é, sem dúvida, perceptível em diversas áreas, como: o comércio eletrônico, a educação à distância, a telemedicina, as redes sociais, o desenvolvimento científico-tecnológico, o desenvolvimento econômico, dentre outros. (Silva e Vieira, 2021, p. 2).

Nesse mesmo sentido, Bandeira (2006) enfatiza que um planejamento estratégico de comunicação é essencial para mitigar crises de imagem, especialmente em contextos de crise. Ela observa que o ambiente digital amplifica a visibilidade das organizações, tornando-as mais suscetíveis a julgamentos públicos imediatos e exigindo uma comunicação consistente e transparente. Segundo a autora:

> As organizações modernas possuem diversas formas de se comunicar com a sociedade e estabelecer seu conceito. A assessoria de imprensa, representada pelo jornalista, é uma delas. Ele deve assumir a posição estratégica da comunicação, estando completamente integrados à alta cúpula das organizações e trabalhando em conjunto com as demais áreas, como marketing, recursos humanos, produtos etc. E, para o êxito, a ferramenta essencial é o planejamento estratégico. Sem planejamento as decisões organizacionais ficariam a mercê do acaso, com soluções aleatórias de última hora (Bandeira, 2006, p. 14).

Além das preocupações com a imagem pública, as questões de privacidade e vigilância digital também desempenham um papel importante. Moreira e Adrião (2023) destacam os desafios éticos e legais do monitoramento constante no ambiente digital, observando que práticas de vigilância podem estabelecer um “estado de vigilância permanente,” que levanta sérias preocupações sobre a privacidade e os direitos individuais. A conformidade com normas como a Lei Geral de Proteção de Dados (LGPD) assume, nesse contexto, uma relevância fundamental para o posicionamento ético e competitivo das organizações. Maldonado (2022) observa que a LGPD exige consentimento explícito para o uso de dados pessoais, impondo responsabilidades às organizações e promovendo uma imagem de segurança e confiabilidade para os consumidores.

A governança corporativa e a cultura organizacional também são fatores decisivos para a proteção da reputação. Prado (2020) aponta que a governança corporativa sólida, aliada a uma comunicação transparente, estabelece as bases para uma reputação resiliente no ambiente digital, onde os *stakeholders* esperam consistência entre discurso e prática. Essa coerência interna reflete na credibilidade

percebida pelo público, essencial para a competitividade.

As plataformas digitais emergem como ferramentas estratégicas para a gestão da reputação. Prado (2020) afirma que as plataformas digitais permitem não apenas a amplificação de mensagens positivas, mas também o monitoramento de percepções e tendências, auxiliando na adaptação ágil das estratégias organizacionais. Este recurso não apenas conecta a organização a seus públicos, mas também fortalece a interação e a confiança, pilares fundamentais da reputação organizacional.

Oliveira (2007) reforça que o crescimento no uso de tecnologias digitais trouxe um volume imenso de dados, que servem como combustível para decisões estratégicas relacionadas à reputação organizacional. As organizações que adotam práticas de análise de dados são capazes de identificar crises em potencial e responder de forma mais eficiente.

A comunicação proativa se consolida como uma estratégia essencial para prevenir crises reputacionais. Duarte (2018) destaca que ações planejadas e antecipatórias são fundamentais para reduzir os impactos de crises que poderiam prejudicar a imagem institucional. Essa abordagem proativa é particularmente relevante no ambiente digital, onde a disseminação de informações é instantânea.

A inclusão dos *stakeholders* na formulação de estratégias reputacionais é outro elemento crucial. Segundo Prado (2018), a interação constante com os públicos de interesse aumenta a confiança e reduz as barreiras entre a organização e seus consumidores. Esse engajamento gera um círculo virtuoso de confiança mútua e credibilidade.

A capacidade de inovação também está diretamente relacionada à reputação organizacional. Duarte (2020) observa que a adaptação ao ambiente digital não é mais uma escolha, mas uma necessidade estratégica para manter a relevância no mercado. Essa adaptação exige o desenvolvimento de novas habilidades e a integração da tecnologia às práticas de comunicação.

Em face dessa ciência, a habilidade das organizações de responder prontamente a incidentes de segurança também contribui para a construção de uma imagem resiliente. Cunha e Cortizo (2019) enfatizam a importância de uma colaboração mútua e integrada para enfrentar os desafios globais do cibercrime, afirmando que:

> Dessa maneira, devido ao acréscimo dos crimes virtuais e ao aumento do número de usuários da internet, conforme documentado no primeiro tópico,

> tanto o Senado Federal quanto a Câmara dos Deputados têm destinado recursos para a criação de legislação sobre crimes cibernéticos (Cunha e Cortizo, 2019, p. 12).

Simultaneamente, construir uma imagem sólida e resiliente no ambiente digital requer uma postura proativa e contínua de transparência e conformidade, além de práticas robustas de segurança. A combinação entre uma comunicação eficaz e políticas rígidas de proteção de dados permite que as organizações desenvolvam uma relação de confiança com seus públicos, servindo como um amortecedor em períodos de crise. Ao integrar práticas de segurança com uma comunicação ágil e transparente, as organizações não apenas fortalecem sua reputação, mas também se destacam como entidades responsáveis e éticas, capazes de enfrentar os desafios do mercado digital. Esse compromisso com a integridade e a segurança reforça a percepção de confiabilidade entre consumidores e parceiros, sendo um diferencial importante para a longevidade e competitividade das organizações.

Nesse contexto, torna-se essencial avançar a discussão para compreender como as organizações podem adotar estratégias práticas e eficazes na gestão de crises. Assim, o próximo capítulo será dedicado à análise de diversas possibilidades de estratégias de comunicação e gestão de crises, destacando ferramentas e abordagens que podem ser implementadas para mitigar impactos e fortalecer a resiliência organizacional. Essa abordagem permitirá delinear um panorama mais claro das ações que contribuem para a preservação da reputação corporativa e a superação de desafios no ambiente digital.

4 ESTRATÉGIAS DE COMUNICAÇÃO NA GESTÃO DE CRISE

A gestão de crises tornou-se um elemento essencial para a sobrevivência das organizações no ambiente contemporâneo, caracterizado por incertezas e pela velocidade da disseminação de informações nas redes digitais. As crises corporativas podem surgir de eventos inesperados, como desastres naturais, problemas internos, escândalos ou falhas tecnológicas, afetando não apenas a reputação da organização, mas também sua sustentabilidade operacional e financeira. Assim, a comunicação desempenha um papel central na mitigação dos impactos de crises.

As crises geradas por crimes cibernéticos, discutidas no capítulo anterior, demandam estratégias de comunicação efetivas, que possam mitigar impactos e fortalecer a resiliência organizacional. Em um cenário onde os ataques cibernéticos podem comprometer profundamente a imagem e a confiança pública, uma abordagem estruturada de comunicação pode ser a diferença entre o sucesso e o fracasso no enfrentamento dessas situações.

Duarte (2018) afirma que “nenhuma organização, por mais sólida, admirada e moderna que seja, está imune à crise. Esse princípio básico da gestão de crise, mesmo repetido, continua esquecido por muitas organizações” (DUARTE, 2018, p. 538).

Esse alerta sublinha a importância de as organizações adotarem uma abordagem estratégica e proativa na preparação para crises. Isso inclui a criação de manuais de crise, o treinamento de equipes e a definição clara de papéis e responsabilidades.

Além disso, o planejamento é a base de qualquer estratégia eficaz de gestão de crises. Farias (2011) reforça que sem uma estrutura prévia que defina papéis, responsabilidades e fluxos de comunicação, uma crise pode rapidamente escapar ao controle, amplificando seus danos. Um planejamento adequado permite que as organizações identifiquem possíveis cenários de risco, desenvolvam protocolos de resposta e alinhem suas ações a valores institucionais. Dessa forma, é possível não apenas responder às crises, mas também antecipá-las, reduzindo significativamente seus impactos.

No contexto digital, a tecnologia oferece ferramentas indispensáveis para a comunicação em situações de crise. Conforme observado por Terra (2011): “As formas

de aproximação e contato da área de comunicação corporativa mudam do *pitch*[4] para a participação, cooperação e colaboração, para a troca de ideias em tempo real" (TERRA, 2011, p. 28).

Isso demonstra a importância de plataformas digitais, como redes sociais, para monitorar crises em tempo real, engajar *stakeholders* e disseminar informações de maneira rápida e precisa.

Paralelamente, Duarte (2018) enfatiza que ao adotar a premissa de que prevenção não é um gasto inútil, a maioria dos autores admite que o planejamento prévio pode ser a diferença entre o sucesso e o fracasso de uma organização. A prevenção não deve ser vista como um custo, mas como um investimento estratégico que protege a organização de danos financeiros e reputacionais, enquanto demonstra um compromisso com a responsabilidade e a ética.

Da mesma forma, a comunicação pós-crise deve incluir um processo de aprendizado contínuo. Após cada crise, é necessário revisar os procedimentos adotados, identificar falhas e compartilhar as lições aprendidas com a organização como um todo. Isso fortalece a resiliência corporativa e prepara a organização para lidar com futuras crises de maneira mais eficiente e estratégica.

4.1 Conceitos Fundamentais na Gestão de Crises

Os fundamentos da gestão de crises são elementos cruciais para a construção de uma estratégia sólida e integrada que possibilite às organizações enfrentar eventos adversos com confiança e clareza. Uma das primeiras etapas para a gestão eficaz de crises é compreender a sua definição e as características que a diferenciam de outros problemas organizacionais.

Duarte (2018, p.539) descreve crise como: “uma ruptura da normalidade da organização; uma ameaça real ao negócio, à reputação e ao futuro de uma corporação ou de um governo”. Essa definição destaca a gravidade das crises e a necessidade de abordá-las com seriedade e preparo.

Entre os conceitos fundamentais da gestão de crises está o planejamento estratégico. Farias (2011) pontua que a ausência de um planejamento prévio pode transformar uma crise controlável em uma situação devastadora. Para ele, sem uma estrutura prévia que defina papéis, responsabilidades e fluxos de comunicação, uma crise pode rapidamente escapar ao controle, catalisando seus danos. Isso evidencia

[4] Apresentação curta e objetiva, geralmente utilizada para transmitir uma ideia, projeto ou proposta com o objetivo de captar a atenção de uma audiência específica, como investidores, parceiros ou clientes.

a importância de definir previamente os mecanismos de resposta e os protocolos de comunicação para garantir agilidade e eficiência.

Outro conceito essencial é a transparência. Durante uma crise, é imprescindível que as organizações sejam claras e honestas com seus *stakeholders*. Duarte (2018) destaca que não existe comunicação efetiva, que salve a reputação de uma organização, se não houver um efetivo trabalho de gestão de riscos, que compreenda a prevenção e a preparação. A transparência é especialmente relevante no ambiente digital, onde as informações circulam rapidamente e podem ser facilmente distorcidas.

A integração entre diferentes níveis organizacionais também desempenha um papel central na gestão de crises. Como destaca Terra (2011, p. 73), é necessário: “engajar em níveis múltiplos: ser transparente com todos os níveis organizacionais”. Esse engajamento interno assegura que todos os colaboradores compreendam seu papel durante a crise e colaborem para uma resposta coesa e eficaz.

Diante do exposto, a ideia de aprendizado contínuo deve ser incorporada como um princípio da gestão de crises. Analisar crises passadas permite que as organizações identifiquem vulnerabilidades, aprimorem suas estratégias e fortaleçam sua resiliência. Conforme Duarte (2018), é essencial transformar cada crise em uma oportunidade de aprendizado e crescimento organizacional, promovendo uma cultura de preparação e melhoria contínua.

4.2 Planejamento Estratégico na Comunicação de Crises

O planejamento estratégico na comunicação de crises é uma peça central para a resiliência organizacional em um mundo repleto de incertezas e desafios. A capacidade de prever, mitigar e responder a crises depende da estruturação de estratégias que conectem os objetivos organizacionais à preservação de sua reputação e funcionamento. Nesse sentido, o planejamento estratégico não é apenas uma ferramenta reativa, mas também preventiva e orientadora de processos.

Segundo Duarte (2018), um planejamento estratégico de comunicação deve:

> Traduzir a identidade da organização; ter objetivos (de negócios e comunicação) que gerem estratégias; não perder de vista a missão, os valores e o propósito da organização; ser criativo – ter olhos para o futuro; ser flexível e adaptável; zelar e prever mecanismos de fiscalização da sua

> própria implementação; ser medido, acompanhado, avaliado (DUARTE, 2018, p. 305).

Essa descrição reflete a importância de alinhar o planejamento às características fundamentais da organização, permitindo que a identidade corporativa seja preservada durante situações críticas. Ademais, reforça-se a relevância de uma abordagem contínua, que envolva monitoramento e ajuste constante para assegurar a eficácia das ações.

O planejamento estratégico também requer um diagnóstico detalhado da organização e de seus ambientes interno e externo. Kunsch (2021) destaca que a comunicação estratégica, por ser processual, deve estabelecer canais de conversação contínuos entre a organização e seus interlocutores com vistas ao fortalecimento da cultura e dos objetivos organizacionais.

Esse processo dialógico reforça a necessidade de integração entre as partes interessadas, permitindo uma comunicação que não apenas responda a crises, mas também fortaleça a confiança e a credibilidade junto aos *stakeholders*.

No contexto das crises corporativas, as redes sociais desempenham um papel central na execução de planos estratégicos. Essas plataformas digitais transformam as interações da comunicação organizacional, priorizando a participação ativa, a cooperação e a troca de ideias em tempo real. Essa abordagem não apenas facilita o monitoramento de crises, mas também possibilita respostas rápidas e eficazes, fundamentais para mitigar impactos e preservar a reputação organizacional

Ademais, o planejamento estratégico deve contemplar ações de contingência e protocolos claros de resposta, como destacado por Duarte (2018, p. 565) “uma organização deve informar da maneira mais rápida e completa possível as ocorrências negativas e prejudiciais à imagem principalmente se esses fatos tiverem alguma interveniência no interesse de terceiros”. Esse enfoque na agilidade de resposta é essencial para conter danos e evitar a escalada de crises. No entanto, a rapidez deve ser acompanhada por precisão e transparência, conforme ressaltado por Farias (2011), que argumenta que a falta de planejamento pode amplificar os danos, tornando a crise ainda mais devastadora para a organização.

Sintetizando, o aprendizado organizacional é um elemento essencial do planejamento estratégico de comunicação em crises. Analisar e documentar lições aprendidas, como enfatizado por Duarte (2018), fortalece a resiliência organizacional,

permitindo que as organizações estejam mais preparadas para desafios futuros. Assim, transformar cada crise em uma oportunidade de aprendizado e crescimento organizacional é essencial para promover uma cultura de preparação e melhoria contínua.

Deste modo, o planejamento estratégico na comunicação de crises vai além da reação a eventos adversos, abrangendo a construção de estruturas robustas que antecipem cenários de risco, promovam respostas eficazes e fortaleçam a organização no longo prazo.

4.3 Resiliência Organizacional na Gestão de Crises

A resiliência organizacional é um elemento indispensável para a gestão de crises eficaz. Essa habilidade reflete a capacidade das organizações de antecipar, responder e se recuperar de situações adversas, garantindo a continuidade de suas operações e a preservação de sua reputação. De acordo com Duarte (2018), a resiliência organizacional é diretamente influenciada pelo planejamento estratégico de comunicação, que deve ser flexível, adaptável e alinhado aos valores institucionais.

No ambiente digital, onde crises podem se intensificar rapidamente devido à disseminação de informações em tempo real, a resiliência organizacional assume um papel ainda mais crítico. Terra (2011) destaca que o uso de ferramentas digitais e estratégias colaborativas são essenciais para construir a capacidade de resposta ágil, bem como para promover a confiança entre *stakeholders*.

No mais, a resiliência organizacional não se limita à superação de crises; ela também é um fator estratégico que contribui para o aprendizado contínuo e o fortalecimento das relações com o público. Kunsch (2006) aponta que organizações resilientes conseguem transformar adversidades em oportunidades para reafirmar seus valores e demonstrar compromisso com a responsabilidade social e ética.

Portanto, a resiliência organizacional deve ser cultivada como parte integrante das estratégias de gestão de crises. Ela não apenas mitiga os impactos negativos de eventos adversos, mas também fortalece a credibilidade e a sustentabilidade das organizações no longo prazo. Isso reforça que, além de medidas reativas, é necessário investir continuamente em práticas proativas que sustentem a capacidade de adaptação e recuperação diante de cenários incertos.

4.4 Comunicação Proativa e Transparência

A comunicação proativa e a transparência são pilares fundamentais para a gestão eficaz de crises nas organizações. Esses elementos não apenas mitigam os

impactos negativos sobre a reputação corporativa, mas também fortalecem a confiança dos *stakeholders* e garantem que a organização esteja preparada para lidar com desafios de maneira ética e estratégica. Em um ambiente organizacional dinâmico e altamente conectado, a ausência de transparência e de uma comunicação eficiente pode potencializar os efeitos de uma crise.

Kunsch (2003) enfatiza que a comunicação integrada e estratégica deve abranger todas as dimensões da organização, desde a comunicação institucional até as relações mercadológicas, internas e administrativas. Segundo a autora, “o importante, para uma organização social, é a integração de suas atividades de comunicação, em função do fortalecimento de seu conceito institucional, mercadológico e corporativo junto a todos os seus públicos” (KUNSCH, 2003, p. 10). A proatividade na comunicação durante uma crise inclui a antecipação de problemas potenciais, o que permite que a organização se posicione de maneira eficaz e assertiva. Segundo Duarte (2018, p. 565), “as organizações que não se prepararam, não treinaram, nem praticaram para crises em potencial não serão capazes de reagir com eficiência no ambiente de comunicação em tempo real que terão pela frente”.

Além do mais, a transparência é essencial para preservar e restaurar a confiança. No contexto digital, onde a disseminação de informações ocorre em tempo real, ser transparente ajuda a combater rumores e a apresentar os fatos de forma clara e precisa. Conforme enfatiza Duarte (2018, p. 567), “receber a imprensa, informando tudo com transparência, funciona melhor. Dá mais credibilidade à resposta”.

A ideia defendida pelo autor evidencia que a transparência é uma ferramenta indispensável para preservar e reconstruir a confiança em tempos de crise, especialmente no contexto digital, onde a disseminação de informações é rápida e constante. Informar de forma clara e precisa, inclusive por meio da imprensa, permite não apenas combater rumores, mas também fortalecer a credibilidade da organização perante os públicos. Ao adotar essa postura, as instituições demonstram comprometimento com a verdade e ética, elementos que são cruciais para estabelecer conexões genuínas e duradouras.

4.4.1 A Relação entre Proatividade e Transparência

A proatividade está intrinsecamente ligada à transparência. Enquanto a proatividade se refere à capacidade de antecipar problemas e preparar respostas eficazes, a transparência assegura que todas as ações sejam comunicadas de forma honesta e ética. Terra (2011) destaca a importância de engajar em níveis múltiplos: ser transparente com todos os níveis organizacionais.

Adicionalmente, o uso de plataformas digitais e redes sociais facilita a comunicação transparente, permitindo que as organizações forneçam informações diretamente aos seus *stakeholders* sem depender exclusivamente dos meios tradicionais de comunicação. Este ponto é reforçado por Kunsch (2006, p. 8), quando afirma que “pensar e administrar estrategicamente a comunicação organizacional pressupõe [...] reconhecimento e auditoria da cultura organizacional”.

A relação entre proatividade e transparência, conforme destacado, é essencial para uma comunicação organizacional estratégica e eficaz. Enquanto a proatividade permite a antecipação de problemas e a preparação de respostas assertivas, a transparência garante que as ações sejam comunicadas de forma ética e clara, fortalecendo a confiança dos *stakeholders*.

Terra (2011) destaca que essa transparência deve ser exercida em todos os níveis organizacionais, promovendo um engajamento amplo e consistente. Além disso, como aponta Kunsch (2006), a gestão estratégica da comunicação requer uma compreensão profunda da cultura organizacional, o que possibilita a construção de mensagens alinhadas e coerentes. Nesse sentido, o uso de plataformas digitais e redes sociais se torna uma ferramenta indispensável para viabilizar uma comunicação direta e transparente, adaptada às demandas de um ambiente corporativo cada vez mais conectado. Assim, a integração de proatividade e transparência configura-se como um diferencial estratégico para a gestão organizacional contemporânea.

4.4.2 Benefícios da Comunicação Proativa e Transparente

A comunicação proativa e transparente durante crises contribui para minimizar danos e aumentar a resiliência organizacional. Quando bem implementada, cria um ambiente de confiança que facilita o alinhamento interno e a compreensão externa das ações da organização. Como observa Duarte (2018, p. 568), “uma boa comunicação requer diálogo direto, cara a cara, entre funcionários da organização e representantes do povo”.

Concluindo, essas estratégias devem ser parte de uma política contínua de

gestão de riscos e não apenas uma resposta a crises emergentes. O compromisso com a transparência e a comunicação proativa não apenas fortalece a reputação organizacional, mas também estabelece a base para a superação de desafios futuros.

4.5 Uso de Tecnologias na Gestão de Crises

Conforme já mencionado, o uso de tecnologias tornou-se essencial na gestão de crises, transformando a maneira como as organizações identificam, respondem e aprendem com eventos críticos. A rapidez e a abrangência da comunicação digital demandam ferramentas avançadas para monitoramento, análise e interação em tempo real.

Duarte (2018) aponta como as novas tecnologias redefiniram os conceitos de tempo e espaço na comunicação de crises: “nossos conceitos de tempo e espaço estão sendo redefinidos, porque praticamente não existe mais espaço de tempo entre o acontecer e o divulgar” (DUARTE, 2018, p. 545).

Essa instantaneidade obriga as organizações a adotarem estratégias digitais integradas. Conforme Terra (2011), a comunicação digital é caracterizada pela bilateralidade, permitindo não apenas a disseminação de informações, mas também a coleta de *feedback*[5] imediato: “a comunicação de duas mãos ou bilateral é obtida por meio dos comentários dos usuários ou leitores que participam” (TERRA, 2011, p. 101).

Ferramentas como redes sociais e sistemas de alerta desempenham um papel central no gerenciamento de crises, oferecendo monitoramento em tempo real e canais para respostas rápidas. Farias (2011) pontua que o monitoramento de notícias e respectivos desdobramentos/*clipping*[6] unificado é essencial para identificar tendências e agir antes que crises escalem.

A combinação de monitoramento, análise e resposta digital eficaz pode reduzir significativamente os impactos de crises. Contudo, Duarte (2018, p. 558) ressalta que o tempo de resposta é crítico. Para o autor, “o *timing*[7] também é importante, quando se trata de posicionamento nas redes sociais. A reação é imediata e é preciso ter estrutura para responder a eventuais comentários ou críticas”.

Em suma, a integração tecnológica deve ser acompanhada de políticas claras

[5] Informação que o emissor obtém da reação do receptor à sua mensagem, e que serve para avaliar os resultados da transmissão.
[6] Processo de coleta e análise de notícias e informações sobre uma marca, empresa ou tema.
[7] Sensibilidade para o momento propício de realizar ou de perceber a ocorrência de algo, ou senso de oportunidade quanto à duração de um processo, uma ação etc.

para mitigar riscos, como a divulgação de informações sensíveis ou a propagação de boatos. Terra (2011) conclui que a simplicidade das ferramentas de comunicação digital chamou a atenção das organizações, que podem se valer delas para produzir, captar, organizar e disseminar informações e conhecimentos.

Diante disso, o uso estratégico de tecnologias digitais na gestão de crises não apenas aumenta a capacidade de resposta das organizações, mas também fortalece sua resiliência e credibilidade frente aos desafios contemporâneos.

4.6 Engajamento de *Stakeholders*

O engajamento de *stakeholders* é um componente essencial da gestão de crises, uma vez que envolve a construção e a manutenção de relações de confiança entre a organização e seus diferentes públicos de interesse. Esses grupos, que incluem empregados, investidores, clientes, mídia, governo e comunidade, desempenham um papel crítico no processo de mitigação de crises e na preservação da reputação corporativa.

Duarte (2018) ressalta que o público interno deveria ser o primeiro a saber, mas as agências de notícias, a internet, os blogs e as redes sociais acabam, na maioria das vezes, 'furando' os veículos internos.

Essa observação destaca a necessidade de estratégias de comunicação que priorizem o público interno, mesmo em um ambiente altamente dinâmico e conectado. Segundo o autor, uma abordagem proativa e transparente pode minimizar os danos potenciais e fortalecer a confiança mútua.

A comunicação com *stakeholders* não se limita à disseminação de informações, mas inclui também um esforço contínuo para ouvir, compreender e responder às necessidades e preocupações de cada grupo. Terra (2011) observa que ser transparente com todos os níveis organizacionais é fundamental para garantir que os objetivos da organização estejam alinhados com as expectativas dos *stakeholders.*

De mais a mais, o papel da tecnologia no engajamento de *stakeholders* é imprescindível. Como Terra (2011) afirma:

> Isso obriga a organização a se posicionar estrategicamente em termos de comunicação, primando por uma comunicação on-line e off-line sistematizada, e sabendo que suas ações terão desdobramentos (podendo ser alvo de manifestações de usuários, consumidores, stakeholders em geral) no meio físico ou digital (TERRA, 2011, p. 21).

A ideia do autor ilustra como as mudanças tecnológicas pelas quais as empresas e a sociedade passam no momento exigem uma comunicação mais direta

e eficaz com os *stakeholders.*

Por fim, a integração de estratégias de engajamento dentro de um plano de comunicação de crise deve considerar as especificidades de cada público. Conforme Farias (2004), a comunicação organizacional ou empresarial, deve possibilitar à organização o equilíbrio do público interno, de modo a repercutir nas relações com o público externo.

Essa abordagem adotada pelo autor se mostra mais equilibrada, sendo essencial para evitar mal-entendidos e potencializar os resultados positivos durante uma crise.

O engajamento estratégico de *stakeholders*, portanto, não apenas mitiga os riscos associados a crises, mas também contribui para o fortalecimento da resiliência organizacional e para a construção de uma reputação sólida e confiável.

4.7 Recuperação Pós-Crise

A recuperação pós-crise é um momento decisivo para as organizações, uma vez que determina não apenas o restabelecimento da normalidade, mas também a capacidade de aprendizado e adaptação frente aos desafios enfrentados. Esse período exige a implementação de estratégias que reforcem a confiança dos *stakeholders*, minimizem os danos causados e previnam a recorrência de crises semelhantes no futuro, conforme Duarte (2018, p. 565) que observa que: “as crises deixam sinais. É conveniente saber identificar os rastros e estar preparado”.

Esse aprendizado é essencial para que as organizações possam analisar de maneira crítica os erros cometidos durante a crise, ajustando protocolos, políticas e estratégias de comunicação. Assim, cada crise se torna uma oportunidade de fortalecimento institucional e aprimoramento dos processos internos.

A comunicação desempenha um papel central na recuperação pós-crise, tanto internamente quanto externamente. Como destaca Kunsch (2006, p. 8): “pensar e administrar estrategicamente a comunicação organizacional pressupõe[...] reconhecimento e auditoria da cultura organizacional”.

A transparência com os stakeholders sobre as medidas tomadas para resolver a crise, aliada a um compromisso visível com mudanças estruturais, contribui para a restauração da confiança. Essa abordagem reflete o engajamento organizacional em promover um diálogo honesto e inclusivo com os públicos de interesse.

Portanto, o período pós-crise deve incluir o desenvolvimento de planos estratégicos que abordem potenciais riscos e detalhem ações de contingência. Essa

etapa de planejamento contínuo aumenta a capacidade de resposta da organização e reduz sua vulnerabilidade a novos desafios.

Em finalização, o monitoramento constante das percepções e *feedbacks* dos *stakeholders* é essencial para avaliar o impacto das ações implementadas. Essa prática transforma as dinâmicas de interação da comunicação corporativa, enfatizando a participação ativa, a cooperação e a colaboração. Essa abordagem contínua permite que as organizações ajustem suas estratégias de forma proativa, garantindo a melhoria contínua de seus processos e práticas.

A recuperação pós-crise, portanto, vai além da simples restauração das operações; ela representa uma oportunidade de crescimento e de fortalecimento da resiliência organizacional. Ao combinar aprendizado, comunicação transparente, planejamento preventivo e monitoramento contínuo, as organizações podem transformar crises em pontos de partida para um futuro mais sólido e adaptável.

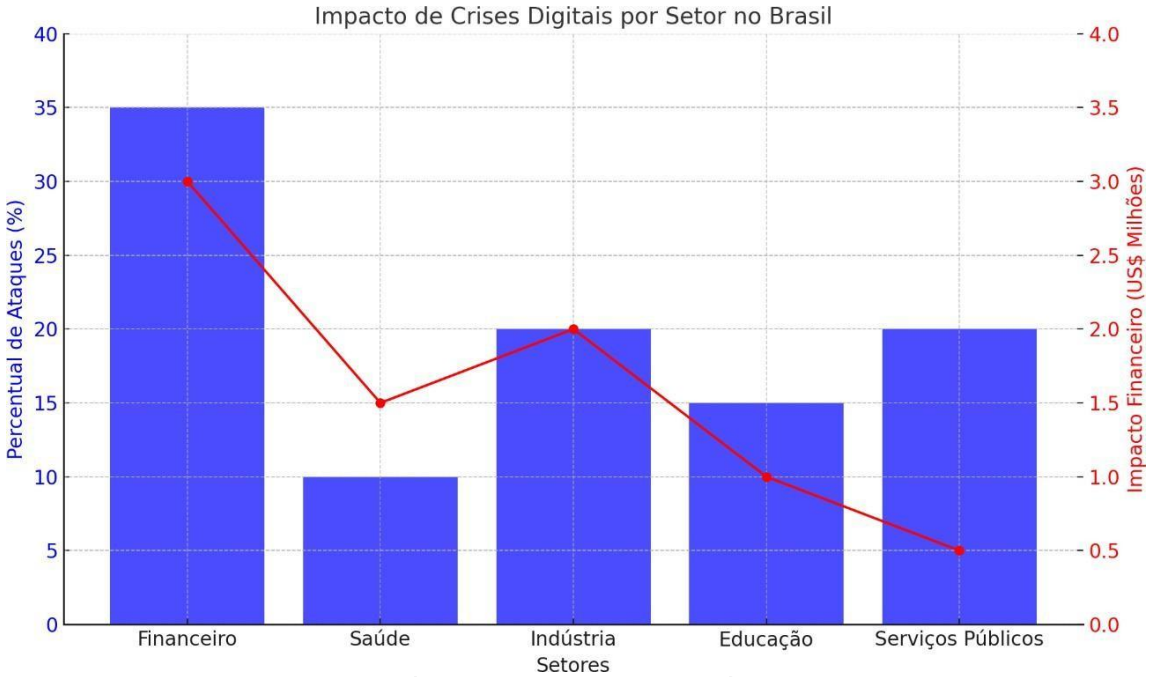
5 ANÁLISES DOS CASOS

Nesta seção, serão analisados três casos que exemplificam como organizações enfrentaram crises no ambiente digital, destacando os desafios enfrentados, as estratégias de comunicação empregadas e os aprendizados obtidos. A partir dessas análises, busca-se compreender como diferentes abordagens podem influenciar a resiliência organizacional e a recuperação da reputação em cenários de crise.

Os ataques cibernéticos têm impactado setores diversos no Brasil, cada um enfrentando desafios específicos relacionados a vulnerabilidades digitais. Dados recentes destacam como setores críticos, como financeiro, saúde, e educação, estão particularmente expostos a ameaças como *ransomware*, *malware e phishing*.

O gráfico abaixo ilustra os principais setores afetados por ataques cibernéticos no Brasil, suas vulnerabilidades predominantes e os impactos financeiros estimados:

Figura 1 - Impacto de Crises Digitais por Setor no Brasil



Fonte: Dados baseados em relatórios de segurança cibernética (Lattine Group, 2024; TiSafe, 2024; Stefanini, 2024).

5.1 Caso Equatorial Alagoas

5.1.1 Contextualização e Impacto da Crise

O caso da empresa de energia Equatorial Alagoas ilustra como a ascensão dos crimes cibernéticos no setor de serviços essenciais pode impactar significativamente consumidores e empresas. Golpistas se aproveitaram da digitalização dos serviços para criar faturas falsas, realizar cobranças indevidas e ameaçar cortes de energia elétrica, tudo isso utilizando de forma fraudulenta a identidade visual da Equatorial Alagoas. Essa crise evidencia não apenas a sofisticação das práticas criminosas, mas também as vulnerabilidades das organizações em um ambiente digital.

5.1.2 A Natureza do Golpe

Os golpes exploraram a confiança dos consumidores em canais digitais, baseando-se em:

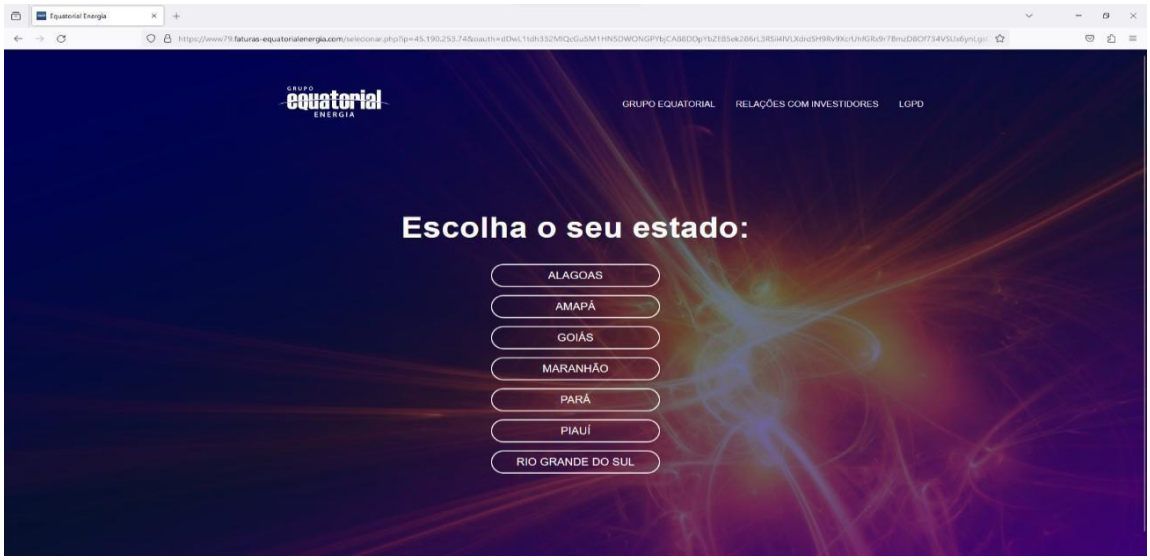
- Criação de sites falsos, com reprodução fiel da identidade visual da empresa, confundindo os consumidores;
- Disseminação de mensagens fraudulentas, alertando sobre cortes iminentes de energia, o que gerava pânico nos clientes;
- Envio de boletos falsificados, contendo dados bancários de criminosos e informações que simulavam legitimidade.

A seguir, seguem exemplos de sites falsos usados no golpe, confundindo consumidores com identidade visual similar à original:

Imagem 1 - Pesquisa para acessar site da Equatorial AL e ter acesso 2ª via da fatura

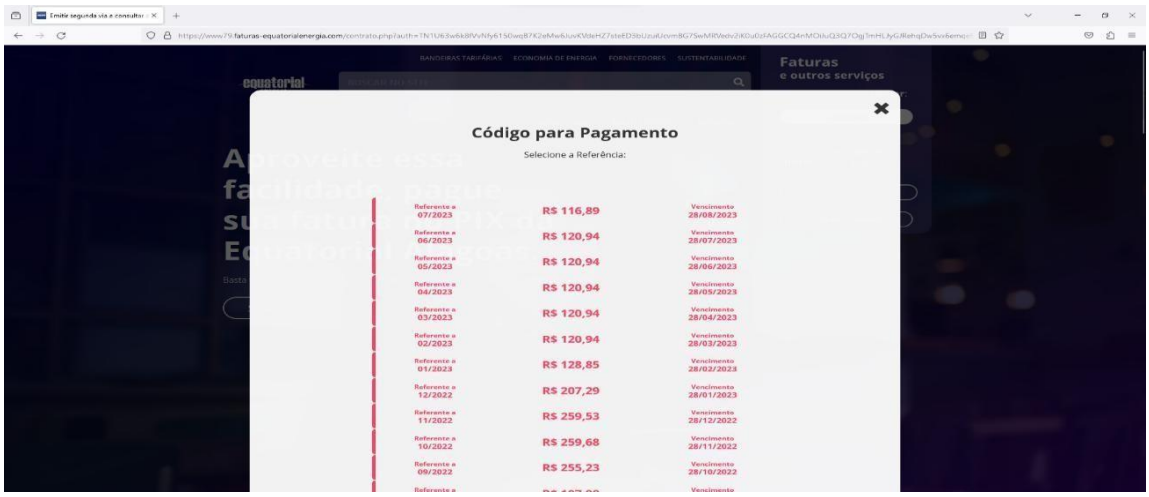
Fonte: Imagem do autor com base no buscador de pesquisas Google

Imagem 2 - Site falso com layout semelhante ao da Equatorial Alagoas



Fonte: Imagem do autor com base no buscador de pesquisas Google

Imagem 3 - Lista de faturas disponíveis para pagamento conforme existente no cadastro do cliente no site falso



Fonte: Imagem do autor com base no buscador de pesquisas Google

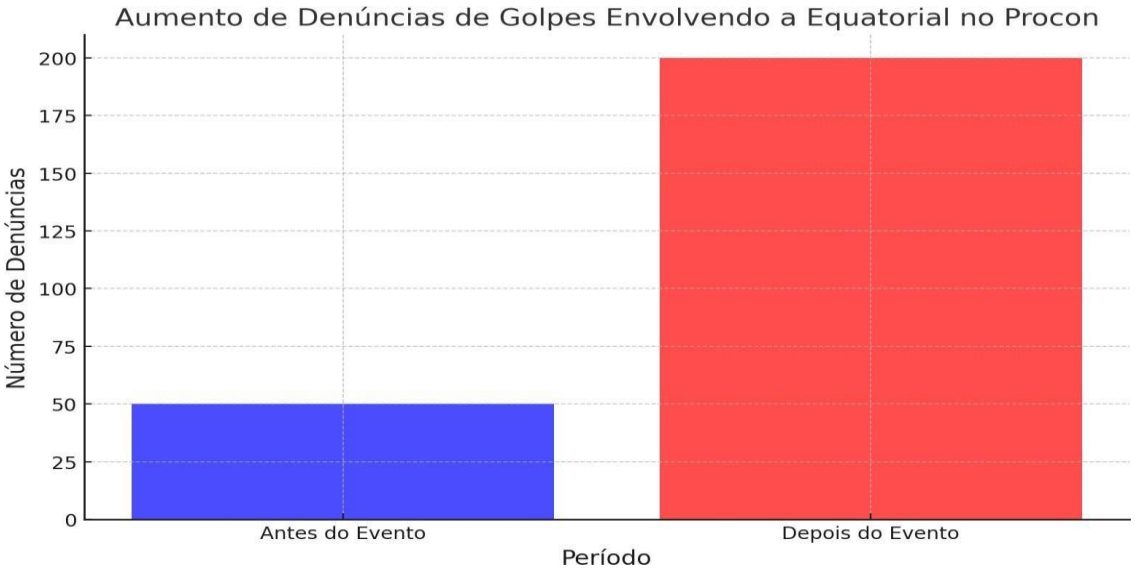
Como observa Duarte (2018), crises desse tipo demonstram como a ausência de mecanismos preventivos de comunicação integrada fragiliza as organizações diante de ataques que exploram brechas tecnológicas e desinformação. A falta de uma estratégia digital robusta contribuiu para que os golpistas ampliassem o alcance das fraudes.

5.1.3 Impactos nos Consumidores

Os consumidores sofreram diversos prejuízos, tanto materiais quanto psicológicos:

- Perda financeira direta: ao realizarem pagamentos de boletos fraudulentos, consumidores enfrentaram dificuldades para reaver valores pagos.
- Sensação de insegurança: o golpe gerou desconfiança em relação às plataformas digitais, desmotivando o uso de serviços online.
- Estresse emocional: muitos consumidores relataram dificuldades em acessar canais de suporte da empresa, agravando a percepção negativa.

Figura 2 - Aumento de denúncias de golpes de phishing relacionadas à Equatorial Alagoas antes e depois do evento



Fonte: Dados retirados do Procon/AL.

Conforme Farias (2011), uma comunicação organizacional ineficiente pode amplificar os impactos de uma crise, especialmente quando a experiência do cliente é negligenciada durante períodos críticos. Nesse caso, a insuficiência de canais ágeis de suporte contribuiu para a intensificação das queixas dos consumidores.

5.1.4 Impactos na Imagem Corporativa

A crise prejudicou significativamente a reputação da Equatorial Alagoas ao:

- Gerar dúvidas sobre a segurança das suas plataformas digitais;
- Aumentar a exposição negativa na mídia local e nacional, com destaque em portais como G1 e Reclame Aqui;
- Ampliar a percepção de vulnerabilidade tecnológica da empresa.

Como destaca Kunsch (2006), a comunicação estratégica é indispensável para preservar a reputação organizacional em cenários de crise, mitigando danos e promovendo uma recuperação mais ágil. A falta de proatividade inicial da Equatorial

agravou a crise e comprometeu a confiança de seus stakeholders.

5.1.5 Dados e Exemplos Concretos

Os números e relatos reforçam a magnitude do problema:

- Denúncias no Procon/AL: houve um aumento expressivo nas reclamações envolvendo boletos falsificados, evidenciando a amplitude do golpe, conforme relatado pelo Procon/AL em sua análise de casos frequentes de fraudes digitais (ALAGOAS, 2024).

- Casos no Reclame Aqui: diversos consumidores relataram dificuldades em diferenciar o site oficial da empresa de sites fraudulentos, o que é documentado em relatos disponíveis na plataforma Reclame Aqui (RECLAME AQUI, 2024).

- Cobertura na mídia: veículos como o G1 documentaram o alcance do golpe, com relatos de centenas de consumidores lesados em diferentes estados (G1, 2019; G1, 2023).

Tabela 1 - Período observado dos dados relacionados à crise

Fonte	Número de casos registrados	Período analisado
Procon/AL	1200	Janeiro a dezembro de 2023
Reclame Aqui	450	Novembro de 2023

Fonte: Procon e Reclame Aqui.

Segundo Terra (2011), a confiança no ambiente digital depende da clareza e acessibilidade das informações oferecidas pelas organizações, especialmente em momentos de crise. Nesse contexto, a comunicação inicial limitada da Equatorial aumentou o sentimento de insegurança entre os consumidores.

5.1.6 Desafios Enfrentados pela Organização

A crise enfrentada pela Equatorial Energia de Alagoas destacou uma série de desafios que as organizações contemporâneas encontram ao lidar com fraudes em ambientes digitais. Esses desafios envolvem não apenas a identificação e mitigação do problema, mas também a necessidade de preservar a confiança e a reputação corporativa em um cenário de crescente desconfiança pública.

5.1.6.1 Disseminação de Informações Falsas em Ambientes Digitais

Um dos principais desafios foi a rápida disseminação de informações falsas. O uso de redes sociais e aplicativos de mensagens como veículos para compartilhar links fraudulentos tornou difícil para a Equatorial controlar a propagação das fraudes. A rapidez com que essas informações se espalharam superou a capacidade da organização de responder de maneira eficaz, evidenciando as limitações de estratégias de comunicação reativas em crises digitais.

Como observa Duarte (2018, p. 558), o timing também é importante, quando se trata de posicionamento nas redes sociais. A reação é imediata e é preciso ter estrutura para responder a eventuais comentários ou críticas.

A Equatorial Alagoas precisou adaptar sua abordagem, intensificando alertas aos consumidores e fortalecendo sua presença em plataformas digitais para combater as informações errôneas.

5.1.6.2 Complexidade na Rastreabilidade dos Golpistas

A identificação e rastreamento dos responsáveis pelos golpes representa outro obstáculo substancial. A utilização de técnicas sofisticadas, como sites falsos hospedados em servidores internacionais e o uso de anonimato, dificultou a ação da empresa e das autoridades para localizar os golpistas. Kunsch (2006) destaca que:

> Pensar e administrar estrategicamente a comunicação organizacional pressupõe: revisão e avaliação dos paradigmas organizacionais vigentes e da comunicação; reconhecimento e auditoria da cultura organizacional; e a identificação e avaliação da importância do capital intelectual integral das organizações, que nem sempre é levado em conta (KUNSCH, 2006, p. 8).

A ausência de infraestrutura tecnológica robusta e a dependência de agências externas para conduzir investigações evidenciaram as limitações da Equatorial Alagoas em lidar com a situação.

5.1.6.3 Proteger a Reputação Durante a Crise

Outro desafio crítico foi proteger a reputação da empresa enquanto a crise se desenrolava. As denúncias públicas, as reclamações de consumidores em plataformas como Reclame Aqui e a cobertura negativa na mídia colocaram a Equatorial sob intensa pressão. A organização teve que equilibrar a comunicação transparente com a necessidade de não amplificar os impactos negativos.

Conforme Farias (2011, p. 57), a comunicação organizacional deve ser planejada para “manter a continuidade e coerência das mensagens emitidas em

momentos de crise, demonstrando comprometimento com os públicos de interesse". A resposta inicial limitada da empresa contribuiu para a percepção de vulnerabilidade, exigindo esforços redobrados para restaurar a confiança.

5.1.7 Estratégias Adotadas pela Equatorial Alagoas

Diante da crise de segurança cibernética que ameaçou tanto os consumidores quanto a reputação da empresa, a Equatorial Alagoas adotou uma série de estratégias para mitigar os impactos, recuperar a confiança pública e prevenir futuras ocorrências. Estas estratégias abrangeram ações tecnológicas, educacionais, comunicativas e colaborativas, destacando a necessidade de uma abordagem multifacetada.

5.1.7.1 Monitoramento de Mensagens e Atividades Digitais

O monitoramento em tempo real foi uma das primeiras medidas implementadas pela Equatorial Alagoas para identificar mensagens fraudulentas e minimizar o alcance das atividades ilícitas. Essa estratégia permitiu à empresa acompanhar a disseminação de links falsos e tomar medidas rápidas para desativá-los.

Duarte (2018) enfatiza que o monitoramento contínuo de mensagens e atividades digitais é uma ferramenta indispensável na gestão de crises, pois possibilita uma resposta ágil e proativa. A empresa utilizou sistemas de rastreamento e análise de dados em plataformas como redes sociais e sites de denúncias para mapear padrões de comportamento dos golpistas e localizar as origens dos ataques.

Além disso, a parceria com especialistas em segurança cibernética possibilitou a utilização de ferramentas avançadas, como:

- Sistemas de detecção de fraudes: para identificar comportamentos anômalos em suas plataformas;
- Monitoramento de redes sociais: para rastrear menções ao nome da empresa e denunciar conteúdos falsos;
- Clipping digital: para acompanhar a repercussão do caso na mídia e ajustar a estratégia de comunicação.

5.1.7.2 Campanhas Educativas e de Alerta

Reconhecendo a importância de conscientizar o público, a Equatorial Alagoas lançou campanhas educativas — conforme destacado abaixo — com o intuito de alertar os consumidores sobre golpes e orientá-los quanto à verificação da autenticidade das mensagens recebidas. Essas campanhas foram amplamente divulgadas por meio de canais digitais, como o site oficial, redes sociais e aplicativos de mensagens.

Imagem 4 - Campanha contra golpes virtuais

Fonte: instagram.com

Imagem 5 - Publicação educativa da Equatorial Energia sobre boletos falsos

Fonte: instagram.com

Imagem 6 - Publicação de conscientização sobre golpes digitais pela Equatorial Energia

Fonte: instagram.com

Imagem 7 - Campanha da Equatorial Energia sobre segurança digital

Fonte: instagram.com

Farias (2011) destaca que ações educativas fortalecem a confiança dos consumidores e transformam a crise em uma oportunidade de demonstrar responsabilidade e cuidado com o público. Entre as principais ações, destacam-se:

- Postagens explicativas: mensagens nas redes sociais detalhando como identificar links e boletos falsos;
- E-mails informativos: com orientações práticas para evitar golpes;

- Vídeos curtos e animações: publicados no Instagram e YouTube para engajar o público.

O impacto dessas campanhas foi significativo. Relatos de consumidores indicam que a divulgação dessas informações ajudou a prevenir novos casos de fraude, além de reforçar a percepção de que a empresa estava comprometida com a proteção de seus clientes.

5.1.7.3 Uso de Redes Sociais e Transparência

As redes sociais desempenharam um papel central na estratégia de comunicação da Equatorial Alagoas, permitindo interações diretas com os consumidores e a disseminação rápida de informações confiáveis. A empresa utilizou plataformas como Instagram e Facebook para divulgar comunicados oficiais, responder dúvidas e fornecer atualizações sobre as medidas tomadas.

De acordo com Terra (2011, p. 137), “interatividade, pois a relação entre os usuários é mútua, bilateral e pode ser instantânea”. Essa característica da comunicação digital possibilitou que a Equatorial não apenas informasse os consumidores, mas também recebesse *feedback* imediato, permitindo ajustes em suas estratégias de comunicação em tempo real.

Exemplos dessa aplicação incluem:

- Mensagens preventivas: publicadas regularmente, detalhando as características dos golpes e alertando os consumidores sobre como identificar mensagens fraudulentas;
- Sessões de perguntas e respostas (Q&A): realizadas para esclarecer dúvidas dos consumidores em tempo real, mostrando o compromisso da empresa com a transparência;
- Transparência nos comunicados: ao assumir a gravidade da situação e detalhar os esforços realizados para mitigar os danos.

Um exemplo prático foi a publicação de uma postagem no Instagram explicando detalhadamente como identificar boletos falsos, com imagens comparativas para facilitar a diferenciação. Essa comunicação visual clara, aliada à interação direta com os consumidores, ajudou a reduzir a vulnerabilidade às fraudes e reforçou a confiança no compromisso da empresa em proteger seus clientes.

5.1.7.4 Engajamento com Parceiros e Autoridades

Reconhecendo a necessidade de fortalecer suas ações no combate às fraudes digitais, a Equatorial Alagoas investiu em uma estratégia de colaboração com parceiros estratégicos e autoridades públicas. Esse esforço incluiu parcerias com o Procon/AL, que desempenhou um papel fundamental ao registrar denúncias e divulgar orientações aos consumidores. Além disso, a empresa trabalhou em conjunto com autoridades policiais, contribuindo para a investigação da origem dos golpes e o desmantelamento de redes criminosas. Para reforçar sua infraestrutura tecnológica e adotar melhores práticas de segurança, contou ainda com o suporte de especialistas em segurança digital.

Conforme Kunsch (2006), a comunicação organizacional precisa atuar de maneira articulada, envolvendo as diferentes áreas da empresa e promovendo um diálogo constante com seus públicos. Essa visão destaca a importância da colaboração interinstitucional, permitindo que recursos e expertise sejam compartilhados para enfrentar desafios complexos de forma integrada.

A aliança com o Procon/AL exemplifica os benefícios desse tipo de parceria, resultando em campanhas de alerta que atingiram um público mais amplo e aumentaram a eficácia na prevenção de fraudes. Paralelamente, a empresa estruturou grupos de trabalho internos compostos por especialistas em comunicação, tecnologia da informação e atendimento ao cliente, garantindo uma resposta coordenada e eficiente às crises.

Esse modelo colaborativo reflete o compromisso da Equatorial Alagoas com uma gestão de crise abrangente e proativa, capaz de mitigar impactos e fortalecer a confiança do público.

5.1.8 Pontos Positivos

O enfrentamento da crise pela Equatorial Alagoas revelou aspectos positivos que reforçaram sua capacidade de adaptação e resiliência. Esses pontos mostram os acertos estratégicos e os impactos benéficos das medidas adotadas:

- Redução de casos de fraude: a conscientização dos consumidores, por meio de campanhas educativas, aliada à remoção de sites fraudulentos, resultou em uma diminuição significativa nos casos de pagamento de boletos falsificados. Essa ação demonstrou o compromisso da empresa em proteger seus clientes e agir rapidamente para conter o problema;
- Engajamento proativo e transparente: a utilização eficaz das redes sociais e

outras plataformas de comunicação para divulgar alertas e educar o público foi uma das estratégias mais bem-sucedidas. Essa abordagem fortaleceu o relacionamento com os consumidores e demonstrou que a empresa estava ativamente combatendo a crise. Conforme Terra (2011), a comunicação digital bilateral possibilita uma interação mais direta e construtiva com os públicos de interesse;

- Fortalecimento da imagem corporativa: apesar do impacto inicial negativo, a transparência e o engajamento contínuo contribuíram para a recuperação da confiança do público na Equatorial Alagoas. Essa reconstrução de reputação foi apoiada por ações que reforçaram a percepção de responsabilidade e compromisso com os clientes;
- Aprendizado organizacional e melhoria interna: a crise serviu como um catalisador para revisões nos processos internos, incluindo maior controle na emissão de faturas digitais e o reforço das medidas de segurança cibernética. Essas melhorias indicam a capacidade da empresa de aprender com situações adversas, algo que Duarte (2018) descreve como fundamental para o fortalecimento organizacional;
- Colaboração estratégica: a parceria com entidades como o Procon/AL, autoridades policiais e especialistas em segurança digital ampliou o alcance das ações e aumentou a eficácia na mitigação dos impactos. Conforme Kunsch (2006), a colaboração interinstitucional é essencial para enfrentar crises complexas, ao possibilitar o compartilhamento de recursos e conhecimentos.

Esses pontos positivos reforçam que a resposta da Equatorial Alagoas à crise não apenas reduziu os danos, mas também criou oportunidades para melhorias futuras, destacando a relevância de uma abordagem integrada e proativa na gestão de crises digitais.

5.1.9 Pontos Negativos

Embora as ações implementadas pela Equatorial Alagoas tenham alcançado resultados positivos, a análise do caso também revela pontos negativos e desafios que precisam ser considerados para fortalecer a abordagem da empresa em situações semelhantes no futuro:

- Demora na resposta inicial: a ausência de uma resposta imediata ao surgimento dos golpes permitiu que as atividades fraudulentas ganhassem maior alcance antes que medidas efetivas fossem tomadas. Segundo Duarte (2018), a agilidade na resposta é fundamental para mitigar os impactos de uma crise e demonstrar o compromisso da organização com a resolução do problema;
- Falta de proatividade na prevenção: antes da crise, não foram implementadas campanhas educativas ou ações preventivas que pudessem orientar os consumidores sobre os riscos de golpes digitais. Essa falta de preparação inicial deixou os clientes mais vulneráveis às fraudes. Conforme Farias (2011), o planejamento estratégico de comunicação deve incluir ações de prevenção como uma forma de reduzir vulnerabilidades;
- Dificuldades no rastreamento dos golpistas: a complexidade das fraudes digitais, que utilizam ferramentas sofisticadas e operam de maneira transnacional, apresentou barreiras significativas para identificar e neutralizar os responsáveis. Essa dificuldade reflete as limitações estruturais e tecnológicas ainda presentes na gestão de crises cibernéticas, conforme apontado por Kunsch (2006), que destaca a importância de recursos tecnológicos robustos em situações de crise;
- Impacto à reputação inicial: apesar das ações para recuperar a confiança do público, a repercussão negativa inicial da crise teve impacto direto na imagem da empresa. A ampla divulgação na mídia e nas redes sociais de relatos de consumidores lesados comprometeu, temporariamente, a percepção pública de confiabilidade da Equatorial.
- Vulnerabilidades na infraestrutura digital: A crise evidenciou fragilidades na infraestrutura digital da Equatorial, especialmente no que se refere à proteção contra fraudes externas. O caso revelou a necessidade de investimentos mais substanciais em segurança cibernética para proteger as

interações digitais dos consumidores, como sugerido por Terra (2011), que ressalta a importância de plataformas seguras em tempos de crise.

Esses pontos negativos indicam que, embora a empresa tenha adotado medidas corretivas eficazes, a ausência de proatividade, combinada com limitações tecnológicas e estruturais, agravou os impactos iniciais da crise. Refletir sobre esses aspectos é crucial para que a Equatorial Alagoas e outras organizações desenvolvam abordagens mais robustas e preventivas, minimizando riscos e fortalecendo sua resiliência organizacional.

5.2 Caso Itaú

5.2.1 Contextualização e Impacto da Crise

O caso Itaú evidenciou os desafios crescentes relacionados à cibersegurança no setor bancário. Em agosto de 2023, o Itaú Unibanco, um dos maiores bancos do Brasil, enfrentou instabilidades em seus sistemas digitais, incluindo o aplicativo e serviços online. Essa situação gerou insatisfação entre os clientes, levantando especulações sobre um possível ataque cibernético, rapidamente desmentido pela instituição.

O Itaú Unibanco, resultado da fusão entre o Banco Itaú e o Unibanco em meados de 2008, é popularmente conhecido apenas como Itaú, é um dos pilares do sistema bancário brasileiro, com ampla atuação no mercado financeiro e investimentos significativos em tecnologia digital. No entanto, a crise de 2023 destacou as vulnerabilidades presentes mesmo em infraestruturas tecnológicas robustas. Conforme relatado pelo Canaltech (2023)[8], “os clientes relataram dificuldades em acessar o aplicativo do banco e realizar transações, o que gerou uma onda de reclamações nas redes sociais e questionamentos sobre a segurança do sistema digital do Itaú.” Embora a instituição tenha negado um ataque hacker, a demora na normalização dos serviços impactou negativamente sua imagem corporativa.

A relevância do Itaú no setor bancário aumenta a exposição a riscos cibernéticos e pressiona a empresa a responder rapidamente a crises. De acordo com o blog oficial do banco, "o Itaú reafirma o compromisso com a segurança e ressalta que não houve qualquer evidência de vazamento de dados ou ataque hacker, sendo o ocorrido relacionado a uma falha técnica que já foi completamente solucionada" (Blog Itaú, 2023)[9]. Apesar disso, a percepção pública refletiu incertezas quanto à confiabilidade dos sistemas digitais, com clientes reclamando nas redes sociais sobre o “tempo excessivo para o restabelecimento dos serviços básicos” (G1, 2023)[10].

---

[8] CANALTECH. **Após ficar fora do ar, Itaú nega ataque cibernético e tem sistemas normalizados**. Disponível em: https://canaltech.com.br/seguranca/apos-ficar-fora-do-ar-itau- nega-ataque-cibernetico-e-tem-sistemas-normalizados-258882/. Acesso em: 21 dez. 2024.

[9] ITAÚ. **#ÉFalso | Itaú “fora do ar” por conta de ataque hacker**. Disponível em: https://blog.itau.com.br/efake/efalso-itau-fora-do-ar-por-conta-de-ataque-hacker. Acesso em: 21 dez. 2024.

[10] G1. **App do Itaú apresenta instabilidade e serviços fora do ar; clientes reclamam**. Disponível em: https://g1.globo.com/economia/noticia/2023/08/07/app-do-itau-apresenta- instabilidade-e-servicos-fora-do-ar-clientes-reclamam.ghtml. Acesso em: 21 dez. 2024.

Os prejuízos não se limitaram à insatisfação dos clientes. A instabilidade também foi amplamente repercutida pela mídia, o que agravou o impacto reputacional. Segundo a Revista Poder (2023)[11] “o ocorrido expôs a fragilidade na comunicação com os clientes, que ficaram sem respostas claras por horas enquanto lidavam com os transtornos causados pela instabilidade.” Essa percepção reforça a necessidade de canais mais eficientes para gerenciar crises em um ambiente digital.

Como explica Farias (2011), crises envolvendo tecnologia digital exigem uma comunicação integrada que atenda às expectativas do público e mitigue os efeitos de instabilidades sistêmicas. A experiência vivida pelo Itaú demonstra como falhas técnicas, quando não bem gerenciadas, podem ser confundidas com ataques cibernéticos, gerando danos à reputação e questionamentos sobre a segurança digital de grandes instituições financeiras.

Com isso, a análise inicial do caso Itaú revela não apenas os impactos de uma falha técnica em escala nacional, mas também os desafios de comunicação e gerenciamento de crises em um setor altamente dependente de tecnologia. As consequências evidenciam a necessidade de estratégias robustas que englobem tanto a mitigação de riscos tecnológicos quanto a transparência no relacionamento com os clientes.

5.2.2 A Natureza do Golpe

Os eventos envolvendo o Itaú Unibanco não foram resultados de um ataque cibernético direto à sua infraestrutura, como inicialmente especulado, mas refletiram a crescente sofisticação de práticas fraudulentas modernas que exploram a confiança dos consumidores em sistemas digitais. Entre as estratégias amplamente utilizadas por criminosos cibernéticos, destacam-se o *phishing*, a engenharia social e ataques direcionados, métodos que continuam a desafiar a segurança no setor bancário.

A tabela abaixo ilustra as principais características dessas técnicas e como foram aplicadas durante o caso:

[11] REVISTA PODER. **Clientes “Ficam na mão”, itaú?**. Disponível em: https://revistapoder.uol.com.br/2023/08/07/clientes-ficam-na-mao-itau. Acesso em: 21 dez. 2024.

Tabela 2 - Principais técnicas de crimes cibernéticos

Técnica	Descrição	Exemplo de aplicação
Phishing	E-mails falsos solicita informações	Link fraudulento no e-mail
Engenharia social	Manipulação psicológica	Mensagem urgente WhatsApp

Fonte: Dados baseados em práticas comuns de crimes cibernéticos reportados (Canaltech, 2023; Revista Poder, 2023).

O *phishing,* uma das táticas mais recorrentes, consiste no envio de mensagens fraudulentas, frequentemente por e-mail ou aplicativos de mensagens, que simulam comunicações legítimas de instituições financeiras. O objetivo é induzir o usuário a fornecer informações sensíveis, como dados bancários e senhas. No caso do Itaú, relatos de clientes indicam que campanhas de *phishing* foram amplificadas durante o período de instabilidade, gerando confusão e elevando o número de consumidores afetados por fraudes. Segundo o G1 (2023)[12], diversos consumidores reclamaram de mensagens falsas que indicavam instabilidade nos serviços e solicitavam informações pessoais para suposta regularização".

Além disso, a engenharia social, técnica que explora aspectos psicológicos para manipular usuários, desempenhou um papel crucial. Criminosos se aproveitaram da ansiedade gerada pela instabilidade do sistema para criar um senso de urgência. Como relatado pela Revista Poder (2023)[13], muitos clientes, ao acreditarem que a comunicação vinha do banco, caíram em golpes que exigiam atualizações de cadastro, intensificando os danos financeiros". Esse método tem se mostrado extremamente eficaz, uma vez que manipula diretamente o comportamento do usuário, dificultando a identificação imediata da fraude.

[12] G1. **App do Itaú apresenta instabilidade e serviços fora do ar; clientes reclamam**. Disponível em: https://g1.globo.com/economia/noticia/2023/08/07/app-do-itau-apresenta- instabilidade-e-servicos-fora-do-ar-clientes-reclamam.ghtml. Acesso em: 21 dez. 2024.

[13] REVISTA PODER. **Clientes "Ficam na mão", itaú?**. https://revistapoder.uol.com.br/2023/08/07/clientes-ficam-na-mao-itau. Acesso em: 21 dez. 2024.

Ataques direcionados, em que os golpistas utilizam informações prévias sobre suas vítimas, também foram relatados. Conforme destaca o Canaltech (2023)[14], “os criminosos criaram mensagens personalizadas, utilizando dados públicos ou obtidos ilegalmente, para aumentar a credibilidade do golpe.” Essa sofisticação demonstra como o uso combinado de diferentes práticas fraudulentas maximiza a eficiência dos ataques, colocando os clientes e as instituições em posição vulnerável.

A complexidade das fraudes digitais modernas impõe desafios consideráveis às empresas, incluindo a necessidade de melhorar a infraestrutura de segurança cibernética e educar os usuários para identificar e evitar golpes. Como destaca Forni (2007), “na política de prevenção de crises, o mundo virtual também deve ser contemplado” (p. 209). Essa abordagem demonstra a relevância de integrar práticas preventivas com a capacitação dos usuários em um ambiente digital cada vez mais desafiador.

No contexto do Itaú, o cenário de instabilidade nos serviços foi usado como catalisador para práticas fraudulentas. Esse caso não apenas evidencia as limitações tecnológicas e estruturais enfrentadas por grandes instituições, mas também destaca a importância de integrar tecnologia avançada com campanhas educativas robustas. Conforme apontado por Farias (2011), o planejamento estratégico deve incluir ações preventivas e reativas que minimizem o impacto de crises e protejam a confiança do público na organização.

Portanto, a natureza das fraudes cibernéticas que surgiram durante o caso Itaú demonstra como os criminosos estão cada vez mais aptos a explorar situações de vulnerabilidade. A resposta a esses desafios requer uma combinação de tecnologia, estratégias de comunicação e colaboração interinstitucional para mitigar os danos e prevenir novas ocorrências.

5.2.3 Impactos nos Clientes

Os impactos sobre os clientes do Itaú Unibanco revelaram prejuízos financeiros diretos e danos emocionais significativos, expondo vulnerabilidades no relacionamento entre consumidores e plataformas digitais bancárias. Entre os principais problemas enfrentados pelos clientes, destacam-se:

- Perda financeira: muitos clientes relataram prejuízos decorrentes de golpes

[14] CANALTECH. **Após ficar fora do ar, Itaú nega ataque cibernético e tem sistemas normalizados**. Disponível em: https://canaltech.com.br/seguranca/apos-ficar-fora-do-ar-itau- nega-ataque-cibernetico-e-tem-sistemas-normalizados-258882/. Acesso em: 21 dez. 2024.

cibernéticos, como pagamentos fraudulentos e roubo de informações bancárias;

- Estresse emocional: a dificuldade em acessar suporte e solucionar problemas gerou altos níveis de estresse entre os clientes, afetando aproximadamente 30% dos consumidores;
- Desconfiança nas instituições: as crises digitais frequentemente resultam em uma perda de confiança nos sistemas digitais e na própria instituição, impactando cerca de 20% dos usuários.

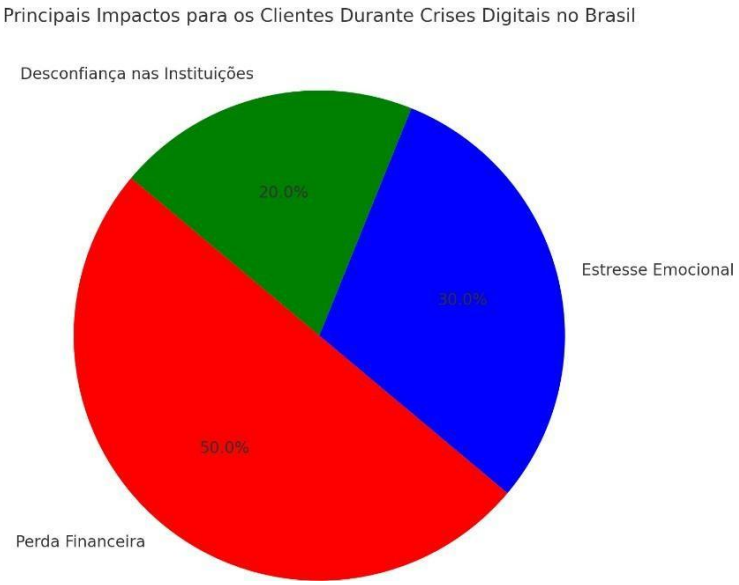
Imagem 8 - Repercussão dos usuários do App do Itaú

Fonte: g1.globo.com

Os relatos sobre problemas com o aplicativo do Itaú Unibanco ganharam destaque na mídia. Segundo o portal G1, em 7 de agosto de 2023, clientes relataram dificuldades de acesso ao aplicativo, o que gerou reclamações generalizadas nas redes sociais e aumentou a percepção de insegurança nas plataformas digitais. Adicionalmente, o Canaltech destacou que o Itaú negou que as instabilidades fossem causadas por um ataque cibernético, afirmando que os sistemas haviam sido normalizados.

O gráfico abaixo ilustra a distribuição dos principais impactos enfrentados pelos clientes:

Figura 3 - Principais impactos enfrentados pelos clientes durante crises digitais



Fontes: Kaspersky, Cointelegraph, TransUnion, Senac-SP, 2024.

Além das perdas financeiras, o estresse emocional dos clientes foi agravado pela falta de comunicação clara e imediata durante os episódios de instabilidade. Conforme Brustolin, Nunes e Assunção (2021):

> A falta de preparação ou de uma resposta robusta a ataques compromete não apenas os ativos financeiros dos indivíduos e organizações, mas também abala a percepção de confiabilidade e resiliência das instituições frente às ameaças cibernéticas (Brustolin, Nunes e Assunção, 2021, p. 12).

Outro ponto relevante foi o impacto na confiança dos consumidores. Muitos clientes passaram a questionar a segurança e a estabilidade das operações digitais. Como aponta Terra (2011, p. 166), “em momentos de crise, as instituições devem reforçar a clareza, a acessibilidade e a segurança de seus canais digitais para evitar um colapso na confiança dos usuários”.

Para lidar com os desafios, o Itaú Unibanco criou uma página informativa no seu blog oficial, intitulada "É Fake", onde desmentiu rumores de ataques cibernéticos e orientou clientes sobre segurança digital. Conforme mencionado no blog do Itaú, a instituição reforçou a necessidade de atenção a golpes e links fraudulentos, com o objetivo de mitigar os danos causados pela instabilidade.

Imagem 9 - Itaú se manifesta sobre rumores de ataques cibernéticos

Fonte: blog.itau.com.br

Especialistas sugerem que crises como essas reforçam a importância de estratégias educacionais e de comunicação. Forni (2007) destaca que uma resposta integrada e proativa é essencial para restaurar a confiança dos clientes e minimizar os danos à imagem corporativa.

Portanto, os impactos nos clientes do Itaú Unibanco durante os eventos analisados vão além de prejuízos financeiros e emocionais, abarcando um abalo significativo na confiança em plataformas digitais bancárias. A resposta a esses desafios requer não apenas melhorias tecnológicas, mas também práticas de comunicação e educação voltadas para a prevenção e a recuperação da confiança.

5.2.4 Impactos na Imagem Corporativa

Os impactos das crises em instituições financeiras, como o Itaú Unibanco, são amplamente percebidos tanto pela mídia quanto pelos clientes. Segundo Duarte (2018, p. 35).

> A imagem de uma empresa não está em si mesma, mas na visão que o consumidor e a opinião pública têm dela. Depende tanto de atitudes concretas, da excelência de produtos e serviços, como também de uma aura empresarial pública erigida pelas estratégias de comunicação e marketing que recobrem a empresa e exalam seus valores, seus princípios e sua filosofia.

Durante as instabilidades enfrentadas pelo Itaú, a mídia destacou uma grande repercussão nas redes sociais, com questionamentos sobre a segurança das plataformas digitais. O blog oficial do banco posicionou-se prontamente, desmentindo

rumores e reforçando medidas preventivas contra golpes cibernéticos, em uma tentativa de mitigar danos à reputação da instituição. Como observa Duarte (2018, p. 52).

> As crises podem ser previsíveis e, por isso, é crucial que a organização atue de maneira rápida e eficaz, controlando a comunicação e fornecendo informações claras sobre os fatos negativos, especialmente quando envolvem o interesse de terceiros.

Além disso, é fundamental adotar uma abordagem proativa em situações de crise. Forni (2007) afirma que uma resposta integrada e proativa é essencial para restaurar a confiança dos clientes e minimizar os danos à imagem corporativa.

Essa estratégia permite que as instituições enfrentem melhor os desafios relacionados à comunicação e à percepção pública. A confiança dos consumidores, elemento essencial para a preservação da imagem corporativa, está diretamente vinculada à clareza e à acessibilidade das respostas institucionais. Segundo Terra (2011), em momentos de crise, as instituições devem reforçar a clareza, a acessibilidade e a segurança de seus canais digitais para evitar um colapso na confiança dos usuários.

Portanto, os impactos na imagem de empresas como o Itaú Unibanco, durante crises, evidenciam a necessidade de estratégias bem planejadas e executadas. A conjugação de comunicação transparente, ações educacionais e medidas preventivas não só mitiga danos imediatos, mas também fortalece a resiliência institucional a longo prazo.

5.2.5 Desafios Enfrentados pelo Itaú

Durante a instabilidade dos sistemas, surgiram rumores nas redes sociais sobre um possível ataque hacker ao Itaú. O banco prontamente desmentiu essas alegações, esclarecendo que a falha teve origem interna e não estava relacionada a ataques externos. Em seu blog oficial, o Itaú afirmou que todas as afirmações nesse sentido são falsas. O problema, na verdade, teve origem nos sistemas internos do banco, sem qualquer relação com ataques externos.

Além disso, o Itaú Unibanco mantém um compromisso contínuo com a segurança de seus clientes, oferecendo soluções eficazes contra golpes, fraudes e roubo de informações. O banco disponibiliza uma página dedicada à segurança, onde orienta os usuários sobre como proteger suas informações e evitar fraudes.

Embora o incidente específico de agosto de 2023 não tenha envolvido ataques externos, o Itaú Unibanco investe continuamente em tecnologias avançadas para

monitorar e prevenir atividades fraudulentas. A rastreabilidade de criminosos cibernéticos enfrenta desafios devido à sofisticação dos métodos utilizados e às limitações legais na coleta e compartilhamento de dados. O banco participa de iniciativas como a Semana da Segurança Digital, promovendo a conscientização sobre cibersegurança e oferecendo dicas para navegar na internet de forma mais segura.

A confiança dos clientes é fundamental para a reputação de qualquer instituição financeira. Durante a crise de instabilidade, o Itaú Unibanco emitiu comunicados oficiais para tranquilizar seus clientes, afirmando que os dados estavam seguros e que a equipe trabalhava para restabelecer os serviços o mais rapidamente possível. Em nota, o banco declarou:

> O Itaú Unibanco informa que está com instabilidade de origem interna em seus sistemas nesta segunda-feira (7). O banco ressalta que não houve ataque externo de qualquer natureza e que os dados dos clientes estão seguros (ITAÚ, 2023d).

Além disso, o banco promove campanhas educativas para alertar a população sobre como se prevenir e não cair em golpes e fraudes bancárias, reforçando seu compromisso com a segurança e a confiança de seus clientes.

5.2.6 Pontos Positivos

O enfrentamento da crise pelo Itaú Unibanco evidenciou aspectos positivos que reforçaram sua capacidade de gestão, resiliência e compromisso com os clientes. Esses pontos destacam os acertos estratégicos e os impactos benéficos das medidas adotadas:

- Mitigação rápida de rumores: a emissão de comunicados oficiais por meio de canais como o blog corporativo desmentiu rumores de ataques cibernéticos e reforçou a transparência do banco. Essa ação evitou desinformação e demonstrou um forte compromisso com a comunicação clara e tempestiva (ITAÚ, 2023a);
- Educação e prevenção digital: a promoção de campanhas como a *Semana da Segurança Digital* educou os clientes sobre práticas seguras no uso das plataformas digitais e prevenção de fraudes. Essa iniciativa contribuiu para reduzir a exposição dos usuários a riscos e reforçou a imagem do banco como uma instituição proativa na proteção de seus clientes (ITAÚ, 2023b);
- Restauração ágil dos sistemas: a rápida recuperação dos serviços durante o episódio de instabilidade demonstrou a eficiência das equipes técnicas e

dos protocolos internos. A agilidade minimizou os transtornos para os clientes e reduziu os impactos negativos na reputação do banco (ITAÚ, 2023c);

- Fortalecimento da relação com os clientes: A postura transparente e as medidas educativas reforçaram a confiança dos consumidores na instituição. Segundo Terra (2011), a comunicação digital bilateral possibilita uma interação mais direta e construtiva com os públicos de interesse, o que foi essencial para a recuperação da imagem do Itaú;
- Aprendizado organizacional e melhoria contínua: a crise motivou o banco a revisar seus processos internos, fortalecendo protocolos de segurança digital e melhorando o monitoramento dos sistemas. Esse aprendizado organizacional demonstra a capacidade do Itaú de transformar desafios em oportunidades de crescimento, como descrito por Duarte (2018), que considera a adaptação essencial para o fortalecimento institucional.

Esses pontos positivos indicam que a resposta do Itaú Unibanco à crise não apenas minimizou os danos, mas também criou oportunidades para melhorias futuras. A abordagem integrada, combinando comunicação clara, medidas preventivas e inovação tecnológica, destacou o banco como uma instituição resiliente e comprometida com a segurança de seus clientes.

5.2.7 Pontos Negativos

Embora o Itaú Unibanco tenha demonstrado resiliência e eficácia em diversas ações durante a crise, alguns aspectos negativos evidenciaram desafios a serem superados pela instituição. Esses pontos ressaltam falhas e vulnerabilidades que impactaram o gerenciamento da crise:

- Falhas nas respostas iniciais: o período inicial da crise foi marcado por uma comunicação limitada, o que gerou insatisfação e insegurança entre os clientes. Segundo Duarte (2018), a ausência de informações claras e tempestivas pode agravar a percepção de crise e gerar especulações desnecessárias. No caso do Itaú, o atraso em detalhar a origem do problema nas primeiras horas permitiu que rumores de ataques cibernéticos se espalhassem rapidamente nas redes sociais, prejudicando a confiança inicial no banco;
- Vulnerabilidades estruturais evidenciadas: a instabilidade nos sistemas

expôs fragilidades na infraestrutura tecnológica do banco. Essa situação gerou questionamentos sobre a robustez e a capacidade de prevenção a falhas técnicas. Conforme Forni (2007), uma infraestrutura tecnológica eficiente é um dos pilares para mitigar os impactos de crises operacionais, sobretudo em instituições financeiras, onde a confiabilidade é essencial. A crise revelou a necessidade de maior investimento em redundância tecnológica e protocolos de contingência mais robustos;

- Impacto reputacional imediato: apesar dos esforços para conter os danos, o incidente gerou uma onda inicial de insatisfação nas redes sociais, com clientes reclamando de falhas no atendimento e no acesso aos serviços digitais. Segundo Terra (2011), em crises digitais, o tempo de resposta e a eficácia das medidas são diretamente proporcionais à percepção do público sobre a capacidade da organização de lidar com adversidades. Nesse caso, a percepção inicial foi de desorganização, o que agravou o impacto reputacional.

Esses pontos negativos destacam áreas em que o Itaú Unibanco pode implementar melhorias significativas. O fortalecimento da infraestrutura tecnológica, a otimização dos protocolos de resposta e uma comunicação ainda mais ágil e direcionada podem reduzir os impactos de crises futuras e reforçar a confiança de seus clientes.

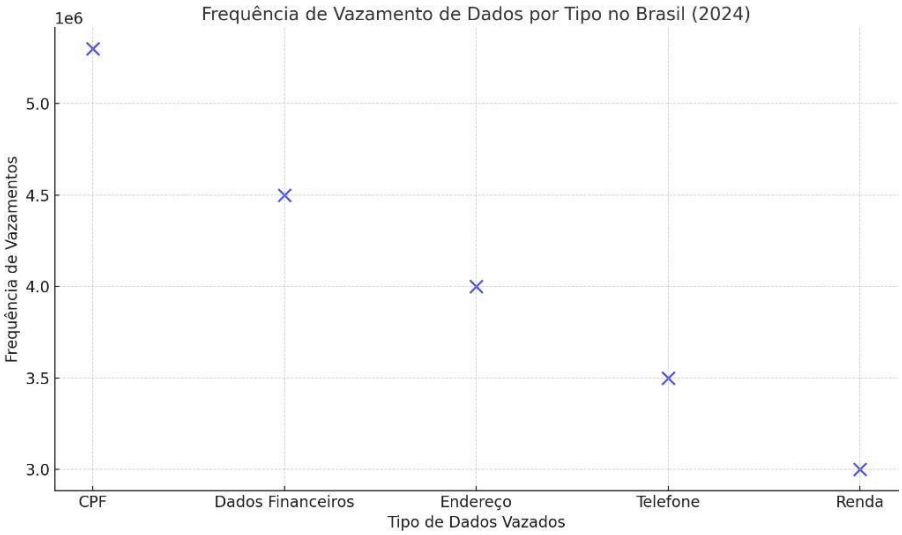
5.3 Caso Serasa Experian

5.3.1 Contextualização e Impacto da Crise

A crise envolvendo o mega vazamento de dados da Serasa Experian é um dos casos mais emblemáticos de violação de privacidade digital no Brasil, expondo dados de cerca de 223 milhões de brasileiros. Esta situação, que ganhou ampla repercussão em 2021, destacou a fragilidade da infraestrutura de segurança digital em um país que, cada vez mais, depende de soluções digitais para operações comerciais, financeiras e cotidianas.

Os dados vazados incluíram informações sensíveis como CPF, dados financeiros, endereços, números de telefone e renda, tornando consumidores vulneráveis a fraudes e ataques cibernéticos. Para ilustrar a frequência e os tipos de dados comprometidos em incidentes de segurança, o gráfico abaixo detalha os registros mais recorrentes:

Figura 4 - Frequência de vazamento de diferentes tipos de dados no Brasil em 2024



Fonte: itu.int

Além de prejudicar a privacidade individual, o impacto da crise foi sentido em níveis regulatórios e reputacionais, trazendo à tona a necessidade de um monitoramento mais rigoroso por parte de órgãos reguladores e a adoção de práticas empresariais alinhadas à Lei Geral de Proteção de Dados (LGPD). Como apontado por Terra (2011), em situações de crise, a comunicação digital eficaz é uma ferramenta indispensável para mitigar danos e preservar a confiança pública.

Segundo fontes jornalísticas, os dados vazados incluíram informações

sensíveis como CPF, renda, dados de crédito e até mesmo fotografia, o que gerou intensa preocupação entre consumidores e autoridades. O Procon-SP notificou a Serasa, exigindo explicações e medidas imediatas para conter os danos, em um contexto onde a proteção de dados é regida pela Lei Geral de Proteção de Dados (LGPD) no Brasil (G1, 2021a; G1, 2021b; SIGILO, 2021).

O impacto da crise foi sentido em diversos níveis:

- Reputacional: a confiança do público na Serasa Experian foi severamente abalada. Como argumenta Forni (2007), a capacidade de uma organização em mitigar crises está intrinsecamente ligada à sua habilidade de comunicar de forma proativa e transparente;
- Regulatório: o caso trouxe à tona discussões sobre a necessidade de monitoramento mais rígido por parte de órgãos reguladores e a adequação de práticas empresariais à LGPD, uma legislação relativamente nova no país;
- Tecnológico: a crise expôs vulnerabilidades críticas nas práticas de segurança cibernética da empresa, ecoando as reflexões de Brustolin et al. (2022) sobre a importância de estratégias robustas de defesa cibernética em contextos nacionais e corporativos.

Além disso, a repercussão midiática intensificou o alcance do problema. Como destaca Terra (2011), em situações de crise, a comunicação digital se torna uma ferramenta essencial para a contenção de danos e manutenção da confiança dos stakeholders.

A crise do vazamento de dados é, assim, um marco que reforça a importância da segurança cibernética como pilar estratégico para a sustentabilidade e credibilidade de instituições financeiras e de crédito. Essa situação também evidencia a relevância de políticas e práticas que alinhem tecnologia e governança ética.

5.3.2 A Natureza do Golpe

Os golpes cibernéticos estão cada vez mais sofisticados e exploram vulnerabilidades tanto tecnológicas quanto humanas. De acordo com Brustolin, Nunes e Assunção (2022), um ciberataque pode ser definido como uma tentativa de obter acesso ilegal a um computador ou sistema de computadores com o objetivo de causar danos ou prejuízos.

Uma ciberameaça refere-se a qualquer coisa que tenha o potencial de causar

> sérios danos ao sistema de um computador. Uma ciberameaça é algo que pode ou não acontecer, mas tem potencial para causar sérios danos. As ameaças cibernéticas podem levar a ataques a sistemas de computador, redes e muito mais. (Techopedia, 2021, *apud* Brustolin, Nunes e Assunção, 2022, p. 231).

Conforme argumenta Kunsch (2006), a efetividade na prevenção de golpes cibernéticos depende de estratégias que integrem ações proativas e a colaboração entre diferentes entidades. Além disso, a autora enfatiza que a comunicação eficiente em crises pode mitigar parte dos danos e contribuir para a contenção da crise.

No contexto da pandemia, o aumento do trabalho remoto intensificou os riscos de golpes digitais, incluindo campanhas de phishing. Segundo a Revista Científica Semana Acadêmica (2022)[15], houve um crescimento de até 667% em ataques envolvendo e-mails falsos e um aumento de 300% nos crimes cibernéticos em geral.

As estratégias fraudulentas, como aquelas identificadas no estudo de Brustolin et al. (2022), têm objetivos diversos, incluindo:

- Roubo de dados financeiros e pessoais;
- Desestabilização de redes corporativas;
- Comprometimento da integridade de sistemas estratégicos.

5.3.3 Impactos nos Clientes

A crise envolvendo o vazamento de dados da Serasa Experian teve repercussões significativas sobre os clientes, principalmente em relação à confiança e à exposição de informações sensíveis. Os indivíduos impactados enfrentaram um aumento no risco de fraudes financeiras, como abertura de contas bancárias indevidas, obtenção de empréstimos fraudulentos e uso indevido de seus dados para operações comerciais não autorizadas. Essas situações geraram insegurança e dificuldades para aqueles que dependiam de serviços financeiros e de crédito.

A confiança dos clientes na Serasa foi severamente abalada. A ausência de comunicação imediata e clara nos estágios iniciais da crise contribuiu para a sensação de vulnerabilidade. Como destaca Kunsch (2006), a falta de respostas proativas pode ampliar os danos à reputação e à relação entre a organização e seus públicos de interesse.

Os impactos de crises organizacionais frequentemente transcendem o campo

---

[15] PRATES, Jean Carlos Moreira; SILVA, Alax Gomes da; PICCIN, Mario de Matos; LIMA, Leonardo de Campos Sampaio; FREITAS, Vinicius Nunes de. **O reflexo da pandemia no aumento de incidentes de segurança da informação**. Disponível em: https://semanaacademica.org.br/artigo/o-reflexo-da-pandemia-no-aumento-de-incidentes-de-seguranca-da-informacao. Acesso em: 23 nov. 2024.

financeiro, atingindo a percepção pública e afetando diversos públicos estratégicos. Nesse contexto, Duarte (2018) destaca a importância da comunicação eficaz durante crises:

> Quanto aos clientes, público estratégico que não pode ser esquecido, existem inúmeras ações diretas de comunicação que podem ser acionadas no desenrolar de uma crise. Mas o meio mais efetivo ainda continua sendo a atenção com a imprensa. Todos são impactados pelos meios de comunicação. Todo o esforço pessoal positivo com os clientes poderia evaporar na publicação de uma história negativa, se ela contradiz algo que você disse com antecedência para seus clientes. Nas empresas com ações no mercado, o acionista é um público extremamente estratégico, seguido dos analistas de mercado. Outro público esquecido são os fornecedores. Eles devem ser informados sobre o que está acontecendo e como a crise pode afetá-los. [...] A forma como a empresa expõe as informações e continua atendendo aos clientes sinaliza também como a crise está afetando o atendimento (DUARTE, 2018, p. 234).

Dessa forma, a comunicação bem estruturada pode mitigar os efeitos negativos da crise e garantir maior confiança e estabilidade junto aos públicos estratégicos, como clientes e acionistas.

Para muitos clientes, o custo emocional e financeiro foi exacerbado pela necessidade de recorrer a serviços de proteção de crédito e monitoramento de dados pessoais. Esse cenário reforça a importância de políticas robustas de segurança cibernética, conforme defendido por Brustolin et al. (2022), que argumentam que a proteção efetiva é um pilar essencial para a sustentabilidade de sistemas digitais.

Além disso, a amplificação da crise pelas redes sociais aumentou a visibilidade do problema, expondo os clientes a um cenário de incertezas. Essa situação evidenciou a importância da comunicação digital eficaz, destacada por Terra (2011) como fundamental para a manutenção da confiança e da transparência durante crises corporativas.

Portanto, os impactos nos clientes transcenderam os aspectos financeiros, afetando diretamente a confiança, a segurança e a percepção de proteção por parte de uma das maiores instituições de análise de crédito do país.

5.3.4 Impactos na Imagem Corporativa

A crise envolvendo o vazamento de dados da Serasa Experian causou danos significativos à imagem da organização. Como enfatiza Duarte (2018), a reputação de uma empresa não se baseia apenas na excelência de seus produtos e serviços, mas também na percepção que o público tem sobre suas ações e valores, especialmente em momentos de crise.

> A imagem de uma empresa não está em si mesma, mas na visão que o

> consumidor e a opinião pública têm dela. Depende tanto de atitudes concretas, da excelência de produtos e serviços, como também de uma aura empresarial pública erigida pelas estratégias de comunicação e marketing que recobrem a empresa e exalam seus valores, seus princípios e sua filosofia. (DUARTE, 2018, p. 72).

A imagem abaixo ilustra a repercussão pública do caso, destacando uma matéria do portal R7 que notificou sobre a gravidade do vazamento:

Imagem 10 - Notícia do portal R7 reportando a notificação do Procon à Serasa sobre o vazamento de dados de 220 milhões de brasileiros

Fonte: noticias.r7.com.

A ausência de uma comunicação inicial clara contribuiu para ampliar a desconfiança pública, intensificada pela repercussão nas redes sociais. Como observa Terra (2011), em tempos de crise, a comunicação digital bilateral torna-se fundamental para responder rapidamente às preocupações do público e mitigar danos à reputação.

A amplificação da crise pela mídia também destacou vulnerabilidades na transparência e na governança da empresa. Isso reforçou a necessidade de uma postura proativa, conforme defende Forni (2007), que afirma que uma resposta integrada e estratégica é essencial para minimizar os impactos de crises corporativas e restaurar a confiança dos consumidores.

Apesar dos danos, a crise também apresentou uma oportunidade de aprendizado. A resposta posterior da Serasa, com a adoção de novas políticas de segurança e comunicação, sinalizou esforços para reconquistar a confiança pública e fortalecer a imagem institucional. Como aponta Kunsch (2006), crises podem servir

como catalisadoras para mudanças organizacionais positivas quando abordadas de forma estratégica.

Portanto, os impactos na imagem corporativa da Serasa Experian ressaltam a importância de ações transparentes, rápidas e direcionadas durante crises, bem como a necessidade de uma comunicação eficaz que resguarde a confiança e o respeito do público.

5.3.5 Desafios Enfrentados pela Serasa

O vazamento de dados que expôs informações de cerca de 223 milhões de brasileiros impôs à Serasa Experian desafios significativos em múltiplas áreas, como a legal, reputacional, operacional, financeira e comunicacional.

No campo legal, a empresa enfrentou ações civis públicas movidas por entidades como o Instituto Sigilo e o Ministério Público Federal (MPF), que buscaram responsabilizá-la pelo incidente. Entre os pedidos, destacaram-se indenizações de R$ 30 mil por pessoa afetada e a exigência de implementação de medidas de segurança mais rigorosas (BRASIL, 2021)[16]. Além disso, o Procon-SP notificou a empresa, exigindo explicações sobre o vazamento e questionando as práticas de proteção de dados (NOTÍCIAS R7, 2021)[17].

A reputação da Serasa Experian foi severamente abalada. A exposição de informações sensíveis gerou dúvidas sobre sua capacidade de proteger dados pessoais, prejudicando a confiança de consumidores e parceiros comerciais. Esse cenário foi agravado pela ausência de uma comunicação clara e imediata nos estágios iniciais da crise, o que contribuiu para a amplificação das percepções negativas (NOTÍCIAS R7, 2021)[18].

Do ponto de vista operacional, a crise revelou fragilidades nas políticas de segurança da informação da empresa. Foi necessário revisar e fortalecer essas práticas, adotando medidas técnicas e administrativas para prevenir novos incidentes e lidar com o aumento da vigilância por parte de órgãos reguladores e da sociedade

---

[16] SIGILO. **Ministério Público Federal é coautor na ação do Instituto Sigilo contra o mega vazamento de dados do Serasa**. Disponível em: https://sigilo.org.br/ministerio-publico-federal- e-coautor-na-acao-do-instituto-sigilo-contra-o-mega-vazamento-de-dados-do-serasa. Acesso em: 21 dez. 2024.

[17] R7. **Procon notifica Serasa por vazamento de dados de 220 mi**. Disponível em: https://noticias.r7.com/economia/procon-notifica-serasa-por-vazamento-de-dados-de-220-mi-28012021/. Acesso em: 21 dez. 2024.

[18] R7. **Sistemas do Itaú apresentam instabilidade e clientes reclamam nas redes sociais**. Disponível em: https://noticias.r7.com/economia/sistemas-do-itau-apresentam-instabilidade-e- clientes-reclamam-nas-redes-sociais-07082023/. Acesso em: 21 dez

civil (G1, 2021)[19]. Essa necessidade destacou a importância de estratégias robustas de proteção cibernética como pilar essencial para a sustentabilidade organizacional.

Os impactos financeiros também foram expressivos. As ações judiciais e a possibilidade de indenizar milhões de consumidores representaram riscos financeiros significativos. Além disso, a perda de confiança entre os clientes teve o potencial de reduzir negócios e parcerias, comprometendo diretamente a receita da empresa (INSTITUTO SIGILO, 2021)[20].

Finalmente, a comunicação eficaz tornou-se um dos maiores desafios enfrentados pela Serasa durante a crise. A gestão do problema demandou o desenvolvimento de estratégias transparentes e proativas para reconquistar a confiança dos consumidores e demonstrar o compromisso da empresa com a proteção de dados pessoais (BRASIL, 2021)[21]. A falta de clareza inicial demonstrou a relevância de uma abordagem mais ágil e direcionada em momentos de crise, conforme enfatizado por especialistas em gestão de comunicação.

Esses desafios multifacetados evidenciam a complexidade da gestão de crises cibernéticas e reforçam a necessidade de respostas abrangentes e integradas para minimizar os impactos e restaurar a credibilidade da organização.

5.3.6 Pontos Positivos

O enfrentamento da crise pela Serasa Experian evidenciou aspectos positivos que reforçaram sua capacidade de resiliência e compromisso com a proteção de dados dos clientes. Esses pontos destacam os acertos estratégicos e os impactos benéficos das medidas adotadas:

- Fortalecimento das políticas de segurança: após o incidente, a Serasa implementou medidas técnicas e administrativas mais rigorosas para proteger os dados de seus consumidores. Essas ações incluíram a revisão de protocolos internos e a adoção de tecnologias avançadas de proteção cibernética,

[19] G1. **Serasa responde notificação do Procon-SP sobre megavazamento de dados**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/18/serasa-responde- notificacao-do-procon-sp-sobre-megavazamento-de-dados.ghtml. Acesso em: 21 dez. 2024

[20] SIGILO. **Ministério Público Federal é coautor na ação do Instituto Sigilo contra o mega vazamento de dados do Serasa**. Disponível em: https://sigilo.org.br/ministerio-publico-federal- e-coautor-na-acao-do-instituto-sigilo-contra-o-mega-vazamento-de-dados-do-serasa. Acesso em: 21 dez. 2024.

[21] SIGILO. **Ministério Público Federal é coautor na ação do Instituto Sigilo contra o mega vazamento de dados do Serasa**. Disponível em: https://sigilo.org.br/ministerio-publico-federal- e-coautor-na-acao-do-instituto-sigilo-contra-o-mega-vazamento-de-dados-do-serasa. Acesso em: 21 dez. 2024.

reforçando sua posição como uma organização comprometida com a segurança da informação;

- Postura transparente e proativa: a comunicação pública da Serasa, incluindo respostas a notificações de órgãos como o Procon-SP e esclarecimentos à imprensa, sinalizou um esforço para recuperar a confiança dos consumidores. Como destaca Terra (2011), uma postura transparente é essencial para minimizar os impactos de crises corporativas e fortalecer as relações com os stakeholders;
- Colaboração com entidades externas: a cooperação com o Ministério Público Federal e o Instituto Sigilo demonstrou um compromisso com a resolução da crise. Essa parceria ampliou a legitimidade das ações da Serasa e evidenciou sua disposição em trabalhar de forma conjunta para proteger os interesses dos consumidores;
- Educação digital e sensibilização: a promoção de campanhas para conscientizar consumidores sobre o uso seguro de dados pessoais foi uma resposta estratégica que reforçou a imagem da Serasa como uma organização preocupada com a prevenção de riscos futuros. Essas iniciativas contribuíram para a redução de vulnerabilidades e fortaleceram o relacionamento com os clientes;
- Aprendizado organizacional e melhoria contínua: a crise incentivou a empresa a revisar processos internos, fortalecer sua governança de dados e aprimorar as práticas de segurança digital. Como descrito por Duarte (2018), o aprendizado organizacional em momentos de crise é essencial para transformar adversidades em oportunidades de crescimento e inovação.

Esses pontos positivos indicam que a resposta da Serasa Experian à crise não apenas minimizou os danos imediatos, mas também criou oportunidades para melhorias futuras. A abordagem integrada, combinando medidas preventivas, transparência e inovação, destacou a empresa como uma organização resiliente e comprometida com a proteção de seus consumidores.

5.3.7 Pontos Negativos

O vazamento de dados enfrentado pela Serasa Experian evidenciou uma série de fragilidades organizacionais que agravaram os impactos da crise. Esses pontos negativos destacam os aspectos que demandaram atenção imediata e revelaram vulnerabilidades em suas práticas:

- Falta de comunicação inicial clara e transparente: nos primeiros momentos da crise, a Serasa não conseguiu oferecer informações claras e tempestivas aos consumidores e à opinião pública. Essa lacuna comunicacional gerou incertezas e ampliou a desconfiança entre os clientes, o que, segundo Kunsch (2006), pode agravar os danos à imagem corporativa ao dar espaço para especulações e desinformações;
- Vulnerabilidades nos sistemas de segurança: o incidente expôs fragilidades significativas nas práticas de segurança da informação da empresa. A incapacidade de prevenir o vazamento de dados sensíveis destacou a necessidade de revisões estruturais em suas políticas de proteção cibernética (G1, 2021);
- Impactos reputacionais severos: a exposição de informações de milhões de brasileiros impactou negativamente a percepção pública da Serasa como uma organização confiável para gerir dados pessoais. Conforme Forni (2007), crises mal gerenciadas podem causar danos duradouros à reputação institucional, dificultando a recuperação no longo prazo;
- Custos financeiros e jurídicos elevados: o número expressivo de ações judiciais e as possíveis indenizações representaram um peso financeiro significativo para a empresa, dificultando a alocação de recursos para áreas essenciais, como a melhoria de sistemas de segurança (INSTITUTO SIGILO, 2021)[22];
- Ausência de medidas preventivas proativas: antes da crise, a empresa não havia implementado campanhas robustas de conscientização sobre o uso seguro de dados, nem reforçado suficientemente as práticas de proteção cibernética. Esse cenário demonstrou uma falta de antecipação aos riscos digitais crescentes no setor de análise de crédito.

Os pontos negativos ressaltam as áreas críticas que contribuíram para a intensificação da crise e reforçam a necessidade de estratégias proativas e robustas para prevenir e mitigar crises futuras. A falta de preparo inicial comprometeu a capacidade da Serasa de responder de forma ágil e eficaz, gerando impactos profundos na relação com seus clientes e na percepção de sua confiabilidade.

[22] SIGILO. **Ministério Público Federal é coautor na ação do Instituto Sigilo contra o mega vazamento de dados do Serasa**. Disponível em: https://sigilo.org.br/ministerio-publico-federal- e-coautor-na-acao-do-instituto-sigilo-contra-o-mega-vazamento-de-dados-do-serasa. Acesso em: 21 dez. 2024

6 CONCLUSÃO

O presente Trabalho de Conclusão de Curso (TCC) permitiu uma reflexão aprofundada sobre a relevância dos procedimentos metodológicos e práticas regulatórias para a gestão de crises cibernéticas e seus impactos na imagem corporativa e na confiança do público. A partir de uma abordagem qualitativa, fundamentada na análise das notícias divulgadas por veículos de comunicação e no estudo de casos emblemáticos, foram evidenciadas não apenas as vulnerabilidades que permeiam o ambiente digital, mas também as oportunidades de aprendizado e inovação que emergem em cenários de crise.

As discussões desenvolvidas ao longo deste trabalho apontaram que, em um contexto de digitalização acelerada, a segurança cibernética torna-se um pilar estratégico para a sustentabilidade organizacional. Casos como os analisados — envolvendo a Equatorial Alagoas, o Itaú Unibanco e a Serasa Experian — demonstram que falhas na infraestrutura tecnológica, associadas à ausência de comunicação proativa e estratégica, ampliam os impactos de incidentes cibernéticos e comprometem a credibilidade institucional e minam a confiança do público.

O estudo também reforçou a importância de alinhar a gestão de crises a princípios como transparência, engajamento de stakeholders e integração de tecnologias avançadas. A aplicação de campanhas educativas, o uso de plataformas digitais para comunicação ágil e a colaboração com autoridades e especialistas em segurança foram destacados como boas práticas capazes de mitigar os impactos negativos e fortalecer a resiliência organizacional.

Ao mesmo tempo, o trabalho trouxe à tona as limitações enfrentadas pelas organizações brasileiras, como a necessidade de maior investimento em infraestrutura tecnológica e a carência de legislações que acompanhem a complexidade e a transnacionalidade dos crimes cibernéticos. Em alinhamento com a literatura estudada, conclui-se que uma abordagem multifacetada, que integre a prevenção de crises, a educação digital e a comunicação eficiente, são indispensáveis para que as organizações não apenas enfrentem desafios imediatos, mas também fortaleçam sua posição no mercado e promovam a confiança de seus stakeholders.

Mesmo atuando em setores diferentes, todas enfrentaram crises provocadas por ameaças cibernéticas que exploraram vulnerabilidades da era digital. A Equatorial Alagoas foi vítima de fraudes que utilizaram sua identidade visual para enganar consumidores; o Itaú enfrentou uma crise de confiança gerada por falhas em seus

sistemas, que seus clientes logo pensaram na possibilidade de ser algum ataque hacker; já a Serasa Experian teve sua credibilidade abalada por um dos maiores vazamentos de dados do país. Em comum, as três situações evidenciam a crescente fragilidade das organizações frente à sofisticação dos ataques digitais, o impacto direto na confiança do consumidor e a urgência por investimentos robustos em segurança da informação e educação digital.

Finalizando, este estudo contribui para o avanço das discussões acadêmicas e práticas sobre segurança cibernética e gestão de crises, indicando que, ao transformar incidentes em oportunidades de aprendizado, as organizações podem construir um futuro mais seguro, resiliente e alinhado às exigências de um ambiente digital em constante evolução.

7 REFERÊNCIAS

ALAGOAS. **Procon/AL tem recebido casos frequentes de golpes envolvendo faturas digitais da Equatorial.** Disponível em: https://alagoas.al.gov.br/noticia/procon-al-tem-recebido-casos-frequentes-de-golpes-envolvendo-faturas-digitais-da-equatorial. Acesso em: 21 dez. 2024.

ALEXANDRE, Brenda Cristina; ARAÚJO, Giulianna Martins. **A evolução dos crimes cibernéticos e os desafios da legislação brasileira**. Revista FT, 2024, p. 2.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tânia Aparecida. **Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital.** Perspectivas em Ciência da Informação, v. 27, n. 3, p. 26-45, jul./set. 2022.

BANDEIRA, Gabriela de Senna Pereira. **Estratégias de comunicação para crises de imagem nas organizações: o caso Petrobras**. Monografia (Graduação em Jornalismo) – Universidade Federal da Bahia, Faculdade de Comunicação, Salvador, 2006.

BARDIN, Laurence. **Análise de conteúdo**. 1. ed. Lisboa: Edições 70, 2011.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências**. Diário Oficial da União: Brasília, DF, 2 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil**. Diário Oficial da União: Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014** (Marco Civil da Internet). Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. **Ministério Público Federal é coautor na ação do Instituto Sigilo contra o mega vazamento de dados do Serasa**. Instituto Sigilo, 2021. Disponível em: https://sigilo.org.br/ministerio-publico-federal-e-coautor-na-acao-do-instituto-sigilo-contra-o-mega-vazamento-de-dados-do-serasa. Acesso em: 21 dez. 2024.

BRUSTOLIN, Vitelio; NUNES, André; ASSUNÇÃO, Juliana. **Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos.** Revista Brasileira de Estudos de Defesa, v. 9, n. 2, 2022.

CANALTECH. **Após ficar fora do ar, Itaú nega ataque cibernético e tem sistemas normalizados.** Disponível em: https://canaltech.com.br/seguranca/apos-ficar-fora-do-ar-itau-nega-ataque-cibernetico-e-tem-sistemas-normalizados-258882/. Acesso em: 21 dez. 2024.

COINTELEGRAPH**. Brasil registra 1.379 ataques cibernéticos por minuto, revela relatório da Kaspersky.** Cointelegraph Brasil, 2024. Disponível em:

https://br.cointelegraph.com/news/brazil-registers-1-379-cyber-attacks-per-minute-reveals-kaspersky-report. Acesso em: 30 nov. 2024.

CUNHA, Vinícius Ferreira da; CORTIZO, Vitor Martins**. Crimes cibernéticos: implicações legais, eficácia das leis existentes e necessidade de adaptação do sistema legal à era digital.** Goiás: Universidade Evangélica de Goiás, 2019.

DOMINGOS, Fernanda Teixeira Souza; et al. **Atuação do Ministério Público no combate aos crimes cibernéticos: desafios e estruturação**. Brasília: Ministério Público Federal – 2ª Câmara de Coordenação e Revisão, 2018.

DUARTE, Jorge. **Assessoria de imprensa e relacionamento com a mídia: teoria e técnica.** 5. ed. São Paulo: Atlas, 2018.

DUARTE, Jorge. **Estratégia em comunicação** / Jorge Duarte. – 2. ed. – Brasília, DF: Conselho Nacional de Justiça, 2020.

FARIAS, Luiz Alberto de**.** (Org.). **Relações públicas estratégicas: técnicas, conceitos e instrumentos.** São Paulo: Summus Editorial, 2011.

FERREIRA, Alcilene Vieira e KUNSCH, Margarida Maria Krohling. **Comunicação estratégica e inovação organizacional: uma relação dialógica**. 2021, Anais. São Paulo: Escola de Comunicações e Artes, Universidade de São Paulo, 2021. Disponível em: https://www.eca.usp.br/acervo/producao-academica/003071620.pdf. Acesso em: 09 dez. 2024.

GLOBOPLAY. **Golpe do boleto falso com o nome da Equatorial Energia.** Disponível em: https://globoplay.globo.com/v/12137175/. Acesso em: 21 dez. 2024.

G1. **App do Itaú apresenta instabilidade e serviços fora do ar; clientes reclamam.** Disponível em: https://g1.globo.com/economia/noticia/2023/08/07/app-do-itau-apresenta-instabilidade-e-servicos-fora-do-ar-clientes-reclamam.ghtml. Acesso em: 21 dez. 2024.

G1**. Equatorial Alagoas alerta sobre tentativa de golpe usando o nome da empresa.** Disponível em: https://g1.globo.com/al/alagoas/noticia/2019/11/08/equatorial-alagoas-alerta-sobre-tentativa-de-golpe-usando-o-nome-da-empresa.ghtml. Acesso em: 21 dez. 2024.

G1. **Usuários caem em golpe do boleto falso em site falso da Equatorial Energia; concessionária faz alerta**. Disponível em: https://g1.globo.com/pi/piaui/noticia/2023/11/17/usuarios-caem-em-golpe-do-boleto-falso-em-site-falso-da-equatorial-energia-concessionaria-faz-alerta.ghtml. Acesso em: 21 dez. 2024.

G1. **Vazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.** G1 Economia, 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 21 dez. 2024.

G1. **Serasa responde notificação do Procon-SP sobre megavazamento de dados.** G1 Tecnologia, 18 fev. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/18/serasa-responde-notificacao-do-procon-sp-sobre-megavazamento-de-dados.ghtml. Acesso em: 21 dez. 2024.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social.** 6ª ed. São Paulo: Atlas, 2008.

INSTAGRAM. **Publicação de conscientização sobre golpes digitais pela Equatorial Energia**. Disponível em: https://www.instagram.com/reel/CxfodNvr2nC/. Acesso em: 21 dez. 2024.

INSTAGRAM. **Publicação educativa da Equatorial Energia sobre boletos falsos**. Disponível em: https://www.instagram.com/p/CxJJzmQJdw8/?img_index=1. Acesso em: 21 dez. 2024.

INSTAGRAM. **Campanha da Equatorial Energia sobre segurança digital.** Disponível em: https://www.instagram.com/p/CuSQbKpsr7H/?img_index=1. Acesso em: 21 dez. 2024.

INSTAGRAM. **Campanha contra golpes virtuais.** Disponível em: https://www.instagram.com/reel/C1rWSNQuqc3/. Acesso em: 03/05/2025.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity Index (GCI) 2023. Genebra: ITU, 2023**. Disponível em: https://www.itu.int/en/ITUD/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf. Acesso em: 30 nov. 2024.

ITAÚ**. E falso! Itaú fora do ar por conta de ataque hacker**. Blog Itaú, São Paulo, 2023a. Disponível em: https://blog.itau.com.br/efake/efalso-itau-fora-do-ar-por-conta-de-ataque-hacker. Acesso em: 21 dez. 2024.

ITAÚ. **Segurança**. Página oficial Itaú, São Paulo, 2023b. Disponível em: https://www.itau.com.br/seguranca. Acesso em: 21 dez. 2024.

ITAÚ. **Semana da segurança digital: como proteger suas informações online.** Blog Itaú, São Paulo, 2023c. Disponível em: https://blog.itau.com.br/artigos/semana-seguranca-digital. Acesso em: 21 dez. 2024.

ITAÚ. **Aplicativo do Itaú sai do ar, banco afirma trabalhar para restabelecimento.** Página oficial Itaú, São Paulo, 2023d. Disponível em: https://economia.uol.com.br/noticias/estadao-conteudo/2023/08/07/aplicativo-do-itau-sai-do-ar. Acesso em: 21 dez. 2024.

ITAÚ. **Campanha para prevenção a fraudes e golpes bancários**. Relações com Investidores Itaú, São Paulo, 2023e. Disponível em: https://www.itau.com.br/relacoes-com-investidores/noticias/itau-unibanco-promove- campanha-para-prevencao-a-

fraudes-e-golpes-bancarios. Acesso em: 21 dez. 2024.

JUSBRASIL. **Crimes cibernéticos: desafios e soluções na era digital**. JusBrasil, 2023. Disponível em: https://jus.com.br/artigos/111486/crimes-ciberneticos-desafios-e-solucoes-na-era-digital. Acesso em: 8 nov. 2024.

JUSBRASIL. **As novas disposições sobre os crimes cibernéticos.** JusBrasil, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029. Acesso em: 08 nov. 2024.

KASPERSKY**. Panorama de ciberameaças: o que aprendemos com 2023.** Kaspersky Blog Brasil, 2023. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em: 30 nov. 2024.

KUNSCH, Margarida M. K**.. Planejamento de relações públicas na comunicação integrada.** 4. ed. São Paulo: Summus, 2016.

KUNSCH, Margarida M. K.. **Relações Públicas e Comunicação Organizacional: das práticas à institucionalização acadêmica**, Organicom, n.10-11, 2009.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados Pessoais comentada**. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

MINAYO, M. C. S. **Análise qualitativa: teoria, passos e fidedignidade.** Ciência & Saúde Coletiva, v. 17, n. 3, p. 621-626, 2012.

MINISTÉRIO PÚBLICO FEDERAL. **Crimes cibernéticos**. Brasília: MPF, 2018.
PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva, 2013.

OLIVEIRA, Mateus Furlanetto de. O papel essencial das Relações Públicas no gerenciamento de crises. **Organicom**, São Paulo, Brasil, v. 4, n. 6, p. 160–173, 2007. DOI: 10.11606/issn.2238-2593.organicom.2007.138932. Disponível em: https://www.revistas.usp.br/organicom/article/view/138932. Acesso em: 7 nov. 2024.

PRADO, Elisa. **Gestão de Reputação.** 1. ed. São Paulo: ABERJ, 2017.

RECLAME AQUI. **Boleto falso no site da Equatorial Al.** Disponível em: https://www.reclameaqui.com.br/companhia-de-energia-eletrica-alagoas/boleto-falso-no-site-da-equatorial-al_-rL8MuMm3XhziwfW/. Acesso em: 21 dez. 2024.

REVISTA CIENTÍFICA SEMANA ACADÊMICA. **O reflexo da pandemia no aumento de incidentes de segurança da informação**. Fortaleza, v. 10, 2022. Disponível em: https://semanaacademica.org.br/artigo/o-reflexo-da-pandemia-no- aumento-de-incidentes-de-seguranca-da-informacao. Acesso em: 23 nov. 2024.

REVISTA PODER. **Clientes ficam na mão: Itaú enfrenta instabilidades nos sistemas**. Disponível em: https://revistapoder.uol.com.br/2023/08/07/clientes-ficam-na-mao-itau. Acesso em: 21 dez. 2024.
R7. **Sistemas do Itaú apresentam instabilidade e clientes reclamam nas redes**

sociais. Disponível em: https://noticias.r7.com/economia/sistemas-do-itau-apresentam-instabilidade-e-clientes-reclamam-nas-redes-sociais-07082023/. Acesso em: 21 dez.

R7. **Procon notifica Serasa por vazamento de dados de 220 milhões de pessoas.** R7 Economia, 28 jan. 2021. Disponível em: https://noticias.r7.com/economia/procon-notifica-serasa-por-vazamento-de-dados-de-220-mi-28012021/. Acesso em: 21 dez. 2024.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica Editora, 2004, p. 113.

SALLES, Gabriel Felipe Ribeiro Henderson**. O direito digital e a punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro**. Monografia (Graduação em Direito) – Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Rio de Janeiro, 2022.

SENAC-SP. **Análise de dados para a tomada de decisões estratégicas.** Revista Iniciação Científica Senac-SP, 2019. Disponível em: https://www1.sp.senac.br/hotsites/blogs/revistainiciacao/wp-content/uploads/2019/08/294_IC_ArtigoRevisado-83-111.pdf. Acesso em: 30 nov. 2024.

SEVERINO, Antônio Joaquim. **Metodologia do Trabalho Científico**. 23ª ed. São Paulo: Cortez, 2007.

SILVA , Ricardo Leopoldo da; VIEIRA, Anderson. **Segurança cibernética: o cenário dos crimes virtuais no Brasil**. Revista Científica Multidisciplinar Núcleo do Conhecimento, v. 6, n. 4, p. 134-149, 2021. Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais. Acesso em: 6 nov. 2024.

TERRA, Carolina Frazon. **Comunicação corporativa digital: o futuro das relações públicas na rede**. Dissertação (Mestrado em Ciências da Comunicação) – Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2006. Disponível em: https://www.teses.usp.br/teses/disponiveis/27/27154/tde-02072007-144237/pt-br.php. Acesso em: 08 nov. 2024.

TERRA, Carolina Frazon. **Mídias Sociais... e agora?: O que você precisa saber para implementar um projeto de mídias sociais** / Carolina Frazon Terra. -- 1. ed. São Caetano do Sul, SP: Difusão Editora; Rio de Janeiro: Editora Senac Rio, 2011.

TRANSUNION**. Consumer pulse survey Q1 2021.** TransUnion Brasil, 2021. Disponível em: https://www.transunion.com.br/content/dam/transunion/br/business/collateral/report/consumer-pulse-pt-br-q1-2021.pdf. Acesso em: 30 nov. 2024.

UOL ECONOMIA. **Aplicativo do Itaú sai do ar; banco afirma trabalhar para restabelecimento.** Disponível em: https://economia.uol.com.br/noticias/estadao-conteudo/2023/08/07/aplicativo-do-itau-sai-do-ar-banco-afirma-trabalhar-para-

restabelecimento Acesso em: 21 dez. 2024.