Revisando a segurança e a privacidade da plataforma de dados abertos ELLAS via engenharia de requisitos

Luana Bulgarelli Mendes
luana-bm@hotmail.com
Universidade Federal do Mato Grosso (UFMT)
Cuiabá, Brazil

Vinicius Cardoso Faria
vinicarfaria@hotmail.com
Universidade Federal do Mato Grosso (UFMT)
Cuiabá, Brazil

Cristiano Maciel
cristiano.maciel@ufmt.br
Universidade Federal do Mato Grosso (UFMT)
Cuiabá, Brazil

Nelcileno Araújo
nelcileno@ic.ufmt.br
Universidade Federal do Mato Grosso (UFMT)
Cuiabá, Brazil

Constantino Neto
constantino.neto@ifmt.edu.br
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso
Cuiabá, Brazil

Abstract

This article examines the security and privacy requirements of the ELLAS Open Data Platform, which aims to promote gender equality in Science, Technology, Engineering and Mathematics (STEM) in Latin America. Through an overview of the literature on security requirements engineering, we identify gaps in the platform's original requirements. We then propose new functional and non-functional requirements to enhance data security and privacy. The analysis highlights the importance of integrating security requirements into the development of open data platforms, ensuring reliability and secure access to information, especially in projects like ELLAS - Equality in Leadership for Latin American STEM.

CCS Concepts

• **Security and privacy → Software security engineering**; *Web application security*; **Usability in security and privacy**.

Keywords

Segurança, Privacidade, Engenharia de Software, Requisitos, Plataforma de Dados Abertos

ACM Reference Format:
Luana Bulgarelli Mendes, Vinicius Cardoso Faria, Cristiano Maciel, Nelcileno Araújo, and Constantino Neto. 2018. Revisando a segurança e a privacidade da plataforma de dados abertos ELLAS via engenharia de requisitos . In *Proceedings of COMPUTER ON THE BEACH 2026 17a Edição (XVII COTB '26).* ACM, New York, NY, USA, 6 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introdução

A crescente relevância de plataforma de dados abertos para pesquisas e formulação de políticas públicas exige uma análise criteriosa dos requisitos de segurança e privacidade, especialmente em projetos que lidam com grandes quantidades de informação. Com foco no campo de STEM *(Science, Technology, Engineering and Mathematics)*, o projeto ELLAS *(Equality in Leadership for Latin America STEM)* tem como um de seus objetivos a criar uma plataforma de dados abertos [Maciel et al. 2023], [Maciel et al. 2024], enfrentando o desafio de desenvolver uma plataforma que seja segura, confiável e que garanta a privacidade das participantes. A engenharia de requisitos de segurança, crucial para o sucesso de qualquer sistema de informação, dedica atenção especial aos requisitos não funcionais, tais como confiabilidade, segurança e confidencialidade, especialmente em sistemas críticos, onde falhas podem ter consequências significativas [Zareen and Anwar 2024], [Sommerville 2011], torna-se ainda mais crítica em contextos como este, onde a proteção de dados é primordial.

A segurança da informação, componente crucial no desenvolvimento de qualquer sistema, se manifesta por meio de requisitos que visam proteger o sistema e seus usuários e as falhas desses requisitos podem colocar em perigo a vida humana, causar sérios danos à infra estruturas econômicas, colocar em risco a privacidade pessoal, facilitar o crime, entre outros [Anderson 2008]. É fundamental reconhecer que, após o processo de elicitação de requisitos, um sistema pode apresentar uma gama extensa de necessidades de segurança. Na prática, contudo, a garantia de segurança absoluta para todos os requisitos pode ser um desafio complexo, demandando a análise e a priorização dos aspectos mais críticos para o sistema em questão [Sadiq et al. 2021]. Diversos estudos têm se dedicado à análise e aprimoramento de métodos para elicitação e especificação de requisitos de segurança [Laborde et al. 2021], [Zareen et al. 2020], [Ansari et al. 2019] e privacidade [Peixoto et al. 2024], [Canedo et al. 2022a], [Peixoto et al. 2022]. A literatura destaca a importância de considerar aspectos como controle de acesso, criptografia, autenticação e proteção contra ameaças cibernéticas [Zareen and Anwar 2024], [Villamizar et al. 2020], [Fujs and Bernik 2022], [Fenz et al. 2016], além de enfatizar a necessidade de equilibrar segurança e usabilidade [Gutmann and Grigg 2005], [Yee 2004], [Cranor and Garfinkel 2004]. No caso de plataformas de dados abertos, questões como barreiras sociotécnicas relacionadas à publicação e uso de dados abertos [Zuiderwijk and Janssen 2014] também devem ser consideradas.

XVII COTB '26, Florianópolis , SC

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/XXXXXXX.XXXXXXX

Todavia, questiona-se: os requisitos elencados como requisitos no projeto de software da plataforma ELLAS são suficientes para garantir a segurança e privacidade da plataforma? Este artigo propõe analisar os requisitos de segurança e privacidade da Plataforma ELLAS, à luz da literatura atual sobre engenharia de requisitos de segurança, com vista à proposição de novos requisitos.

Sob o ponto de vista metodológico, a análise se dará com base em uma *overview* [Gil 2008] sobre o engenharia de requisitos voltado para a área de segurança de plataformas de dados abertos e o uso de método comparativo [Grant and Booth 2009] para confrontar os requisitos de segurança da plataforma em análise, buscando contribuir para o desenvolvimento de uma plataforma segura, confiável e que promova o acesso aberto à informação de forma responsável e ética.

Neste artigo será introduzido o Projeto ELLAS, utilizado para a análise que se segue. Posteriormente, detalhar-se-á a metodologia empregada, acompanhada da descrição dos conceitos-chave essenciais para a compreensão do estudo. Na seção 5, serão apresentados tanto os requisitos definidos para a plataforma de dados abertos ELLAS quanto às diretrizes preconizadas pela literatura para a eficaz estruturação de tais plataformas. Por fim, nas considerações finais, serão explicitados os resultados da comparação realizada entre os requisitos levantados e as necessidades de complementação identificadas.

2 O Projeto ELLAS

Esta seção apresenta uma análise geral da estrutura e objetivos do projeto. Visa primordialmente trazer uma ideia do que é o projetoELLAS e como a plataforma foi idealizada. O projeto busca suprir a escassez de dados sobre disparidades de gênero em STEM na América Latina [Hildebrand et al. 2024], [Ribeiro et al. 2024], facilitando a produção de dados comparáveis para subsidiar políticas de mitigação e incremento da participação feminina em cargos de liderança [Maciel et al. 2023]. Para isso, mapeia políticas, iniciativas e fatores que influenciam a carreira de mulheres em STEM extraindo insights relevantes com o intuito de gerar dados abertos comparáveis que subsidiem a criação de políticas de redução da disparidade de gênero em STEM. Isso se dará por meio de debates sobre o aumento da representatividade feminina em cargos de liderança e do futuro desenvolvimento de aplicativos com dados abertos para sensibilizar a sociedade [Maciel et al. 2023].

O projeto foi estruturado em três fases distintas, com duração total prevista de três anos [Mendes et al. 2024]. A Fase 1 do projeto, com foco na articulação entre *stakeholders* (formuladores de políticas, instituições acadêmicas e sociedade civil), foi implementada em todos os países participantes. Seminários de conscientização foram realizados para apresentar os objetivos da iniciativa e incentivar a adoção da plataforma de dados, com foco no engajamento de formuladores de políticas e universidades. Ainda, nesta fase, a arquitetura da plataforma foi projetada (arquitetura em camadas), e foi disponibilizada e publicada por Maciel et al. [2024].

A Fase 2 focou na coleta, estruturação, análise e disseminação de dados [Lima et al. 2023], [Berardi et al. 2023], [Berardi et al. 2024], [Hildebrand et al. 2024], [Maciel et al. 2024]. A equipe do projeto tem divulgado os dados e suas interpretações em fóruns acadêmicos e debates públicos sobre STEM, além de organizar *workshops* para capacitar *stakeholders* no uso da plataforma [Maciel et al. 2023] compreendendo as atividades 10 a 16.

Em particular, a atividade 14, intitulada "Design da Plataforma de Dados Abertos: Arquitetura e Governança" [Mendes et al. 2024], [Oliveira et al. 2024], focou no projeto da plataforma como um todo, considerando informações e funcionalidades adicionais a serem incorporadas ao website, tais como seções sobre a equipe, publicações e aplicativos para os dados. Essa atividade foi responsável pelo levantamento e documentação de requisitos funcionais e não funcionais. Durante sua execução, as reuniões presenciais e online serviram como oportunidades para testar os requisitos funcionais previamente licitados, por meio de protótipos, e aprimorá-los antes do desenvolvimento da plataforma. Os requisitos não funcionais estão agora sendo ampliados para testes e mensuração, como os aqui apresentados.

3 Metodologia

A presente pesquisa adotou uma abordagem metodológica qualitativa, combinando elementos de overview [Gil 2008] e método comparativo [Grant and Booth 2009]. Dado o objeto em discussão, são utilizados, além de artigos científicos, referenciais sobre engenharia de requisitos [Sommerville 2011] e sua utilização no projeto de sistemas computacionais.

Buscando um embasamento teórico sólido e atualizado, realizamos uma *overview* da literatura em bases de dados renomadas como Springer e IEEE *(Institute of Electrical and Electronic Engineers)*. A *overview* abrangeu trabalhos publicados nos últimos 10 anos nas áreas de segurança da informação, engenharia de requisitos e segurança de dados em plataformas abertas para análise crítica dos requisitos de segurança da plataforma ELLAS. Artigos seminais relevantes também foram considerados. Cabe ressaltar que, apesar de a revisão dos estudos ter sido conduzida com certo protocolo, ela não se trata de uma revisão sistemática da Literatura, tendo sido utilizados os artigos que cotejavam com o proposto na pesquisa e não um protocolo.

Após a coleta e análise dos dados, empregamos o método comparativo para confrontar os requisitos de segurança não funcionais presentes na documentação da plataforma ELLAS com as melhores práticas e recomendações extraídas da literatura. Esse processo permitiu a identificação de similaridades e diferenças, bem como a avaliação da pertinência e suficiência dos requisitos de segurança da plataforma em questão.

Vale salientar que a escolha metodológica justifica-se pela natureza do objeto de estudo e pela necessidade de aprofundar a análise dos requisitos de segurança e privacidade da plataforma ELLAS, buscando garantir sua robustez e confiabilidade em um cenário tecnológico em constante evolução.

4 Conceitos -chave

Esta seção abordará dados abertos e segurança da informação em plataformas de dados abertos. Serão explorados os princípios de dados abertos (disponibilidade, reutilização e acesso irrestrito) e os princípios de segurança da informação (construção de sistemas resilientes e proteção contra ameaças). A tríade sigilo, confidencialidade e privacidade será analisada, juntamente com conceitos

de incidentes, ameaças, vulnerabilidades e riscos, fornecendo base para a análise da segurança em plataformas de dados abertos.

4.1 Dados Abertos

A OpenDefinition [2019] estabelece princípios que delimitam o conceito de "abertura" no contexto de dados e conteúdo. Essa definição busca precisar o significado de "aberto" nas expressões "dados abertos" e "conteúdo aberto", com o intuito de assegurar a qualidade e promover a compatibilidade entre diferentes conjuntos de materiais abertos. A definição dada pela organização é "Aberto significa que qualquer pessoa pode livremente acessar, usar, modificar e compartilhar para qualquer finalidade, sujeitando-se, no máximo, a requisitos que preservem a proveniência e a abertura. A classificação de um dado como "dado aberto" segundo Isotani and Bittencourt [2015] também está condicionada ao atendimento de três critérios fundamentais, ou seja, o dado precisa ser: disponível (acessível online em formato modificável), reutilizável (com termos que permitam reutilização livre) e de acesso irrestrito (universal e não discriminatório). Dados abertos podem ser disponibilizados como arquivos brutos ou em plataformas estruturadas, como proposto no projeto ELLAS.

4.2 Engenharia da segurança

Segurança da informação é a prática de proteger informações, sistemas, recursos e ativos de desastres, erros (intencionais ou não) e acessos não autorizados com o objetivo de reduzir a probabilidade e o impacto de incidentes de segurança, garantindo a continuidade do negócio, minimizando riscos e maximizando o retorno sobre investimentos e oportunidades [Coelho et al. 2014].

A engenharia de segurança se concentra na construção de sistemas que permaneçam confiáveis diante de ataques maliciosos, erros ou imprevistos, focando nas ferramentas, processos e métodos necessários para projetar, implementar e testar sistemas completos, além de adaptar sistemas existentes à medida que seu ambiente evolui [Anderson 2008]. Isso inclui requisitos de segurança e privacidade e, de acordo com Anderson [2008], não podemos falar de privacidade de dados sem entender a diferença entre três conceitos distintos: sigilo, confidencialidade e privacidade. Sigilo é um termo técnico que se refere aos mecanismos, como criptografia ou controles de acesso, usados para limitar o número de entidades que podem acessar uma informação. Confidencialidade, por outro lado, implica na obrigação de proteger os segredos de outra pessoa ou organização. Já a privacidade é a capacidade e/ou o direito de proteger informações pessoais e evitar invasões do espaço individual, com definições que variam entre países.

Para garantir a segurança de uma plataforma de dados abertos, também é fundamental compreender os conceitos de incidente de segurança, ameaça, vulnerabilidade e risco. Segundo Coelho et al. [2014], no livro "Gestão de Segurança da Informação" que tem como base as normas ABNT NBR ISO/IEC 27001 e 27002, um incidente de segurança é qualquer evento adverso, como ataques de negação de serviço (DoS), roubo de informações, vazamento de dados ou acesso não autorizado. Uma ameaça é qualquer evento que explore vulnerabilidades, representando uma causa potencial de incidente e dano à plataforma. Vulnerabilidade, por sua vez, é uma fraqueza, como configurações incorretas, que pode ser explorada por uma ameaça, comprometendo a segurança da plataforma e seus dados. Por fim, risco é a combinação da probabilidade de uma ameaça se concretizar e das consequências negativas para o projeto.

5 Requisitos de Segurança e Privacidade da Plataforma ELLAS

Esta sessão abordará os requisitos de segurança e privacidade da plataforma ELLAS, essenciais para garantir a confiabilidade e a proteção dos dados, detalhando a elicitação e validação dos requisitos não funcionais e funcionais, além de apresentar uma proposta de estrutura complementar baseada na literatura.

5.1 Requisitos da plataforma

A engenharia de requisitos constitui uma subdisciplina da engenharia de sistemas e software que se dedica à elicitação, análise, validação e documentação de requisitos [Sommerville 2011]. A Engenharia de Requisitos de Segurança expande esse escopo, incorporando conceitos de análise de riscos para garantir a segurança das informações e auxiliando as organizações na identificação e especificação de requisitos de segurança. Essa abordagem permite que os requisitos de segurança sejam considerados de forma integrada ao desenvolvimento do sistema, mitigando riscos e promovendo a confiabilidade da solução final [Laborde et al. 2021]. Como elencado por Sommerville [2011], para alcançarmos a uma aplicação confiável, precisamos de quatro pilares, como mostra a Figura 1.

(1) Interação direta com stakeholders: por meio de reuniões e eventos *online* e presenciais, promovendo a participação ativa dos envolvidos no projeto ELLAS.
(2) Análise do contexto: considerando estudos realizados com as equipes de *stakeholder* em evento presencial no Peru e as atividades de mapeamento de fatores, iniciativas e políticas, buscando a contextualização sociocultural da plataforma.
(3) Levantamento de necessidades: com aplicação de questionários junto à equipe interna, dos três países, abrangendo diferentes perspectivas e realidades.
(4) Aplicação de *framework* especializado: com utilização da técnica de inspeção IHC feminista, com a análise de *"dos"* e *"don'ts"* para garantir a inclusão e a acessibilidade na plataforma [Oliveira et al. 2024].

Na Tabela 1, são transcritos os três requisitos identificados no projeto da plataforma.

Essa abordagem metodológica qualitativa, combinando elementos de *overview* [Gil 2008] e método comparativo [Grant and Booth 2009], buscou assegurar a identificação completa e precisa dos requisitos da plataforma ELLAS, refletindo as necessidades e expectativas dos seus usuários.

5.2 Requisitos de Segurança e Privacidade de acordo com a literatura

Nesta seção, com base nos aportes da literatura, pretende-se explorar outras possibilidades de requisitos de segurança e proteção de dados para o ELLAS.

O processo de descoberta de requisitos, como descrito por Alexander and Beus-Dukic [2009], envolve três etapas cruciais: descoberta, documentação e validação. A validação, por sua vez, busca assegurar a completude e consistência dos requisitos. No entanto, quando

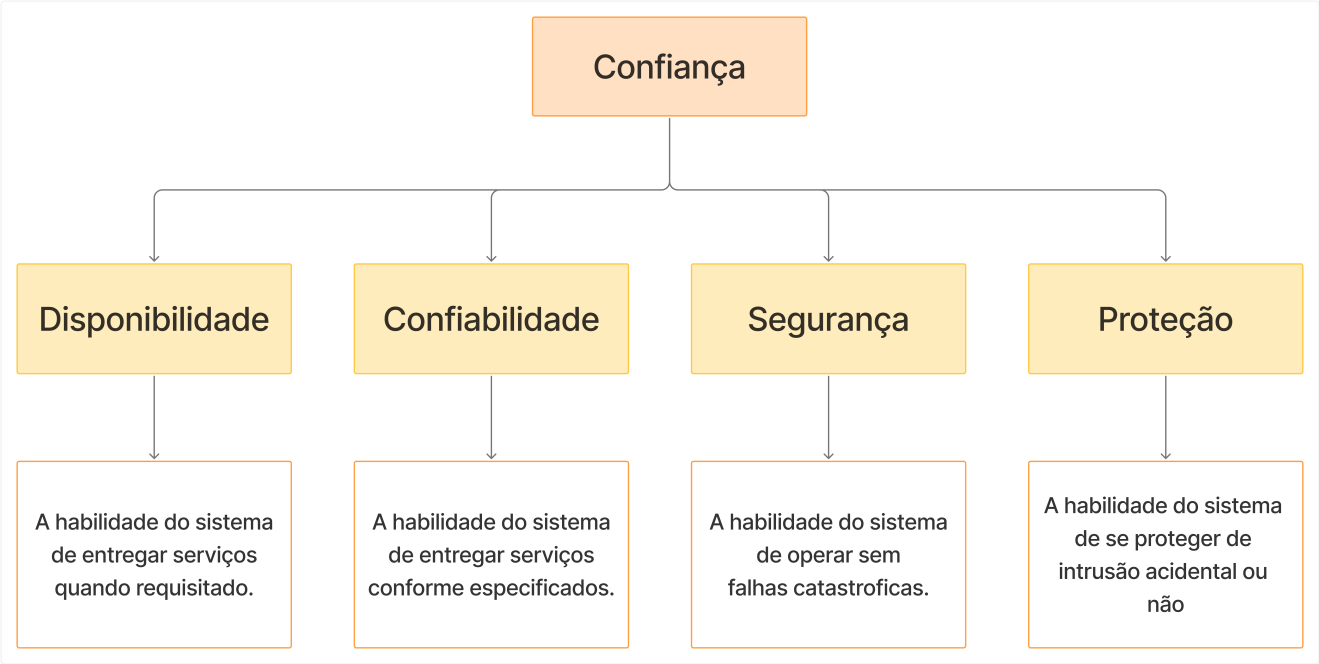

Figure 1: Propriedades da confiança [Sommerville 2011]

Table 1: Requisitos atuais de segurança - Plataforma ELLAS

Categoria	Descrição
Níveis de Segurança	Diferenciar perfis de usuários (Administrativo, Comum e etc)
Segurança	Permitir a atribuição de diferentes níveis de acesso e permissões com base na função do usuário.
Segurança	Implementar medidas de segurança, incluindo criptografia de dados, autenticação em dois fatores e proteção contra ameaças cibernéticas.

se trata de requisitos não funcionais, especialmente os de segurança, a validação se torna um desafio particularmente complexo e como mencionado por Steinmann and Ochoa [2022], engenheiros de requisitos têm baixa conscientização sobre a elicitação de requisitos de segurança. A natureza abstrata e multifacetada dos requisitos de segurança exige métodos de validação específicos e robustos. Técnicas como análise de riscos, simulações, testes de penetração e revisões de código podem ser empregadas para avaliar a efetividade das medidas de segurança implementadas. Além disso, é essencial destacar que a validação dos requisitos de segurança é um processo contínuo e iterativo, que deve acompanhar o ciclo de vida do sistema, adaptando-se às mudanças e aos novos desafios que surgem ao longo do tempo.

No âmbito da segurança da informação, a autenticação desempenha um papel crucial ao verificar a identidade de usuários e entidades [Alexander and Beus-Dukic 2009]. Na plataforma ELLAS, em particular, a autenticação se concentra na figura do "administrador", responsável por gerenciar e garantir a integridade dos dados e, dada a natureza de dados abertos da plataforma, a autenticação robusta dos administradores torna-se ainda mais crítica. Afinal, esses usuários possuem privilégios para adicionar, modificar e remover dados, demandando mecanismos de controle de acesso que previnam alterações indevidas.

Em relação à privacidade, embora a privacidade dos dados tenha se tornado uma preocupação importante no desenvolvimento de software [Canedo et al. 2022b], a plataforma ELLAS se beneficia do fato de os dados coletados por meio de pesquisas serem anonimizados e livres de informações sensíveis. Essa característica minimiza os riscos de privacidade, permitindo que o foco da análise se concentre na segurança da informação e na proteção dos dados contra acessos não autorizados, visto que os requisitos de privacidade são classificados como objetivos de proteção de privacidade ou vulnerabilidades de privacidade [Alkubaisy 2017].

Por outro lado, a elicitação de requisitos de confiabilidade apresenta desafios consideráveis, especialmente pela necessidade de especificações quantitativas precisas. Métricas como POFOD - *Probability of Failure on Demand* (Probabilidade de Falha sob Demanda) e ROCOF - *Rate of Occurrence of Failures* (Taxa de Ocorrência de Falhas) são ferramentas essenciais nesse processo, embora a validação rigorosa possa implicar em custos elevados [Sommerville 2011]. Mesmo diante de tais desafios, a definição de metas de confiabilidade, ao invés de requisitos não funcionais, para a plataforma

demonstra-se crucial para nortear o desenvolvimento e garantir a robustez do sistema. Também deve ser considerada a possibilidade de especificação de requisitos funcionais de confiabilidade, como os elencados por Sommerville [2011] que incluem verificação (impedir processamento de dados inválidos), recuperação (restaurar sistema após falhas) e redundância (garantir continuidade dos serviços apesar de falhas).

Com base na análise da literatura e nas discussões apresentadas neste artigo, propomos uma nova estrutura de requisitos de segurança e privacidade, abrangendo requisitos funcionais e não funcionais para aprimorar a segurança e privacidade de plataformas de dados abertos como a plataforma ELLAS, conforme detalhado na Tabela 2.

É importante levarmos em consideração que, nesta fase inicial de desenvolvimento da Plataforma de Dados Abertos ELLAS, o escopo não prevê a inclusão de um módulo administrativo.

Dessa forma, e por uma questão de priorização de recursos e objetividade no momento, torna-se desnecessária a especificação formal de requisitos relacionados à:

(1) Segurança de senhas;
(2) Mecanismos de autenticação e acesso de usuários;
(3) Segurança e privacidade de sessões.

Tais requisitos deverão ser devidamente elencados e detalhados em fases posteriores, caso o desenvolvimento futuro inclua funcionalidades que demandem acesso restrito.

6 Considerações finais

Este artigo analisou os requisitos de segurança e privacidade da plataforma de dados abertos ELLAS. A partir da *overview* e da comparação com o estado da arte, buscou-se responder se os requisitos inicialmente elicitados para a plataforma eram suficientes para garantir sua segurança e privacidade.

Constatou-se que, apesar dos esforços iniciais da equipe projetista, a plataforma demandava requisitos adicionais para assegurar a proteção dos dados e a privacidade de seus dados. A análise da literatura permitiu identificar lacunas nos requisitos iniciais e propor novos requisitos, com foco em segurança e privacidade, que foram detalhados na Tabela 2.

A implementação completa e a testagem rigorosa de todos os requisitos, em especial os não funcionais, ainda não é possível devido à fase de desenvolvimento em que a plataforma se encontra. A avaliação da eficiência dos requisitos não funcionais, como a imunidade a ameaças e a redundância de servidores, exige a definição de métricas claras e a realização de testes específicos, o que poderá ser explorado em trabalhos futuros.

Acredita-se que as análises e proposições realizadas neste artigo contribuem para o desenvolvimento de uma plataforma de dados abertos mais segura e confiável. Este estudo também reforça a importância da engenharia de requisitos de segurança no desenvolvimento de plataformas de dados abertos. A análise crítica dos requisitos à luz da literatura e a busca por aperfeiçoamento contínuo são essenciais para garantir a segurança e a confiabilidade das plataformas, promovendo o acesso à informação de forma segura e transparente.

Em complemento aos requisitos porpostos aqui para a Fase 1 da plataforma, identificou-se um potencial para a inclusão de requisitos adicionais, tanto funcionais quanto não funcionais, nas etapas subsequentes do projeto.

Essa perspectiva de expansão reforça a importância de estabelecer um processo de revisão e atualização periódica dos requisitos, com atenção às áreas de Segurança da Informação e Privacidade dos Dados, garantindo que estes aspectos sejam regularmente auditados e readequados conforme o projeto evolui, assegurando a integridade e a conformidade da plataforma a longo prazo.

7 Referências Bibliográficas

References

Ian Alexander and L. Beus-Dukic. 2009. *Discovering Requirements.* Wiley, England.

D. Alkubaisy. 2017. A framework managing conflicts between security and privacy requirements. In *2017 11th International Conference on Research Challenges in Information Science (RCIS).*

Ross J. Anderson. 2008. *Security Engineering* (2nd ed.). Wiley Publishing, Inc., Indiana.

T. J. Ansari, D. Pandey, and N. A. Khan. 2019. Comparative Literature Analysis on Security Requirements Engineering. *International Journal of Engineering Sciences & Research Technology* (2019).

R. Berardi, P. Henrique, Cristiano Maciel, G. Davila, I. R. Guzman, and L. Mendes. 2023. ELLAS: Uma plataforma de dados abertos com foco em lideranças femininas em STEM no contexto da América Latina. In *Anais do IX Workshop sobre Aspectos da Interação Humano-Computador para a Web Social.*

R. C. G. Berardi, P. H. S. Auceli, Cristiano Maciel, G. Davila, I. R. Guzman, and L. Mendes. 2024. ELLAS Architecture and Process: Collecting and Curating Data on Women's Presence in STEM. *Journal on Interactive Systems* 15, 1 (2024), 530–540.

E. D. Canedo, I. N. Bandeira, A. T. S. Calazans, P. H. T. Costa, E. C. R. Cançado, and R. Bonifácio. 2022a. Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. *Requirements Engineering* (2022).

E. D. Canedo, A. T. S. Calazans, I. N. Bandeira, P. H. T. Costa, and E. T. S. Masson. 2022b. Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requirements Engineering* (2022).

F. E. S. Coelho, L. G. S. de Araújo, and E. K. Bezerra. 2014. *Gestão da Segurança da Informação.* Escola Superior de Redes, Rio de Janeiro.

Lorrie Faith Cranor and Simson Garfinkel. 2004. Guest Editors' Introduction: Secure or Usable? *IEEE Security & Privacy Magazine* 2, 5 (2004), 16–18.

S. Fenz, S. Plieschnegger, and H. Hobel. 2016. Mapping information security standard ISO 27002 to an ontological structure. *Information and Computer Security* (2016), 452–473.

D. Fujs and I. Bernik. 2022. Characterization of Selected Security-related Standards in the Field of Security Requirements Engineering. *Elektrotehniski Vestnik/Electrotechnical Review* 89, 3 (2022), 73–80.

Antonio Carlos Gil. 2008. *Métodos e técnicas de pesquisa social* (6a ed.). Editora Atlas.

M. J. Grant and A. Booth. 2009. A Typology of reviews: An Analysis of 14 Review Types and Associated Methodologies. *Health Information & Libraries Journal* 26, 2 (2009), 91–108.

P. Gutmann and I. Grigg. 2005. Security Usability. *IEEE Security and Privacy Magazine* 3, 4 (2005), 56–58.

N. D. Hildebrand, B. O. Amador, Cristiano Maciel, and R. C. G. Berardi. 2024. A Escassez de Dados Abertos Estruturados em Países Latino-Americanos com Enfoque de Gênero na Educação Superior. In *Workshop on Women in Information Technology (WIT).*

Seiji Isotani and Ig Ibert Bittencourt. 2015. *Dados abertos conectados: em busca da web do conhecimento.* Novatec Editora.

R. Laborde, S. T. Bulusu, A. S. Wazan, A. Oglaza, and A. Benzekri. 2021. A Methodological Approach to Evaluate Security Requirements Engineering Methodologies: Application to the IREHDO2 Project Context. *Journal of Cybersecurity and Privacy* 1, 3 (2021), 422–452.

S. Lima, L. Cardoso, and S. A. Bim. 2023. The First Step of the Project for the Interaction of an Open Data Platform with an Intersectional Feminist Lens. *Interfaces* (2023).

Cristiano Maciel, I. R. Guzman, R. Berardi, B. Caballero, N. Rodriguez, L. Frigo, P. Tapia, et al. 2023. Open Data Platform to Promote Gender Equality Policies in STEM. In *Proceedings of the Western Decision Sciences Institute.*

Cristiano Maciel, I. R. Guzman, R. C. G. Berardi, N. Rodriguez-Rodriguez, L. Salgado, L. B. Frigo, B. Branisa, and E. Jimenez. 2024. An Open Data Platform to Advance Gender Equality in STEM in Latin America. *Commun. ACM* (2024).

L. Mendes, V. Faria, and Cristiano Maciel. 2024. Project Management in Large-Scale with International Settings: Challenges Faced with Multiculturalism. In *Proceedings of the 26th International Conference on Enterprise Information Systems - Volume 2.*

h

Table 2: Proposta de requisitos complementares de segurança e privacidade

Tipo	Requisito	Descrição
Funcional	Identificação	Identificar usuários que desejam manipular os dados, por meio de login via APIs *(Application Programming Interface)* com chaves de acesso ou outros métodos de identificação.
Funcional	Autorização	Controlar o acesso aos dados com base nas permissões de cada usuário.
Funcional	Detecção de Intrusão	Ser capaz de detectar atividades suspeitas e tentativas de acesso não autorizado. Isso pode incluir monitoramento de tráfego, análise de logs e sistemas de detecção de intrusão.
Funcional	Auditoria de Proteção	Registrar as ações dos usuários e permitir a auditoria do sistema para fins de segurança e conformidade.
Não Funcional	Imunidade	Ser resistente a vírus, worms e outras ameaças à segurança. Isso inclui mecanismos de proteção como firewalls, software antivírus e atualizações regulares de segurança.
Não Funcional	Integridade	Garantir a integridade dos dados, evitando corrupção e perda de informações. Isso pode incluir cópias de segurança (backups) regulares, controle de versões e mecanismos de detecção de erros.
Não Funcional	Privacidade	Proteger a privacidade dos dados, garantindo que informações sensíveis sejam acessíveis apenas a usuários autorizados. Isso pode incluir criptografia, anonimização e políticas de acesso a dados.
Não Funcional	Proteção de Manutenção de Sistema	Garantir que as atualizações e manutenções não comprometam os mecanismos de segurança. Isso pode incluir testes rigorosos, controle de mudanças e backups antes de qualquer alteração.
Não Funcional	Redundância de Servidor	Utilizar redundância de servidores (servidores replicados, *clusters* ou outras soluções) para garantir a alta disponibilidade dos dados, evitando perdas e corrupção em caso de falha de *hardware*.

29–40.

R. Oliveira, L. Salgado, and S. A. Bim. 2024. Desenvolvimento de uma plataforma de dados abertos a partir do design sensível ao gênero. In *Anais do XV Workshop sobre Aspectos da Interação Humano-Computador na Web Social (WAIHCWS)*. Sociedade Brasileira de Computação, Porto Alegre, 29–36.

OpenDefinition. 2019. *Defining Open in Open Data, Open Content and Open Knowledge*. Retrieved Jan, 2025 from https://opendefinition.org/od/2.1/en/

M. Peixoto, T. Gorschek, D. Mendez, D. Fucci, and C. Silva. 2024. A natural language-based method to specify privacy requirements: an evaluation with practitioners. *Requirements Engineering* 29, 3 (2024), 279–301.

M. Peixoto, C. Silva, J. Araújo, T. Gorschek, A. Vasconcelos, and J. Vilela. 2022. Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned. In *2022 IEEE 30th International Requirements Engineering Conference (RE)*.

K. S. F. M. Ribeiro, B. R. Aguiar, and J. M. Gomes. 2024. Openness and Availability of Gender Data on Leadership of Brazilian Women in IT. In *Proceedings of the Americas Conference on Information Systems (AMCIS 2024)*. Salt Lake City, Utah.

M. Sadiq, V. S. Devi, J. Ahmad, and C. W. Mohammad. 2021. Fuzzy logic driven security requirements engineering process. *Journal of Information and Optimization Sciences* 42, 7 (2021), 1685–1707.

Ian Sommerville. 2011. *Engenharia de Software* (9a ed.). Pearson Prentice Hall, São Paulo.

J. Steinmann and O. Ochoa. 2022. Supporting Security Requirements Engineering through the Development of The Secure Development Ontology. In *2022 IEEE 16th International Conference on Semantic Computing (ICSC)*.

H. Villamizar, M. Kalinowski, A. Garcia, and D. Mendez. 2020. An efficient approach for reviewing security-related aspects in agile requirements specifications of web applications. *Requirements Engineering* (2020).

Ka-Ping Yee. 2004. Aligning security and usability. *IEEE Security & Privacy Magazine* 2, 5 (2004), 48–55.

S. Zareen, A. Akram, and S. A. Khan. 2020. Security Requirements Engineering Framework with BPMN 2.0.2 Extension Model for Development of Information Systems. *Applied Sciences* 10, 14 (2020), 4981.

S. Zareen and S. M. Anwar. 2024. BPMN extension evaluation for security requirements engineering framework. *Requirements Engineering* 29, 2 (2024), 261–278.

A. Zuiderwijk and M. Janssen. 2014. Barriers and Development Directions for the Publication and Usage of Open Data: A Socio-Technical View. In *Public Administration and Information Technology*. Springer, 115–135.

8 Agradecimentos

Ao projeto ELLAS, pela oportunidade de utilizar a Plataforma de Dados Abertos Conectados ELLAS como estudo de caso, à CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e ao CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) pelo financiamento parcial desta pesquisa. Gostariamos também de indicar o uso das ferramentas de inteligência artificial ChatGPT e Gemini, empregadas no processo de revisão e melhoria textual. Destacamos o uso da ferramenta NotebookLM, que contribuiu para a organização, análise e estudo dos artigos selecionados para esta revisão.

Received 24 December 2025; revised 10 January 2026; accepted 24 February 2026