Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

REVISTA SOCIEDADE CIENTÍFICA, VOLUME 7, NÚMERO 1, ANO 2024

ARTIGO ORIGINAL

Aplicação da segurança da informação e LGPD para a experiência e usabilidade dos usuários em aplicativos móveis

Isadora Faria carvalho[1];Rommel Gabriel Gonçalves Ramos [2];Anderson Ferreira de Souza[3]; Luiz Fernando Moura Piantino[4]

Como Citar:
CARVALHO, Isadora Faria; RAMOS, Rommel Gabriel Gonçalves;DE SOUZA, Anderson Ferreira; PIANTINO, Luiz Fernando Moura. Aplicação da segurança da informação e LGPD para a experiência e usabilidade dos usuários em aplicativos móveis. Revista Sociedade Científica, vol.7, n.1, p.1717-1738, 2024.
https://doi.org/10.61411/rsc202437717

DOI: 10.61411/rsc202437717

Área do conhecimento: Sistema de Informação

Palavras-chaves: Segurança da informação, , Usabilidade, Satisfação do usuário, Melhorias práticas, Ameaças à segurança, Recomendações, Tecnologia da informação, Crimes virtuais.

Publicado: 28 de março de 2024

Resumo

O contexto atual de aumento dos crimes virtuais exige que a segurança esteja em constante evolução. Para solucionar essas questões, foram identificadas as principais ameaças à segurança da informação em aplicativos móveis, assim como a usabilidade na sua experiência. Os usuários de aplicativos podem variar desde jovens que estão começando sua vida financeira e nunca tiveram conta em instituições financeiras, até pessoas com baixa escolaridade e dificuldades no uso de aparelhos eletrônicos. São apresentadas recomendações para garantir a segurança da informação e a LGPD em aplicativos, visando a satisfação e a confiança dos usuários. Espera-se que este trabalho seja útil para profissionais da área de tecnologia da informação, desenvolvedores de aplicativos e usuários em geral.

1. Introdução

No cenário atual de utilização generalizada dos recursos da internet, nos deparamos frequentemente com mensagens iniciais que solicitam aos usuários concordância com os "termos de privacidade", "termos de segurança" e permissão de acesso do dispositivo. Muitas vezes, essas solicitações são feitas de forma rotineira e

[1]UEMG ✉
[2]UEMG ✉
[3]UEMG ✉
[4]UEMG ✉

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

automática, e os usuários não apresentam a devida preocupação com a segurança de seus dados pessoais.

A falta de orientações adequadas e o desconhecimento das possíveis consequências decorrentes da negligência em seguir procedimentos simples podem ocasionar sérios problemas de segurança.

A crescente popularização dos *smartphones* a partir da primeira década dos anos 2000 impulsionou a adoção de aplicativos financeiros por clientes de instituições bancárias. Os usuários buscavam nessas ferramentas uma maneira mais rápida e conveniente de realizar transações bancárias e gerenciar suas contas.

Em 2020, durante a pandemia de Covid-19, a interação digital tornou-se ainda mais crucial devido ao isolamento social, aumentando consideravelmente a relevância dos aplicativos financeiros para a manutenção das atividades cotidianas.

Nesse momento de pandemia, uma matéria do site do G1 intitulada “Crimes virtuais: no auge da pandemia, fraudes cometidas no mundo digital aumentaram 175%” (GLOBO, 2022), verificou-se um índice de 175% a mais de crimes cibernéticos em comparação ao período pré-pandemia.

Uma instituição desprovida de uma estrutura sólida que garanta a privacidade dos dados e a administração ética das informações não consegue atrair e manter sua clientela. Além disso, a segurança da informação desempenha um papel crucial na economia de recursos dos cooperados, evitando custos judiciais, pagamentos de indenizações em casos de litígios e minimizando o desgaste da equipe envolvida.

Na perspectiva acadêmica, este estudo sobre segurança da informação possui relevância social ao prevenir vulnerabilidades nos sistemas que poderiam ter um impacto significativo na vida dos usuários, particularmente no contexto financeiro. Dessa forma, esta pesquisa aborda uma temática que transcende o ambiente de trabalho, contribuindo para a proteção dos interesses dos indivíduos e da sociedade como um todo.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

2. Referencial teórico

2.1 Conceito de segurança da informação

Segurança da Informação é um conceito fundamental que envolve a proteção dos dados de propriedade das organizações e de pessoas físicas e jurídicas, garantindo a mitigação de riscos e a continuidade das operações.

De acordo com Campos (2007), a informação é um elemento essencial para todos os processos de negócio de uma organização. A aplicação da segurança da informação envolve o uso de processos de governança empresarial, que abrangem recursos humanos, infraestrutura e lógicos (computacionais).

Para Fontes (2010), a segurança da informação é definida como um conjunto de orientações, normas, procedimentos, políticas e outras ações com o objetivo de proteger o recurso "informação". Zapater e Suzuki (2005) também enfatizam que a segurança da informação envolve a identificação de vulnerabilidades nos diversos ativos de informação de uma organização e a gestão dos riscos associados a esses ativos.

Conforme Laureano (2012), a segurança da informação não deve ser encarada como um evento isolado, mas sim como um processo contínuo e abrangente. Ela deve fornecer às organizações meios eficientes para prevenir e mitigar os possíveis riscos relacionados ao ambiente em que estão inseridas.

Isso implica na implementação de políticas, práticas e controles que visam proteger os ativos de informação da organização contra ameaças internas e externas, como acessos não autorizados, perda de dados e danos físicos ou lógicos.

Segundo a ABNT NBR ISO 27002:2013, a segurança da informação é definida como "a preservação da confidencialidade, integridade e disponibilidade da informação", sendo esses os três principais pilares fundamentais da segurança da informação. Tais pilares devem estar contidos no plano de gestão da segurança da informação das organizações, com o objetivo de implementar as estratégias necessárias para a proteção da informação.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Podemos afirmar que a segurança da informação nas organizações tem como premissa primordial a proteção da informação contra o acesso não autorizado (confidencialidade), a preservação da integridade da informação, evitando violações, e a garantia de acesso aos usuários autorizados (disponibilidade), sempre que necessário (Campos, 2007).

Conforme estabelecido pela ABNT NBR ISO 27002:2013, o princípio da confidencialidade visa assegurar que somente pessoas autorizadas tenham acesso ao conteúdo de informações específicas.

Assegurar a proteção da informação é um princípio fundamental para garantir que uma organização forneça serviços de qualidade, bem como um ambiente controlado e organizado, independentemente do meio em que a informação é armazenada, seja ele eletrônico ou em formato físico (Campos, 2007).

Diante desse contexto, os sistemas de informações estão cada vez mais interconectados, o que significa que os dados e informações estão mais expostos a um número crescente e variado de ameaças e vulnerabilidades (Netto; Silveira, 2007).

2.2 História da segurança da informação

A evolução da Segurança da Informação e suas ferramentas passou por um processo gradual ao longo do tempo. Conforme Santos (2006), desde o momento em que o ser humano deixou de realizar trabalhos braçais para serem substituídos por máquinas, a segurança da informação tornou-se uma preocupação essencial. Inicialmente, quando as informações eram escritas em papel, a segurança era garantida pelo fato de poderem ser guardadas em locais seguros.

No entanto, com a evolução da tecnologia, o armazenamento de informações em mídias digitais as tornou mais vulneráveis a roubos e perdas para enfrentar a vulnerabilidade dos dados no mundo digital, a criptografia surgiu como uma solução.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Segundo Fernandes (2020), a criptografia é um mecanismo de segurança eficaz que consiste em codificar uma mensagem, tornando-a ilegível para pessoas não autorizadas.

A decodificação é feita somente ao chegar ao seu destino, usando uma chave secreta que permite restaurar a mensagem original. Esse processo garante privacidade e integridade das informações, evitando que terceiros possam ler a mensagem original ou alterá-la.

Durante a Segunda Guerra Mundial, a quebra da criptografia da máquina Enigma, usada pelas forças armadas alemãs, por Alan Turing e sua equipe de criptoanalistas utilizando o computador *Bomb*, foi um marco importante para a segurança da informação (LYCETT, 2011).

Na sequência, após a Segunda Guerra Mundial, os Estados Unidos e a União Soviética enfrentaram tensões ideológicas. Os EUA buscavam um meio de comunicação resistente a uma possível Guerra Nuclear e, assim, a agência de investigação DARPA (*Defense Advanced Research Projects*) lançou o projeto ARPANET, em 1969, que desenvolveu a base para o protocolo TCP/IP (*Transmission Control/Internet Protocol*) usado ainda nos dias de hoje. O TCP/IP divide os dados em pequenos pacotes, que são reagrupados no destino, garantindo a confiabilidade da comunicação (SANTOS, 2006).

Na década de 60, a segurança da informação começou a ser considerada fundamental no desenvolvimento de softwares e computadores, como mostrou o caso da IBM, que durante os testes de seus computadores se deparou com estudantes obtendo acesso a partes restritas do sistema com certa facilidade (*Hacking Etico*) (BRANCO, 2021).

Nos anos 90, com o *boom* da Internet e a popularização da interface gráfica para facilitar o uso, a expansão da internet ocorreu em grande escala. Nessa época, a necessidade de antivírus se tornou crucial, impulsionando o surgimento de empresas

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

como a *Avast* e a *McAfee*, focadas na prevenção de ações de *malwares* (BRANCO, 2021).

2.3 Ataques Cibernéticos

Ao longo do tempo, diversos tipos de ataques cibernéticos têm sido utilizados por criminosos para acessar informações sensíveis dos usuários da internet. É importante destacar que muitos desses ataques não são de conhecimento comum da população, especialmente do público-alvo discutido neste trabalho:

- **Engenharia Social:** uma das formas mais comuns de atingir um cliente é por meio da engenharia social, em que o fraudador se passa por um conhecido ou funcionário de instituição conhecida pela vítima. Nesse contato, a vítima acaba repassando seus dados pessoais acreditando ser um procedimento de rotina, percebendo o golpe apenas quando uma transação financeira não autorizada ou algum dano acontece (SANTOS, 2006).
- ***Phishing*:** consiste em pescar informações das vítimas usando e-mails como iscas. Os golpistas enviam mensagens se passando por instituições financeiras ou pessoas conhecidas pela vítima, solicitando acesso a sites, preenchimento de formulários ou download de aplicativos e códigos para obter dados pessoais e financeiros (SANTOS, 2006).
- ***Spam*:** trata-se do recebimento de e-mails com propagandas que podem conter links maliciosos ou direcionar para páginas não confiáveis, podendo expor o usuário a riscos de segurança (SANTOS, 2006).
- **Vírus:** são programas que se executam no dispositivo, podendo se espalhar em outros programas, causando lentidão, travamentos, exclusão de dados e falhas nos programas (SANTOS, 2006).
- ***Worm*:** é um programa independente que se auto propaga através das redes, enviando cópias de si mesmo de computador para computador,

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

explorando vulnerabilidades de programas e sistemas ou falhas na configuração de softwares instalados (BUGS, SD).

- ***Keyloggers* e *Screamloggers*:** esses programas coletam informações digitadas pelos usuários, seja através do teclado físico (*keyloggers*) ou de um teclado virtual exibido na tela (*screamloggers*), repassando esses dados para o fraudador (BUGS, SD).
- ***Adware* e *Spyware*:** mostra propagandas ao público, enquanto o *spyware* acompanha os dados de um sistema e os envia ao destinatário. Em casos maliciosos, eles podem permitir o acesso a senhas bancárias, cartões de crédito, arquivos do computador e histórico de pesquisas (BRANCO, 2021).
- ***Backdoors*:** são formas de hospedagem maliciosa que garantem novas entradas para realizar outros golpes, após recolher os dados considerados interessantes (BRANCO, 2021).
- ***Pharming*:** utiliza o sequestro ou a "contaminação" do DNS (*Domain Name System*) para levar os usuários a um site falso, alterando o DNS do site de destino. O programa mal-intencionado utiliza um certificado auto assinado para fingir a autenticação e induzir o usuário a inserir os dados pessoais no site falsificado (BUGS, SD).

Além desses, existem outros ataques menos comuns, como IP *Spoofing*, que tem o objetivo de assumir a identidade de outro computador, e ataques de força bruta, que utilizam criptoanálise para buscar exaustivamente a descoberta de senhas em diversos meios tecnológicos (MASCARENHAS NETO; ARAÚJO, 2019).

2.4 Classificação dos invasores

Com o aumento dos crimes cibernéticos e seus impactos na sociedade, tornou-se necessário classificar os invasores para medir as perdas e definir as punições de acordo com o tipo de golpe aplicado.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

- ***Hacker:*** é um exímio conhecedor do sistema computacional, possuindo amplo conhecimento para identificar e explorar falhas no sistema. Suas habilidades de análise, assimilação e compreensão permitem que ele acesse o que deseja no computador, usando diversas técnicas (BUGS, SD).
- ***Cracker:*** possui um amplo conhecimento computacional, similar ao *hacker*, mas sua motivação é diferente. O *cracker* busca reconhecimento e notoriedade por meio de seus ataques. Suas ações podem incluir a destruição de funcionalidades e partes de sistemas, alterações em sistemas e remoção de travas, abrindo espaço para a pirataria (BUGS, SD).
- ***Lammer* (novato):** está na fase inicial de aprendizado e geralmente utiliza as mesmas ferramentas que o *hacker* e o *cracker*, mas com menos habilidade e conhecimento. Ele ainda está em processo de aperfeiçoamento de suas técnicas (BUGS, SD).
- ***Bancker:*** é especializado em invadir sistemas bancários, buscando coletar dados como números de cartões de crédito, senhas e números de contas bancárias (BUGS, SD).
- ***Phisher*:** É o aplicador do golpe de *phishing*, interceptando informações digitadas e clicadas pelo usuário para redirecioná-lo a sites falsos, com o objetivo de obter dados pessoais e financeiros (BUGS, SD).
- ***Spammer*:** envia milhares de e-mails não solicitados para os usuários, muitas vezes coletando dados dos usuários para vendê-los a terceiros (BUGS, SD).
- ***Defacer*:** prefere invadir sites, alterando informações e inserindo mensagens idealistas nos sites invadidos, buscando reconhecimento (BUGS, SD).

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

- ***Phreacker*:** é especializado na área de telefonia, realizando atividades como instalação de escutas, reprogramação de centrais telefônicas e realização de ligações gratuitas (BUGS, SD).

2.5 Lei geral de proteção dE dados(LGPD)

A Lei Geral de Proteção de Dados (LGPD), promulgada no Brasil em 2018, tem causado um impacto significativo nas práticas de proteção de dados pessoais em várias áreas, incluindo instituições financeiras (BRAGA, 2022).

A LGPD foi estabelecida com o objetivo de proteger a privacidade e os direitos dos indivíduos, bem como estabelecer regras claras para o tratamento de dados pessoais por parte das organizações (BRAGA, 2022).

Segundo Cost (2019), o objetivo da LGPD é salvaguardar os direitos fundamentais de liberdade, privacidade e o pleno desenvolvimento da personalidade natural. O verbo "salvaguardar" expressa claramente a perspectiva adotada pelo legislador ao considerar o titular dos dados como uma parte vulnerável em relação aos responsáveis pelo tratamento dos dados. Isso evidencia a sua condição de fragilidade.

Para Bioni (2019), a finalidade da LGPD é proteger a privacidade, especialmente em um contexto dominado pelas tecnologias de informação, onde os riscos de invasão da esfera privada do indivíduo são acentuados. Isso torna a esfera da privacidade mais vulnerável a invasões indevidas e injustificadas.

Conforme a Lei 13.709/2018, a LGPD possui a finalidade de preservar a privacidade dos dados, proporcionando mecanismos de defesa eficazes. O artigo 1º dessa lei delimita claramente seu escopo, abrangendo dados de pessoas naturais e jurídicas, independentemente de sua natureza:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

> de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018, Art. 1)

De acordo com Braga e Daniel (2022), a LGPD tem impactado significativamente as instituições financeiras, exigindo uma revisão e ajuste de suas políticas e procedimentos internos relacionados ao tratamento de dados.

Essa adequação implica na implementação de medidas técnicas e organizacionais para assegurar a segurança e a confidencialidade dos dados pessoais coletados, processados e armazenados.

Além disso, as instituições financeiras devem obter o consentimento apropriado dos indivíduos para a utilização de seus dados, bem como fornecer informações claras sobre como esses dados serão utilizados (SÊMOLA, 2014).

No entanto, as instituições financeiras devem estar preparadas para lidar com possíveis violações de dados, conforme destacado por Braga (2022). Nesse sentido, a LGPD estabelece a obrigação de notificar as autoridades competentes e os titulares dos dados em caso de incidentes de segurança que possam comprometer a privacidade das informações pessoais.

Portanto, é essencial que as instituições financeiras tenham planos de resposta a incidentes estabelecidos e testados, visando minimizar os danos e cumprir as exigências legais correspondentes (BIONI, 2019).

Nesse sentido, a conformidade com a LGPD vai além de uma mera questão legal, implicando também em uma transformação cultural nas instituições financeiras, conforme apontado por Braga (2022).

É essencial promover a conscientização e capacitação dos funcionários em relação às práticas de proteção de dados, além de realizar auditorias e avaliações regulares para assegurar a conformidade contínua, como ressaltado por Daniel (2022).

Além disso, é fundamental que as instituições financeiras estabeleçam políticas claras de governança de dados e implementem medidas de *accountability* para garantir a responsabilização em caso de não conformidade (SÊMOLA, 2014).

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Portanto, é relevante destacar que a LGPD possui um potencial significativo para trazer benefícios às instituições financeiras, ao mesmo tempo em que protege os direitos dos indivíduos, conforme afirmam Braga e Daniel (2022).

Ao adotar uma postura de conformidade e implementar práticas robustas de proteção de dados, as instituições financeiras podem fortalecer a confiança dos clientes, aprimorar a gestão de riscos e estabelecer uma vantagem competitiva no mercado, demonstrando um compromisso sólido com a privacidade e a segurança dos dados pessoais (COST, 2019).

2.5.1 Classificação de dados pela LGPD

Com a Lei Geral de Proteção de Dados (LGPD), os dados são classificados de acordo com seu nível de sensibilidade e a necessidade de proteção. A LGPD estabelece diferentes categorias de dados, visando garantir a privacidade e segurança das informações pessoais dos titulares.

- **Dados sensíveis:** Referem-se a informações pessoais relacionadas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II, da Lei n. 13.709/2018). Exemplos incluem biometria facial, DNA, CID's (Classificação Internacional de Doenças), orientação sexual, entre outros.
- **Dados pessoais de crianças e adolescentes:** Devem ser utilizados visando ao melhor interesse e cuidado do menor e requerem consentimento dos pais ou responsáveis. As informações sobre os dados de titulares menores devem estar em linguagem acessível à compreensão desse público-alvo.
- **Existem duas exceções para a necessidade de consentimento:** quando a coleta de informações for necessária para entrar em contato com os pais ou o responsável pela criança ou adolescente, ou quando os dados forem necessários

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

para proteger o titular menor de idade. Nessas hipóteses, o compartilhamento é proibido (art. 14 da Lei n. 13.709/2018). Por exemplo, os dados não essenciais não podem ser requisitos para que um titular menor de idade tenha acesso a aplicativos ou jogos.

- **Dados anonimizados:** Referem-se a dados relativos a um titular que não pode ser identificado ou tornar-se identificável, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III, da Lei n. 13.709/2018). Exemplo: são os dados que não são passíveis de reversão para a identificação de seu titular; podem ser tratados por técnicas como supressão de parte dos dados, criptografia sem chaves de acesso, generalização, substituição de valores por categorias mais amplas, entre outras.
- **Dado pseudonimizado:** Trata-se do tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art. 13, § 4º, da Lei n. 13.709/2018). Por exemplo, a pseudonimização é uma técnica para anonimização do dado, sendo configurada por uma chave secreta para que apenas aqueles com acesso a essa chave possam pseudonimizar as entradas na mesma saída.

2.5.2 Requisitos para o tratamento de dados pela LGPD

O tratamento de dados pessoais conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD) requer o cumprimento de alguns requisitos essenciais para garantir a proteção dos direitos e privacidade dos titulares dos dados. Segue a lista dos principais requisitos para o tratamento de dados:

- **Consentimento expresso do titular:** antes de iniciar o tratamento de dados pessoais, o titular deve dar seu consentimento de forma clara, livre e inequívoca. O consentimento deve ser específico para cada finalidade do tratamento e pode ser revogado a qualquer momento pelo titular.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

- **Necessidade para contratos ou documentos**: o tratamento de dados pessoais é permitido quando é necessário para a elaboração e execução de contratos ou documentos nos quais o titular é parte ou para a realização de medidas pré-contratuais a pedido do titular.
- **Atendimento a obrigações legais ou regulatórias:** o tratamento de dados pessoais também pode ser realizado para o cumprimento de obrigações legais ou regulatórias impostas ao controlador dos dados.
- **Proteção do crédito:** o tratamento de dados é permitido para a proteção do crédito, desde que em conformidade com a legislação pertinente.
- **Consentimento para cumprir obrigação legal:** em casos de processos administrativos, judiciais ou arbitragem, o tratamento de dados pode ser realizado para o cumprimento de uma obrigação legal a qual o controlador está sujeito.
- **Interesses legítimos do controlador ou terceiros:** o tratamento de dados pessoais é permitido quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto nos casos em que prevaleçam os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- **Proteção da vida e da integridade física:** Oo tratamento de dados pessoais pode ser realizado sem consentimento do titular em casos de proteção da vida e da integridade física do titular ou de terceiros.
- **Tutela da saúde:** o tratamento de dados sensíveis relacionados à saúde pode ser realizado, mediante o cumprimento de normas éticas e de sigilo profissional, por profissionais da área da saúde ou por entidades de saúde, exclusivamente, para fins de saúde pública, vigilância sanitária, assistência farmacêutica, entre outros.
- **Estudos e pesquisas:** o tratamento de dados pessoais para fins de estudos e pesquisas pode ser realizado com garantia de anonimização ou

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

pseudonimização dos dados, sempre que possível, e mediante cumprimento de normas éticas e de segurança.

Ao seguir esses requisitos, as organizações podem assegurar que o tratamento de dados pessoais esteja em conformidade com a LGPD e respeite os direitos dos titulares, promovendo uma abordagem ética e responsável no manuseio das informações.

É importante destacar que os requisitos podem variar dependendo do contexto e finalidade do tratamento, portanto, é fundamental que as organizações se mantenham atualizadas com a legislação vigente e apliquem boas práticas de privacidade e segurança da informação.

2.5.3 O ciclo de tratamento de dados pela LGPD

O ciclo de tratamento de dados pela LGPD é composto por etapas que devem ser seguidas pelas organizações ao coletar, processar e armazenar dados pessoais. Abaixo na Figura 1 segue o ciclo de tratamento.

Figura 1 – Ciclo de tratamento de dados pessoais. Fonte: guia rápido da LGPD (2021).

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

É importante lembrar que a LGPD visa proteger os direitos dos titulares de dados e promover uma cultura de privacidade e segurança da informação nas organizações. Portanto, seguir o ciclo de tratamento de dados é fundamental para garantir a conformidade com a lei e promover a confiança dos titulares em relação ao uso de seus dados pessoais.

2.5.4 Direito do titular dos dados pela LGPD

Conforme o guia de proteção de dados (2020, pág:13), a LGPD estabeleceu uma estrutura legal que empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os controladores de dados. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade de acordo com os seguintes itens:

- **Confirmação da Existência de Tratamento de Dados:** o titular tem o direito de obter a confirmação de que seus dados pessoais estão sendo tratados pelo controlador.
- **Acesso aos Dados Pessoais:** o titular tem o direito de acessar todos os seus dados pessoais que estão sendo tratados pelo controlador, bem como informações sobre como esses dados estão sendo utilizados.
- **Correção de Dados:** o titular tem o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados que estejam em posse do controlador.
- **Anonimização, Bloqueio ou Eliminação de Dados:** o titular tem o direito de solicitar a anonimização, bloqueio ou eliminação de dados pessoais que sejam desnecessários, excessivos ou estejam sendo tratados em desconformidade com a lei.
- **Portabilidade dos Dados:** o titular tem o direito de receber os seus dados pessoais em um formato estruturado, de uso comum e leitura

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

automática, bem como o direito de transmitir esses dados a outro fornecedor de serviços ou produtos, se assim desejar.

- **Eliminação e Cancelamento de Dados:** o titular pode solicitar a eliminação ou cancelamento de dados pessoais que não sejam mais necessários para os fins que foram coletados ou quando o consentimento for revogado.
- **Informação sobre Compartilhamento de Dados:** o titular tem o direito de ser informado sobre com quais entidades públicas e privadas o controlador compartilhou seus dados pessoais.
- **Informação sobre o Consentimento:** o titular tem o direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, quando o tratamento de dados depende de autorização.
- **Revogação do Consentimento:** o titular pode revogar o seu consentimento a qualquer momento, mediante manifestação expressa, caso não queira mais que seus dados sejam tratados pelo controlador.
- **Oposição ao Tratamento:** o titular pode se opor ao tratamento de seus dados pessoais quando esse tratamento é realizado com base em uma das hipóteses de dispensa de consentimento, caso não estejam em conformidade com a lei.

É fundamental que as organizações estejam cientes desses direitos e estejam preparadas para atender às solicitações dos titulares de dados. O respeito aos direitos do titular é essencial para estabelecer uma relação de confiança com os clientes e usuários, além de estar em conformidade com a legislação de proteção de dados.

3. Metodologia

A metodologia adotada para esta pesquisa é do tipo exploratória, cujo objetivo é

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

proporcionar maior familiaridade com o problema e construir hipóteses para a investigação (GIL, 2017).

A pesquisa exploratória é desenvolvida ao longo da coleta de informações, buscando aproximar o pesquisador do ambiente de interesse por meio de entrevistas com pessoas com conhecimento na área, levantamentos bibliográficos, pesquisas de campo e análises.

O presente estudo tem como propósito compreender um assunto ou problema que possui poucas informações disponíveis (GIL, 2017). Dessa forma, torna-se necessário definir informações e características fundamentais para apresentar o estudo ao público.

Durante a análise, tornou-se evidente que usabilidade e segurança não são elementos isolados, mas sim componentes interdependentes que colaboram para estabelecer uma experiência mais robusta e confiável.

Iniciativas como a criação de um canal para relato de fraudes, a implementação de autenticação de dois fatores e a promoção da educação dos usuários foram positivamente recebidas.

As opiniões dos usuários desempenham um papel fundamental, suas perspectivas reforçaram a importância de considerar cuidadosamente os passos necessários para otimizar tanto a usabilidade quanto a segurança, reconhecendo que ambas são essenciais para atender às expectativas e demandas dos usuários.

No âmbito mais amplo da área financeira, as práticas sugeridas têm o poder de influenciar positivamente outras instituições, incentivando a adoção de medidas similares em prol da segurança dos clientes.

Do ponto de vista dos sistemas de informação, as melhorias não apenas refletem a integração de tecnologias, como o reconhecimento facial e autenticação biométrica, mas também enfatizam a importância da educação do usuário.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

A conscientização sobre práticas seguras e a comunicação eficaz sobre fraudes surgem como elementos-chave para aprimorar a usabilidade, proporcionando uma experiência mais informada e protegida aos usuários.

Essa abordagem centrada no usuário contribuiu significativamente para a formulação de estratégias que visam não apenas a eficácia da segurança da informação, mas também a otimização da experiência do usuário.

Avaliar o impacto de novas tecnologias no mercado é essencial para compreender e adaptar estratégias de desenvolvimento. Reconhecer a constante inovação é de grande importância; portanto, novas tecnologias devem ser acompanhadas por contínuas tentativas de inovação para se manterem relevantes.

4. Conclusões

A conscientização sobre práticas seguras e a comunicação eficaz sobre fraudes surgem como elementos-chave para aprimorar a usabilidade, proporcionando uma experiência mais informada e protegida aos usuários.

A aplicação da segurança da informação para a experiência e usabilidade dos usuários, oferece contribuições significativas para a evolução contínua da segurança digital no setor financeiro e para o avanço dos sistemas de informação de maneira mais abrangente.

A abordagem proativa na segurança digital é essencial para assegurar confiança e satisfação contínua dos usuários diante das ameaças em constante mutação.

Antecipar necessidades emergentes de usuários não associados é fundamental, exigindo proatividade na identificação e antecipação de demandas Avaliar o impacto de novas tecnologias no mercado, é essencial para compreender e adaptar estratégias de desenvolvimento.

Reconhecer a constante inovação é de grande importância; portanto, novas tecnologias devem ser acompanhadas por contínuas tentativas de inovação para se manterem relevantes.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Incorporar testes práticos e feedback direto dos usuários é vital para garantir a eficácia das soluções propostas, considerando experiências reais de utilização. Desenvolver soluções com flexibilidade e adaptabilidade é crucial diante da rápida evolução do ambiente tecnológico.

Este trabalho deve servir como referência valiosa para pesquisadores que buscam contribuir para a segurança e aprimoramento da usabilidade no contexto tecnológico. Encorajar abordagens alternativas é crucial para enfrentar desafios complexos, integrando segurança, usabilidade e tendências de mercado.

5. Dclaração de direitos

O(s)/A(s) autor(s)/autora(s) declara(m) ser detentores dos direitos autorais da presente obra, que o artigo não foi publicado anteriormente e que não está sendo considerado por outra(o) Revista/Journal. Declara(m) que as imagens e textos publicados são de responsabilidade do(s) autor(s), e não possuem direitos autorais reservados à terceiros. Textos e/ou imagens de terceiros são devidamente citados ou devidamente autorizados com concessão de direitos para publicação quando necessário. Declara(m) respeitar os direitos de terceiros e de Instituições públicas e privadas. Declara(m) não cometer plágio ou auto plágio e não ter considerado/gerado conteúdos falsos e que a obra é original e de responsabilidade dos autores.

6. Referências

1. Associação Brasileira de Normas Técnicas (ABNT). NBR ISO 27002. Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.
2. Bioni, B. R. Proteção de dados pessoais. Rio de Janeiro: Forense Editora, 2019.
3. Braga, R. G. D. Direito bancário em ênfase no sigilo bancário: Responsabilidade pela Segurança Digital nas Instituições Financeiras. Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba. Rubiataba – GO. 2022. 58p.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

4. Branco, D. C. História da segurança virtual: a origem da cibersegurança. 2021. Disponível em: <https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-da-ciberseguranca-200930/>. Acesso em 02 de maio de 2023.
5. BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09 de jul. 2023
6. Bugs, W. Segurança da Informação. Pilares e conceitos de proteção e segurança. SD.
7. Campos, A. L. N. Sistema de segurança da informação: controlando os riscos. Florianópolis: Visual Books, 2007.
8. Cenzi, Nerii Luiz. Cooperativismo: desde as origens ao Projeto de Lei de Reforma do Sistema Cooperativo Brasileiro. Curitiba: Editora Juruá, 2009.
9. Ciso Advisor. Teste revela falhas críticas de segurança em apps de *mobile banking*. 2020. Disponível em: <https://www.cisoadvisor.com.br/teste-revela-falhas-criticas-de-seguranca-em-apps-de-mobile-banking/>. Acesso em: 02 de jul. 2023.
10. Cots, M. Lei Geral de Proteção de Dados Pessoais Comentada. 1ª ed. rev. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. E-book.
11. Daniel, M. A. A evolução e aplicação da segurança da informação por meio da Lei Geral de Proteção de Dados Pessoais (LGPD): Um estudo de caso em uma instituição financeira. Trabalho de Conclusão de Curso de Graduação em Tecnologias da Informação e Comunicação da UFSC. Araranguá – SC. 2022. 63p.
12. Farias, C. M; Gil, M. F. Cooperativismo. Instituto Federal de Educação, Ciência e Tecnologia. Santa Maria. Universidade Federal de Santa Maria. 2013. 92p.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

13. Farias, F. R; Martins, K. M; Costa, L. V; Vilela, N. G. S. Inovações Tecnológicas nas Cooperativas de Crédito: Uma Investigação do Atendimento Mobile em uma Cooperativa de Crédito da Cidade de Guanhães – MG. Revista Eletrônica do Alto Vale do Itajaí – REAVI, v.10, n°16, p. 102-124, ago. 2021.
14. Federação Brasileira de Bancos (FEBRABAN). Pesquisa FEBRABAN de Tecnologia Bancária 2019. Realização Deloitte. 2019.
15. Fontes, E. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2010.
16. GIL, A. C. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.
17. Global Estratégias Financeiras. O que é *mobile banking*? Entenda como funciona. 2022. Disponível em: <https://www.somosglobal.com.br/blog/mobile-banking#closePopup>. Acesso em: 13 de jun. 2023.
18. Guia Rápido da LGPD. Lei Geral de Proteção de Dados. Escola Superior do Ministério Público da União. 2021.
19. Laureano, M. A. P. Segurança da informação. Curitiba: Livro Técnico, 2012.
20. Lycett, A. Breaking Germany's Enigma Code. (Pinching the Codes). 2011. Disponível em: <https://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml>. Acesso em: 02 de maio de 2023.
21. Mascarenhas Neto, P. T; Araújo, W. J. Segurança da Informação: Uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019. 160p.
22. Netto, A. S.; Silveira, M. A. P. G estão da Segurança da Informação: Fatores que influenciam sua adoção em pequenas e médias empresas. In: Revista de Gestão da Tecnologia e Sistemas de Informação, v.4, n.3, 2007, p.375-397.
23. Organizações das Cooperativas Brasileiras (OCB). História do Cooperativismo. 2020. Disponível em: <https://www.ocb.org.br/historia-do-cooperativismo>. Acesso em: 25 de jun. 2023.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

24. OneSpan Blog. Como proteger o *mobile banking* com segurança avançada de aplicativos. 2022. Disponível em: <https://www.onespan.com/pt-br/blog/como-proteger-o-mobile-banking-com-seguranca-avancada-de-aplicativos>. Acesso em: 01 de jun. 2023.
25. Santos, R. L. C. Aspectos da Segurança da Informação: Sua Importância para as Organizações. 2006.
26. Sêmola, M. Gestão da segurança da informação: uma visão executiva. 2. ed. – Rio de Janeiro: Elsevier, 2014.
27. Zapater, M.; Suzuki, R. Segurança da Informação: Um diferencial determinante na competividade das corporações. Rio de Janeiro: Promon Businnes & Tecnology Review, 2005.