UNIVERSIDADE
FEDERAL RURAL
DE PERNAMBUCO

Gabriel Ramos de Souza

Análise de um sistema web sob o olhar de segurança da LGPD: Estudo de Caso

Recife

2026

Gabriel Ramos de Souza

Análise de um sistema web sob o olhar de segurança da LGPD: Estudo de Caso

Monografia apresentada ao Curso de Bacharelado em Ciências da Computação da Universidade Federal Rural de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Ciências da Computação.

Universidade Federal Rural de Pernambuco – UFRPE

Departamento de Computação

Curso de Bacharelado em Ciências da Computação

Orientador: Rafael Perazzo Barbosa Mota

Recife

2026

Dados Internacionais de Catalogação na Publicação
Sistema Integrado de Bibliotecas da UFRPE
Bibliotecário(a): Suely Manzi – CRB-4 809

S719a Souza, Gabriel Ramos de.
Análise de um sistema web sob o olhar desegurança da LGPD: estudo de caso / Gabriel Ramos de Souza. – Recife, 2026.
51 f.; il.

Orientador(a): Rafael Perazzo Barbosa Mota.

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal Rural de Pernambuco, Bacharelado em Ciência da Computação, Recife, BR-PE, 2026.

Inclui referências e apêndice(s).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Processamento de listas (Computadores). 3. Auditoria . 4. Proteção de dados 5. Processamento de listas. I. Mota, Rafael Perazzo Barbosa, orient. II. Título

CDD 004

Gabriel Ramos de Souza

Análise de um sistema web sob o olhar de segurança da LGPD: Estudo de Caso

Monografia apresentada ao Curso de Bacharelado em Ciências da Computação da Universidade Federal Rural de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Ciências da Computação.

Trabalho aprovado em 12 de fevereiro de 2026:

Prof. Dr. Rafael Perazzo Barbosa Mota
(Orientador)
Universidade Federal Rural de Pernambuco

Profa. Dra. Maigan Stefanne da Silva Alcantara (Examinadora Interna)
Universidade Federal Rural de Pernambuco

Recife
2026

Resumo

Este trabalho apresenta o desenvolvimento e a aplicação de um instrumento de auditoria técnica voltado à conformidade de sistemas web com a Lei Geral de Proteção de Dados (LGPD). A principal contribuição da pesquisa consiste na criação de um *checklist* replicável, fundamentado no mapeamento sistemático entre os requisitos normativos da LGPD e os controles técnicos do Open Web Application Security Project (OWASP) *Application Security Verification Standard* (ASVS). O instrumento é composto por 40 requisitos distribuídos em 10 categorias temáticas, visando traduzir princípios jurídicos em critérios técnicos verificáveis. Para validar a ferramenta, realizou-se um estudo de caso no sistema de gestão do Programa Institucional de Bolsas de Iniciação Científica (PIBIC)/Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico e Inovação (PIBITI) da Universidade Federal do Cariri (UFCA), empregando análise estática de código-fonte, observação funcional e entrevistas técnicas com o desenvolvedor do sistema. Os resultados revelam que 27,5% dos itens atingiram conformidade total e 12,5% atingiram parcialmente, enquanto 60% foram classificados como não conforme. Observou-se, entretanto, que diversos controles de segurança já se encontram implementados, com destaque para aqueles relacionados à segurança no transporte de dados e à proteção de senhas. Com base na análise realizada, este trabalho apresenta recomendações técnicas e organizacionais voltadas ao fortalecimento da conformidade legal, à melhoria da governança e ao aumento da segurança da informação. Conclui-se que o *checklist* desenvolvido constitui um recurso de verificação em conformidade com as diretrizes da LGPD, fundamentado no padrão OWASP ASVS como suporte técnico, o que fornece um roteiro estruturado para que outras instituições e equipes de desenvolvimento possam avaliar e fortalecer a proteção de dados em seus sistemas de forma sistemática e replicável.

Palavras-chave: LGPD; OWASP ASVS; auditoria de segurança; proteção de dados; checklist de conformidade.

Abstract

This work presents the development and application of a technical auditing instrument aimed at evaluating the compliance of web systems with the Brazilian General Data Protection Law (LGPD). The main contribution of the research is the creation of a replicable checklist, based on a systematic mapping between LGPD regulatory requirements and the technical controls of the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS). The instrument comprises 40 requirements distributed across ten thematic categories, with the purpose of translating legal principles into verifiable technical criteria. To validate the proposed instrument, a case study was conducted on the management system of the Institutional Program for Scientific Initiation Scholarships (PIBIC) and the Institutional Program for Technological Development and Innovation Initiation Scholarships (PIBITI) at the Federal University of Cariri (UFCA). The study employed static source code analysis, functional observation and technical interviews with the system's developer. The results indicate that 27.5% of the evaluated items achieved full compliance and 12.5% showed partial compliance, while 60% were classified as non-compliant. Nevertheless, several security controls were found to be already implemented, particularly those related to transport layer security and password protection. Based on the analysis, this work presents technical and organizational recommendations aimed at strengthening legal compliance, improving governance, and enhancing information security. It is concluded that the proposed checklist constitutes a structured and replicable instrument, grounded in the OWASP ASVS standard, capable of supporting developers and institutions in evaluating and strengthening data protection practices in accordance with LGPD guidelines.

Keywords: Keywords: LGPD; OWASP ASVS; security audit; data protection; compliance checklist.

Sumário

Lista de tabelas

1 INTRODUÇÃO

A crescente digitalização de serviços institucionais tem ampliado de forma significativa o volume de dados pessoais tratados por sistemas de informação, especialmente no âmbito das instituições públicas. Esse cenário impõe desafios relevantes relacionados à segurança da informação e à proteção de dados pessoais, tornando indispensável a adoção de mecanismos técnicos e organizacionais capazes de mitigar riscos associados a acessos não autorizados, vazamentos e uso indevido dessas informações.

Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), instituída pela Lei nº 13.709/2018, estabelece princípios, direitos e obrigações voltados à proteção de dados pessoais, exigindo dos agentes de tratamento a adoção de medidas técnicas e administrativas aptas a garantir a segurança das informações tratadas em sistemas informatizados. A conformidade com a LGPD não se limita à elaboração de documentos normativos, mas demanda a implementação efetiva de controles técnicos que assegurem a proteção dos dados ao longo de todo o seu ciclo de vida.

Entre essas medidas, destacam-se mecanismos como a criptografia, a autenticação forte e o controle de acesso, que visam assegurar a confidencialidade, a integridade e a disponibilidade das informações. Conforme destaca Doneda (2021), tais medidas são fundamentais para a proteção dos direitos dos titulares de dados e para a mitigação de riscos decorrentes de incidentes de segurança, especialmente em ambientes que processam dados pessoais em larga escala.

A LGPD estabelece, entre seus fundamentos, princípios como a segurança, a prevenção e a responsabilização (BRASIL, 2018). O princípio da segurança impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou alteração. Já o princípio da prevenção orienta a adoção de ações proativas para evitar a ocorrência de danos aos titulares, enquanto a responsabilização exige a demonstração da adoção de medidas eficazes para o cumprimento da legislação.

No contexto das instituições públicas, como a Universidade Federal do Cariri (UFCA), a implementação desses princípios apresenta desafios adicionais, em razão da complexidade dos sistemas, da multiplicidade de perfis de acesso e do volume de dados pessoais tratados. Diante desse cenário, torna-se essencial dispor de instrumentos técnicos que auxiliem desenvolvedores e gestores na verificação sistemática da conformidade de sistemas com os requisitos da LGPD.

Assim, este trabalho propõe a análise do sistema de gerenciamento de projetos de pesquisa do Programa Institucional de Bolsas de Iniciação Científica (PIBIC) e do Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico e Inovação (PIBITI), por meio do desenvolvimento e da aplicação de um instrumento de auditoria técnica que integra os requisitos normativos da LGPD aos controles de segurança definidos pelo *Open Worldwide Application Security Project* (OWASP) *Application Security Verification Standard* (ASVS) (OWASP, 2025a). O instrumento proposto consiste em um checklist estruturado, concebido para traduzir princípios jurídicos em critérios técnicos verificáveis, com o objetivo de apoiar a avaliação da conformidade legal e o fortalecimento das práticas de segurança da informação em sistemas web.

1.1 Problema de Pesquisa

Diante das exigências da LGPD quanto à adoção de medidas técnicas de segurança da informação, questiona-se:

"O sistema analisado da UFCA adota práticas que garantem sua conformidade com a LGPD?"

Nesse contexto, entende-se por conformidade a adequação do sistema aos princípios de confidencialidade de informações sensíveis, prevenção e responsabilização previstos na LGPD (BRASIL, 2018), especialmente no que diz respeito à adoção de medidas técnicas, como a criptografia, autenticação, configuração segura e proteção de dados sugeridas pela OWASP (OWASP, 2025a), que possuem relação direta com os requisitos exigidos pela LGPD.

1.2 Justificativa

Este trabalho justifica-se pela importância da proteção de dados pessoais em instituições públicas, como a UFCA, que tratam grandes volumes de informações sensíveis. A LGPD exige a adoção de medidas técnicas, sendo a criptografia uma das ferramentas essenciais para mitigar riscos e garantir a segurança da informação (BRASIL, 2018).

Diversos estudos têm buscado compreender os desafios e caminhos possíveis para a adequação à LGPD em diferentes contextos. Lima (2023), por exemplo, analisou o processo de implementação da LGPD em empresas privadas, utilizando entrevistas com gestores e análise documental para evidenciar lacunas como a ausência de políticas formalizadas, a desarticulação entre os setores e a falta de mecanismos técnicos como a criptografia. Seu trabalho reforça a necessidade de governança e segurança da informação.

No contexto do setor público, Valentin (2023) desenvolveu um estudo voltado à aplicação de técnicas de anonimização em bases de dados de uma empresa pública, mostrando, por meio de uma análise prática, como a anonimização pode contribuir para a proteção de dados pessoais. Seus resultados destacaram que, embora viável, essa abordagem exige forte base técnica e deve ser cuidadosamente contextualizada conforme o tipo de dado tratado.

Arruda (2025) seguiu por outro caminho, propondo um *framework* técnico para aumentar a segurança em ambientes de computação em nuvem, com base nas exigências da LGPD e nas recomendações da OWASP. A partir de uma revisão de ameaças e boas práticas, seu trabalho resultou em uma estrutura metodológica voltada à mitigação de riscos, com recomendações concretas como autenticação multifator, criptografia e monitoramento.

Ainda no setor público, Melo e Ferreira (2022) investigaram a segurança da informação em órgãos municipais, por meio de entrevistas com responsáveis da área de TI. A pesquisa revelou que, apesar de alguma conscientização sobre a LGPD, persistem falhas importantes: inexistência de relatórios de impactos, falta de controle de acessos e ausência de criptografia na maioria dos sistemas.

Complementando esse cenário, Santos (2021) analisou uma empresa de tecnologia por meio de questionários aplicados à equipe de infraestrutura. Os resultados apontaram que, apesar da existência de políticas formais de segurança, incidentes eram frequentes, como o comprometimento de sistemas por vírus e acessos não autorizados. Esse cenário sugere que a aplicação prática das diretrizes ainda era deficiente, principalmente no que tange ao fator humano.

Diferentemente dos trabalhos anteriores, baseados em métodos indiretos como entrevistas e questionários, esta pesquisa se destaca por sua metodologia: a análise técnica direta do código-fonte de um sistema em produção. Essa abordagem permite uma auditoria objetiva para verificar a implementação real de medidas de segurança, como a criptografia, superando a lacuna entre a política documentada e a prática. A principal contribuição é, portanto, o desenvolvimento de um método de verificação de conformidade com a LGPD que é tecnicamente robusto e replicável para outros sistemas.

1.3 Objetivos

1.3.1 Objetivo Geral

Avaliar a conformidade de um sistema web institucional em relação aos requisitos de segurança da informação previstos na LGPD, utilizando como referência os

controles técnicos definidos pelo OWASP ASVS.

1.3.2 Objetivos Específicos

- Identificar os principais requisitos de segurança da informação relacionados à proteção de dados pessoais estabelecidos pela LGPD;
- Correlacionar os requisitos legais da LGPD com os controles técnicos definidos pelo OWASP ASVS;
- Avaliar a adequação das soluções criptográficas e de segurança às exigências legais e técnicas previstas na LGPD;
- Desenvolver uma ferramenta de *checklist* para avaliação dos aspectos de segurança relacionados com a LGPD que possa ser aplicada em outros sistemas semelhantes de outras instituições;
- Aplicar o *checklist* de conformidade ao sistema web institucional analisado;
- Propor recomendações para o aperfeiçoamento da segurança da informação, com foco na aplicação de práticas criptográficas e/ou de autenticação recomendadas pela OWASP, como de conformidade à legislação.

2 METODOLOGIA

2.1 Tipo de Pesquisa

A presente pesquisa caracteriza-se como um estudo de caso, de natureza aplicada, com abordagem qualitativa e caráter exploratório e descritivo. O estudo de caso mostra-se adequado por permitir a análise aprofundada de um sistema específico em seu contexto real de uso, possibilitando a avaliação detalhada de práticas técnicas de segurança da informação à luz da legislação vigente.

A abordagem qualitativa justifica-se pela necessidade de interpretar os mecanismos de segurança implementados no sistema, avaliando sua adequação aos princípios e exigências da LGPD, bem como às boas práticas técnicas definidas pela OWASP, não se limitando à quantificação de dados, mas à análise do conteúdo técnico e funcional do sistema analisado.

2.2 Objeto de Estudo

O objeto deste estudo é um sistema web institucional utilizado pela UFCA para o gerenciamento de projetos vinculados aos PIBIC e PIBITI. O sistema realiza o tratamento de dados pessoais de diferentes perfis de usuários, incluindo discentes, docentes, coordenadores e gestores institucionais, envolvendo informações cadastrais, acadêmicas e administrativas. Em razão do volume e da sensibilidade dos dados tratados, o sistema configura-se como um objeto relevante para análise sob a perspectiva da proteção de dados pessoais e da segurança da informação.

2.3 Abordagem Metodológica

A abordagem adotada fundamenta-se na realização de uma auditoria técnica de conformidade, operacionalizada por meio do mapeamento sistemático entre os requisitos normativos da LGPD e os controles práticos definidos pelo OWASP ASVS.

Essa metodologia permite a tradução de princípios jurídicos em critérios técnicos verificáveis, viabilizando uma análise objetiva dos mecanismos de segurança implementados. Ao correlacionar preceitos legais com padrões globais de segurança de software, a pesquisa supera a subjetividade interpretativa da legislação, permitindo um diagnóstico preciso da proteção aplicada aos dados pessoais no sistema analisado.

2.4 Instrumento de Verificação

O instrumento de coleta de dados consiste em um *checklist* técnico de conformidade, estruturado para consolidar os requisitos normativos da LGPD relacionados à segurança, prevenção e responsabilização requisitos técnicos verificáveis derivados do OWASP ASVS.

Para assegurar o rigor acadêmico e mitigar a subjetividade na fase de diagnóstico, cada requisito do instrumento é classificado conforme uma escala tripartida:

- **Conforme:** quando o controle de segurança está plenamente implementado e atende aos requisitos avaliados;
- **Parcialmente Conforme:** quando o controle existe, mas apresenta limitações técnicas ou implementação incompleta;
- **Não Conforme:** quando o controle está ausente ou é inadequado frente às exigências legais e técnicas.

A estrutura lógica deste instrumento, contendo o mapeamento completo entre os requisitos legais e as referências técnicas, constitui o modelo de auditoria apresentado no Apêndice A.

2.5 Procedimentos de Aplicação

A aplicação do instrumento de auditoria ocorre por meio de um diagnóstico técnico no sistema PIBIC/PIBITI da UFCA. Esta fase de verificação fundamenta-se em três pilares: a análise estática do código-fonte e da arquitetura da base de dados; a observação funcional em ambiente de testes; e a realização de entrevistas técnicas com o programador responsável pelo sistema.

O procedimento de verificação cobre domínios críticos como autenticação, controle de acesso, criptografia, gerenciamento de sessões e geração de logs. A execução desta etapa permite confrontar as práticas reais do sistema com os requisitos estabelecidos, gerando o diagnóstico detalhado e as evidências técnicas que estão consolidados no Apêndice B.

O procedimento seguiu um fluxo estruturado em três fases:

1. Mapeamento de Fluxos: foram identificados os processos de coleta, armazenamento e compartilhamento de dados pessoais, correlacionando-os aos perfis de usuários.

2. Avaliação de Controles: os mecanismos de segurança foram testados individualmente frente aos critérios do *checklist*, com foco especial nos domínios de autenticação (ASVS V2), controle de acesso (ASVS V4), criptografia (ASVS V6) e registro de eventos (ASVS V7) (BRASIL, 2018; OWASP, 2025a).

3. Registro e Diagnóstico: as evidências técnicas encontradas no código foram confrontadas com os requisitos da LGPD, resultando na classificação do grau de conformidade de cada item conforme a escala definida nesta metodologia.

Os resultados detalhados desta aplicação, incluindo as evidências técnicas e as recomendações de melhoria, estão consolidados no Apêndice B.

2.6 Organização dos Apêndices

Para assegurar a transparência metodológica e facilitar a replicabilidade deste estudo, os instrumentos e resultados foram organizados em seções complementares ao final deste trabalho:

- Apêndice A: apresenta o modelo do *checklist* de conformidade LGPD–OWASP em sua forma original, servindo como o instrumento metodológico padronizado para auditorias de sistemas similares.
- Apêndice B: contém o *checklist* preenchido com o diagnóstico real do sistema analisado, detalhando as conformidades, lacunas técnicas e as respectivas sugestões de mitigação de riscos baseadas nas boas práticas da OWASP.

3 RESULTADO E DISCUSSÃO

Neste capítulo, são apresentados e discutidos os dados obtidos através da auditoria técnica realizada no sistema de gestão de projetos PIBIC/PIBITI da UFCA. A análise quantifica o grau de conformidade e detalha as vulnerabilidades encontradas durante a inspeção do código-fonte e da base de dados.

3.1 Visão Geral da Conformidade

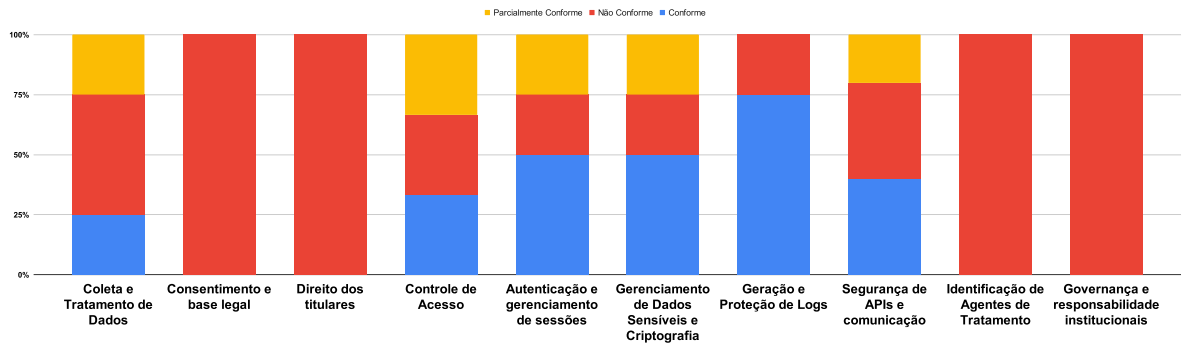
A auditoria contemplou 40 requisitos técnicos, permitindo um diagnóstico sobre o estágio atual de proteção de dados no sistema. Os resultados indicam que 27,5% dos itens avaliados apresentam conformidade total, evidenciando oportunidades para o fortalecimento dos mecanismos de segurança existentes. A Tabela 1 sintetiza o desempenho identificado em cada domínio avaliado.

Tabela 1 – Resumo de conformidade por categoria técnica

Categoria Técnica	**Total**	**Conforme**	**Parcial**	**Não Conforme**
Coleta e Tratamento de Dados	4	1	1	2
Consentimento e Base Legal	2	0	0	2
Direito dos Titulares	4	0	0	4
Controle de Acesso	3	1	1	1
Autenticação e Gerenciamento de Sessões	4	2	1	1
Gerenciamento de Dados Sensíveis e Criptografia	4	2	1	1
Geração e Proteção de Logs	4	3	0	1
Segurança de APIs e Comunicação Segura	5	2	1	2
Identificação de Agentes de Tratamento	4	0	0	4
Governança e Recomendações Gerais	6	0	0	6
Total Geral	**40**	**11**	**5**	**24**

Fonte: Elaborado pelo autor (2025).

Figura 1 – Distribuição geral de conformidade do sistema avaliado



Fonte: Elaborado pelo autor (2025).

A visualização apresentada na Figura 1 complementa a leitura tabular ao oferecer uma síntese do panorama geral de proteção de dados do sistema avaliado. Observa-se que uma parcela significativa dos requisitos encontra-se atendida ou parcialmente atendida, especialmente aqueles relacionados às camadas técnicas básicas de segurança, como proteção no transporte, autenticação e geração de logs. Esse resultado indica que o sistema apresenta um nível consistente de adoção de práticas padrão de segurança da informação, alinhadas a requisitos operacionais amplamente consolidados na engenharia de software. Por outro lado, a distribuição dos resultados também evidencia oportunidades de aprimoramento em dimensões associadas à governança, à transparência e à gestão do tratamento de dados pessoais, aspectos centrais para a plena conformidade com a LGPD. Nesse sentido, o instrumento de auditoria proposto mostrou-se adequado não para a crítica isolada do sistema, mas para evidenciar de forma objetiva em quais eixos estratégicos a solução já se encontra madura e em quais pontos pode evoluir para atender integralmente às exigências legais.

3.2 Análise das Vulnerabilidades

A análise qualitativa realizada a partir do checklist preenchido no Apêndice B permitiu identificar vulnerabilidades relevantes que impactam diretamente os princípios da segurança, da prevenção, da minimização e da responsabilização previstos na LGPD (BRASIL, 2018). As constatações apresentadas nesta seção fundamentam-se em evidências técnicas documentadas nas tabelas do Apêndice B, obtidas por meio da análise estática do código-fonte, da observação do comportamento do sistema e de entrevistas técnicas com o desenvolvedor responsável.

3.2.1 Minimização e Coleta Excessiva

No que se refere ao princípio da necessidade, verificou-se que a função `efetivarIndicacao` realiza a coleta de dados pessoais sensíveis, como sexo e estado civil, além de informações financeiras, inclusive em situações nas quais tais dados não se mostram estritamente necessários para a finalidade do tratamento. Essa constatação está documentada na Tabela 12 do Apêndice B, na qual o requisito 1.1 foi classificado como não conforme.

Essa prática contraria o disposto no Art. 6º, inciso III, da LGPD, que determina que o tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades (BRASIL, 2018). Além disso, observa-se a ausência de aderência ao princípio de *privacy by default*, o qual estabelece que a proteção da privacidade deve ser a configuração padrão de qualquer sistema, garantindo que o tratamento de dados seja automaticamente limitado ao estritamente necessário, sem exigir ações proativas do titular para garantir seus direitos. Tal conceito reforça a aplicação prática do princípio da necessidade previsto no Art. 6º, inciso III, da LGPD (BRASIL, 2018), ao exigir que as aplicações sejam projetadas para restringir a coleta e o processamento de dados ao que é indispensável para a finalidade declarada, mitigando riscos de exposição excessiva do titular desde a fase de concepção do software (CAVOUKIAN et al., 2009).

3.2.2 Armazenamento de Dados Sensíveis

A análise do armazenamento de dados sensíveis evidenciou fragilidades que impactam a confidencialidade das informações em longo prazo. Conforme registrado na Tabela 17 do Apêndice B, o requisito 6.1 foi classificado como não conforme, uma vez que campos críticos como CPF, endereços e informações bancárias permanecem armazenados em texto plano nas tabelas da base de dados. É importante notar que, embora a infraestrutura possa apresentar mecanismos de criptografia em repouso ao nível de disco ou sistema de arquivos, tal medida protege o dado apenas contra o acesso físico indevido ao suporte de armazenamento.

Sob a ótica da LGPD e do OWASP ASVS V6, a proteção deve ser aplicada de forma granular (BRASIL, 2018; Joint Task Force, 2020). Essa abordagem consiste na implementação de controles de segurança direcionados especificamente a campos ou registros individuais, em vez de proteger apenas o volume de dados de forma genérica. Na prática, a aplicação de criptografia em nível de coluna ou de aplicação garante que informações sensíveis sejam cifradas antes mesmo de serem enviadas ao banco de dados. Isso cria uma camada de proteção onde o dado permanece ilegível para o próprio Sistema de Gerenciamento de Banco de Dados (SGBD), que passa a atuar apenas como um repositório de informações cifradas.

Dessa forma, mitiga-se o risco de exposição caso o banco de dados seja acessado por usuários com altos privilégios administrativos ou em situações de vazamento de credenciais de serviço, uma vez que a chave de decodificação permanece isolada na camada lógica do sistema. Essa abordagem evidencia a falta de uma estratégia de *defense in depth*, que propõe a estruturação da segurança em múltiplas camadas redundantes e independentes.

Segundo a Joint Task Force (2020), essa abordagem garante que, caso um mecanismo de proteção seja comprometido, como a criptografia de disco ou o controle de acesso perimetral, outras camadas defensivas permaneçam ativas para impedir o acesso direto à informação. Segundo o Art. 46 da LGPD (BRASIL, 2018), as medidas de segurança devem ser eficazes para proteger os dados de acessos não autorizados, o que exige que informações sensíveis sejam ilegíveis para quem não possui a necessidade estrita de conhecê-las, inclusive dentro do ambiente de administração do sistema.

3.2.3 Quebra de Controle de Acesso

No domínio de controle de acesso, foram identificadas fragilidades que podem permitir a ampliação indevida de privilégios por usuários não autorizados. Conforme evidenciado na Tabela 15 do Apêndice B, apesar da existência de mecanismos básicos de segregação de perfis, não há processos sistemáticos de revisão periódica de acessos, o que resultou na classificação de não conformidade para o requisito 4.2.

Adicionalmente, conforme documentado na Tabela 19 do Apêndice B, rotas que disponibilizam recursos sensíveis não possuem mecanismos adequados de autenticação e autorização, permitindo o acesso mediante a manipulação direta de URLs. Esse cenário caracteriza uma vulnerabilidade de *Broken Access Control*, que ocupa a primeira posição no *ranking* global de riscos de segurança da informação (OWASP, 2025b).

De acordo com a OWASP, esta categoria possui a maior incidência nos dados coletados, sendo que 100% das aplicações testadas apresentaram alguma forma de falha nesta área, envolvendo fraquezas críticas como a exposição de informações sensíveis (OWASP, 2025b).

Tal fragilidade viola diretamente o princípio do menor privilégio. Este princípio fundamental da segurança estabelece que todo usuário, programa ou processo deve ter acesso apenas ao conjunto mínimo de privilégios necessários para realizar suas funções legítimas, de modo a limitar os danos decorrentes de falhas ou comprometimentos (SALTZER; SCHROEDER, 1975).

A inobservância deste preceito compromete diretamente os deveres de segu-

rança e prevenção estabelecidos no Art. 46 e no Art. 6º, inciso VII, da LGPD (BRASIL, 2018). A ausência de verificações rigorosas no *backend* amplia a superfície de ataque do sistema e impossibilita a demonstração de medidas eficazes de controle e eficácia, exigida pelo princípio da responsabilização previsto no Art. 6º, inciso X, da referida lei (BRASIL, 2018).

3.2.4 Validação de Entrada e Possibilidade de Injeção

A análise dos mecanismos de validação de entrada, conforme registrado na Tabela 19 do Apêndice B, identificou pontos no código nos quais dados fornecidos pelo usuário eram utilizados diretamente na construção de consultas SQL e na composição de URLs externas. Tal prática caracteriza a possibilidade de exploração de vulnerabilidades como *SQL Injection*.

Conforme documentado pela *OWASP Foundation*, a falha ocorre quando dados não confiáveis são inseridos em uma consulta de forma que o interpretador os processe como parte da lógica de execução, permitindo que o atacante manipule a instrução original (OWASP, 2025b). Atualmente, a categoria *Injection* ocupa a quinta posição no *ranking* do OWASP Top 10 de 2025, sendo uma das áreas mais exaustivamente testadas, com presença em 100% das aplicações avaliadas. No contexto desta categoria, o *SQL Injection* destaca-se pelo seu altíssimo impacto, dada a capacidade de comprometer a integridade e a confidencialidade de toda a base de dados institucional (OWASP, 2025b).

A existência dessa vulnerabilidade compromete diretamente o princípio da segurança e o princípio da integridade dos dados, previstos no Art. 6º, inciso VII, da LGPD (BRASIL, 2018), pois permite que um atacante realize acessos não autorizados, modifique registros ou até mesmo exclua toda a base de dados institucional (BRASIL, 2018). No entanto, conforme informado pelo desenvolvedor durante as entrevistas técnicas, essa fragilidade específica foi corrigida antes da conclusão deste estudo por meio da adoção de consultas parametrizadas, técnica que assegura a separação entre os dados e o código de execução. A manutenção desta constatação no registro de auditoria reforça o papel do instrumento desenvolvido como apoio à identificação precoce de falhas e à garantia do dever de segurança estabelecido pelo Art. 46 da LGPD (BRASIL, 2018).

3.3 Propostas de Aperfeiçoamento

Com base nas vulnerabilidades identificadas, propõe-se um conjunto de ações estruturadas em múltiplas frentes complementares, visando a conformidade técnica e jurídica do sistema.

- **Criptografia e Gestão de Segredos**: Além da adoção do AES-256 para dados em repouso e Argon2 para senhas, é imperativo implementar um sistema de gerenciamento de chaves *Key Management System* (KMS) isolado do servidor de banco de dados. Isso garante que, mesmo em um cenário de comprometimento do SGBD, os dados permaneçam inacessíveis, pois as chaves de decodificação não residem no mesmo ambiente que os dados cifrados.

- **Segurança no Ciclo de Vida do Desenvolvimento**: Recomenda-se a integração de ferramentas de análise estática de segurança no fluxo de desenvolvimento para identificar precocemente falhas como *SQL Injection* e *Broken Access Control*. Complementarmente, deve-se adotar a parametrização de consultas como padrão arquitetural e a sanitização rigorosa de entradas em todas as camadas da aplicação.

- **Operacionalização da Minimização e Privacidade**: Propõe-se a revisão dos formulários de coleta, como o `efetivarIndicacao`, para aplicar o *Privacy by Default*. Isso inclui a remoção de campos de dados sensíveis e financeiros desnecessários para voluntários, garantindo que o sistema trate apenas o volume mínimo de dados para cada finalidade específica, conforme o Art. 6º, III da LGPD(BRASIL, 2018).

- **Resiliência e Governança Organizacional**: Além do Relatório de Impacto (RIPD), sugere-se a criação de um Plano de Resposta a Incidentes de Segurança. Este documento deve definir fluxos de notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares em caso de vazamentos, atendendo ao princípio da responsabilização e reduzindo riscos jurídicos e reputacionais para a UFCA.

4 CONSIDERAÇÕES FINAIS

O presente trabalho atingiu seu objetivo principal ao propor e validar um instrumento de auditoria técnica para a proteção de dados de acordo com a LGPD em sistemas web, utilizando como referência os controles do *OWASP Application Security Verification Standard* (ASVS). A pesquisa demonstrou que a segurança de aplicações modernas exige uma integração profunda entre requisitos regulatórios e práticas de engenharia de *software*, onde a conformidade deve ser tratada como um requisito funcional crítico.

O estudo de caso realizado no sistema institucional permitiu constatar que, embora existam implementações robustas de segurança no transporte de dados, persistem lacunas técnicas significativas, como a ausência de criptografia granular em repouso e falhas lógicas de controle de acesso. Tais constatações reforçam que a proteção de dados de acordo com a LGPD em sistemas web não é um estado estático, mas um processo contínuo que demanda ferramentas de verificação objetivas e fundamentadas em padrões internacionais.

4.1 Contribuições do Trabalho

A principal contribuição deste estudo reside no desenvolvimento do *checklist* apresentado no Apêndice A. Ao traduzir princípios jurídicos em controles técnicos verificáveis, o instrumento oferece um roteiro prático para que desenvolvedores e arquitetos de sistemas web possam avaliar a segurança de suas aplicações de forma sistemática. A ferramenta reduz a ambiguidade na interpretação da lei, fornecendo critérios claros para a implementação de controles de segurança alinhados às exigências de proteção de dados de acordo com a LGPD.

A versatilidade do instrumento permite que sua estrutura seja replicada em diferentes arquiteturas de sistemas web, independentemente das tecnologias ou linguagens utilizadas na implementação. Assim, o trabalho entrega um guia técnico que facilita a integração de controles de proteção de dados no ciclo de vida e na evolução de sistemas web, promovendo a conformidade tanto em novos projetos quanto em aplicações já consolidadas.

4.2 Limitações e Trabalhos Futuros

Como limitação, destaca-se que o instrumento foi construído sob a ótica exclusiva do ordenamento jurídico brasileiro (LGPD). Além disso, a validação concentrou-se na análise de um único sistema institucional, o que sugere a necessidade de novas aplicações para consolidar a abrangência do *checklist* em diferentes arquiteturas, como microsserviços ou aplicações *single-page*.

Como trabalhos futuros, recomenda-se a expansão do instrumento para abordar especificidades de sistemas web legados, cujas restrições técnicas podem exigir controles compensatórios distintos. Sugere-se também o desenvolvimento de um guia de padrões de projeto (*design patterns*) focado na remediação técnica das falhas identificadas pelo *checklist*. Por fim, propõe-se a aplicação da ferramenta em sistemas web de diferentes setores, como *e-commerce* ou plataformas de saúde, visando avaliar a sensibilidade do instrumento em cenários com fluxos de dados mais complexos.

Referências

ARRUDA, O. do A. *Melhorando a segurança na nuvem: Um framework para mitigar ameaças e se enquadrar nas regras da LGPD*. 2025. Citado na página 11.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm>. Citado 8 vezes nas páginas 9, 10, 15, 17, 18, 19, 20 e 21.

CAVOUKIAN, A. et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, v. 5, n. 2009, p. 12, 2009. Citado na página 18.

DONEDA, D. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2021. Citado na página 9.

Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD, 2020. NIST Special Publication 800-53, Revision 5. Citado 2 vezes nas páginas 18 e 19.

LIMA, V. H. P. *LGPD: Análise dos impactos da implementação em ambientes corporativos: estudo de caso*. 2023. Citado na página 10.

MELO, V. S.; FERREIRA, M. L. *Aplicação da LGPD em uma empresa da região de Criciúma: Estudo de caso em banco de dados*. 2022. Citado na página 11.

OWASP. *The OWASP Foundation*. 2025. Disponível em: <https://owasp.org/>. Citado 2 vezes nas páginas 10 e 15.

OWASP. *OWASP Top 10:2025*. 2025. Disponível em: <https://owasp.org/Top10/2025/>. Citado 2 vezes nas páginas 19 e 20.

SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. *Proceedings of the IEEE*, IEEE, v. 63, n. 9, p. 1278–1308, 1975. Citado na página 19.

SANTOS, J. P. A. dos. *Estudo de caso em uma empresa de tecnologia voltado para segurança da informação e LGPD*. 2021. Citado na página 11.

VALENTIN, S. L. *Estudo de caso: exemplo de aplicação da anonimização em uma empresa pública baseado na LGPD*. 2023. Citado na página 11.

APÊNDICES

APÊNDICE A – INSTRUMENTO DE AUDITORIA DE SEGURANÇA E PROTEÇÃO DE DADOS

Este apêndice apresenta o modelo do instrumento de auditoria estruturado em 10 categorias temáticas. O instrumento foi desenhado para correlacionar requisitos normativos e técnicos, permitindo o registro de evidências e recomendações.

Tabela 2 – Coleta e Tratamento de Dados (Categoria 1)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
1.1	LGPD: Art. 6º, III - Necessidade/minimização, Controle ASVS: V8.1 – *Data Protection*	Minimização de dados: Verificar se o sistema coleta apenas os dados pessoais estritamente necessários para a finalidade declarada, quais são esses dados e os motivos por trás da sua coleta.		
1.2	LGPD: Art. 6º, I - Finalidade, Adequação ASVS: V8.1 – *Data Protection*	Finalidade e adequação: Verificar se existe documentação clara das finalidades do tratamento e se os dados são usados somente para essas finalidades informadas.		
1.3	LGPD: Art. 15º - Responsabilização/prevenção, Eliminação de dados ASVS: V12.4; V14.4 – Configuração, HTTP *Headers*	Retenção e descarte de dados: Verificar políticas de retenção que garantam a eliminação de dados pessoais após o término do tratamento, salvo exceções legais.		

Continua na próxima página...

Continuação da tabela 2 — Categoria 1

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
1.4	LGPD: Art. 6º, VII - Segurança e confidencialidade ASVS: V6.1 – Classificação de Dados	Classificação e tratamento de dados sensíveis: Verificar se dados pessoais sensíveis são identificados e tratados com cuidado adicional.		

Fonte: Elaborado pelo autor (2025).

Tabela 3 – Consentimento e Base Legal (Categoria 2)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
2.1	LGPD: Art. 8º - Consentimento ASVS: V14.5 - *Headers*	Coleta de consentimento explícito: Verificar se o sistema exige manifestação livre e informada.		
2.2	LGPD: Art. 7º - Responsabilização ASVS: V8.1 - *Data Protection*	Base legal alternativa: Verificar se há outra base jurídica adequada.		

Fonte: Elaborado pelo autor (2025).

Tabela 4 – Direito dos titulares (Categoria 3)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
3.1	LGPD: Art. 18 – Direitos do titular ASVS: V7.1 – Conteúdo de *log*	Canal de atendimento ao titular: Verificar a existência de mecanismos que permitam ao titular exercer seus direitos.		

Continua na próxima página...

Continuação da tabela 4 — Categoria 3

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
3.2	LGPD: Art. 18 II e III ASVS: V6.1; V8.1.3	Direito de acesso e correção: Verificar se titulares podem consultar e corrigir seus dados armazenados.		
3.3	LGPD: Art. 18 - IV e VI ASVS: V6.1; V8.1.3	Anonimização e eliminação por solicitação: Verificar se o sistema permite bloquear, anonimizar ou excluir dados desnecessários, excessivos ou com consentimento revogado.		
3.4	LGPD: Art. 18 - VII e VIII	Informação sobre compartilhamento: Verificar se há transparência sobre com quem os dados são compartilhados.		

Fonte: Elaborado pelo autor (2025).

Tabela 5 – Consentimento e Base Legal (Categoria 4)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
4.1	LGPD: Art. 6º, VII - Segurança ASVS: V4.1.1 *Server-side Enforcement*	Segregação de funções e privilégios mínimos: Verificar se o sistema aplica controle de acesso baseado em funções, garantindo que cada usuário tenha apenas as permissões estritamente necessárias.		

Continua na próxima página...

Continuação da tabela 5 — Categoria 4

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
4.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V4.3.2 - *Insecure Direct Object Reference* (IDOR)/*Broken Object Level Authorization* (BOLA)	Revisão periódica de acessos: Verificar se existe processo de auditoria de contas e privilégios.		
4.3	LGPD: Art. 46 - Medidas de Segurança ASVS: V4.1.5 - *Admin Functions*	Proteção de credenciais: Verificar armazenamento seguro de credenciais e uso de autenticação forte para administradores.		

Fonte: Elaborado pelo autor (2025).

Tabela 6 – Autenticação e gerenciamento de sessões(Categoria 5)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
5.1	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V2.4.1 – Controle para armazenamento de *hashes*; V2.9 – Criptografia de senha; V2.7 – *CAPTCHA/Throttling*	Política de senhas e autenticação: Verificar requisitos de senha e proteção contra ataques automáticos.		
5.2	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V2.8.1 – MFA	Multi-fator para acessos críticos: Verificar uso de autenticação multifator para acessos administrativos ou de alto privilégio.		

Continua na próxima página...

Continuação da tabela 6 — Categoria 5				
ID	**Requisitos**	**Verificação**	**Resultado**	**Observação e Recomendação**
5.3	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V3.2.1 e V3.3.1	Gerenciamento de sessão: Verificar se as sessões expiram após período ocioso e se há logout seguro.		
5.4	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V3.4.1 e V3.4.3	Cookies seguros e tokens: Verificar as flags de segurança em cookies e o uso adequado de tokens de sessão.		

Fonte: Elaborado pelo autor (2025).

Tabela 7 – Gerenciamento de Dados Sensíveis e Criptografia(Categoria 6)

ID	**Requisitos**	**Verificação**	**Resultado**	**Observação e Recomendação**
6.1	LGPD: Art. 6º, VII; Art. 46 - Medidas de Segurança; Art. 5º, II - Dados sensíveis ASVS: V6.1.2; V6.1.3 - *Criptographic Storage*	Criptografia em repouso: Verificar se dados pessoais e especialmente sensíveis são criptografados no armazenamento.		
6.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V9.1.1 – *Transport Layer Security* (TLS)	Criptografia em trânsito: Verificar se todos os dados trafegam sobre canais criptografados.		
6.3	LGPD: Art. 46 - Medidas de Segurança ASVS: V6.4.1 – Gerenciamento de Segredos	Gerenciamento de chaves: Verificar armazenamento e rotação de chaves criptográficas usadas pelo sistema.		
6.4	LGPD: Art. 6º, VII e Art. 46 - Medidas de Segurança ASVS: V2.4.2	Hashing de senhas: Verificar uso de algoritmos de hash adequados para senhas.		

Fonte: Elaborado pelo autor (2025).

Tabela 8 – Geração e Proteção de Logs (Categoria 7)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
7.1	LGPD: Art. 6º, X - Responsabilização e prestação de contas; Art. 6º, VIII - Prevenção ASVS: V7.1 – Conteúdo de Log	Conteúdo dos logs: Verificar se logs de segurança registram eventos críticos.		
7.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V7.3 – Proteção de Log	Proteção de logs: Verificar se os arquivos de log são protegidos contra acesso não autorizado e alterações indevidas.		
7.3	LGPD: Art. 6º, III - Necessidade; Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V7.1.2 – Conteúdo de Log	Não registrar dados sensíveis: Verificar que informações pessoais sensíveis não sejam logadas em texto claro.		
7.4	LGPD: Art. 6º, X - Responsabilização e prestação de contas; Art. 6º, III - Necessidade; Art. 46 - Medidas de Segurança ASVS: V7.2 – Processamento de Log	Retenção de logs: Verificar política de retenção de logs compatível com necessidades de segurança e regulamentos.		

Fonte: Elaborado pelo autor (2025).

Tabela 9 – Segurança de APIs e comunicação (Categoria 8)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
8.1	LGPD: Art. 6º, VII - Segurança; Art. 6º, VIII - Prevenção; Art. 46 - Medidas de Segurança ASVS: V9.1 – Segurança em Comunicação	Uso de HTTPS/TLS: Verificar se todas as APIs e interfaces web usam TLS forte.		
8.2	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V13.1; V13.2 – Segurança em *Web Services* Representational State Transfer (REST)	Autenticação e autorização de APIs: Verificar se APIs expõem controles seguros de acesso.		
8.3	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V5.1 – Validação de Entrada	Validação de entrada: Verificar proteção contra injeções e validação de parâmetros.		
8.4	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V14.4 – Cabeçalhos HTTP	Cabeçalhos de segurança HTTP: Verificar configurações de cabeçalhos para mitigar ataques em navegação.		
8.5	LGPD: Art. 6º, VII - Segurança; Art. 6º, VIII - Prevenção; Art. 46 - Medidas de Segurança ASVS: V7.4 - *Rate Limiting*	Proteção contra ataques DDoS e abuso: Verificar mecanismos de limitação de taxa e proteção contra bots.		

Fonte: Elaborado pelo autor (2025).

Tabela 10 – Identificação de Agentes de Tratamento (Categoria 9)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
9.1	LGPD: Art. 5º, VI – Controlador	Definição do Controlador: Confirmar que está identificado o controlador do sistema, quem decide finalidades.		
9.2	LGPD: Art.5 VII; Art. 6º, X – Responsabilização e prestação de contas	Definição do Operador: Confirmar quem são os operadores, quem processa dados em nome do controlador.		
9.3	LGPD: Art. 41 – Encarregado pelo tratamento de dados pessoais; Art. 6º, X – Responsabilização e prestação de contas	Papel do Encarregado: Verificar se há um encarregado indicado e seus contatos públicos.		
9.4	LGPD: Art. 39 – Operador deve realizar o tratamento conforme instruções do controlador; Art. 6º, X – Responsabilização e prestação de contas	Conformidade contratual: Verificar que contratos de TI definem as obrigações de controlador e operador.		

Fonte: Elaborado pelo autor (2025).

Tabela 11 – Governança e responsabilidade institucionais (Categoria 10)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
10.1	LGPD: Art. 46 - Medidas de Segurança; Art. 6º, X – Responsabilização e prestação de contas ASVS: V1.1.2 - *Governance*	Política de Segurança da Informação: Verificar existência e aplicação de uma política formal de segurança da informação.		

Continua na próxima página...

Continuação da tabela 11 — Categoria 10

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
10.2	LGPD: Art. 50 - Boas Práticas; Art. 6º, X – Responsabilização ASVS: V1.1.3 – *Security Awareness and Training*	Treinamento e conscientização: Verificar programas de capacitação sobre LGPD e segurança para funcionários.		
10.3	LGPD: Art. 38 – Relatório de Impacto à Proteção de Dados Pessoais ASVS: V1.1.4 – *Documentation of Security Requirements*	Registro de operações: Verificar manutenção de registro de todas as operações de tratamento de dados pessoais.		
10.4	LGPD: Art. 48 - Incidentes ASVS: V1.12.3 – *Incident Response*	Avaliação de impacto: Verificar se já foi realizado Relatório de Impacto de Proteção de Dados, especialmente em tratamentos de alto risco.		
10.5	LGPD: Art. 6, VII - Segurança e Art. 46 - Medidas de Segurança ASVS: V14.2.1 – *Dependency Management*; V1.2.6 – *Patch Management*	Monitoramento de incidentes: Verificar existência de plano de resposta a incidentes de segurança e obrigatoriedade de notificação.		
10.6	LGPD: Art. 6, VIII - Prevenção e Art. 46 - Medidas de Segurança ASVS: V14.2.3 - *Scanning*	Atualização e manutenção: Verificar controles de atualização de sistemas e dependências. .		

Fonte: Elaborado pelo autor (2025).

APÊNDICE B – RELATÓRIO DE DIAGNÓSTICO E AUDITORIA DE SEGURANÇA: ESTUDO DE CASO UFCA

Este apêndice apresenta o modelo do instrumento de auditoria estruturado em 10 categorias temáticas. O instrumento foi desenhado para correlacionar requisitos normativos e técnicos, permitindo o registro de evidências e recomendações.

Tabela 12 – Coleta e Tratamento de Dados (Categoria 1)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
1.1	LGPD: Art. 6º, III - Necessidade/minimização, Controle ASVS: V8.1 – *Data Protection*	Minimização de dados: Verificar se o sistema coleta apenas os dados pessoais estritamente necessários para a finalidade declarada, quais são esses dados e os motivos por trás da sua coleta.	Não conforme	A função `efetivarIndicacao` coleta dados de alto risco que parecem desnecessários para a finalidade, como `estado_civil`, `sexo` e dados financeiros mesmo para voluntários. Revisar o formulário `efetivarIndicacao` para condicionar a coleta de dados bancários à vaga. Reavaliar a real necessidade da coleta dos dados sensíveis `sexo` e `estado_civil`.
1.2	LGPD: Art. 6º, I - Finalidade, Adequação ASVS: V1.4.2 – *Data Protection*	Finalidade e adequação: Verificar se existe documentação clara das finalidades do tratamento e se os dados são usados somente para essas finalidades informadas.	Parcialmente conforme	A documentação da finalidade é um item de Governança. No entanto, a adequação é conforme: o código utiliza os dados para os fins de gerenciamento do edital. A Política de Privacidade e o Relatório de Impacto (RIPD) do sistema devem documentar formalmente a finalidade de cada tratamento de dados.

Continua na próxima página...

Continuação da tabela 12 — Categoria 1

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
1.3	LGPD: Art. 15º - Responsabilização/prevenção, Eliminação de dados ASVS: V12.4; V14.4 – Configuração, HTTP *Headers*	Retenção e descarte de dados: Verificar políticas de retenção que garantam a eliminação de dados pessoais após o término do tratamento, salvo exceções legais.	Conforme	O código utiliza os dados coletados de forma consistente com a finalidade de gerenciamento de bolsas e projetos.
1.4	LGPD: Art. 6º, III – Necessidade; Art. 15 – Término do tratamento ASVS: V6.1 – Classificação de Dados	Classificação e tratamento de dados sensíveis: Verificar se dados pessoais sensíveis são identificados e tratados com cuidado adicional.	Não conforme	Não foi identificado nenhum mecanismo no `pesquisa.py` para anonimização ou exclusão automática de dados de editais antigos, de modo que os dados parecem ser mantidos indefinidamente, sendo necessária a implementação de uma tarefa agendada para anonimizar ou excluir dados pessoais de editais encerrados após o período de retenção legal/necessário.

Fonte: Elaborado pelo autor (2025).

Tabela 13 – Consentimento e Base Legal (Categoria 2)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
2.1	LGPD: Art. 8º - Consentimento ASVS: V1.4.2 – *Privacy Requirements*	Coleta de consentimento explícito: Verificar se o sistema exige manifestação livre e informada.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi confirmado que o aluno não acessa a plataforma e que o *upload* do `arquivo_termo` é realizado pelo orientador, porém sem validação sistêmica de que este documento contém as cláusulas de privacidade e consentimento exigidas pela LGPD, o que requer a atualização do modelo oficial do ”Termo de Compromisso”para inclusão de cláusula destacada de ciência para tratamento de dados e a configuração do *upload* do `arquivo_termo` como tecnicamente obrigatório e auditável.

Continua na próxima página...

Continuação da tabela 13 — Categoria 2

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
2.2	LGPD: Art. 6º - Responsabilização; Art. 7º - Base legal ASVS: V8.1 - *Data Protection*	Base legal alternativa: Verificar se há outra base jurídica adequada.	Não conforme	Em conversa com o programador responsável, notou-se que o sistema trata o *upload* do termo como um arquivo genérico, sem distinguir no código se o tratamento se baseia no Consentimento ou na Execução de Políticas Públicas, sendo necessário definir formalmente tal fundamentação jurídica e garantir que, caso se trate de consentimento, o arquivo não seja substituído ou excluído sem rastro de auditoria, preservando a integridade da prova legal da autorização do aluno.

Fonte: Elaborado pelo autor (2025).

Tabela 14 – Direito dos titulares (Categoria 3)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
3.1	LGPD: Art. 18 – Direitos do titular ASVS: V7.1 – Conteúdo de *log*	Canal de atendimento ao titular: Verificar a existência de mecanismos que permitam ao titular exercer seus direitos.	Não conforme	O `pesquisa.py` não implementa nenhuma rota ou função específica destinada a receber e processar solicitações dos titulares de dados para exercer seus direitos, o que demanda a criação de um canal de atendimento dedicado ou um e a divulgação desse canal publicamente para que os titulares possam fazer suas solicitações.

Continua na próxima página...

Continuação da tabela 14 — Categoria 3

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
3.2	LGPD: Art. 18 II e III ASVS: V6.1; V8.1.3	Direito de acesso e correção: Verificar se titulares podem consultar e corrigir seus dados armazenados.	Não conforme	O titular não tem acesso e o `pesquisa.py` também não possui rotas administrativas que permitam a um operador do sistema buscar e editar os dados de um aluno para atender a uma solicitação externa, o que torna necessária a criação de rotas administrativas que permitam a um operador buscar, visualizar e editar os dados de uma `indicacao` para atender a uma solicitação de correção vinda do titular.
3.3	LGPD: Art. 18 - IV e VI ASVS: V6.1; V8.1.3	Anonimização e eliminação por solicitação: Verificar se o sistema permite bloquear, anonimizar ou excluir dados desnecessários, excessivos ou com consentimento revogado.	Não conforme	Não foi identificada nenhuma rota ou função no `pesquisa.py` que execute a anonimização ou exclusão de dados pessoais mediante solicitação, sendo observado que a função `desligarIndicacao` apenas altera o *status* do registro sem remover as informações, o que torna necessária a criação de funções de *backend*, restritas ao `role='admin'`, para anonimizar ou excluir dados de um titular específico quando solicitado e garantir o cumprimento do direito de eliminação.

Continua na próxima página...

Continuação da tabela 14 — Categoria 3

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
3.4	LGPD: Art. 18 - VII e VIII	Informação sobre compartilhamento: Verificar se há transparência sobre com quem os dados são compartilhados.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi confirmado que o sistema não possui uma Política de Privacidade ou qualquer aviso na interface que informe aos usuários com quais entidades terceiras os dados são compartilhados, o que torna necessário elaborar e publicar a Política de Privacidade no sistema, detalhando explicitamente todas as entidades com as quais os dados são compartilhados e a finalidade desse compartilhamento.

Fonte: Elaborado pelo autor (2025).

Tabela 15 – Consentimento e Base Legal(Categoria 4)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
4.1	LGPD: Art. 6º, VII - Segurança ASVS: V4.1.1 *Server-side Enforcement*	Segregação de funções e privilégios mínimos: Verificar se o sistema aplica controle de acesso baseado em funções, garantindo que cada usuário tenha apenas as permissões estritamente necessárias.	Conforme	O `pesquisa.py` implementa um decorador `@login_required (role='...')` que é aplicado consistentemente nas rotas para diferenciar `role='admin'` de `role='user'`.

Continua na próxima página...

Continuação da tabela 15 — Categoria 4

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
4.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V7.1/V7.2 - Logging & Monitoring *Broken Object Level Authorization* (BOLA)	Revisão periódica de acessos: Verificar se existe processo de auditoria de contas e privilégios.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi confirmado que não há processo definido para revisão de contas e que o código não possui funcionalidades que suportem essa auditoria, o que torna necessário estabelecer um processo formal e periódico para revisar as contas de usuários e seus níveis de permissão, além de implementar um relatório no sistema que liste todos os usuários e seus acessos para facilitar essa auditoria.

Continua na próxima página...

Continuação da tabela 15 — Categoria 4

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
4.3	LGPD: Art. 46 - Medidas de Segurança ASVS: V4.1.5 - *Admin Functions*	Proteção de credenciais: Verificar armazenamento seguro de credenciais e uso de autenticação forte para administradores.	Parcialmente conforme	O sistema armazena senhas de forma segura por meio da utilização de algoritmo de *hash* forte com *salt*, atendendo aos requisitos do OWASP ASVS V2.4. Entretanto, não foram identificadas evidências da implementação de Autenticação de Múltiplos Fatores (MFA) para contas administrativas, conforme recomendado pelo ASVS V2.8.1. Dessa forma, embora o uso do algoritmo `Argon2id` esteja adequado, observa-se a necessidade de adoção de mecanismos adicionais de autenticação para usuários com `role='admin'`, a fim de mitigar riscos associados a comprometimento de credenciais.

Fonte: Elaborado pelo autor (2025).

Tabela 16 – Autenticação e gerenciamento de sessões (Categoria 5)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
5.1	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V2.4.1 – Controle para armazenamento de *hashes*; V2.9 – Criptografia de senha; V2.7 – *CAPTCHA/Throttling*	Política de senhas e autenticação: Verificar requisitos de senha e proteção contra ataques automáticos.	Parcialmente conforme	O sistema implementa corretamente a proteção contra ataques automáticos na rota `/login` usando `flask-limiter`, no entanto, não há evidência de uma política de complexidade de senha sendo aplicada quando o usuário define uma senha, sendo necessária a manutenção da proteção de *rate limit* e a implementação de uma política de complexidade de senhas a ser aplicada em todas as rotas onde o usuário define ou altera sua senha.
5.2	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V2.8.1 – MFA	Multi-fator para acessos críticos: Verificar uso de autenticação multifator para acessos administrativos ou de alto privilégio.	Não conforme	O `pesquisa.py` implementa apenas a autenticação de fator único para todos os níveis de acesso, incluindo `role='admin'`, não havendo implementação de Autenticação de Múltiplos Fatores, o que torna necessária a implementação obrigatória de MFA para todas as contas com privilégios administrativos, conforme exigido pelo ASVS V2.8 para proteger dados sensíveis.
5.3	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V3.2.1 e V3.3.1	Gerenciamento de sessão: Verificar se as sessões expiram após período ocioso e se há logout seguro.	Conforme	O sistema está configurado com um tempo de vida de sessão e possui uma função de logout segura que limpa a sessão.

Continua na próxima página...

Continuação da tabela 16 — Categoria 5

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
5.4	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V3.4.1 e V3.4.3	Cookies seguros e tokens: Verificar as flags de segurança em cookies e o uso adequado de tokens de sessão.	Conforme	O uso de flask-session e Talisman em modo de produção aplica as flags Secure, HttpOnly e SameSite aos cookies de sessão. Além disso, a biblioteca CSRFProtect é usada para gerar tokens anti-CSRF.

Fonte: Elaborado pelo autor (2025).

Tabela 17 – Gerenciamento de Dados Sensíveis e Criptografia (Categoria 6)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
6.1	LGPD: Art. 6º, VII – Segurança; Art. 46 – Medidas de Segurança ASVS: V6.1.2; V6.1.3 – *Cryptographic Storage*	Criptografia em repouso: Verificar se dados pessoais e dados pessoais sensíveis são criptografados no armazenamento.	Não conforme	A função `efetivarIndicacao` aplica criptografia a apenas cinco campos, mantendo dados pessoais, incluindo dados sensíveis, como `nome`, `cpf`, `email`, `sexo`, `estado_civil` e informações bancárias, armazenados em texto plano. Tal prática não atende aos requisitos do OWASP ASVS para armazenamento criptográfico, indicando a necessidade de ampliar a proteção criptográfica para todos os campos classificados como dados pessoais e sensíveis no banco de dados.

Continua na próxima página...

Continuação da tabela 17 — Categoria 6

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
6.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V9.1.1 – *Transport Layer Security* (TLS)	Criptografia em trânsito: Verificar se todos os dados trafegam sobre canais criptografados.	Conforme	O código utiliza flask-talisman e está configurado para forçar HTTPS em produção.
6.3	LGPD: Art. 46 - Medidas de Segurança ASVS: V6.4.1 – Gerenciamento de Segredos	Gerenciamento de chaves: Verificar armazenamento e rotação de chaves criptográficas usadas pelo sistema.	Parcialmente conforme	As chaves `AES_KEY` e `GPG_KEY` são carregadas de variáveis de ambiente, o que evita o *hardcoding*, porém a `AES_KEY` é utilizada diretamente sem evidência de um sistema de gerenciamento ou rotação, o que exige a implementação de um sistema de gerenciamento de segredos para armazenar e rotacionar as chaves de criptografia, garantindo, no mínimo, a rotação periódica da `AES_KEY`o que pode comprometer a confidencialidade dos dados em caso de vazamento prolongado da chave.
6.4	LGPD: Art. 6º, VII; Art. 46 - Medidas de Segurança ASVS: V2.4.2	Hashing de senhas: Verificar uso de algoritmos de hash adequados para senhas.	Conforme	O sistema utiliza `cripto.hash_argon2id` e `cripto.hash_argon2id_verify`. Argon2id é um algoritmo de hash moderno, com uso de salt e resistência a ataques de força bruta, atendendo plenamente à recomendação.

Fonte: Elaborado pelo autor (2025).

Tabela 18 – Geração e Proteção de Logs (Categoria 7)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
7.1	LGPD: Art. 6º, X - Responsabilização e prestação de contas; Art. 6º, VIII - Prevenção ASVS: V7.1 – Conteúdo de Log	Conteúdo dos logs: Verificar se logs de segurança registram eventos críticos.	Conforme	O código implementa o registro de eventos críticos: o decorador `@log_required` registra os acessos a rotas; a função `verify_password` registra falhas de autenticação; e blocos `try...except` registram erros. Manter a estratégia de logs centralizados via *Logtail*.
7.2	LGPD: Art. 46 - Medidas de Segurança ASVS: V7.3 – Proteção de Log	Proteção de logs: Verificar se os arquivos de log são protegidos contra acesso não autorizado e alterações indevidas.	Conforme	O sistema utiliza *LogtailHandler* para externalizar os *logs* em produção, além de rotação e compressão no arquivo local `app.json`, garantindo a integridade dos registros.
7.3	LGPD: Art. 6º, III - Necessidade; Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V7.1.2 – Conteúdo de Log	Não registrar dados sensíveis: Verificar que informações pessoais sensíveis não sejam logadas em texto claro.	Não conforme	O decorador `@log_required`, aplicado a quase todas as rotas, registra dados pessoais em texto claro para cada acesso, violando o Princípio da Minimização, o que exige a modificação do referido decorador para anonimizar ou remover dados pessoais dos *logs* de acesso geral, por exemplo, registrando um *hash* do `username` ou apenas registrando o identificador em eventos de falha de segurança, e não em cada acesso bem-sucedido.

Continua na próxima página...

Continuação da tabela 18 — Categoria 7

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
7.4	LGPD: Art. 6º, X - Responsabilização e prestação de contas; Art. 6º, III - Necessidade; Art. 46 - Medidas de Segurança ASVS: V7.2 – Processamento de Log	Retenção de logs: Verificar política de retenção de logs compatível com necessidades de segurança e regulamentos.	Conforme	O pesquisa.py implementa uma política de retenção de logs. A configuração do loguru define explicitamente um período de retenção de 30 dias para os arquivos de log.

Fonte: Elaborado pelo autor (2025).

Tabela 19 – Segurança de APIs e comunicação (Categoria 8)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
8.1	LGPD: Art. 6º, VII - Segurança; Art. 6º, VIII - Prevenção; Art. 46 - Medidas de Segurança ASVS: V9.1 – Segurança em Comunicação	Uso de HTTPS/TLS: Verificar se todas as APIs e interfaces web usam TLS forte.	Conforme	O código utiliza flask-talisman e está configurado para forçar HTTPS em produção.
8.2	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V13.1; V13.2 – Segurança em *Web Services* Representational State Transfer (REST)	Autenticação e autorização de APIs: Verificar se APIs expõem controles seguros de acesso.	Não conforme	Embora rotas de *admin* estejam protegidas, rotas que funcionam como API de arquivos não possuem nenhuma autenticação, permitindo que dados sensíveis sejam acessados por qualquer um com o link, o que exige a aplicação dos decoradores `@login_required` ou `@auth.login_required` a todas as rotas que servem dados sensíveis, incluindo `/verArquivosProjeto`.

Continua na próxima página...

Continuação da tabela 19 — Categoria 8

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
8.3	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V5.1 – Validação de Entrada	Validação de entrada: Verificar proteção contra injeções e validação de parâmetros.	Não conforme	O código falha em validar e sanitizar entradas em pontos críticos, sendo observado que funções como `obterColunaUnica_str` e `processarPontuacaoLattes` usam dados de entrada diretamente na concatenação de strings para SQL e URLs, levando a vulnerabilidades de Injeção de SQL e SSRF, o que exige a implementação da validação de entrada em todas as rotas, o uso exclusivo de *queries* parametrizadas para SQL e a validação do *input* contra uma *allow-list* de domínios para SSRF.
8.4	LGPD: Art. 6º, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V14.4 – Cabeçalhos HTTP	Cabeçalhos de segurança HTTP: Verificar configurações de cabeçalhos para mitigar ataques em navegação.	Parcialmente conforme	O `flask-talisman` está implementado, contudo a Política de Segurança de Conteúdo (CSP), um dos cabeçalhos de segurança mais importantes, encontra-se explicitamente desabilitada na configuração, o que torna necessária a definição de uma política restritiva e sua configuração correta no `Talisman` para mitigar ataques de *Cross-Site Scripting* (XSS).
8.5	LGPD: Art. 6º, VII - Segurança; Art. 6º, VIII - Prevenção; Art. 46 - Medidas de Segurança ASVS: V7.4 - *Rate Limiting*	Proteção contra ataques DDoS e abuso: Verificar mecanismos de limitação de taxa e proteção contra bots.	Conforme	O sistema utiliza flask-limiter de forma robusta, aplicando limites de taxa globais e limites mais estritos em rotas sensíveis como /login e /enviarMinhaSenha.

Fonte: Elaborado pelo autor (2025).

Tabela 20 – Identificação de Agentes de Tratamento (Categoria 9)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
9.1	LGPD: Art. 5º, VI – Controlador	Definição do Controlador: Confirmar que está identificado o controlador do sistema, quem decide finalidades.	Não conforme	Em conversa com o programador responsável pela criação do sistema, constatou-se a ausência de documentos, termos de uso ou avisos no sistema que identifiquem formalmente a instituição como a Controladora dos dados perante os usuários, o que torna necessária a elaboração e publicação dos Termos de Uso e da Política de Privacidade no sistema, identificando explicitamente a instituição como a Controladora dos dados pessoais tratados.
9.2	LGPD: Art.5 VII; Art. 6º, X – Responsabilização e prestação de contas	Definição do Operador: Confirmar quem são os operadores, quem processa dados em nome do controlador.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi confirmado o uso de serviços terceiros, mas não há documentação que os classifique formalmente como Operadores, o que torna necessário mapear e listar na documentação interna e externa todos os fornecedores de TI que atuam como Operadores, definindo o escopo de atuação de cada um.

Continua na próxima página...

Continuação da tabela 20 — Categoria 9

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
9.3	LGPD: Art. 41 – Encarregado pelo tratamento de dados pessoais; Art. 6º, X – Responsabilização e prestação de contas	Papel do Encarregado: Verificar se há um encarregado indicado e seus contatos públicos.	Não conforme	Em conversa com o programador responsável pela criação do sistema, confirmou-se que o sistema não possui a identidade ou o contato do encarregado de dados, o que torna necessária a inclusão, de forma visível e permanente, da identidade e das informações de contato do Encarregado da instituição no sistema.
9.4	LGPD: Art. 39 – Operador deve realizar o tratamento conforme instruções do controlador; Art. 6º, X – Responsabilização e prestação de contas	Conformidade contratual: Verificar que contratos de TI definem as obrigações de controlador e operador.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi relatado que não houve verificação ou atualização recente dos contratos de serviços de TI para incluir cláusulas específicas sobre responsabilidades da LGPD, o que torna necessária a solicitação ao setor jurídico ou de contratos para a revisão dos acordos com prestadores de serviço de TI, garantindo a inclusão de cláusulas de proteção de dados e responsabilidade solidária.

Fonte: Elaborado pelo autor (2025).

Tabela 21 – Governança e responsabilidade institucionais (Categoria 10)

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
10.1	LGPD: Art. 46 - Medidas de Segurança; Art. 6º, X – Responsabilização e prestação de contas ASVS: V1.1.2 - *Governance*	Política de Segurança da Informação: Verificar existência e aplicação de uma política formal de segurança da informação.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi confirmado que o projeto não possui uma Política de Segurança da Informação formalmente documentada e divulgada para os usuários e administradores do sistema, o que torna necessário desenvolver, aprovar e publicar uma Política de Segurança da Informação que estabeleça as diretrizes, normas e responsabilidades de todos os envolvidos no uso e manutenção do sistema.
10.2	LGPD: Art. 50 - Boas Práticas; Art. 6º; X – Responsabilização ASVS: V1.1.3 – *Security Awareness and Training*	Treinamento e conscientização: Verificar programas de capacitação sobre LGPD e segurança para funcionários.	Não conforme	Em conversa com o programador responsável pela criação do sistema, constatou-se que não foram realizados treinamentos ou ações de conscientização sobre proteção de dados para a equipe técnica ou para os usuários administrativos do sistema, o que torna necessária a implementação de um programa de conscientização e treinamento periódico e obrigatório sobre LGPD e boas práticas de segurança para todos os usuários com acesso privilegiado ou administrativo.

Continua na próxima página...

Continuação da tabela 21 — Categoria 10

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
10.3	LGPD: Art. 37 – Registro de operações ASVS: V1.1.4 – *Documentation of Security Requirements*	Registro de operações: Verificar manutenção de registro de todas as operações de tratamento de dados pessoais.	Não conforme	Em conversa com o programador responsável pela criação do sistema, verificou-se a inexistência de um documento formal que mapeie o ciclo de vida dos dados coletados pelo sistema, o que torna necessária a elaboração e manutenção atualizada do Registro de Operações de Tratamento, documentando a coleta, retenção, compartilhamento e eliminação de dados, conforme exigido pelo Art. 37 da LGPD.
10.4	LGPD: Art. 38 – Relatório de impacto; Art. 48 - Incidentes ASVS: V1.12.3 – *Incident Response*	Avaliação de impacto: Verificar se já foi realizado Relatório de Impacto de Proteção de Dados, especialmente em tratamentos de alto risco.	Não conforme	Em conversa com o programador responsável pela criação do sistema, confirmou-se que nunca foi realizado um Relatório de Impacto, apesar de o sistema tratar dados sensíveis e financeiros em larga escala, o que torna necessária a elaboração do RIPD para avaliar os riscos aos titulares e definir medidas de mitigação, dado o alto risco do tratamento.

Continua na próxima página...

Continuação da tabela 21 — Categoria 10

ID	Requisitos	Verificação	Resultado	Observação e Recomendação
10.5	LGPD: Art. 6, VII - Segurança; Art. 46 - Medidas de Segurança ASVS: V14.2.1 – *Dependency Management*; V1.2.6 – *Patch Management*	Monitoramento de incidentes: Verificar existência de plano de resposta a incidentes de segurança e obrigatoriedade de notificação.	Não conforme	Em conversa com o programador responsável pela criação do sistema, foi relatada a ausência de um Plano de Resposta a Incidentes formalizado, não havendo protocolo definido para notificar a Agência Nacional de Proteção de Dados (ANPD) ou os titulares em caso de vazamento, o que torna necessário estabelecer formalmente um Plano de Resposta a Incidentes que defina a equipe de resposta, os procedimentos de contenção e os fluxos de comunicação e notificação obrigatória à ANPD.
10.6	LGPD: Art. 6, VIII - Prevenção; Art. 46 - Medidas de Segurança ASVS: V14.2.3 - *Scanning*	Atualização e manutenção: Verificar controles de atualização de sistemas e dependências. .	Não conforme	O `pesquisa.py` importa diversas bibliotecas externas, no entanto não há evidência de um processo ou ferramenta de auditoria de dependências sendo executado para verificar se estas bibliotecas possuem vulnerabilidades conhecidas, o que exige a implementação de um processo de Gerenciamento de Dependências com o uso de ferramentas automatizadas para verificar continuamente as bibliotecas do projeto contra vulnerabilidades conhecidas.

Fonte: Elaborado pelo autor (2025).