Uma Proposta de Plataforma para Avaliação Contínua de Maturidade em Governança de Cibersegurança no Setor Público

João G. I. Braga[1,2], Francisco J. S. Sousa[1,2], Paola S. Pereira[2], Tales P. Nogueira[3,2]
Antonia M. A. da Silva[1,2], Emanuel Bezerra Rodrigues[1,2]
Alexandre S. Cialdini[4], Rossana M. C. Andrade[1,2]

[1]Universidade Federal do Ceará (UFC)

[2]Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat)

[3]Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

[4]Secretaria do Planejamento e Gestão do Ceará (Seplag-CE)

{gustavoirineu,franciscojean,paolapereira,mayaraalmeida}@alu.ufc.br

emanuel@dc.ufc.br, rossana@ufc.br

alexandre.cialdini@seplag.ce.gov.br, tales@unilab.edu.br

Abstract. *This paper proposes a web-based platform to support continuous cybersecurity maturity assessment in the public sector, aligned with the Information Privacy and Security Program (PPSI). Motivated by limitations of unstructured assessment practices, such as spreadsheet-based monitoring, the proposed solution centralizes sensitive information, supports evidence management, and improves traceability through role-based access and audit mechanisms. The platform operationalizes PPSI guidelines through structured forms, data analysis, dashboards, and action plans, enabling organizations to assess maturity levels, identify gaps, prioritize corrective measures, and monitor progress over successive evaluation cycles. By integrating governance, monitoring, and improvement activities, the solution will contribute to greater transparency, accountability, and consistency in cybersecurity management for public entities.*

1. Introdução

A crescente digitalização dos serviços públicos e a expansão dos sistemas eletrônicos utilizados pela administração estatal aumentaram significativamente a superfície de ataque e a exposição a riscos cibernéticos (Hossain *et al.*, 2025). No setor público brasileiro, ataques de ransomware, fraudes digitais e vazamentos de dados têm crescido em volume, sofisticação e impacto. Nesse contexto, a cibersegurança torna-se um pilar estratégico para garantir a continuidade das políticas públicas, proteger dados pessoais e manter a confiança da sociedade no Estado (Hamid; Huda, 2025).

Estudos recentes destacam fraquezas estruturais na governança de segurança da informação do setor público, como o uso limitado de indicadores-chave de desempenho, avaliações de risco insuficientes, modelos inadequados de maturidade em segurança e a ausência de auditorias, que em conjunto minam a eficácia estratégica (Magnusson *et al.*, 2025). No Brasil, o Governo Federal avançou em uma agenda regulatória e institucional

para fortalecer a proteção de dados, a privacidade e a segurança da informação, alinhando-se a frameworks consolidados de cibersegurança (Sousa; Silva; Soares, 2025).

Do ponto de vista operacional, um sistema de informação dedicado é essencial para a avaliação de maturidade em cibersegurança porque centraliza informações sensíveis sobre ativos críticos, vulnerabilidades e efetividade dos controles. Quando as avaliações são conduzidas de forma não estruturada, por exemplo, através de planilhas eletrônicas, os dados tendem a se fragmentar, serem atualizados de forma inconsistente e carecem de controles de acesso adequados e meios de auditoria. Em contraste, um sistema desenvolvido para essa finalidade permite controle de acesso baseado em funções, versionamento, gerenciamento de evidências e registro de logs, reduzindo o risco de divulgação inadvertida ao mesmo tempo em que garante integridade, rastreabilidade e conformidade.

Nesse sentido, este trabalho propõe uma plataforma de avaliação de maturidade em cibersegurança alinhada ao Programa de Privacidade e Segurança da Informação (PPSI) (BRASIL, 2025). O Programa, originalmente concebido pela Secretaria de Governo Digital (SGD), tem como objetivo aumentar a maturidade e a resiliência em privacidade e segurança da informação dos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), sendo estruturado em torno de cinco áreas temáticas: Governança, Maturidade, Metodologia, Pessoas e Tecnologia, estabelecendo uma abordagem integrada para a gestão de riscos, proteção de dados e a adoção sistemática de controles e boas práticas no ambiente digital da Administração Pública Federal.

A plataforma operacionaliza os requisitos de governança por meio de formulários de avaliação estruturados, análise sistemática de dados e visualização baseada em painéis, permitindo que as organizações avaliem níveis de maturidade, identifiquem lacunas e priorizem ações corretivas. A plataforma será implantada e utilizada por entidades públicas (administração direta, autarquias, fundações e empresas públicas) no Estado do Ceará.

2. Trabalhos Relacionados

A literatura recente tem dado grande atenção à governança e à avaliação contínua de segurança da informação. Com o avanço da digitalização, os riscos também aumentaram, o que exige um cuidado constante das organizações. Nesse cenário, Lima *et al.* (2025) enfatizam a necessidade de um monitoramento contínuo da segurança ao analisarem a facilidade de se explorar vulnerabilidades em ambientes com um grande número de sistemas que compartilham os mesmos recursos. Os autores evidenciam que diagnósticos estáticos (i.e., sem que a aplicação esteja em execução) não são suficientes para o cenário atual, sendo essencial a adoção de ferramentas ágeis para o acompanhamento dos riscos.

Observando especificamente os trabalhos no contexto do setor público, diretrizes como o PPSI vêm motivando estudos mais aplicados. Sousa, Silva e Soares (2025) sugerem uma forma de priorizar os controles de segurança do PPSI dentro da realidade brasileira, orientando gestores que lidam com orçamentos e recursos limitados. Spósito, Moreira e Canedo (2025) estruturam uma jornada de capacitação em Cibersegurança para servidores federais, evidenciando que a maturidade institucional exige alinhar ferramentas gerenciais com o treinamento das equipes. Ampliando para conformidade geral, Saraiva, Souza e Soares (2025) apresentam o MMAI-LGPD para adequação de instituições de TI, enquanto Drivas *et al.* (2020) propõem um método de auditoria cíclica baseado na Diretiva NIS para infraestruturas críticas. Diferente dessas abordagens majoritariamente

teóricas, este trabalho apresenta uma experiência real que integra diagnóstico, elaboração de planos de ação e a reavaliação contínua da segurança no contexto do setor público.

3. Framework de Privacidade e Segurança da Informação (PPSI)

O PPSI (BRASIL, 2023), desenvolvido pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), é um guia estruturado voltado principalmente para órgãos e entidades da Administração Pública Federal. Seu objetivo central é auxiliar as instituições a identificar, acompanhar e preencher lacunas em suas práticas de privacidade e segurança da informação, em conformidade com a LGPD e a Política Nacional de Segurança da Informação (PNSI).

A estrutura do framework é fundamentada em referências internacionais reconhecidas, como o CIS Controls v8, o NIST Cybersecurity Framework, o NIST Privacy Framework e as normas ISO/IEC e ABNT NBR. Assim, o framework organiza seus controles em três grandes blocos:

1. **Estruturação Básica (Controle 0):** estabelece os papéis e responsabilidades institucionais necessários para sustentar o programa, como o Gestor de TI, o Encarregado pelo Tratamento de Dados Pessoais (DPO), o Gestor de Segurança da Informação e as equipes de resposta a incidentes (ETIR).
2. **Controles de Cibersegurança (1 a 18):** abrangem desde o inventário de ativos e configurações seguras até a gestão de vulnerabilidades, proteção contra malware, segurança de aplicações e resposta a incidentes, seguindo os CIS Controls 8.0.
3. **Controles de Privacidade (19 a 31):** tratam do mapeamento de dados pessoais, das hipóteses legais de tratamento, da minimização de dados, da gestão de compartilhamento, da transparência com os titulares e da avaliação de impacto à proteção de dados (RIPD).

O processo segue um ciclo contínuo de melhoria, composto por autoavaliação, análise de *gaps*, planejamento e execução de medidas, organizado em Grupos de Implementação graduados conforme a maturidade da instituição. A avaliação de maturidade é expressa por indicadores quantitativos, chamados *iSeg* (Indicador de Segurança) e *iPriv* (Indicador de Privacidade), que permitem acompanhar a evolução da instituição ao longo do tempo.

A versão 2.0 do PPSI amplia o conjunto de referências internacionais adotadas. Enquanto o PPSI 1.0 se baseava principalmente no CIS Controls v8, no NIST Cybersecurity Framework, no NIST Privacy Framework e nas normas ISO/IEC e ABNT NBR, a nova versão incorpora também o Secure Controls Framework (SCF), atualiza suas referências para o CIS Controls v8.1 e o NIST Cybersecurity Framework 2.0, e inclui um guia complementar específico para computação em nuvem.

A maior mudança diz respeito à reorganização dos controles. O PPSI 1.0 organiza seus controles em três blocos (estruturação básica, cibersegurança e privacidade). O PPSI 2.0 mantém a lógica de três segmentos, mas reduz e reorganiza os controles de forma significativa. O segmento base é agora dividido em estruturação básica para governança e instrumentos fundamentais; O segmento de segurança da informação permanece com os Controles 1 a 18, agora baseados no CIS Controls 8.1; O segmento de privacidade sofreu a maior reestruturação: os 13 controles do PPSI 1.0 foram reduzidos a 7 controles, reorganizados segundo as obrigações da LGPD e das resoluções vigentes da ANPD.

4. Sistema Proposto

O sistema proposto utiliza uma metodologia de avaliação criada a partir de conceitos presentes no PPSI 1.0 e 2.0. A primeira versão do framework fundamenta o uso de formulários estruturados para avaliação de impacto, vulnerabilidade, controles de segurança e indicadores de maturidade, além da abordagem ciclíca de avaliação da maturidade. A segunda versão do framework introduz a padronização dos controles de segurança com conceitos teóricos já consolidados, como o CIS Controls, garantindo que as medidas de segurança sejam alinhadas a práticas reconhecidas e eficazes. Dessa forma, é implementado um modelo cíclico de gestão de segurança da informação baseado em três componentes: diagnóstico por meio de formulários, planejamento estruturado e ações orientadas.

A primeira parte do sistema estrutura-se em um conjunto de avaliações que calculam automaticamente a maturidade de segurança da organização. Inicialmente, o órgão realiza avaliações de impacto e vulnerabilidade para cada sistema cadastrado, respondendo a formulários estruturados que contém questões objetivas e campos de justificativa opcionais para cada uma das questões. Estas avaliações alimentam automaticamente o cálculo do índice de criticidade e, conforme a classificação prevista, enquadram o órgão em um dos Grupos de Implementação (G1, G2 ou G3). Essa etapa é fundamental porque define o conjunto de controles que será considerado nas respostas posteriores e, por consequência, na consolidação dos indicadores de maturidade.

Posteriormente, o órgão responde a avaliações de controles de segurança, indicando quais medidas estão implementadas e qual é o nível de capacidade de execução de cada controle em uma escala de zero a cinco. A partir dessas respostas, a plataforma calcula o nível de maturidade como uma consolidação dos dados registrados para os controles cabíveis: cada controle recebe um indicador de maturidade próprio, o *iMC*, obtido a partir das respostas informadas para suas medidas. O sistema agrega, então, esses indicadores para obter o nível de maturidade do órgão pela média aritmética dos *iMCs* dos controles considerados. Esse modelo permite transformar respostas operacionais em um índice único, comparável e rastreável, identificando, para além do nível presente, as lacunas que demandam ações corretivas.

A segunda fase traduz este diagnóstico em planos de ação estruturados em ciclos de implementação. Cada ciclo inicia com a definição de uma meta de maturidade que se deseja alcançar e com a seleção dos controles que serão abordados naquele período. O sistema apresenta, após isso, uma lista de medidas incompletas relacionadas aos controles do ciclo em questão. Essas medidas são identificadas a partir das respostas não satisfatórias aos próprios controles. Para cada medida incompleta, o sistema sugere tarefas pré-definidas que contribuem para sua resolução, permitindo que o gestor selecione as mais apropriadas ou crie, manualmente, tarefas adicionais baseadas em suas prioridades e nas capacidades do órgão. O plano resultante consolida um conjunto coerente de controles, melhorias em medidas e tarefas estruturadas, formando uma base forte para a execução direcionada de melhorias em segurança.

O acompanhamento de planos de ação ocorre em duas dimensões complementares. Durante a realização de um ciclo, na terceira fase, o sistema permite a edição e o rastreamento do progresso das tarefas, registrando avanços e facilitando a comunicação entre responsáveis. Ao fim do ciclo, o plano é consolidado e uma reavaliação dos controles que foram abordados deve ser feita, permitindo que o sistema recalcule seus indicadores de

maturidade a partir das ações executadas. Assim, é possível comparar o estado anterior da organização com o estado posterior, validando empiricamente se as tarefas realizadas produziram os ganhos de segurança esperados.

O modelo proposto caracteriza-se como um processo cíclico em que diagnóstico, planejamento, execução e medição formam um fluxo de avaliação contínuo de maturidade (Figura 1). A maturidade de segurança é a métrica central que unifica todo o sistema: é medida no diagnóstico, usado para priorizar tarefas no plano, alvo das ações de implementação e validada através da reavaliação. Esta estrutura permite que a organização não apenas identifique suas deficiências de segurança, mas as aborde de forma sistemática e controlada, com visibilidade clara do progresso e da aproximação em relação aos objetivos de segurança definidos.

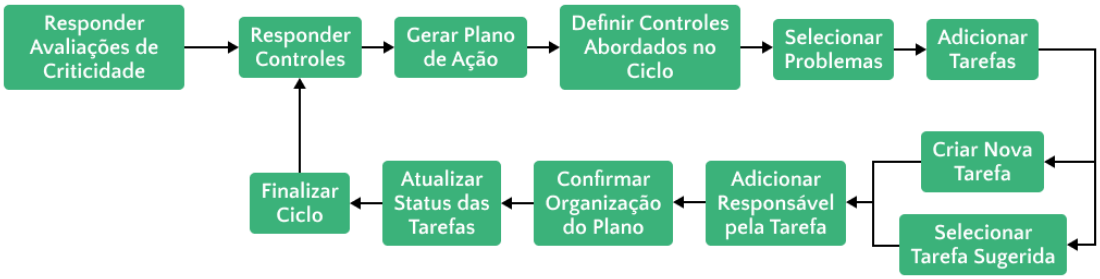

Figura 1. Fluxo de Avaliação Contínua de Maturidade em Cibersegurança

5. Perspectiva Técnica da Plataforma

A arquitetura da plataforma compreende uma aplicação web estruturada em frontend, backend, camada de dados e integrações externas (Figura 2). Ela oferece suporte a dois perfis principais de usuário: o Gestor de Segurança da Informação e o Gestor. A autenticação é centralizada por meio do sistema de autenticação única (Single Sign-On – SSO) do Estado, utilizando OAuth 2.0, com o Nginx atuando como proxy reverso para receber e encaminhar requisições HTTP.

O frontend é implementado em Angular e dá suporte às interfaces dos módulos de formulários, painéis e planos de ação. O backend, desenvolvido em Java com Spring Boot, trata a lógica de negócio central, incluindo o processamento das avaliações, o cálculo dos níveis de maturidade, a gestão dos ciclos e o envio de notificações por e-mail. A camada de dados compreende um banco de dados relacional PostgreSQL para dados estruturados (por exemplo, usuários, respostas, indicadores e planos de ação) e um serviço de armazenamento de objetos NoSQL para evidências e documentos das avaliações, garantindo rastreabilidade, suporte a auditorias e análises históricas de maturidade.

6. Conclusão

Este artigo apresentou a visão de uma plataforma para apoiar a avaliação contínua de maturidade em cibersegurança alinhada ao PPSI no setor público. A proposta consolida a coleta estruturada de dados, painéis baseados em perfis de acesso e gestão de planos de ação para aprimorar a governança, a rastreabilidade e a tomada de decisão, ao mesmo tempo em que protege dados sensíveis das avaliações. Como trabalhos futuros, pretende-se refinar os indicadores de maturidade com especialistas do domínio, realizar pilotos da

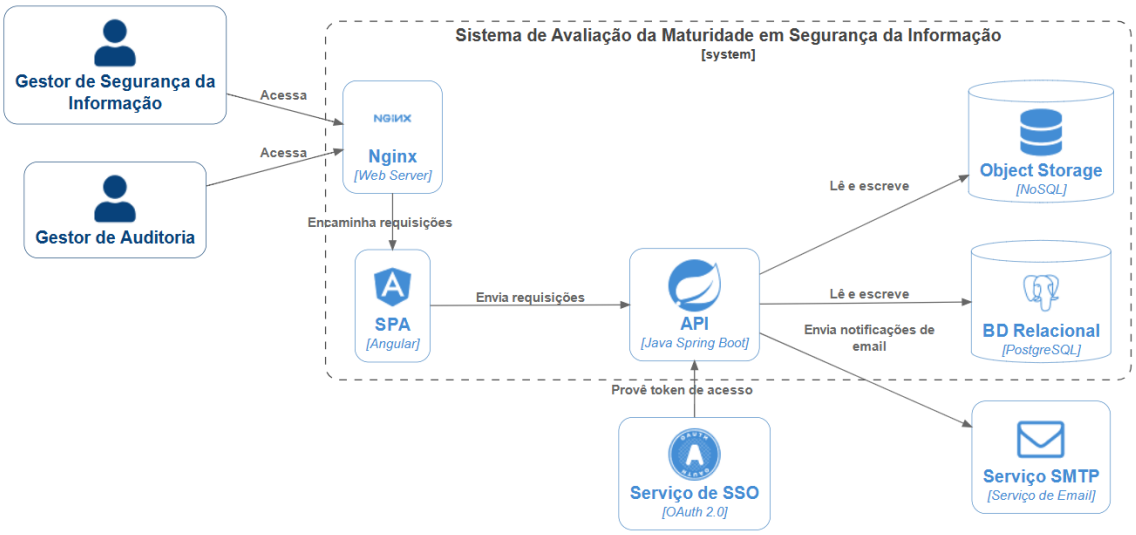

Figura 2. Arquitetura do Sistema

plataforma em entidades públicas selecionadas e avaliar seu impacto na conformidade e na redução de riscos ao longo dos ciclos de avaliação.

Agradecimentos

Ao CNPq pela bolsa de produtividade de R. M. C. Andrade (306362/2021-0) e à Funcap pelo apoio financeiro na execução dos projetos “Governança da Informação na Seplag” e “Testes de Vulnerabilidades e Monitoramento de Segurança Cibernética nos Sistemas Computacionais e Redes de Computadores da Seplag”.

Declaração de Uso de Inteligência Artificial Generativa

Declara-se que a ferramenta OpenAI Prism foi utilizada para redação deste artigo. A ferramenta tem integração com o modelo GPT-5.2, que foi utilizado exclusivamente para a revisão gramatical de trechos do texto. Os autores assumem total responsabilidade pelo conteúdo conceitual e a redação final do texto.

Referências

BRASIL. **PPSI 1.0: Programa de Privacidade e Segurança da Informação**. 2023. Disponível em: `https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca`. Acesso em: 26 maio 2026.

BRASIL. **PPSI 2.0: Programa de Privacidade e Segurança da Informação**. 2025. Disponível em: `https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/`. Acesso em: 26 maio 2026.

DRIVAS, George; CHATZOPOULOU, Argyro; MAGLARAS, Leandros; LAMBRINOUDAKIS, Costas; COOK, Allan; JANICKE, Helge. A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. *In:* 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). [*S. l.*]: IEEE, 2020. p. 1641–1646. DOI: `10.1109/COMPSAC48688.2020.00-20`.

HAMID, Supardi; HUDA, Mohammad Nurul. Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. **Social Sciences & Humanities Open**, Elsevier, v. 11, p. 101234, 2025.

HOSSAIN, Sk Tahsin; YIGITCANLAR, Tan; NGUYEN, Kien; XU, Yue. Cybersecurity in local governments: A systematic review and framework of key challenges. **Urban Governance**, Elsevier, v. 5, n. 1, p. 1–19, 2025.

LIMA, João C. C. *et al.* Análise de Severidade e Explorabilidade de Vulnerabilidades de Segurança no Setor Público. *In:* ANAIS Estendidos do Simpósio Brasileiro de Cibersegurança (SBSeg). [*S. l.*]: SBC, 2025. p. 409–416. DOI: 10.5753/sbseg_estendido.2025.12672.

MAGNUSSON, L.; IQBAL, S.; ELM, P.; DALIPI, F. Information Security Governance in the Public Sector: Investigations, Approaches, Measures, and Trends. **International Journal of Information Security**, Springer, v. 24, n. 4, p. 177, 2025.

SARAIVA, Juliana; SOUZA, Cleidson de; SOARES, Sérgio. MMAI-LGPD: A Maturity Model for Governance and Data Compliance in Information Systems Institutions. *In:* ANAIS do Simpósio Brasileiro de Sistemas de Informação (SBSI). [*S. l.*]: SBC, 2025. p. 788–797. DOI: 10.5753/sbsi.2025.246644.

SOUSA, M.; SILVA, D.; SOARES, H. Prioritization Strategy for Measures in the Brazilian Security Framework. *In:* ANAIS do XIII Latin American Symposium on Digital Government. Maceió/AL: SBC, 2025. p. 261–272. DOI: 10.5753/lasdigov.2025.9349.

SPÓSITO, Stefano Luppi; MOREIRA, Fernando Rocha; CANEDO, Edna Dias. Designing a Training Journey for Privacy and Information Security Practitioners in the Federal Public Administration. *In:* ANAIS do Simpósio Brasileiro de Sistemas de Informação (SBSI). [*S. l.*]: SBC, 2025. p. 95–104. DOI: 10.5753/sbsi.2025.246040.