DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Automação Segura no Moodle: Integração com Bancos Institucionais e Fortalecimento da Governança Digital

Luis Marcos Martins do Nascimento

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Automação Segura no Moodle: Integração com Bancos Institucionais e Fortalecimento da Governança Digital

Luis Marcos Martins do Nascimento

Orientador: Prof. Dr. Daniel Chaves Café, FT/UnB

PUBLICAÇÃO: PPEE.MP.105 BRASÍLIA-DF, DEZEMBRO- 2025

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Automação Segura no Moodle: Integração com Bancos Institucionais e Fortalecimento da Governança Digital

Luis Marcos Martins do Nascimento

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica

como requisito parcial para obtenção

do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Daniel Chaves Café, FT/UnB _____
Orientador

Prof. Dr. William Divino Ferreira, UFG _____
Examinador Externo

Prof. Dr. João Souza Neto, , FT/UnB _____
Examinador interno

Prof. Dr. Georges Daniel Amvame Nze, , FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

NASCIMENTO, LUIS MARCOS MARTINS DO
AUTOMAÇÃO SEGURA NO MOODLE: INTEGRAÇÃO COM BANCOS INSTITUCIONAIS E FORTALECIMENTO DA GOVERNANÇA DIGITAL
[Distrito Federal] 2025.
xii, 55 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica
1. Administração Pública
2. Segurança da Informação
3. Servidores Web
4. Software de Código Aberto
5. Gestão Automatizada no Moodle
6. Aprendizado de Máquina
I. ENE/FT/UnB
II. Título (série)
PUBLICAÇÃO: PPEE.MP.105

REFERÊNCIA BIBLIOGRÁFICA
NASCIMENTO, LUIS MARCOS MARTINS DO. Automação Segura no Moodle: Integração com Bancos Institucionais e Fortalecimento da Governança Digital. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 55 p.

Luis Marcos Martins do Nascimento
Depto. de Engenharia Elétrica (ENE) - FT Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho a toda a minha família, esposa, filhos, minha mãe, irmão, a meu pai *(in memoriam)*, dedico também a toda a equipe CEAD / UnB, pelo trabalho, por acreditarem em mim, nossa Diretora Drª. Profª. Alice Melo Ribeiro, ao nosso coordenador, Sebastião Henrique de Britto Lopes, ao nosso técnico corresponsável por nosso sistema do estudo, do projeto, Palton Lima Alves, ao meu orientador, muito dedicado, dedico aos demais amigos do Curso, Carlão e Jango e aos demais professores do curso, dedico também a meus professores e minhas professoras do antigo CEFET-PI, atualmente IFPI – Floriano – PI.

AGRADECIMENTOS

A Deus, primeiramente, a toda a minha família, mãe, esposa, filhos e amigos em geral por me confortar, me dar muito carinho, tivemos uma perda muito grande na família, mas fomos muito bem confortados, agradeço também a direção do CEAD pela liberação para estudar e me dedicar a este mestrado, agradeço aos amigos do Centro pela força e apoio, aos professores e coordenadores, pessoal do atendimento e secretaria do PPEE, da FT.

Agradeço pela atenção e orientação do Drº. Profº. Daniel Chaves Café, que torna o projeto e a execução deste trabalho parecerem fáceis.

Agradeço a meus amigos da TI do CEAD / UnB, dentre eles Sebastião Henrique pela grande amizade e incentivo, pelo grande Palton, por está comigo na programação e execução do sistema PRP01, sistema responsável pela interligação entre os sites e Bancos de Dados.

Agradeço o apoio de ferramentas de inteligência artificial (ChatGPT e COPILOT), utilizadas de forma complementar para aprimorar a redação e a estrutura textual deste trabalho, sem substituição da autoria intelectual.

RESUMO

Este trabalho apresenta o desenvolvimento e a implementação de um sistema automatizado e seguro para o gerenciamento de usuários e disciplinas no ambiente Moodle da Universidade de Brasília (UnB). O estudo aborda limitações estruturais do processamento manual, como inconsistências de dados, vulnerabilidades de segurança e alta carga operacional. Para superar esses desafios, foi criada a ferramenta institucional PRP01 (Palton's Robot in Python), desenvolvida em Python, web automation (Selenium), integrada a sistemas acadêmicos oficiais por meio de automação web, validação cruzada e transmissão segura de informações.

O sistema realiza validações automáticas de dados, garante conformidade com o Programa de Privacidade e Segurança da Informação (PPSI) da Portaria SGD/MGI nº 852, de 28 de março de 2023, alinhado a Lei Nº 13.709/2018 - Geral de Proteção de Dados (LGPD) e ABNT NBR ISO/IEC 27001:2022, para reduz erros humanos, além de aplicar controles de segurança, como autenticação institucional e rejeição automática de dados inconsistentes. Os resultados demonstram redução superior a 90% no tempo de processamento, aumento da escalabilidade operacional, mitigação de incidentes de segurança e maior satisfação dos usuários. Conclui-se que a automação segura aprimora a governança digital e fortalece a confiabilidade dos processos acadêmicos, constituindo um modelo replicável para outras instituições de ensino.

Palavras-chave: Moodle. Automação de processos. API. Segurança da informação. LGPD.

ABSTRACT

This paper presents the development and implementation of an automated and secure system for managing users and courses in the Moodle environment at the University of Brasília (UnB). The study addresses structural limitations of manual processing, such as data inconsistencies, security vulnerabilities, and high operational load. To overcome these challenges, the institutional tool PRP01 (Palton's Robot in Python) was created, developed in Python, web automation (Selenium), integrated with official academic systems through web automation, cross-validation, and secure information transmission.

The system performs automatic data validation, ensures compliance with the Information Privacy and Security Program (PPSI) of Ordinance SGD/MGI No. 852, of March 28, 2023, in line with Law No. 13,709/2018 - General Data Protection Law (LGPD) and ABNT NBR ISO/IEC 27001:2022, to reduce human error, in addition to applying security controls, such as institutional authentication and automatic rejection of inconsistent data. The results show a reduction of more than 90% in processing time, increased operational scalability, mitigation of security incidents, and greater user satisfaction. It is concluded that secure automation improves digital governance and strengthens the reliability of academic processes, constituting a replicable model for other educational institutions.

Keywords: Moodle. Process automation. API integration. Information security. Data privacy.

SUMÁRIO

LISTA DE SIGLAS

2FA	Two-Factor Authentication
ABNT	Associação Brasileira de Normas Técnicas
API	Application Programming Interface
AVA	Ambiente Virtual de Aprendizagem
CDT/UnB	Centro de Apoio ao Desenvolvimento Tecnológico da Universidade de Brasília
CEAD/UnB	Centro de Educação a Distância da da Universidade de Brasília
COAP	Constrained Application Protocol
COVID-19	Coronavirus Disease 2019
CPU	Unidade Central de Processamento
CSF	Cybersecurity Framework
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
DGP	Decanato de Gestão de Pessoas
DoS	Denial of Service
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
GDPR	General Data Protection Regulation
HDD	Hard Disk Drives
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Inteligência Artificial
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
IIOT	Industrial Internet of Things
IoT	Internet das Coisas
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
LAN	Rede de Área Local
LGPD	Lei Geral de Proteção de Dados
LTS	Long Term Support

MAC	Media Access Control address
DNS	Domain Name System
MFA	Autenticação Multifator
ML	Machine Learning
MOODLE	Modular Object-Oriented Dynamic Learning Environment
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
OCS	Open Computer and Software Inventory Next Generation
OSI	Open Systems Interconnection
OAuth2	Open Authorization
PHP	Hypertext Preprocessor
PPEE	Programa de Pós-Graduação Profissional em Engenharia Elétrica
PRP01	Palton's Robot in Python
PPSI	Programa de Privacidade e Segurança da Informação
RAM	Memória de Acesso Aleatório
RFID	Radio-Frequency Identification
SAA/UnB	Secretaria de Administração Acadêmica da Universidade de Brasília
SHA-256	Secure Hash Algorithm 256 bits
SIEM	Security Information and Event Management
SIGAA	Sistema Integrado de Gestão de Atividades Acadêmicas
SIGER	Sistema de Gerenciamento de Relatórios
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response
SSD	Unidade de Estado Sólido
SSDP	Simple Service Discovery Protocol
SSH	Secure Shell
SQL	Structured Query Language
STI/UnB	Secretaria de Tecnologia da Informação da Universidade de Brasília
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
TICs	Tecnologias da Informação e Comunicação
TLS	Transport Layer Security
UAB	Universidade Aberta do Brasil
UDP	User Datagram Protocol
UnB	Universidade de Brasília
UPnP	Universal Plug and Play
WMI	Windows Management Instrumentation

LISTA DE FIGURAS

LISTA DE TABELAS

1 – INTRODUÇÃO

Devido aos desafios nos últimos anos, as instituições de ensino superior vêm enfrentando dificuldades crescentes, dentre eles, ataques relacionados à segurança da informação compreende ações que objetivam assegurar a confidencialidade, a integridade dos dados acadêmicos em seus ambientes virtuais. As Plataformas de ensino como o Moodle, uma das principais ferramentas de apoio à gestão do ensino presencial e a distância em todo o mundo, as equipes de segurança cibernética têm como dever ampliar, necessariamente, soluções para garantam confiabilidade, automação e proteção de dados. No trabalho destacaremos a governança digital como elemento central na gestão de instituições públicas e privadas, sendo fundamental para assegurar transparência, eficiência e segurança em ambientes digitais.

O Moodle é utilizado como ambiente institucional de ensino na Universidade de Brasília (UnB)**,** sob o domínio Aprender3, Aprender2 entre outros. Estes portais gerenciam milhares de disciplinas e usuários, entre professores, técnicos e estudantes, isto demanda alto nível de coordenação e controle no processo de criação e atualização de cursos e de usuários, o Aprender2 é dedicado aos cursos da UAB (Universidade Aberta do Brasil – UnB), alguns cursos de extensão e pós-graduação latu sensu, para ele os cursos e as inscrições de usuários são totalmente de forma manual, já que tem muitos alunos externos e são a maioria temporários, no caso dos cursos de extensão, no Aprender3 tem todos os cursos presenciais da UnB, onde estão todos os alunos regulares, professores e técnicos administrativos da universidade.

O estudo é focado no Aprender3, onde a demanda é maior, constante e complexa, para o processo que envolvia ação manual entre usuários e administradores dos portais e administradores do sistema, essa intervenção manual pode ser falha e resultar em retrabalho, atrasos e riscos de segurança, também como inconsistências de dados, perfis indevidos e vulnerabilidades de acesso.

A UnB possui mais de 2,6 mil professores e mais de 12 mil novos alunos por ano, incluídos em seus portais de dado, tornou-se necessária uma ação automatizada para agilizar os serviços entre o Moodle e os sistemas institucionais, como o SIGAA (Sistema Integrado de Gestão de Atividades Acadêmicas - UnB) e o SIGER (Sistema de Gerenciamento de Relatórios - UnB), além disso, a alta demanda sobrecarregava a equipe técnica responsável pelo cadastramento e aprovação de cursos, comprometendo a eficiência e a experiência dos usuários, impactando negativamente na avaliação do trabalho feito pela equipe, atendimentos em tempo real e respostas as solicitações, por exemplo.

Para isso, surgiu a necessidade de automatizar o processo de gerenciamento de usuários e disciplinas no Moodle com banco de dados terceiros, sempre focando na segurança, conformidade e integridade dos dados**.**

A equipe técnica da CTIC/CEAD desenvolveu o PRP01 (Palton’s Robot in Python) — um sistema automatizado construído em Python que integra o Moodle aos bancos de dados institucionais da UnB. Este robô, como podemos chamá-lo, utiliza técnicas de varredura da web e autenticação institucional para validar solicitações de criação de cursos e atualizar registros de forma segura, reduzindo o tempo de resposta e minimizando falhas de processamento, melhorando as respostas aos usuários e aos administradores do Moodle.

A automação contribui diretamente para o aprimoramento da governança digital universitária**,** permitindo que apenas solicitações com dados válidos sejam aprovadas, mitigando riscos de duplicidade ou manipulação indevida de dados. As respostas de solicitações negativas são enviadas aos técnicos, para tomada de decisões. Além disso, o sistema automatizado garante maior agilidade administrativa**,** transparência no processo de aprovação e adequação ao Programa de Privacidade e Segurança da Informação **(PPSI)** e consequemente a Lei Geral de Proteção de Dados (LGPD), destacando estabelecer os direitos e princípios de proteção de dados, fornecer diretrizes práticas e controles técnicos, formando uma base da governança digital e da proteção da privacidade.

No contexto acadêmico, a presente pesquisa busca demonstrar como a aplicação de técnicas de automação seguras, baseadas em linguagens como Python e em boas práticas de segurança da informação, pode melhorar significativamente a gestão de ambientes virtuais de aprendizagem**.** O estudo parte de uma análise da infraestrutura do Moodle na UnB e de seus fluxos de cadastro, propondo uma integração tecnológica capaz de unir eficiência operacional e segurança digital**.**

1.1 Motivação e justificativa

O ensino superior tem se impulsionado com a transformação digital, por meio do uso de ambientes virtuais de aprendizagem (AVA). O Moodle é uma das plataformas que mais se destacam neste meio no mundo, por sua flexibilidade, por ser código aberto e por ter uma ampla adoção mundial; está presente em mais de 240 países e em mais de 180 mil instalações ativas (MILOSEVIC, 2022). No entanto, devido a sua ampliação de uso traz também sérios e novos desafios relacionados à segurança, escalabilidade e confiabilidade na gestão de dados.

Na Universidade de Brasília (UnB)**,** como dito antes, no Moodle hospedam-se alguns portais, como Aprender2, Aprender3, os quais desempenham papéis estratégicos nas organizações de disciplinas presenciais, híbridas e à distância, a última é da UAB (Universidade Aberta do Brasil) hospedada no Aprender2.

A UnB possui mais de 50 mil alunos ativos, cerca de 2,6 mil professores e mais de 3 mil técnicos administrativos, todos eles são institucionalmente cadastrados nos portais, principalmente no Aprender3, o portal tem mais de 8,3 mil cursos cadastrados, a equipe de AVA recebe diariamente um grande volume de solicitações de criação de turmas, atualização de perfis e inscrição de usuários, quando realizados de forma manual, os processos tornam-se suscetíveis a falhas humanas, atrasos, inconsistências cadastrais e riscos à segurança**,** especialmente em períodos de início de semestre letivo, quando o número de demandas cresce, com novos cursos, trocas de matrículas e de professores.

1.2 Desafios de segurança e integridade dos dados

Dentre um dos requisitos críticos em plataformas educacionais é a segurança da informação. Devido a constantes altas demandas e equipe muito pequena, ocorriam falhas serviços duplicados ou em atrasos, abandonados, já até aconteceu casos de inserção de códigos maliciosos**,** também perfis inativos que ainda tinham privilégios administrativos, solicitações indevidas de criação de cursos foram identificadas no principal portal da UnB. Esses incidentes revelaram vulnerabilidades estruturais tanto na autenticação quanto na validação das solicitações enviadas pelos docentes e ou discentes.

Numa ocasião, em nosso Moodle, foram registrados pedidos de centenas de pendências anteriores de um mesmo usuário, que era discente e não tinha permissão para solicitações regulares. Isto, além de sobrecarregar a equipe técnica administrativa**,** abria margem para ataques de negação de serviço (DoS) e para a injeção de scripts por usuários com acessos indevidos.

Diante disso, o Centro de Educação a Distância – CEAD / UnB adotou mecanismos automatizados de controle e verificação, os quais validam cada solicitação de criação de disciplina ou cadastro / atualização de usuário de forma cruzada com os bancos de dados institucionais oficiais, como o SIGER e o SIGAA.

1.3 A necessidade de automação e integração institucional

Com o crescimento constante e o elevado número de atualizações de dados de usuários, as operações se tornaram complexas, na evidência da limitação dos processos manuais. Com equipe reduzida, levava-se um tempo elevado para análise e aprovação das solicitações, havia retrabalhos frequentes devido a erros de digitação, informações desatualizadas e solicitações duplicadas.

A automação e implementação de um sistema surgiram como resposta direta a esses desafios, para melhorar eficiência, precisão e segurança. Um novo sistema com a utilização de scripts programados em Python, linguagem (como *Selenium* e *Requests*), devido ao processo de registro de software no CDT / UnB, fomos recomendados a não postar o código fonte do software, até que se regularize. Permitem criar soluções que executam tarefas repetitivas com maior consistência e em conformidade com as políticas de segurança da instituição.

Após o desenvolvimento do PRP01 (Palton's Robot in Python), o nosso robô institucional, para realizar tarefas de forma automática e automatizada, faz varredura de dados de usuários e disciplinas a partir do SIGER ou SIGAA. Fazendo comparação e confrontação com as solicitações enviadas ao Moodle, nomeamos este robô em homenagem ao nosso técnico Palton Lima (aluno regular, mestrando na UnB e da área técnica do CEAD, em atendimento a usuários em seus portais), o mesmo dedicou-se bastante para o aprimoramento na implementação do sistema, a cada dia buscamos novas integrações.

Este sistema garante que apenas solicitações válidas, isto é, compatíveis com os registros nos bancos de sites de terceiros sejam aprovadas. Reduzindo significativamente a intervenção humana, os erros de cadastro e o tempo de resposta para criação de cursos, ao mesmo tempo em que fortalece a segurança cibernética institucional. Os dados não compatíveis ou não existentes são retornados à equipe técnica para avaliar e analisar de como finalizar o pedido, aprovando ou rejeitando.

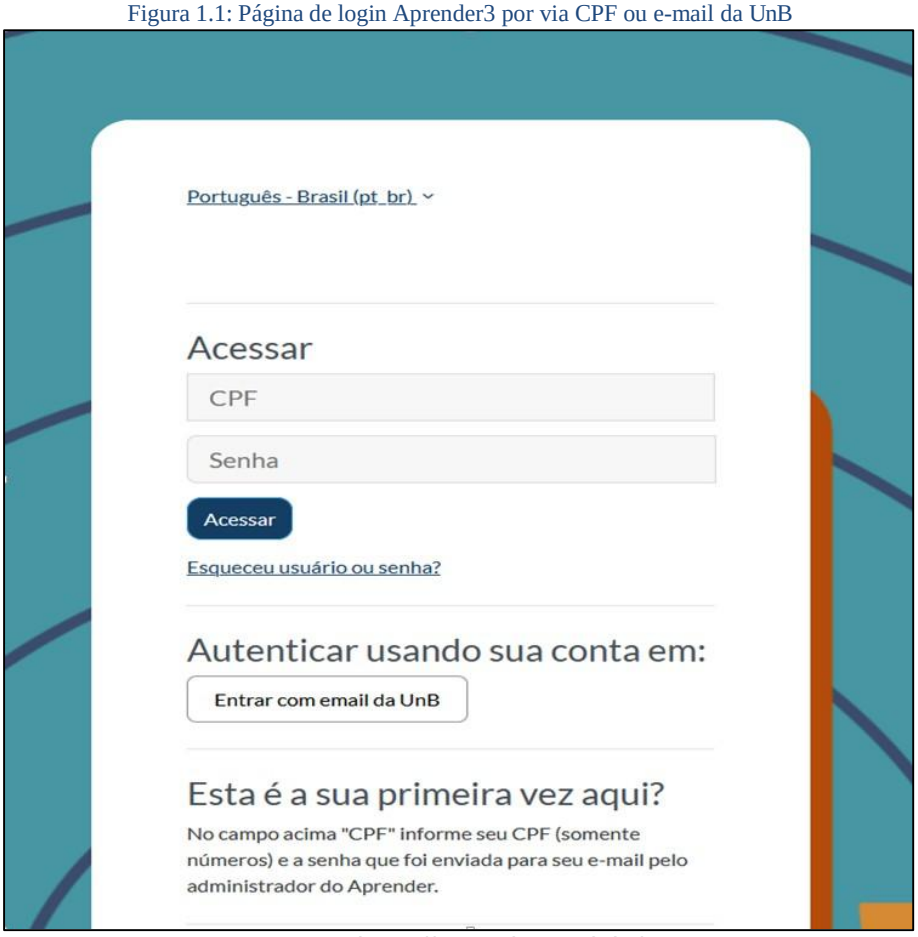
1.4 Conformidade com a legislação e boas práticas de segurança

Entre outros fatores que justificaram esta pesquisa foi a necessidade de conformidade com a Portaria SGD/MGI nº 852/2023 e LGPD – Lei nº 13.709/2018**,** a qual regulamentou o tratamento de dados pessoais, até mesmo em ambientes acadêmicos. O Moodle, por ser um ambiente multiusuário, processa informações sensíveis como nomes, CPFs, e-mails, matrículas e dados de login, exigindo políticas claras de proteção, autenticação robusta e rastreabilidade das ações realizadas no sistema.

Além da conformidade com a LGPD e normas internacionais de segurança, este trabalho também se insere no contexto da governança digital, que orienta a transformação digital e a gestão eficiente dos recursos tecnológicos na administração pública (BRASIL, Decreto nº 10.332/2020). A automação proposta fortalece a governança digital universitária ao garantir transparência, segurança da informação e confiabilidade nos processos acadêmicos, consolidando práticas alinhadas às políticas nacionais de proteção de dados e inovação tecnológica.

Ultimamente foi implantada uma integração com o e-mail institucional da UnB, através do Azure, facilitando o acesso dos alunos regulares, professores e técnicos administrativos, pois podem validar seus acessos pelo usuários criados no Moodle, ao mesmo tempo podem usar o e-mails institucionais, já que ambos estão relacionados ao mesmo CPF, isso foi graças a várias reuniões e testes com a equipe da STI (Secretaria de Tecnologia da Informação – UnB), a Figura 1.1 Ilustra os dois tipos de logins que podem ser feitos (via CPF ou e-mail da UnB).

Figura 1.1: Página de login Aprender3 por via CPF ou e-mail da UnB



Fonte: https://aprender3.unb.br/

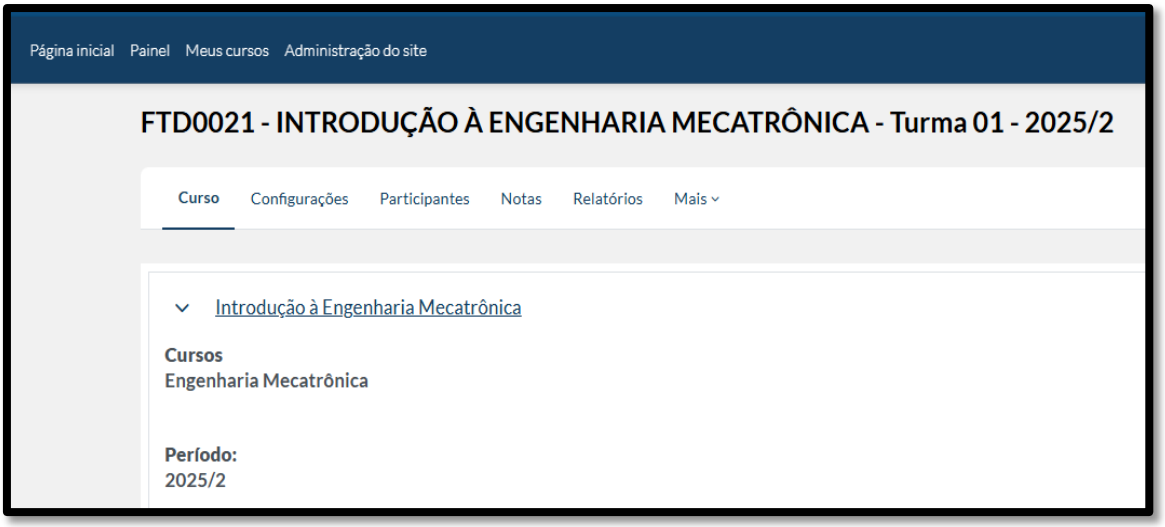
A automação incorporou camadas de autenticação e criptografia, garantindo que os dados fossem transmitidos e armazenados de forma segura. Lembrando que o sistema deve adotar protocolos como HTTPS e TLS, além de utilizar o e-mail institucional como identificador de confiança, minimizando o risco de acesso indevido. Essas práticas alinham-se às recomendações internacionais, como o NIST Special Publication 800-63-4, 2024

(TEMOSHOK, 2024), que orienta padrões para autenticação segura e verificação de identidade digital. Já Temoshok et al. (2025), atualizou que as diretrizes de identidade digital estabelecem parâmetros atualizados para prova e inscrição de identidade, reforçando a importância da padronização internacional na gestão de identidades eletrônicas.

Na relevância acadêmica e institucional, a pesquisa apresentou tanto na academia quanto na prática e do ponto de vista técnico, contribui bastante para o avanço do conhecimento na área de automação e segurança da informação aplicada, com o uso de Python e apoio técnico da equipe de TI. Do ponto de vista institucional, ofereceu uma solução concreta e testada que melhora a eficiência operacional, reduz drasticamente o volume de tarefas manuais e o retrabalho da equipe.

O modelo utilizado na UnB tem potencial para ser replicado em outras universidades, tanto públicas quanto privadas, que utilizam o Moodle como sistema central de ensino, promovendo uma ontologia nos dados apresentados, uma padronização e integridade, além da segurança no gerenciamento de usuários e cursos. As disciplinas são criadas no mesmo padrão, facilitando a compreensão e leitura. Em nossa formatação, ficou conforme a Figura 1.2, onde todos os cursos seguem essa organização visual de fácil compreensão a todos os usuários:

Figura 1.2: Código do Curso – Nome do Curso – Turma – Ano/Semestre



Fonte: https://aprender3.unb.br/

O trabalho e a pesquisa foram motivados por uma busca por um sistema que trouxesse equilíbrio entre inovação tecnológica, segurança e eficiência, alinhando a automação institucional às boas práticas de proteção de dados e governança.

A adoção do sistema PRP01 representou um passo significativo na modernização da infraestrutura acadêmica do CEAD – UnB, consolidando processos automatizados confiáveis no âmbito da educação superior.

1.5 Problema de Pesquisa e Objetivos

O avanço das tecnologias digitais na educação trouxe benefícios substanciais para o ensino superior, com isso, também ampliou os riscos associados à segurança e integridade dos dados institucionais**.** A plataforma Moodle é amplamente utilizada na Universidade de Brasília (UnB) como ambiente virtual de ensino, desempenhando papel estratégico na organização de cursos, turmas e usuários. Entretanto, a gestão manual desses cadastros tem se mostrado ineficiente e vulnerável, especialmente diante do crescimento exponencial da comunidade acadêmica e da complexidade dos fluxos administrativos.

O processo de criação de cursos no Moodle da UnB, hospedado no portal Aprender3, envolve duas instâncias distintas: o professor solicitante e o administrador do sistema, responsável por validar a solicitação. Essa separação de papéis, embora necessária para evitar sobrecarga, gera fluxos de aprovação demorados**,** retrabalho constante e falhas na comunicação entre sistemas, uma vez que o Moodle não está diretamente integrado aos bancos de dados institucionais do SIGER e do SIGAA.

Para trabalhos futuros pretendemos implantação de plug-ins, onde fazem este papel de integração via API, reduzindo consideravelmente o tempo de execução.

A ausência de integração automática expõe o sistema a riscos de inserção de dados falsos**,** duplicidade de perfis, uso indevido de credenciais e até mesmo ataques cibernéticos por meio de formulários de solicitação adulterados. Houve situações em que contas administrativas inativas inseriram códigos maliciosos em links de solicitação, o que causou lentidão e instabilidade no ambiente de produção.

Diante desse cenário, surgiu a seguinte questão central desta pesquisa:

Como iríamos automatizar o processo de gerenciamento de usuários e disciplinas no Moodle da Universidade de Brasília, garantindo segurança, integridade e conformidade com a LGPD por meio da integração com bancos de dados institucionais?

A resposta não implica apenas criar uma solução técnica, mas também compreender os aspectos organizacionais, tecnológicos e regimentais, que envolvem a automação segura em ambientes acadêmicos.

1.6 Hipótese de Pesquisa

Partimos da hipótese de que a integração automatizada entre o Moodle e os sistemas institucionais da UnB (SIGER, SIGAA), implementada por meio de um robô desenvolvido em Python**,** mitiga falhas humanas, reduz o tempo de processamento de solicitações e reforça a segurança no controle de usuários e disciplinas.

Essa integração iria permitir que apenas solicitações compatíveis com os registros válidos nos bancos de dados, dos sistemas da UnB fossem aprovadas, assegurando coerência entre as bases de dados **e** prevenção contra manipulações indevidas**.** Espera-se ainda que a automação contribua para o cumprimento da Lei Geral de Proteção de Dados (LGPD)**,** mediante

autenticação institucional e controle de acesso por perfis administrativos validados, em mais de dois anos de uso não tivemos reclamações sobre vazamentos ou insegurança de dados por parte dos usuários.

1.7 Objetivos

Objetivo Geral

O objetivo inicial, desenvolver e implementar um sistema automático, seguro e integrado para o gerenciamento de usuários e disciplinas no Moodle da Universidade de Brasília**,** para aprimorar a eficiência, reduzir erros e garantir conformidade com as normas de segurança e proteção de dados, além de melhorar os índices de qualificação no atendimento.

Objetivos Específicos

1. Identificar os principais gargalos e vulnerabilidades do processo manual de cadastro no Moodle da UnB.
2. Analisar os riscos de segurança e inconsistências de dados decorrentes da ausência de integração automática.
3. Propor um modelo conceitual de automação segura e integrada, em conformidade com a LGPD, PPSI e ISO 27001.
4. Avaliar a contribuição da automação para a governança digital e a experiência dos usuários.
5. Verificar a aderência da solução às boas práticas e normas internacionais de segurança da informação.
6. Examinar o impacto da automação sobre a redução de erros humanos, retrabalho e tempo de processamento.
7. Explorar a possibilidade de replicação do modelo em outras instituições de ensino que utilizem o Moodle.

Delimitação da Pesquisa

Este estudo concentra-se na automação do processo de criação e atualização de usuários e disciplinas no ambiente Moodle da Universidade de Brasília, ainda não abrange outros módulos administrativos do SIGAA ou sistemas externos. A solução proposta foi desenvolvida especificamente para a infraestrutura da UnB, entretanto, o modelo poderá ser replicável para outras instituições que enfrentem desafios semelhantes, para a integração entre ambientes de aprendizagem e bancos de dados acadêmicos.

Nesta dissertação será apresenta uma abordagem inovadora para a UnB como para demais universidades que utilizam o Moodle e possuem portais com dados semelhantes ao SIGAA e SIGER. A automação segura do gerenciamento de usuários no Moodle destacou-se em seu impacto positivo na gestão acadêmica da UnB e suas potencialidades.

O trabalho está estruturado da seguinte forma:

- Capítulo 2 – Revisão Bibliográfica: apresenta os conceitos teóricos relacionados ao Moodle, segurança da informação, automação com Python e integração de sistemas educacionais, também meus trabalhos correlatos.
- Capítulo 3 – Metodologia: descreve os procedimentos utilizados no desenvolvimento, testes e análise do robô PRP01, incluindo técnicas de varredura da web, autenticação segura e uso da API do Moodle.
- Capítulo 4 – Resultados: analisa os efeitos da automação na gestão acadêmica da UnB, com base em dados quantitativos e qualitativos.
- Capítulo 5 – Conclusão: sintetiza as principais descobertas, as limitações do estudo e as perspectivas para pesquisas futuras e para a replicação da solução em outros contextos.

2 - REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica apresentada neste capítulo tem como objetivo contextualizar as teorias, os principais conceitos estudados, as bases tecnológicas e os estudos fundamentados para o desenvolvimento de uma solução automatizada e segura para o gerenciamento de usuários e disciplinas no Moodle da UnB. Nessas bases temos abordagens de temas relacionados à segurança em ambientes virtuais de aprendizagem**,** integração de sistemas educacionais**,** uso de Python em processos de automação**,** e principalmente, normas de proteção de dados e privacidade**.**

O Moodle como a base do portal Aprender2 e Aprender3 na UnB, onde são hospedados diversos cursos, que vão de extensões a doutorados, disciplinas, recursos educacionais e interações entre alunos e professores, requer cuidados específicos com segurança e interoperabilidade com sistemas internos, como o SIGAA e o SIGER.

A governança digital refere-se ao conjunto de princípios e práticas que orientam o uso de tecnologias digitais para promover inovação, participação cidadã e eficiência administrativa (THORSTENSEN; ZUCHIERI, 2020).

Podemos definir como um conjunto de práticas e políticas que orientam a criação, manutenção e uso de portais institucionais, garantindo que eles cumpram funções de, transparência, segurança, eficiência, participação da comunidade acadêmica e confiabilidade, assegurando que os conteúdos publicados sejam oficiais e atualizados, reforçando a credibilidade institucional.

2.1 O Moodle como ambiente de aprendizagem e gestão acadêmica

Um pouco sobre nosso principal objeto do estudo, a plataforma Moodle (Modular Object-Oriented Dynamic Learning Environment) ou (Ambiente de Aprendizagem Dinâmico Modular Orientado a Objetos), de código aberto, criada por Martin Dougiamas em 2002, projetada para oferecer um ambiente flexível e escalável de ensino e aprendizagem (MOODLE, 2025). Sua arquitetura modular permite a criação de cursos, o gerenciamento de usuários, a avaliação de atividades e a comunicação entre professores e alunos em contextos presenciais, híbridos ou totalmente online**.**

Segundo Mosharraf e Taghiyareh (2018), o Moodle destacou-se por sua capacidade de organizar aplicativos, de estes comunicarem e trocarem informações de forma eficaz, mesmo que não sejam do mesmo fornecedor ou tenham sido projetados para trabalhar juntos, e pela possibilidade de integração com bases de dados externas, tornando-o uma solução adaptável às necessidades de cada instituição. No entanto, essa flexibilidade também amplia os riscos de vulnerabilidades de segurança caso os acessos e permissões não sejam rigidamente controlados.

Milosević et al. (2022) alertam que o Moodle, por ser amplamente utilizado, torna-se frequentemente alvo de ataques cibernéticos, especialmente por meio de plug-ins maliciosos e falhas de autenticação. Ataques que podem comprometer a integridade e confidencialidade dos dados armazenados, incluindo informações pessoais de alunos e docentes. Assim, a manutenção de um ambiente atualizado e monitorado é essencial para mitigar tais riscos.

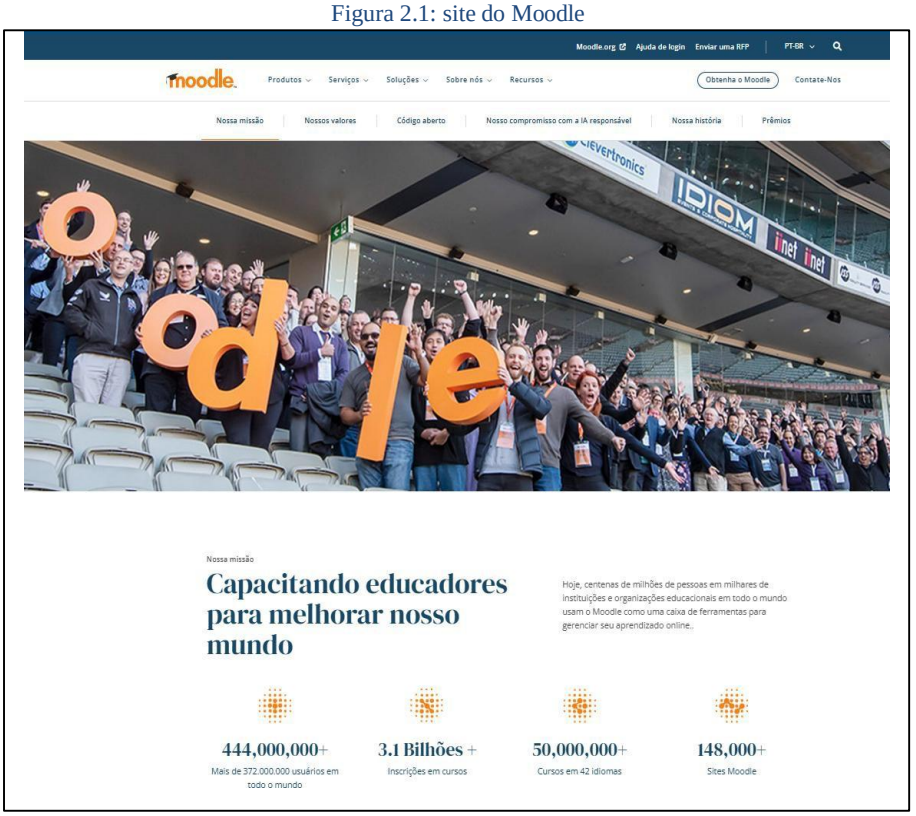
Na UnB existem equipes especializadas em várias camadas, organizadas e atentas a estes riscos, as quais partem da empresa GIGA CANDANGA, responsável pelo desenvolvimento e aprimoramento, STI para disponibilização de redes e seguranças nos acessos externos e a Equipe Técnica do CEAD – UnB, pelo atendimento e controle de acessos de usuários e criação de cursos no portal.

O Moodle é uma das plataformas de gestão de aprendizagem mais utilizadas no mundo, presente em mais de 240 países e operando em mais de 180.000 sites educacionais (MILOSEVIC et al., 2022). Sua flexibilidade, código aberto e capacidade de personalização o tornam uma escolha recorrente entre as instituições de ensino superior. A plataforma permite o gerenciamento de cursos, usuários, avaliações e atividades pedagógicas, sendo compatível com diversos dispositivos e formatos de conteúdo.

Além de ser um ambiente de aprendizagem, o Moodle também funciona como sistema de gestão acadêmica, centralizando dados de usuários, cursos, avaliações e acessos. Isso o torna uma ferramenta crítica na infraestrutura universitária, o que justifica a necessidade de aprimorar seus mecanismos de integração e segurança.

Na Figura 2.1 uma ilustração do portal oficial do Moodle e informações quanto a quantidade de usuários, cursos e sites da plataforma, no mundo, tem bastantes fóruns, eventos a se inscrever, implementações, dúvidas sobre programações, plug-ins:

Figura 2.1: site do Moodle



Fonte: https://Moodle.org/

2.2 Segurança da informação em ambientes educacionais digitais

A segurança da informação em ambientes educacionais é um tema de crescente relevância. Conforme Braeken e Touhafi (2020), a autenticação de usuários e o controle de acesso são pilares fundamentais para preservar a privacidade e a rastreabilidade das ações realizadas em plataformas virtuais. A falta de mecanismos robustos de autenticação pode permitir que usuários não autorizados obtenham acesso a informações sensíveis, como dados de matrícula e registros acadêmicos.

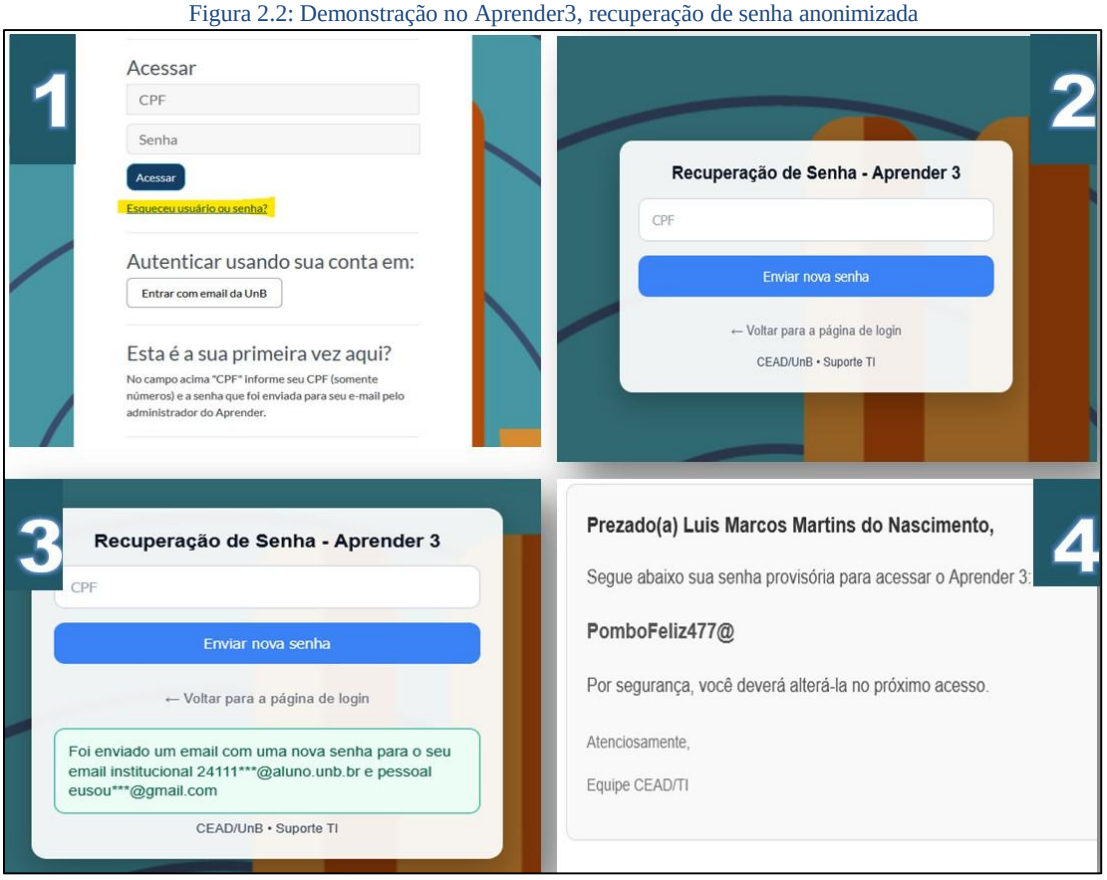
Zabala, et al. (2022) propuseram um modelo de segurança em múltiplas camadas para o Moodle, envolvendo autenticação multifator, monitoramento contínuo e políticas de auditoria. Tais abordagens reforçam a importância de combinar métodos técnicos e administrativos para atingir níveis adequados de proteção.

Rahim et al. (2018) destacam que falhas humanas são uma das principais causas de incidentes em plataformas de ensino, seja por configurações incorretas, senhas fracas ou uso indevido de perfis administrativos. A automação de tarefas sensíveis, como cadastros e validações, reduz significativamente o risco de exposição de dados e a probabilidade de erros operacionais.

Para De Almeida et al. (2020), as instituições devem adotar práticas que garantam o tratamento ético e seguro das informações de alunos e servidores, estabelecendo políticas de acesso restrito, de anonimização de dados e de consentimento informado. No contexto da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), a educação superior pública brasileira vem buscando adequar seus sistemas à nova realidade regulatória.

Na Figuras 2.2 um exemplo de anonimização estabelecida pelo CEAD em quatro imagens, após o usuário solicitar nova senha, na sequência, o usuário que esqueceu (imagem1) a senha no Aprender3 vai até a Recuperação de Senha (Imagem2), digita o CPF, o sistema retorna para ele de forma anonimizada (Imagem3), com indução dos dois e-mails cadastrados no portal, assim somente o portador irá encontrar a mensagem enviada com a senha de recuperação, conforme a terceira (Imagem4):

Figura 2.2: Demonstração no Aprender3, recuperação de senha anonimizada



Fonte: https://aprender3.unb.br/

Como é necessária, a importância da segurança é sempre destacada pelos citados no estudo. Os riscos e vulnerabilidades na gestão de usuários do Moodle, como qualquer ambiente online, estão sempre sujeitos a vulnerabilidades que, se exploradas, podem comprometer dados sensíveis e o funcionamento da plataforma.

Problemas relacionados à autenticação, permissões excessivas, plugins maliciosos e injeções de código são frequentemente relatados na literatura (ZABALA; VELASCO; PARADA, 2022; BRAEKEN; TOUHAFI, 2020).

2.3 Integração e interoperabilidade de sistemas educacionais

A integração entre plataformas institucionais é um dos maiores desafios na administração acadêmica moderna. Na UnB, sistemas como o SIGAA, o SIGER e o Moodle (Aprender3) operam de forma complementar, mas com bancos de dados distintos e protocolos independentes. Há uma previsibilidade de que os bancos sejam interconectados, mas a STI – UnB ainda não encontrou de forma segura para a implementação de APIS ou tokens acessarem de forma contínua as bases de dados, o software e plug-ins estão em fase de registro. A atual fragmentação dificulta a sincronização das informações.

He et al. (2015) apontam que integrar serviços em nuvem e bancos de dados externos é essencial para atender grandes volumes de usuários com segurança e escalabilidade.

Já Mihai et al. (2023) defendem o uso de serviços de alto desempenho e de cargas automatizadas para reduzir gargalos e melhorar o desempenho das plataformas de e-learning.

Na prática, integrar sistemas heterogêneos requer o uso de protocolos padronizados de comunicação**,** como APIs REST, autenticação via OAuth2 e transmissão criptografada por HTTPS/TLS. No caso da UnB, onde alguns sistemas ainda não disponibilizam APIs públicas, a utilização de robôs automatizados com técnicas de varredura na web torna-se uma alternativa eficiente e viável, desde que implementada com segurança e controle de acesso.

Estamos disponibilizando algumas APIs e plug-ins para o Moodle. Ele já garantiu em testes uma alta eficiência e agilidade sem erros em implementação.

Li et al. (2022) reforçam que a combinação entre domínios e sites externos exige validação cruzada de dados e políticas de confiança mútua entre as plataformas, de modo a prevenir fraudes, interceptações e manipulações de dados sensíveis. Nisto, a equipe de TI do CEAD – UnB está atenta, sempre proativa nas validações dos portais e suas respectivas seguranças.

Uma integração segura com sistemas acadêmicos é vital diante das limitações operacionais, riscos de segurança, a comunicação entre o Moodle e sistemas institucionais é uma estratégia vista promissora. Futuramente, a integração com bancos de dados confiáveis permitirá o cruzamento de informações oficiais e a validação automática de solicitações, como a criação de disciplinas, o cadastro de usuários e até mesmo a modelagem dos cursos, de acordo com seus ambientes e categorias.

MIHAI et al. (2023) apontam que a automação de serviços de alto volume em ambientes educacionais contribui para a padronização, a rastreabilidade e a redução de falhas humanas. O uso de bots e técnicas de varredura na web, quando aliado a autenticação robusta, viabiliza a

Execução segura de tarefas repetitivas. Isso se mostra particularmente útil em instituições com alto número de solicitações, como é o caso da UnB.

2.4 Automação e uso de Python em ambientes educacionais

No contexto de nosso estudo, destaca-se novamente o PRP01 (Palton’s Robot in Python), um robô desenvolvido em Python que integra o Moodle aos sistemas SIGAA e SIGER da UnB, realizando integração contínua entre o Moodle e os sistemas SIGAA e SIGER da UnB. O PRP01 valida solicitações de docentes com base em planilhas institucionais e rejeita automaticamente registros inconsistentes, promovendo maior confiabilidade ao processo acadêmico. As rejeitadas são enviadas para os analistas, para aprovação ou não.

A automação de processos repetitivos é uma das áreas em que a linguagem Python tem se mostrado mais eficiente, graças à sua sintaxe simples e ao vasto conjunto de bibliotecas voltadas à manipulação de dados, à automação web e à integração com APIs.

Huang e Wu (2018) demonstram que o uso de bibliotecas Python, como *Selenium*, *Requests* e *Pandas*, permite criar soluções capazes de coletar, processar e enviar informações automaticamente para plataformas educacionais. Esses sistemas podem gerar relatórios de desempenho, cadastrar usuários, atualizar cursos e até monitorar interações no Moodle em tempo real.

No caso desta pesquisa, o PRP01 (Palton's Robot in Python) foi concebido como uma aplicação que une varredura da web**,** validação de dados e comunicação segura entre o Moodle e o SIGER / SIGAA. O robô atua como um agente automatizado, responsável por validar solicitações, rejeitar inconsistências e gerar relatórios automáticos para os administradores.

Na abordagem de Shan, Guijuan. (2021), demonstrou como técnicas de mineração de dados e associação de regras podem otimizar a análise de grandes volumes de informações, aumentando a eficiência de plataformas de comércio eletrônico e sistemas educacionais. Além da eficiência, a automação também reforça a segurança ao reduzir o número de intervenções humanas nos processos administrativos.

Conforme Kulkarni et al. (2024), a mitigação de ataques de fraudes digitais e de injeções de código malicioso depende, em grande parte, da redução de pontos de vulnerabilidade humana, substituindo operações manuais por processos automáticos auditáveis.

2.5 Normas e boas práticas de segurança da informação

A implementação de qualquer sistema automatizado que manipule dados sensíveis deve estar em conformidade com padrões e normas internacionais de segurança, como a ABNT NBR ISO/IEC 27001:2022 (Gestão de Segurança da Informação) e as Diretrizes do NIST (National Institute of Standards and Technology)**.**

Em nosso país, além das normas internacionais, como a ISO/IEC 27001 e as diretrizes do NIST, há instrumentos normativos específicos voltados à proteção de dados e à segurança da informação. Destacam-se, entre eles, o Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023. O PPSI complementa a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), funcionando como um framework de governança digital e boas práticas de segurança, especialmente no setor público (BRASIL, 2023).

O documento Digital Identity Guidelines: Identity Proofing and Enrollment (NIST, 2024) estabelece princípios para autenticação forte, validação de identidade e registro de logs de auditoria. Esses princípios são especialmente relevantes para ambientes de ensino, onde a autenticidade das informações impacta diretamente a validade acadêmica de cursos e certificações. A adoção de políticas rígidas de senhas, além de monitoramento contínuo de acessos (TEMOSHOK et al., 2024). Já em publicação posterior, Temoshok (2025) amplia essas diretrizes para incluir novos padrões de segurança.

Braeken e Touhafi (2020) e Rahim et al. (2018) veem práticas como autenticação multifator (2FA), hash de senhas, controle de logs e restrição de privilégios administrativos como sendo recomendadas por autores como sendo aplicáveis ao contexto do Moodle e ao robô PRP01. A Segurança da Informação é um pilar fundamental na gestão de plataformas virtuais.

Kulkarni et al. (2024) defendem o uso de soluções complementares como filtros anti-phishing, especialmente em serviços integrados por e-mails institucionais.

Já De Almeida et al. (2020) destacam que, para além das soluções técnicas, é necessário garantir a conformidade com princípios éticos e legais relativos à privacidade dos usuários.

A aplicação desses princípios em soluções, no caso do PRP01, reflete uma preocupação crescente com a governança digital, visando garantir a confidencialidade, a integridade e a disponibilidade dos dados. A adoção de conexões seguras (HTTPS, TLS) e a configuração adequada dos servidores são elementos indispensáveis nesse processo.

2.6 Síntese da revisão

É evidenciado que a automação segura e integrada de processos acadêmicos é uma tendência necessária para o fortalecimento da governança digital nas universidades e demais instituições que desejam implementar este sistema. Trabalhos anteriores apontam que a conjugação entre mecanismos de autenticação robustos**,** comunicação segura entre sistemas **e** automação com Python representa uma solução eficiente para problemas de escala e segurança.

O estudo insere-se nesse contexto ao propor e aplicar um modelo prático de automação para o Moodle da UnB, explorando e contribuindo para o avanço das pesquisas sobre segurança e integração em ambientes virtuais de aprendizagem**.**

O uso da linguagem Python para automação educacional tem crescido devido à sua simplicidade, robustez e vasta gama de bibliotecas. Ferramentas como Selenium e Requests permitem a execução de scripts que interagem com sites e sistemas externos, sendo ideais para tarefas como varredura de web, envio de notificações automáticas e integração com APIs.

Huang e Wu (2018) demonstraram como o uso de Python pode auxiliar na análise de dados educacionais e na criação de perfis de cursos.

Sun, Wang e Su (2023) também apontam o potencial da linguagem para o desenvolvimento estruturado e para sistemas de visualização integrados ao Moodle. No caso do PRP01, o uso de bibliotecas específicas permitiu a automação segura da criação de cursos e vinculação de docentes a disciplinas, reduzindo a dependência de intervenções humanas e aumentando a eficiência operacional.

O avanço da tecnologia da informação e o surgimento da computação em nuvem como um modelo inovador para o uso e gestão de recursos computacionais. Essa tecnologia oferece serviços sob demanda, alta confiabilidade e baixo custo operacional, permitindo que empresas e usuários utilizem recursos de forma mais eficiente e segura. São descritos três principais tipos de nuvem: pública, privada e comunitária, cada uma com diferentes níveis de acesso e finalidade, (HE; QIU; ZHAI, 2015).

Eles apresentam o sistema de gerenciamento de aprendizagem (LMS) de código aberto voltado para a criação e administração de cursos online.

Durante a pandemia foi observada a intensificação do uso de plataformas de gestão de aprendizagem (LMS), ampliando a importância da segurança dos dados nelas armazenados. Contudo, estudos apontam que muitos desses sistemas, incluindo o Moodle, ainda carecem de mecanismos de proteção suficientemente robustos para prevenir ataques cibernéticos, (ZABALA; VELASCO; PARADA, 2022).

Essa fragilidade pode permitir o acesso não autorizado e a extração de informações sensíveis, gerando riscos tanto para usuários quanto para instituições. Entre as principais vulnerabilidades identificadas estão o uso de versões desatualizadas e não suportadas, a ausência de criptografia (HTTPS), falhas na configuração de arquivos e a falta de atualização do interpretador PHP.

A análise de diversos sites baseados em Moodle revelou mais de cinquenta tipos de vulnerabilidades, com uma média de cinco falhas por instalação, evidenciando a necessidade urgente de aprimorar a segurança nas plataformas educacionais online. Na UnB, corrigimos várias dessas falhas, entre elas o sistema atualizado, versão 4.0 e posterior, o portal com certificação HTTPS e PHP 8.4.

Recentemente, têm sido desenvolvidas abordagens que integram o Moodle ao conceito de Linked Data, (metodologia para publicar e interligar dados estruturados na Web, permitindo que eles sejam lidos, entendidos e reutilizados por máquinas, e não apenas por humanos), permite a disseminação e o enriquecimento de recursos educacionais por meio da vinculação com repositórios e dados estruturados na web, (MOSHARRAF; TAGHIYAREH, 2018).

A ontologia utilizada segue os princípios do Linked Data, como um mapa estruturado que facilita a compreensão e organização de informações tanto por humanos quanto por máquinas, promovendo um LMS conectado à web de dados, uso de vocabulários padronizados (Exemplo no Aprender3: código do curso, título do curso, sua turma, ano e semestre, professor vinculado ao curso e à instituição, a instituição como entidade educacional.)

O código em Python é uma ferramenta para facilitar a coleta e a análise de grandes volumes de dados educacionais. O método visa simplificar o processo de avaliação das informações provenientes do Moodle, que são registradas em planilhas Excel (em CSV), embora a análise desses dados possa ser desafiadora e exigir tempo considerável, (ME et tal, 2023).

O estudo aborda o phishing por e-mail como uma ameaça persistente a indivíduos e organizações, explorando vulnerabilidades humanas e técnicas de manipulação digital. A pesquisa examina táticas como o comprometimento de e-mails corporativos e a falsificação de mensagens.

Entre as medidas de mitigação destacam-se a autenticação multifator (MFA), que adiciona camadas extras de verificação para prevenir acessos não autorizados, e o uso do Microsoft Defender (antigo ATP – Advanced Threat Protection), pode ser usado de forma semelhante ao CrowdStrike e ao SentinelOne, são soluções de Endpoint Detection and Response (EDR) e Endpoint Protection Platforms (EPP)**,** o Defender é altamente integrado ao ecossistema Windows e Microsoft 365, enquanto CrowdStrike e SentinelOne oferecem recursos avançados de resposta e maior independência de plataforma, uma solução de segurança voltada à proteção contra phishing, malware e ataques avançados tanto em e-mails quanto em dispositivos (KULKARNI et tal, 2024).

Além da prevenção contra injeções de SQL em sites, reforçando a necessidade de estratégias integradas de cibersegurança. A UnB já utiliza MFA nos e-mails institucionais, no caso do "@unb.br", através da conexão por meio do AZURE o Moodle da UnB faz login alternativo ao usuário criado diretamente no Aprender3, pois a base do login é o CPF.

A questão da escalabilidade no gerenciamento de dados em ambientes universitários que utilizam plataformas de aprendizagem, como o Moodle. A automação de processos torna-se essencial diante do grande número de usuários e cursos, eliminando a necessidade de gerenciamento manual de contas e matrículas (MIHAI et al., 2023).

A solução proposta envolve a criação automatizada de perfis de alunos e professores, sincronizados com os bancos de dados institucionais por meio de scripts em MySQL e tarefas agendadas via RunDeck (em processamento na UnB). Esses mecanismos permitem a geração e a atualização de perfis, além da inscrição automática em cursos com base em dados coletados em sites de terceiros e homologados.

O sistema de autenticação externa garante segurança e integração, enquanto a automação otimiza o desempenho, a escalabilidade e a consistência dos dados na plataforma Moodle.

Propor uma metodologia para aprimorar a análise e classificação de dados educacionais por meio da coleta e processamento de conjuntos de dados relacionados a cursos e palavras-chave, (LI et tal, 2022).

A pesquisa examina a dependência de plataformas em serviços de terceiros, analisando a frequência de caracteres em nomes de domínio e a relação entre sites e serviços externos. Utilizando módulos de metadados e fusão baseados em técnicas de aprendizado conjunto. Os resultados demonstram que a combinação de representações em nível de caractere e de domínio aumenta significativamente a precisão das análises.

Discutir aspectos fundamentais no tratamento da informação — acesso, disponibilização, manipulação e tratamento de dados — enfatizando a importância da ética, privacidade e segurança nesse processo, (DE ALMEIDA, 2020). A pesquisa destaca a tríade essencial da segurança da informação: confidencialidade, integridade e disponibilidade.

Baseado na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18), ele reforça a necessidade de políticas rigorosas de controle de acesso, definição de permissões por nível (objeto, campo e registro) e responsabilidade dos usuários quanto ao uso seguro das credenciais.

Os dados acadêmicos e pessoais devem ser tratados com sigilo e transparência, assegurando que educadores e estudantes compreendam como suas informações são utilizadas.

Os riscos de segurança associados à instalação de plugins externos no Moodle, embora ampliem as funcionalidades do sistema, podem introduzir vulnerabilidades graves. Por ser uma plataforma de código aberto amplamente utilizada em mais de 240 países.

O Moodle permite personalizações que, sem o devido controle, expõem suas bases de dados compostas por informações sensíveis de alunos, professores e conteúdos avaliativos a ameaças como acesso não autorizado, injeção de SQL, falsificação de requisições entre sites e ataques por e-mail malicioso (spoofing) (MILOSEVIC et tal, 2022).

Os bancos de dados, como MySQL e PostgreSQL, utilizados pelo Moodle podem ser comprometidos por violações de segurança caso práticas inadequadas de instalação ou engenharia social sejam empregadas.

A necessidade de boas práticas para a gestão de senhas em conformidade com a Lei Geral de Proteção de Dados (LGPD), visando garantir a segurança e privacidade dos dados pessoais dos usuários, (BREAKEN; TOUHAFI, 2020).

Entre as medidas destacam-se o armazenamento criptografado das senhas, o uso de políticas de complexidade, autenticação em duas etapas (2FA), renovação periódica e proteção contra ataques de força bruta. Além disso, são enfatizados a confidencialidade das credenciais e o uso de algoritmos de hash, como SHA-256, para impedir que senhas sejam acessadas em caso de comprometimento do banco de dados. Tais práticas reduzem riscos de segurança e contribuem para a conformidade com a LGPD.

Os desafios contemporâneos da Educação a Distância (EAD) sob a perspectiva dos direitos fundamentais e emergentes, destacando a necessidade de inclusão digital e equidade no acesso à educação. Ressalta-se a importância da capacitação de professores, da criação de conteúdos acessíveis e do uso de plataformas online seguras.

Questões relacionadas à privacidade e proteção de dados são enfatizadas, com referência às legislações GDPR (General Data Protection Regulation) e ao Regulamento Geral de Proteção de Dados da União Europeia, e à LGPD, que oferecem diretrizes para o manejo seguro das informações estudantis (JUNIOR; GERSTENERGER, 2024).

O Moodle oferece uma plataforma flexível, de código aberto e com forte suporte comunitário, permitindo a criação e gestão de cursos on-line com foco em acessibilidade, segurança e escalabilidade, (SUN; WANG; SU, 2023). Para analisar o comportamento de aprendizagem dos alunos, o estudo utiliza a API do Moodle em Python, acessando dados sobre inscrições em cursos, status de conclusão, participação em fóruns, notas e informações dos usuários.

A aplicação da mineração de dados, especificamente da mineração de regras de associação, para identificar relações entre produtos e auxiliar comerciantes em recomendações, compra, venda e armazenamento de itens, (SHAN, 2021). Destaca-se a importância de aprimorar a eficiência, a adaptabilidade e a usabilidade dos algoritmos de mineração, que envolvem a definição do suporte mínimo.

Enfatiza a construção de plataformas de compartilhamento de informações multiplataforma, que devem garantir disponibilidade, precisão, eficácia e pontualidade dos serviços, oferecendo funcionalidades de consulta, adição, modificação, exclusão, importação e exportação de dados.

Plataformas de código aberto, como o Moodle, oferecem ferramentas de análise e visualização de dados, como painéis de aprendizagem e relatórios estatísticos. Desenvolveram um sistema de relatórios baseado em logs do Moodle utilizando Python, com uma interface unificada para aquisição e armazenamento de dados de múltiplos bancos ou arquivos, (HUANG; WU, 2018).

Destacaram o Moodle, com mais de 68 milhões de usuários e 55.000 sistemas em uso global, concentrando milhares de materiais de aprendizagem que exigem proteção rigorosa da informação, (RAHIM et al, 2018). Identificaram que fatores humanos e deficiências nos procedimentos de manuseio de conteúdos podem representar ameaças à segurança, incluindo acesso não autorizado, modificações indevidas e interrupção do serviço.

De acordo com as Digital Identity Guidelines publicadas pelo NIST (2024), os sistemas educacionais que operam por meio de APIs e Webservices, como o Moodle, devem adotar políticas de autenticação multifatorial (2FA) e procedimentos de recuperação de senha que garantam equivalência de segurança ao método de login original, (THEMOSHOK, 2024).

A publicação enfatiza que os fluxos de redefinição de credenciais representam pontos críticos de vulnerabilidade, exigindo a validação da identidade em múltiplos fatores, como e-mail seguro, tokens temporários ou autenticação via aplicativo. Essa abordagem é especialmente relevante em ambientes integrados, em que o Moodle se conecta a serviços externos por meio de APIs, pois evita acessos indevidos e reduz o risco de violação de dados sensíveis, assegurando a conformidade com padrões internacionais de segurança da informação.

A autenticação de dois fatores (2FA) para a plataforma Moodle, visa mitigar vulnerabilidades associadas ao uso exclusivo de login e senha. A solução consiste na integração de certificados digitais emitidos por autoridades certificadoras como segundo fator de autenticação, além das credenciais tradicionais, (BANEŞ et al. 2023).

Testes realizados em laboratório e em ambiente real demonstraram maior proteção contra ataques comuns, como phishing, força bruta e keylogging, além de redução no número de tentativas de acesso não autorizado e na perda de dados. A análise comparativa com outros métodos de 2FA evidenciou que a proposta oferece maior robustez e conveniência, especialmente pela flexibilidade de uso tanto em dispositivos físicos quanto na nuvem.

Conforme JÚNIOR, Albino Szesz et al. (2016), eles mostram que a evolução do Moodle no NUTEAD/UEPG aumentou a usabilidade e a acessibilidade, promovendo maior inclusão digital. Contudo, destaca que criar interfaces totalmente adequadas ainda é um desafio, e que a acessibilidade deve ser continuamente aprimorada.

A acessibilidade e a usabilidade estão diretamente ligadas à confiabilidade do sistema e à experiência segura do usuário. Desde este tempo já tinham preocupações com layouts e identificações em seus templates, o CEAD – UnB já estuda este avanço nas criações de disciplinas no Moodle.

De acordo com ELMAGHRABI, Azza Yousif; BADAWI, Maria Altaib. (2020) Demonstram que o Moodle, quando hospedado em IaaS, exige uma abordagem em camadas de segurança, que integra configurações internas, plugins externos e boas práticas administrativas.

O modelo proposto mostrou-se eficaz em um ambiente experimental, servindo como um guia prático para administradores que desejam reforçar a segurança dos sites Moodle contra ameaças da nuvem.

Segundo ROGERS, Jamal Kay B.; SALAZAR, Romel P.; BULADACO, Mark Van M. (2025) em uma breve comparação entre Moodle e outras plataformas, dentre elas o Google Classroom, o estudo mostra que o Moodle é uma plataforma mais completa e robusta, enquanto o Google Classroom é mais adequado para situações de menor complexidade. Ambas podem ser eficazes, desde que alinhadas às necessidades da instituição e ao perfil dos usuários.

Reforça que o Moodle se sobressai em segurança e controle de dados em comparação a outras plataformas, justamente por permitir a personalização de acessos, o uso de plugins de proteção e maior autonomia das instituições.

Esse ponto fortalece sua argumentação de que, embora mais complexo, o Moodle é preferível quando a segurança da informação e a confiabilidade do ambiente virtual são prioridades.

O Moodle consolidou-se como uma ferramenta essencial no ensino superior e profissional, favorecendo a aprendizagem significativa e colaborativa. Além disso, o estudo destaca sua importância especialmente em contextos de educação remota e híbrida, como no período da pandemia de Covid-19, (GONES; TANI, 2020).

O Moodle tem impacto transformador na EaD ao quebrar barreiras geográficas, promover acessibilidade, personalização e engajamento ativo. Sua capacidade de integração com outras tecnologias e sua comunidade global garantem constante atualização e inovação, (FERREIRA et al. 2024).

Os autores trazem pontos como o controle de acessos, a confiabilidade dos dados dos alunos, a necessidade de formação adequada dos tutores e o suporte técnico permanente.

As TICs mostraram-se essenciais para a resiliência do sistema educacional durante a pandemia, mas evidenciaram desigualdades sociais e carências estruturais. A continuidade da EaD exige investimentos em infraestrutura, formação digital de professores e políticas públicas de inclusão tecnológica, (MAIA, 2025).

Este estudo reforça que, em cenários de crise e uso massivo, cresce a necessidade de garantir a segurança da informação, a privacidade dos dados dos usuários e a confiabilidade do ambiente virtual, já que a dependência dessas plataformas se torna central para o funcionamento da educação**.**

O Moodle é um ambiente virtual de aprendizagem (AVA) que permite a criação de cursos a distância e híbridos, com base na filosofia de software livre e colaborativo (LIMA, 2021).

A plataforma oferece diversos recursos pedagógicos: fóruns, questionários, glossários, chats, wikis, tarefas e diários, favorecendo a aprendizagem ativa e significativa. O artigo destaca que o Moodle transforma o professor em mediador e não apenas transmissor de conhecimento, estimulando maior autonomia dos estudantes.

O Moodle consolidou-se como uma plataforma estratégica de mediação tecnológica, favorecendo flexibilidade, interação e personalização da aprendizagem. Amplia o acesso à educação, mas exige envolvidos para que seu potencial seja plenamente aproveitado.

A EaD é um fenômeno antigo (desde cursos por correspondência), mas foi impulsionada pela internet e pela pandemia, tornando-se parte essencial do ecossistema educacional, (GUIMARÃES et al. 2025).

As plataformas digitais oferecem benefícios como flexibilidade, democratização do acesso, interatividade e aprendizagem colaborativa. Destacam-se ferramentas corporativas adaptadas ao ensino (Zoom, Google Meet, Microsoft Teams) e os Ambientes Virtuais de Aprendizagem (AVA), com destaque para o Moodle, por ser livre, gratuito e voltado à aprendizagem colaborativa.

Mesmo em softwares de código aberto como o Moodle, a segurança depende não apenas da ausência de falhas críticas, mas também da qualidade estrutural do código, (UCHMIN; KRYLOV, 2025).

Uma interface é proposta para automatizar a extração e a disponibilização de dados do Moodle, utilizando Python e APIs do Google, com o objetivo de reduzir barreiras de acesso às informações e otimizar o acompanhamento de cursos online.

Essa abordagem reforça a importância da integração segura entre o banco de dados do Moodle e serviços externos, um aspecto essencial em projetos que envolvem Web Services e segurança da informação (ALVES ANDRADE; SILVA; CORDEIRO, 2022).

A automatização por meio do agendamento de tarefas do sistema operacional permite a predefinição da frequência com que o script deve ser executado, sem necessidade de interferências, o que exclui a dependência anterior do profissional com acesso ao banco de dados.

A integração entre o Moodle e serviços externos por meio de APIs tem se mostrado uma estratégia relevante para otimizar o gerenciamento de dados educacionais e reforçar a segurança em ambientes virtuais de aprendizagem.

Os autores desenvolveram uma interface de automação para o Moodle utilizando Python e APIs do Google Cloud, propondo um modelo que reduz a dependência humana no acesso direto ao banco de dados e aumenta a integridade das informações.

Um serviço de aprendizagem desenvolvido e personalizado compatível com o Moodle, que se conecta a um sistema de gestão de informações estudantis (SIMS) por meio de sincronização de dados. Essa integração permite oferecer cursos personalizados de acordo com o perfil e o progresso do aluno, ao mesmo tempo em que reforça a integridade e a segurança dos dados por meio do controle automatizado de acesso e atualização de informações (SHAN, 2022).

Eles propuseram um serviço de aprendizagem personalizado compatível com o Moodle que sincroniza dados de usuários a partir de um sistema de gestão de informações estudantis (SIMS),oferecendo cursos e materiais personalizados conforme o perfil de cada aprendiz. A solução utiliza automação para minimizar erros humanos e garantir a integridade das comunicações entre plataformas externas e o ambiente Moodle.

Segundo Gil (2002), a pesquisa aplicada busca resolver problemas práticos, enquanto a pesquisa descritiva procura caracterizar fenômenos. Neste trabalho, a metodologia adotada é aplicada, descritiva e de caráter experimental, conforme a tipologia da proposta.

Com base em Gil (2019), a pesquisa é aplicada a resolver um problema prático da UnB. Descritiva, pois caracteriza processos e resultados. Quantitativa, onde se baseia em dados objetivos, métricas, logs, questionários estruturados. E, em caráter experimental, com o desenvolvimento e a validação de uma ferramenta inédita.

2.7 Meus trabalhos

Em minhas duas publicações, fiz análises sobre falhas humanas e um estudo voltado ao fortalecimento da segurança no gerenciamento de usuários do Moodle, utilizando integração automatizada com bancos de dados de terceiros.

A usabilidade está diretamente ligada à eficácia das medidas de segurança, uma vez que sistemas mal projetados tendem a induzir erros humanos e vulnerabilidades. Essa relação também se aplica ao ambiente Moodle, onde a interface e o design impactam na adoção de boas práticas de segurança pelos usuários, (REIS et al. 2025)**.** "A segurança cibernética é potencializada quando o sistema promove uma interação intuitiva e reduz a probabilidade de falhas humanas."

Também escrevi um artigo intitulado *"Aumentando a Segurança do Gerenciamento de Usuários do Moodle Usando Bancos de Dados de Terceiros"* que apresenta uma ferramenta implementada na Universidade de Brasília (UnB) que conecta o Moodle ao sistema acadêmico SIGER, permitindo validação automática das solicitações de criação de turmas e atualização de cadastros (NASCIMENTO; SILVA; CAFÉ, 2025)**.**

Essa automação teve como objetivo reduzir retrabalho, aumentar a confiabilidade das informações e mitigar riscos relacionados a acessos indevidos, demonstrando o potencial da tecnologia para aprimorar a segurança e a eficiência administrativa em ambientes virtuais de aprendizagem.

3 - METODOLOGIA

A metodologia desta pesquisa foi baseada em características aplicadas, tecnológicas, quantitativas, descritivas e experimentais. Orientada tanto por referenciais normativos quanto científicos. Do ponto de vista normativo, foram adotados princípios da governança digital, que estabelecem diretrizes para a transformação digital e para a gestão eficiente dos recursos tecnológicos na administração pública (BRASIL, Decreto nº 10.332/2020). Nesse sentido, o desenvolvimento e a validação do PRP01 foram estruturados para garantir conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), assegurando transparência, segurança da informação e confiabilidade nos processos acadêmicos.

Do ponto de vista científico, a pesquisa seguiu o método descrito por Gil (2008), caracterizando-se como aplicada, descritiva e tecnológica, voltada à solução de problemas reais identificados nas rotinas administrativas da Universidade de Brasília.

Assim, a metodologia foi organizada em fases (quantitativas) de levantamento de requisitos, por meio de observação de processos, análise de logs e coleta de dados estruturados, de desenvolvimento da solução, onde envolve programação, no caso nosso robô o PRP01, integração e testes técnicos, pois se baseia em métricas de desempenho e segurança, de implementação com testes e validação, foram aplicados testes funcionais, de desempenho, segurança e conformidade com indicadores numéricos e resultados objetivos e de pesquisa de satisfação, permitindo a coleta de evidências empíricas sobre os benefícios da automação segura em ambientes acadêmicos digitais, com aplicação de questionário estruturado (Microsoft Forms) coleta de percepções, mas em formato fechado, mensurável e descritivo.

Vamos à metodologia deste trabalho, estruturada para desenvolver, implementar e avaliar um sistema automatizado de integração segura entre o Moodle da Universidade de Brasília (Aprender3) e os bancos de dados institucionais da universidade (SIGER/SIGAA).

Focando principalmente em riscos de segurança da informação e de conformidade legal, mas também cobrindo riscos operacionais (retrabalho, falhas humanas) e técnicos (ataques, inconsistências de dados).

Além das medidas de segurança descritas, na Tabela 3.1, foi elaborado um mapa visual de riscos que sintetiza os principais pontos críticos identificados na integração entre SIGER/SIGAA, PRP01 e o Moodle. Esse mapa apresenta cada risco, suas medidas de mitigação e o impacto esperado, reforçando que a segurança da informação e a conformidade legal foram tratadas como elementos centrais da metodologia.

Tabela 3.1: mapa de riscos

RISCO IDENTIFICADO	MEDIDA DE MITIGAÇÃO	IMPACTO ESPERADO
1. Acesso não autorizado	Autenticação multifator (2FA)	Maior segurança da Informação
2. Interceptação de dados	Criptografia TLS 1.3	Maior segurança da Informação
3. Roubo de credenciais	Hashing SHA-256	Maior segurança da Informação
4. Ataques externos (IP suspeito)	Bloqueio automático de IPs suspeitos	Maior segurança da Informação
5. Invasão via e-mail	Monitoramento de tráfego SMTP/IMAP	Maior segurança da Informação
6. Violação da LGPD	Armazenamento temporário e descarte	Conformidade legal (LGPD, ISO/IEC 27001)
7. Retrabalho e duplicidade	Validação cruzada SIGER/SIGAA	Eficiência operacional
8. Falhas humanas	Automação completa do fluxo	Redução de falhas humanas
9. Ataques técnicos (SQL injection, DoS)	Testes de segurança controlados	Maior segurança da Informação
10. Erros de processamento de dados	Filtragem de duplicados e validação de CPFs	Eficiência operacional
11. Inconsistência entre sistemas	Relatórios automáticos e auditoria	Transparência e auditabilidade

O sistema, denominado PRP01 (Palton's Robot in Python), foi concebido com o propósito de reduzir falhas humanas, aprimorar a eficiência no cadastramento de usuários e de disciplinas e garantir a conformidade com padrões de segurança da informação e de proteção de dados.

A metodologia adotada contempla aspectos técnicos, operacionais e de segurança da informação, com o objetivo de garantir precisão, eficiência e conformidade legal na criação e atualização de disciplinas e de usuários no ambiente Moodle.

A seguir, são descritas as etapas metodológicas adotadas, desde o levantamento de requisitos até os testes de validação e monitoramento do sistema em ambiente de produção.

Durante a elaboração desta dissertação, foram utilizadas ferramentas de inteligência artificial (IA) como apoio técnico para a revisão de estilo, a clareza textual e a organização da redação. Ressalta-se que a análise crítica, interpretação dos resultados e conclusões são de inteira responsabilidade do autor.

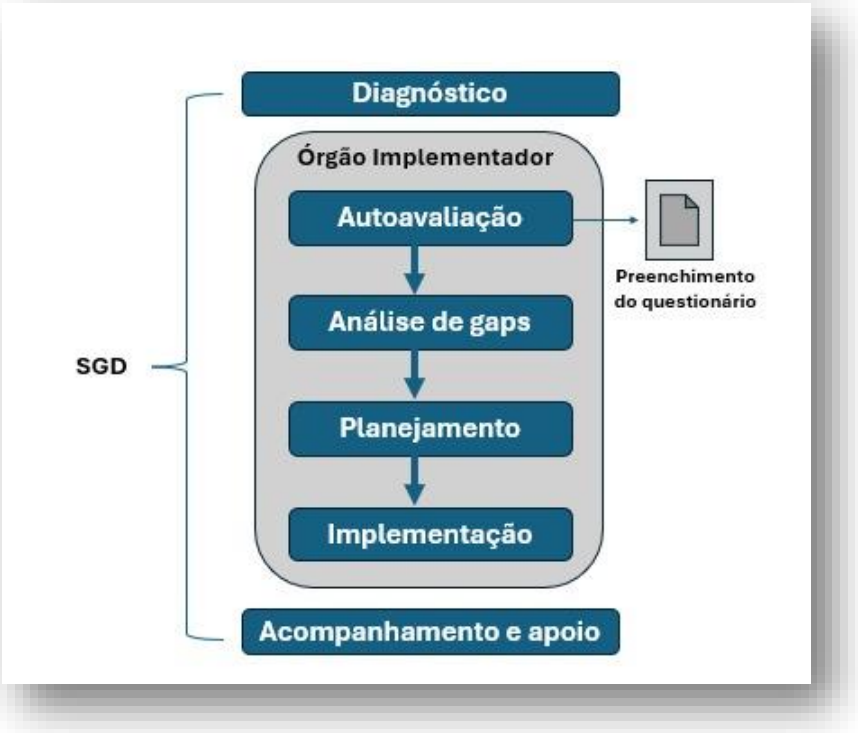
Abordagem metodológica

Trata-se de uma pesquisa com objetivos exploratórios e descritivos. O trabalho possui características exploratórias, já que seu principal objetivo é identificar e analisar riscos do conhecimento no contexto do PPSI, que, de acordo com a revisão de literatura, não foi estudado sob esse contexto (Gil, 2019). Ele é descritivo pois "consiste em investigações de pesquisa empírica cuja principal finalidade é o delineamento ou análise das características de fatos ou fenômenos, a avaliação de programas, ou o isolamento de variáveis principais ou chave" (Marconi; Lakatos, 2003, p. 187).

A primeira etapa da pesquisa consistiu em uma revisão da literatura sobre gestão de riscos de conhecimento, especialmente no contexto de segurança e privacidade da informação. Foram consultados artigos acadêmicos, relatórios técnicos e publicações institucionais, com o objetivo de fundamentar teoricamente os principais conceitos e identificar estudos prévios que abordassem riscos de conhecimento em organizações públicas. Essa revisão permitiu contextualizar os desafios enfrentados pela Administração Pública Federal na gestão do conhecimento e embasar a análise dos riscos identificados.

O modelo conceitual da pesquisa teve como foco as atividades de implementação do PPSI por parte dos órgãos da APF, sob supervisão da SGD/MGI, conforme ilustrado na Figura 3.1.

Figura 3.1 – Modelo Conceitual da Pesquisa



Fonte: Adaptado de SGD/MGI (Portaria nº 852/2023, Cartilha PPSI).

Estrutura do Modelo Conceitual da Pesquisa, Fluxo principal:

- **SGD/MGI (supervisão e apoio) ↓**
- **Diagnóstico inicial do órgão ↓**
- **Autoavaliação (questionário) ↓**
- **Análise de gaps (lacunas) ↓**
- **Planejamento de ações ↓**
- **Implementação do PPSI ↓**
- **Retroalimentação para SGD/MGI**

Esse fluxo pode ser ilustrado como uma cadeia de blocos conectados, destacando que o risco de conhecimento humano está presente em cada transição (por exemplo, interpretação incorreta de lacunas, resistência cultural, falhas de comunicação).

O modelo conceitual apresentado mostra que o fluxo de conhecimento se inicia com o diagnóstico do órgão orientado pela SGD/MGI. A etapas seguintes estão sob a responsabilidade dos órgãos implementadores, consistindo em autoavaliação (por meio de questionário), análise de gaps (lacunas), planejamento e implementação, tudo sob supervisão e apoio da SGD/MGI.

A pesquisa de campo foi conduzida por meio de um grupo focal, realizado com gestores da Secretaria de Governo Digital (SGD), que são responsáveis pela implementação do PPSI. O grupo focal teve a participação de cinco gestores com vasta experiência em tecnologia da informação e segurança, escolhidos por sua atuação direta no processo de gestão de riscos e implementação dos controles de segurança e privacidade do PPSI.

Conforme destacado por Ribeiro, Demo e Santos (2021), o grupo focal é uma técnica valiosa em pesquisas qualitativas, pois possibilita a coleta de percepções detalhadas e facilita a compreensão das experiências dos participantes. A utilização do grupo focal permitiu identificar aspectos subjetivos e específicos dos riscos de conhecimento no contexto do PPSI, justificando a escolha desse método para explorar em profundidade as percepções dos gestores envolvidos.

A operacionalização do grupo focal foi realizada por meio de plataforma *Microsoft Teams*. Os pesquisadores iniciaram os trabalhos por meio de alinhamento de conceitos sobre a Gestão de Riscos do Conhecimento, utilizando como base os conceitos de Durst e Henschel (2020), seguida da apresentação de três perguntas norteadoras com o intuito de identificar riscos do conhecimento, a saber:

1. Modelo Conceitual – Diagnóstico e Autoavaliação:

    - Risco de interpretação subjetiva: gestores podem interpretar de forma diferente os questionários.
    - Resistência cultural: servidores podem não reconhecer a importância da gestão de riscos.
    - Falta de capacitação: ausência de treinamento adequado para compreender conceitos de segurança e privacidade.

2. Modelo Conceitual – Análise de Gaps e Planejamento:

    - Viés cognitivo: gestores podem minimizar ou ignorar lacunas críticas.
    - Comunicação deficiente: falhas na troca de informações entre equipes e órgãos.
    - Dependência de conhecimento tácito: excesso de confiança em experiência individual sem registro formal.

3. Modelo Conceitual – Implementação e Supervisão:

    - Rotatividade de pessoal: perda de conhecimento quando servidores mudam de função ou órgão.
    - Sobrecarga de trabalho: gestores podem priorizar tarefas operacionais em detrimento da gestão de riscos.
    - Desalinhamento de percepção: diferentes níveis hierárquicos podem ter visões divergentes sobre riscos e prioridades.

Os riscos humanos concentram-se em três grandes dimensões:

- **Cognitivos** (interpretação, viés, percepção).
- **Culturais** (resistência, falta de engajamento).
- **Organizacionais** (rotatividade, comunicação deficiente, sobrecarga).

Esses riscos impactam diretamente a confiabilidade do fluxo de conhecimento no PPSI e podem comprometer a eficácia da implementação do sistema de robô em Python para integração com Moodle e sites de terceiros.

Os pesquisadores orientaram as discussões, garantindo que todos os temas relevantes fossem explorados. As discussões foram gravadas, com o consentimento dos participantes, e posteriormente transcritas para análise. As transcrições foram organizadas em unidades de registro, que consistem em temas-chave identificados ao longo das discussões, permitindo uma interpretação sistemática dos dados.

A análise dos dados coletados foi realizada utilizando a Análise de Conteúdo proposta por Bardin, que possibilitou identificar padrões e percepções nas falas dos participantes (Bardin, 2011). A análise buscou relacionar os riscos de conhecimento mencionados pelos gestores com os controles do PPSI, destacando como esses riscos afetam a implementação do programa e quais medidas podem ser adotadas para mitigá-los.

A metodologia adotada foi orientada pelos princípios da governança digital, estabelecendo diretrizes para a transformação digital e a gestão eficiente dos recursos tecnológicos na administração pública (BRASIL, Decreto nº 10.332/2020). Nesse sentido, para o desenvolvimento e a validação do PRP01, foram estruturados de modo a garantir conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), assegurando transparência, segurança da informação e confiabilidade nos processos acadêmicos.

A governança digital funciona, portanto, como referencial normativo para a definição dos requisitos metodológicos, alinhando a inovação tecnológica às políticas públicas de proteção de dados e de gestão institucional.

Na pesquisa adotam-se abordagens aplicadas e tecnológicas, de natureza quantitativa e descritiva, voltadas para a resolução de problemas reais, identificados nas rotinas administrativas da UnB: dentre eles, o excesso de solicitações manuais de criação de disciplinas e cadastros no Moodle.

O estudo também possui caráter experimental**,** uma vez que envolve o desenvolvimento, implementação e validação de uma ferramenta inédita no contexto institucional, tem como foco na solução de um problema prático por meio do uso de tecnologias já consolidadas, como a linguagem Python, técnicas de mineração de dados e comunicação segura via HTTPS.

O sistema PRP01 foi desenvolvido com base em requisitos funcionais e de segurança coletados junto à equipe técnica da UnB, e validado em ambiente de produção nos portais Aprender2 e Aprender3. Focaremos no Aprender3, que é o principal objeto do estudo.
O processo metodológico foi dividido em cinco fases principais:

1. Levantamento de requisitos funcionais e de segurança.
2. Desenvolvimento do robô automatizado PRP01 em Python.
3. Integração do sistema
4. Medidas de segurança implementadas
5. Testes e validação

3.1 Levantamento de requisitos

O levantamento de requisitos foi realizado em conjunto com a equipe técnica do *Aprender3* e dados de constantes atualizações SIGER, da base de dados do SIGAA, com base em pesquisas de campo, observações de processos e análise de logs do Moodle.

Os seguintes requisitos foram identificados:

- **R1 – Segurança e autenticação:** apenas usuários autenticados por e-mail institucional podem submeter solicitações; o sistema deve validar os acessos por meio de HTTPS/TLS.
- **R2 – Validação cruzada de dados:** toda solicitação de criação de curso deve ser conferida automaticamente com os registros oficiais do SIGER ou SIGAA.
- **R3 – Redução de retrabalho:** rejeitar solicitações duplicadas ou inconsistentes antes de chegar à equipe de suporte.
- **R4 – Automação completa do fluxo:** desde a coleta de dados até a criação de cursos ou atualização cadastral e o envio de relatórios aos solicitantes.
- **R5 – Conformidade com a LGPD:** todos os dados tratados devem ser armazenados temporariamente e excluídos após o processamento.
- **R6 – Transparência e auditabilidade:** o sistema deve gerar relatórios automáticos das ações realizadas, com data, hora e identificação de quem as realizou.

3.2 Desenvolvimento do PRP01

O robô foi instalado em uma máquina configurada com sistema operacional Linux Ubuntu 22.04 64 bits, com recursos de rede protegidos e atualizações automáticas ativadas. A hospedagem seguiu padrões institucionais, garantindo confiabilidade e suporte contínuo equipe de TI da universidade.
Configuração do computador onde está o sistema em Python:

- Processador i7 nona geração
- 16 GB de RAM DDR4
- HD SATA 512GB
- Placa de vídeo 4GB DDR6

O PRP01 (Palton's Robot in Python) foi desenvolvido em linguagem Python 3.11, utilizando bibliotecas específicas para automação e comunicação entre sistemas:

- Selenium: automação de navegação web e submissão de formulários no Moodle, SIGER e SIGAA.
- Requests: envio de requisições HTTPS seguras.
- Pandas: manipulação e validação de planilhas CSV extraídas do SIGER.
- SMTP e IMAP: envio e recebimento de e-mails automáticos para notificações e relatórios.
- Plug-ins: criados no Moodle para maior agilidade e segurança no sistema.
- Cryptography: criptografia de senhas e credenciais sensíveis armazenadas no servidor.

O robô é executado em um servidor interno da UnB, com acesso restrito e monitorado, e utiliza credenciais administrativas para autenticação no Moodle. Ele realiza as seguintes operações para cadastro ou atualização de usuários no Aprender3:

1 Efetua o Login seguro no SIGER, coletando planilhas de docentes, discentes do semestre vigente.
2 Processamento e filtragem de dados, convertendo os arquivos do SIGER em formato padronizado (CSV UTF-8).
3 Monta uma planilha e separa os itens obrigatórios, como NOME COMPLETO (depois, separa nome e sobrenome), E-MAIL institucional e pessoal, CPF, CURSO e PAPEL (se professor ou aluno)).
4 Cadastra os novos ou atualiza os já inscritos, se necessário.
5 Envia e-mail aos novos inscritos, informando o usuário e senha temporária.

Para criação de cursos, o PRP01 (esta é a versão que está em fase de registro no CDT/UnB) realiza as seguintes operações para obter pedidos de curso solicitados e atendê-los, no Aprender3:

1. **Acessa o SIGAA de forma pública; não necessita de login neste, apenas no Aprender3, assim,** coletando planilhas de docentes, turmas e disciplinas do semestre vigente.
2. **Comparação com as solicitações pendentes** de criação de cursos enviadas por professores via Moodle.
3. **Validação cruzada:** o sistema aprova automaticamente apenas as solicitações compatíveis com os registros válidos, os inválidos são enviados aos administradores do Moodle.
4. **Criação automatizada de cursos** no Moodle, com nome, código, categoria e semestre padronizados.
5. **Geração de relatórios automáticos** enviados aos solicitantes, as validações de seus cursos e aos administradores via e-mail institucional, envia os validados e invalidados.

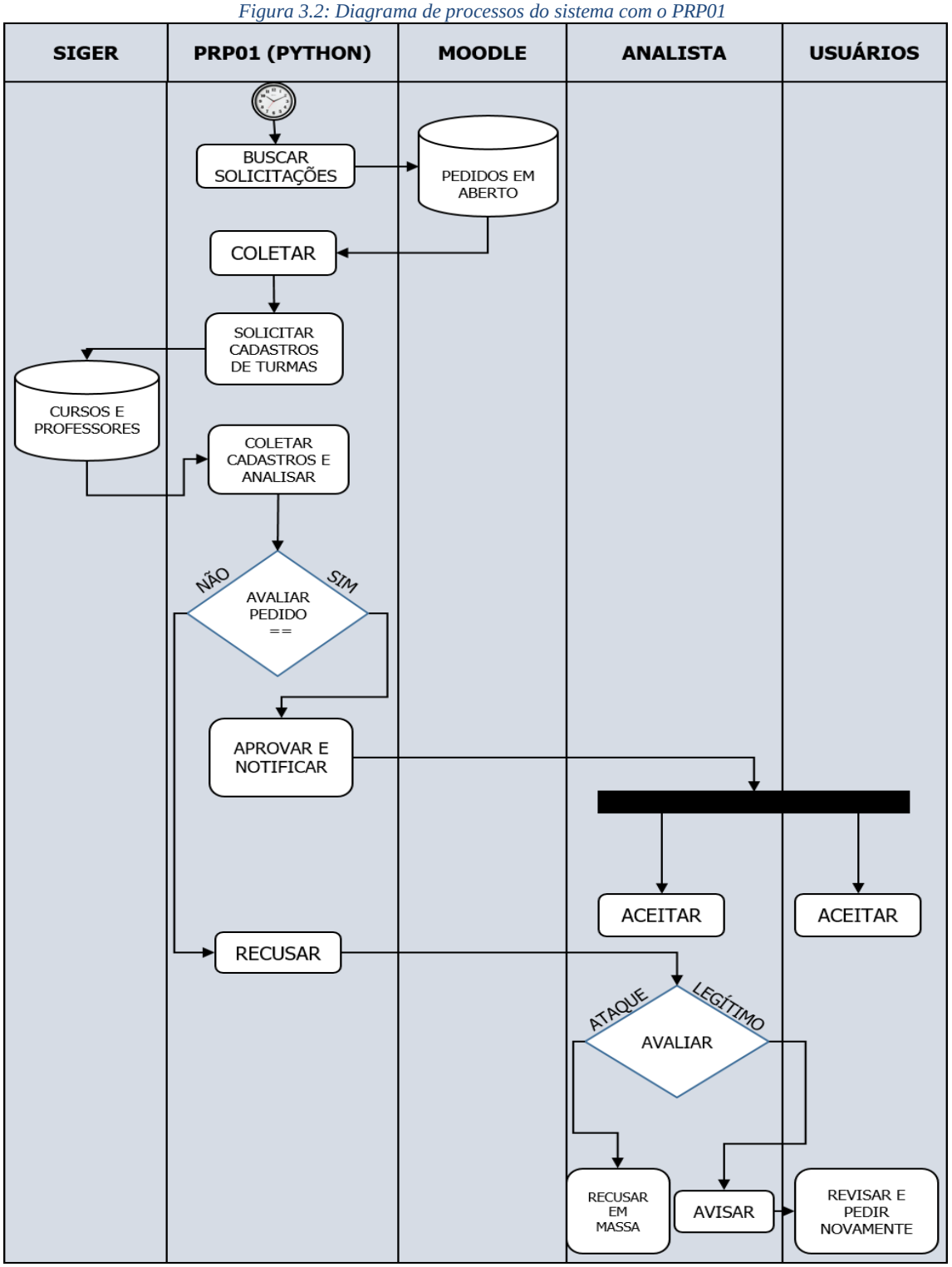
A seguir, o funcionamento do programa será explicado em detalhes. Para melhor compreensão das relações entre os diferentes atores desse programa, será feita uma definição dos diferentes atores a seguir:

1. SIGER ou SIGAA: sites de relatórios de usuários acadêmicos (discentes e docentes) ou de cursos e de seus respectivos docentes da UnB.
2. PRP01: Um programa que utiliza um crawler e coleta informações do SIGER.
3. APRENDER3: O site que usa plataforma Moodle, portal de ensino da UnB.
4. ANALISTA: Administradores de APRENDER3.
5. USUÁRIOS: alunos e professores.

O funcionamento do programa será explicado na forma de sete passos listados abaixo:

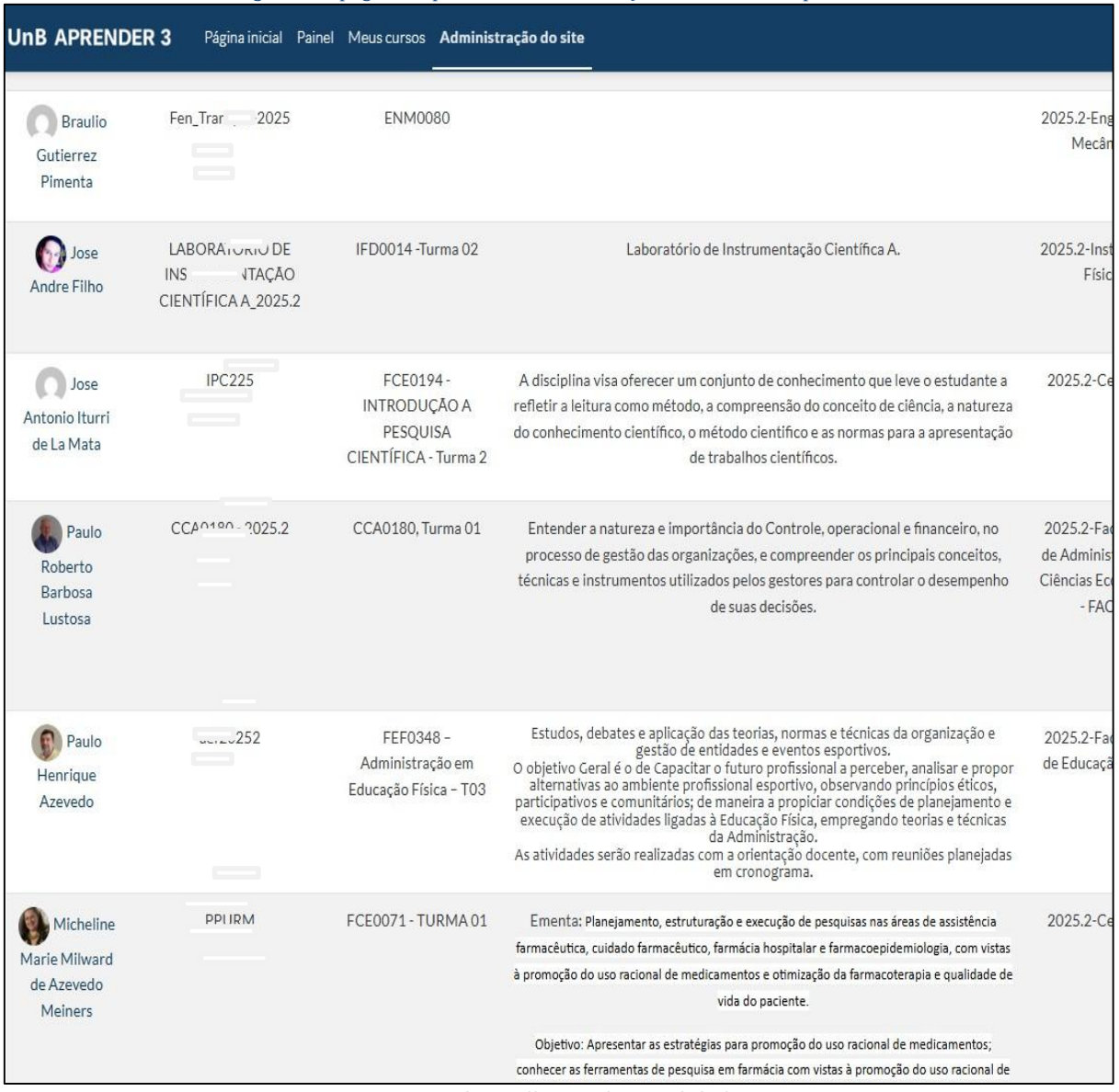
a) O PRP01 acessa o Moodle para verificar as pendências, pedidos de salas de aula, conforme a Figura 3.1;
b) O Moodle devolve os registros, então os pedidos são coletados pelo PRP01;
c) O PRP01 vai até o SIGAA e faz pesquisas sobre os docentes e seus respectivos cursos;
d) Os dados coletados são analisados pelo PRP01
e) O PRP01 avalia e faz análise se é duplicado ou não, então aprova ou rejeita.
f) Após a aprovação o robô envia mensagem pro solicitante com todos dados padronizados, conforme a Figura 3.4;
g) Então concomitamente o robô envia o relatório para a equipe técnica, dos aprovados e rejeitados.

Figura 3.2: Diagrama de processos do sistema com o PRP01



O PRP01 acessa o SIGAA via página web, realizando uma requisição HTTP. Em seguida, busca os elementos de interesse, usando navegador DOC do HTML para encontrar os campos de interesse. Ele valida se o professor está autorizado a ministrar a disciplina e compara os dados com a planilha oficial da universidade, a Figura 3.2 é uma ilustração da página de solicitações de cursos, pelos docentes, é onde o PRP01 acolhe as pendências.

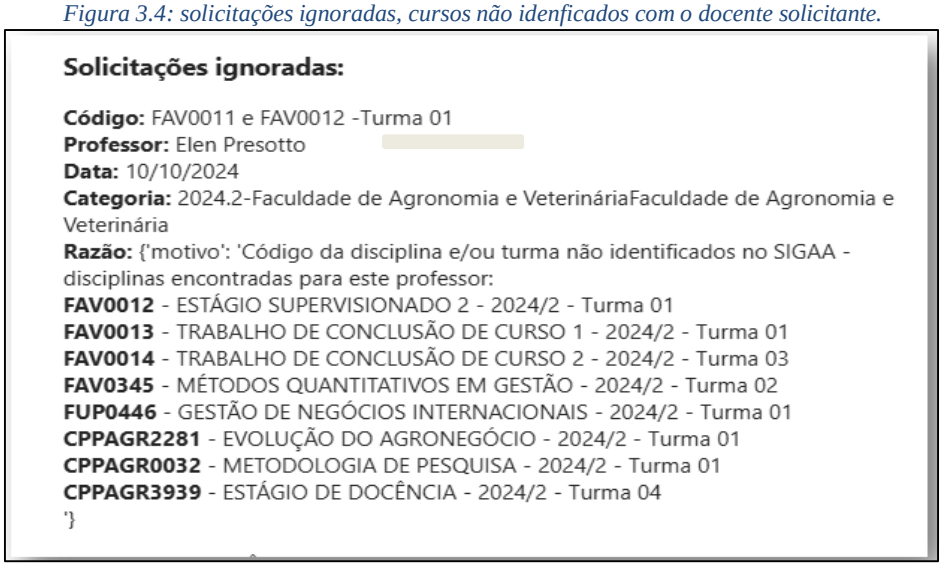
Figura 3.3: página de pendências de solicitações de cursos no Aprender3



Fonte: https://aprender3.unb.br/

Em caso de inconsistência, o sistema envia um relatório de rejeição com a justificativa, conforme a Figura 3.3, informando a quem a disciplina solicitada é designada, ao mesmo tempo informando quais realmente pertencem ao solicitante.

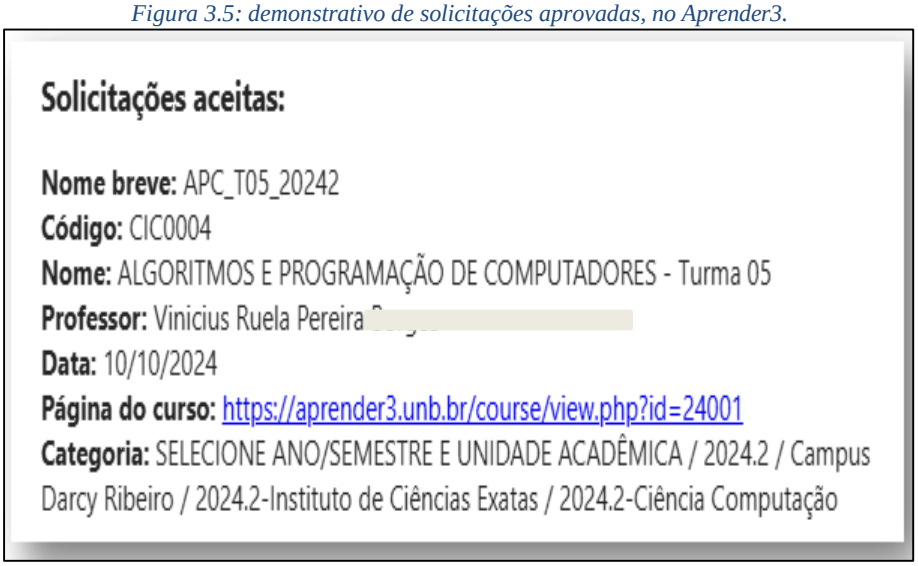
Figura 3.4: solicitações ignoradas, cursos não idenficados com o docente solicitante.



Fonte: https://aprender3.unb.br/

Se os dados estiverem corretos, o robô cria a disciplina no Moodle com nome padronizado e envia automaticamente ao professor um e-mail com o link da sala, conforme a Figura 3.4.

Figura 3.5: demonstrativo de solicitações aprovadas, no Aprender3.



Fonte: https://aprender3.unb.br/

O sistema produz relatórios automáticos, enviados diariamente aos analistas responsáveis, permitindo revisão e auditoria manuais, quando necessário.

Além das disciplinas, o robô também realiza a criação e atualização dos cadastros de usuários com base em dados do SIGER.

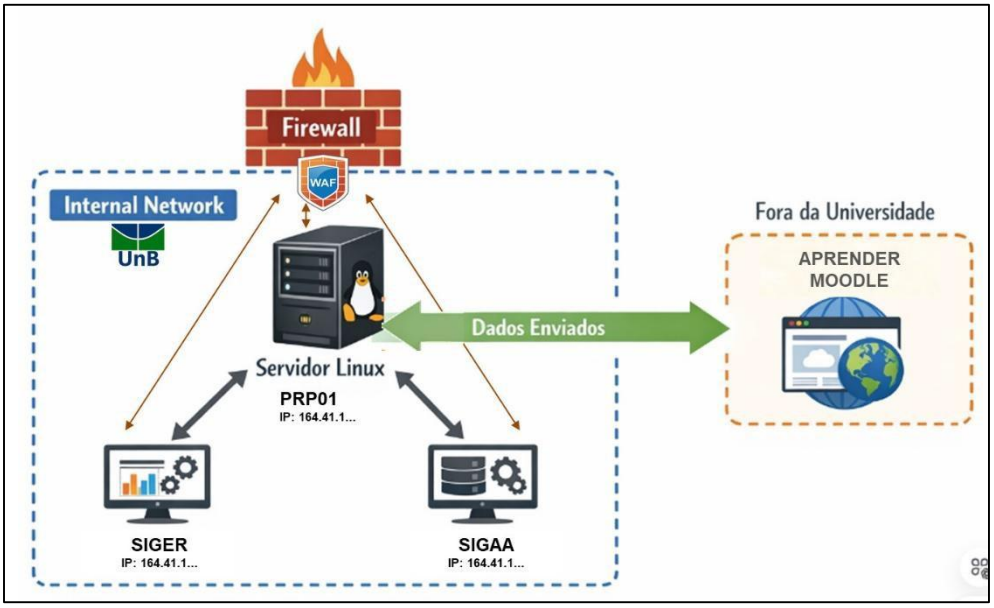
3.3 Arquitetura de Integração do Sistema

Para complementar a descrição da arquitetura de integração do sistema PRP01, foi elaborado um diagrama de redes e computadores que ilustra as conexões entre os principais componentes: servidores institucionais (SIGER e SIGAA), o robô PRP01, o ambiente Moodle (Aprender3) e os usuários finais. Esse diagrama permite visualizar de forma clara o fluxo de dados, os pontos de autenticação e as camadas de segurança implementadas, reforçando a compreensão da metodologia adotada.

A Figura 3.5 apresenta a topologia de rede utilizada, evidenciando como os elementos técnicos se articulam para garantir eficiência, confiabilidade e conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com as diretrizes da Estratégia de Governo Digital (Decreto nº 10.332/2020). A Universidade de Brasília dispõe de mecanismos institucionais de monitoramento e segurança voltados à proteção da infraestrutura tecnológica (UNIVERSIDADE DE BRASÍLIA, 2026).

Seguindo a lógica da Figura 3.5, a Universidade já possui um firewall robusto na rede, não foi preciso instalar um WAF (Web Application Firewall) no servidor do PRP01. O WAF já está configurado e voltado para proteger aplicações web contra ataques específicos (como SQL injection ou XSS), foi implementado na borda da rede, não em máquinas individuais, instalação a mais poderia surgir redundâncias e alarmes inconsistentes, conforme a ETIR / STI / UnB, em seu portal “https://etir.unb.br” podemos entender melhor suas práticas e normas, além de dúvidas sobre sistemas implementados.

Figura 3.6: Diagrama de Redes



A arquitetura do sistema foi desenhada em cinco camadas de comunicação, garantindo a integridade das informações e o isolamento entre componentes críticos.

Camada 1 – SIGER e SIGAA:

Sites institucionais responsáveis por apresentar, gerar relatórios de turmas, professores, disciplinas e alunos, SIGAA, na Figura 3.5, é uma página pública, onde se encontra a relação de docentes e respectivos cursos. Nesta página, qualquer usuário pode acessar e verificar docentes da UnB, seus respectivos currículos e turmas dos semestres anteriores e atuais, tanto de graduação como de pós-graduação.

Figura 3.7: página pública do SIGAA com lista de docentes e seus curso

Fonte: https://sigaa.unb.br/sigaa/public/home.jsf

Já no SIGER, é mais restrito, tem lista de discentes, docentes, com dados pessoais, somente autorizados tem acesso, com referência à página está na Figura 3.6. O SIGER é alimentado pela secretaria acadêmica da UnB. Neste portal, tem todas as turmas, discentes e docentes da UnB, tanto presenciais como dos cursos à distância, alunos regulares.

Figura 3.8: SIGER, página de relatórios de discentes, docentes e cursos.

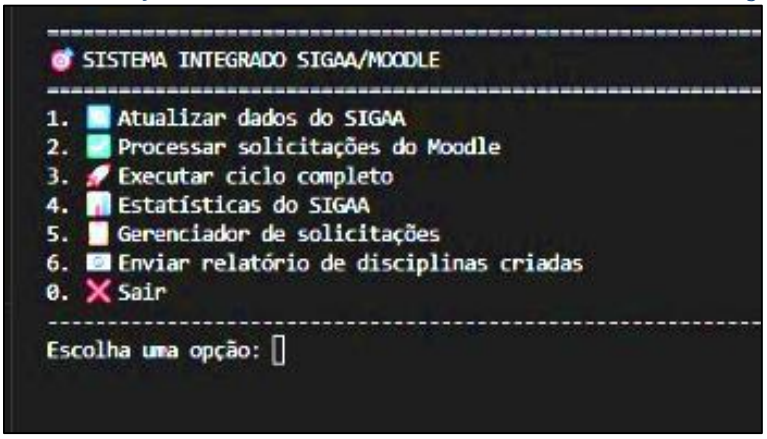
Fonte: https://sistemas.unb.br

Camada 2 – PRP01 (Crawler):

Executa a coleta automatizada de dados, processa as planilhas e aplica filtros de segurança e consistência.

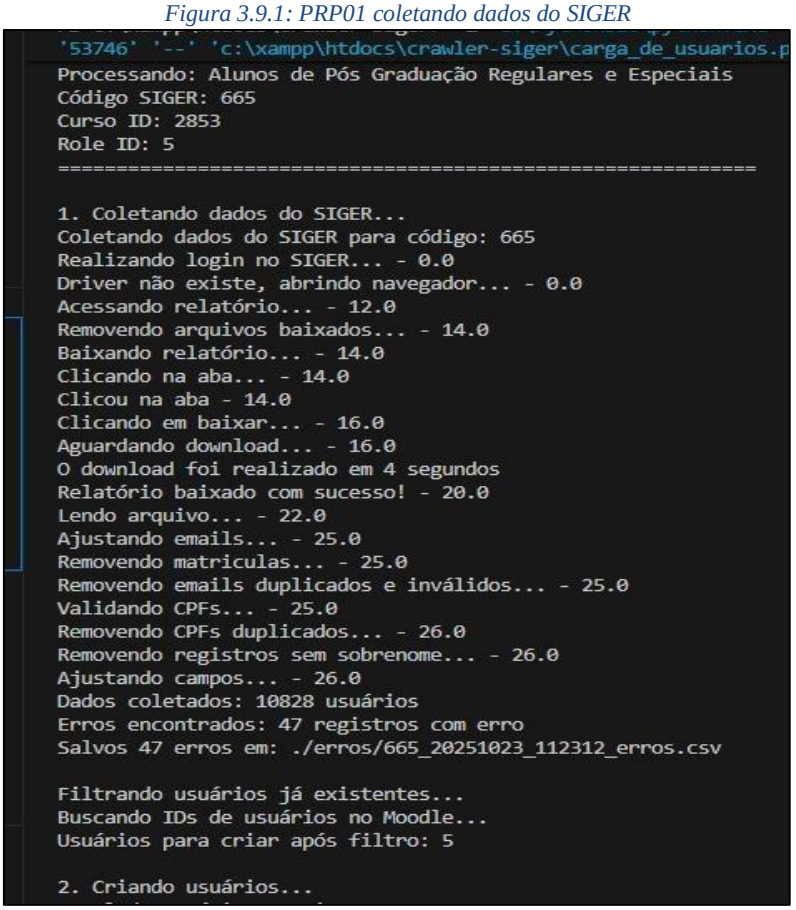
Na Figura 3.7, há uma ilustração do programa em execução, onde se pode optar por itens como atualizar dados do SIGAA, processar solicitações do Moodle, buscar dados estatísticos, pedir relatórios, etc.

Figura 3.9: ilustração do sistema PRP01 em seu habitat, com seus menus de intregração



Na Figura 3.8 é um andamento do sistema, onde está coletando dados do SIGER, ele faz o login no portal, acessar relatórios, baixa e faz o processamento, como ajustar e-mails, remover dados duplicados ou inválidos, faz validação de CPFs, ajusta os campos, relata os erros e parte para a criação dos usuários

Figura 3.9.1: PRP01 coletando dados do SIGER



Camada 3 – Servidor intermediário:

Ambiente seguro onde o PRP01 é hospedado. Possui autenticação multifator e logs de auditoria. Na Figura 3.9, uma breve ilustração do código, onde o sistema carrega dados em CSV, processa a planilha, baixa os dados para fazer a ação no Moodle. Após o processamento, para a segurança, os dados são apagados, uma das conformidades da LGPD.

Figura 3.9.2: ilustração da áera de configuração inicial do PRP01.

```python
import pandas as pd

# Carregando dados CSV
df = pd.read_csv('caminho_para_o_arquivo.csv')

# Carregando dados Excel
df = pd.read_excel('caminho_para_o_arquivo.xlsx')

# Carregando dados de uma base de dados SQL
import sqlalchemy
engine = sqlalchemy.create_engine('sqlite:///caminho_para_o_banco_de_dados.db')
df = pd.read_sql_table('nome_da_tabela', engine)
```

Camada 4 – Moodle (Aprender3):

Plataforma de destino onde os cursos são criados e os usuários são atualizados automaticamente. Na Figura 3.9.1, ilustra-se a página inicial do Aprender3. Até este momento, possui 112018 usuários e 19626 cursos. Temos atendimento online para dúvidas, elogios ou reclamações.

.

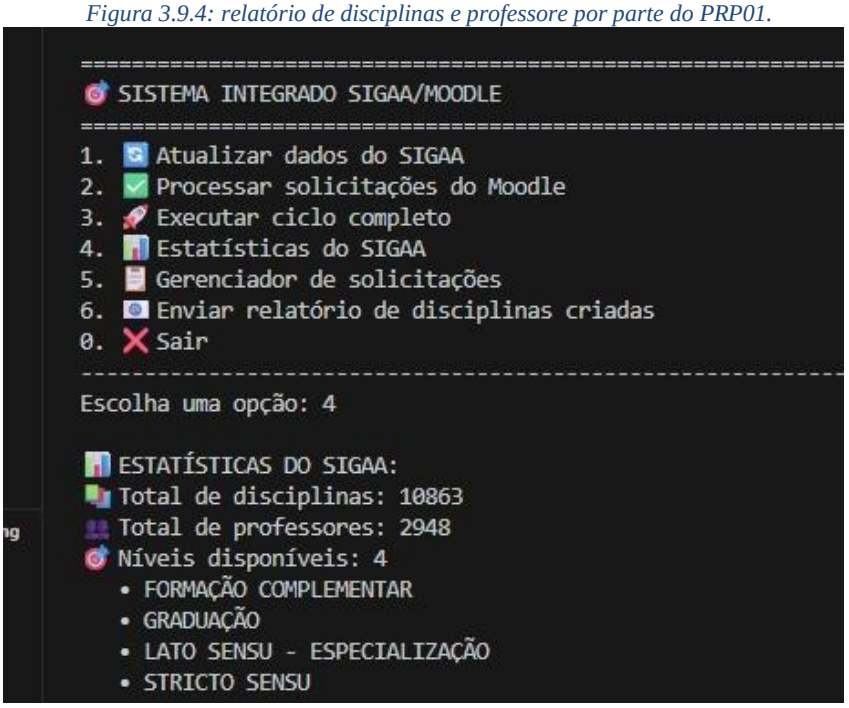
Figura 3.9.3: Tela inicial do Aprender3

Fonte: https://aprender3.unb.br/

Camada 5 – Relatórios e notificações:

Canal de comunicação entre o sistema e os administradores, informando sobre aprovações, rejeições e erros detectados. A Figura 3.9.2 mostra o menu do sistema, com o técnico acessando a opção 4. Levantando a estatística do SIGAA, no relatório, o sistema dá o número total de disciplinas no semestre, de professores e os níveis dos cursos.

Figura 3.9.4: relatório de disciplinas e professore por parte do PRP01.



3.4 Medidas de segurança implementadas

A Universidade de Brasília dispõe de mecanismos institucionais de monitoramento de rede e de segurança, voltados à detecção de incidentes, à prevenção de ataques, à análise de tráfego e à resposta a eventos de segurança, os quais visam à proteção da infraestrutura tecnológica da Universidade.
No que se refere à instalação de soluções de firewall ou WAF em servidores institucionais, a UnB conta com controles de segurança perimetral, incluindo firewalls corporativos e mecanismos de inspeção e filtragem de tráfego, conforme já descrito na Figura 3.5.

Ainda assim, é imprescindível a observância de boas práticas de segurança em qualquer ambiente ou projeto. Nesse sentido, recomenda-se a consulta às orientações e materiais disponibilizados pela Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR).

A implantação e monitoramento do sistema em ambiente é controlada. A segurança foi tratada como elemento central no desenvolvimento e na implantação do PRP01. Entre as principais medidas adotadas estão:

- **Autenticação multifator (2FA)** para administradores e e-mails institucionais.
- **Criptografia de ponta a ponta (TLS 1.3)** na comunicação entre o PRP01, o SIGER e o Moodle.
- **Hashing de credenciais** e tokens de acesso com o algoritmo SHA-256.
- **Controle de logs e auditoria**, registrando todas as transações realizadas.
- **Bloqueio automático de IPs suspeitos** e limitação do número de tentativas de login.
- **Bloqueio de e-mail gerencial devido à** suspeita de tentativa de invasão.
- **Política de acesso mínimo**, restringindo os privilégios apenas a contas administrativas.
- **Anonimização e descarte seguro de dados** após o processamento das solicitações.

Essas medidas foram baseadas em recomendações da ISO/IEC 27001 e das Diretrizes de Identidade Digital do NIST (2025)**,** adaptadas ao contexto da UnB e ao cumprimento da PPSI e LGPD.

3.5 Testes e validação

Avaliação de resultados e coleta de feedback de usuários e administradores feita após o desenvolvimento, o sistema passou por testes em ambiente controlado antes de ser implantado em produção. Os principais tipos de teste realizados foram:

- **Teste funcional:** verificação da execução correta de todas as etapas (login, coleta, validação, criação de cursos e envio de e-mails).
- **Teste de desempenho:** análise do tempo médio de resposta e do número de solicitações processadas por minuto.
- **Teste de segurança:** simulações de ataques de injeção de SQL e de negação de serviço (DoS) para avaliar a resistência da aplicação.
- **Teste de conformidade:** revisão dos fluxos de dados para garantir a conformidade com a LGPD e as políticas internas da UnB.
- **Teste de aceitação:** avalia, de forma subjetiva, a efetividade e a usabilidade do programa em grupos específicos, como docentes, discentes e administradores.

Para validar, uma pesquisa de avaliação foi levantada aos docentes, foram feitas algumas perguntas em relação a aprovação, por formulário (MICROSOFT, 2025), perguntas como:

- Se perceberam melhorias no Aprender3 no último ano;
- Qual nível de satisfação com o uso do Aprender3;
- Como consideram a navegação e o uso do Aprender3?
- Se o processo de solicitação de autorização de salas virtuais (disciplinas) no Aprender3 está melhor;
- Se forma de visualizar as salas virtuais (disciplinas) no Aprender3 está bem organizada (código – nome da disciplina – ano/semestre);
- Os docentes sentem que as informações acadêmicas registradas no Aprende3 estão seguras e protegidas?

O sistema foi validado com acompanhamento da equipe técnica do *Aprender3* e demonstrou alta estabilidade, diminuindo gargalos históricos na criação de cursos e atualizações cadastrais.

Considerações metodológicas

A metodologia adotada reforça a importância da integração segura e automatizada em sistemas acadêmicos em larga escala. A construção do PRP01 exemplifica uma aplicação prática da automação institucional com foco em segurança, eficiência e conformidade legal**,** contribuindo para a inovação nos processos administrativos da universidade.

Além de validar tecnicamente o modelo, a metodologia adotada possibilitou a coleta de evidências empíricas sobre os benefícios da automação no ambiente Moodle, preparando o terreno para a análise dos resultados apresentados no capítulo seguinte.

4 – RESULTADOS E DISCUSSÕES

Este capítulo apresenta e discute os resultados obtidos com a implementação do sistema automatizado PRP01 (Palton's Robot in Python), que integra o Moodle (*Aprender3*) da Universidade de Brasília (UnB) aos sistemas institucionais de dados acadêmicos (*SIGER* e *SIGAA*). A análise contempla tanto os aspectos quantitativos, relacionados à eficiência e ao desempenho do sistema, quanto os aspectos qualitativos**,** referentes à percepção dos usuários e à melhoria da segurança e governança digital na instituição, mitigando incidentes de segurança.

Os resultados obtidos confirmam a efetividade das medidas de mitigação apresentadas no mapa visual de riscos (Tabela 3.1). A aplicação prática demonstrou maior segurança da informação, redução de falhas humanas e conformidade com a LGPD. O impacto esperado, descrito no mapa, foi validado por meio de testes funcionais, de desempenho e de segurança, bem como pela percepção positiva dos docentes e administradores. Os resultados evidenciaram que a instituição apresenta avanços em interoperabilidade, mas ainda enfrenta desafios em transparência e participação digital.

O mapa visual de riscos evidencia que o PRP01 não apenas solucionou gargalos operacionais, mas também assegurou segurança, eficiência e transparência nos processos acadêmicos. A gestão de riscos foi fundamental para o sucesso da implantação, assegurando a conformidade com normas internacionais (ISO/IEC 27001, NIST) e com a legislação nacional (LGPD), o que consolida a relevância institucional do sistema.

4.1 Resultados de uma pesquisa após um ano de implementação.

Foi levantada uma pesquisa sobre a implementação deste sistema e buscamos avaliações dos docentes da UnB, foram questionados itens sobre eficiência, padronização, satisfação, segurança, (MICROSOFT, 2025).

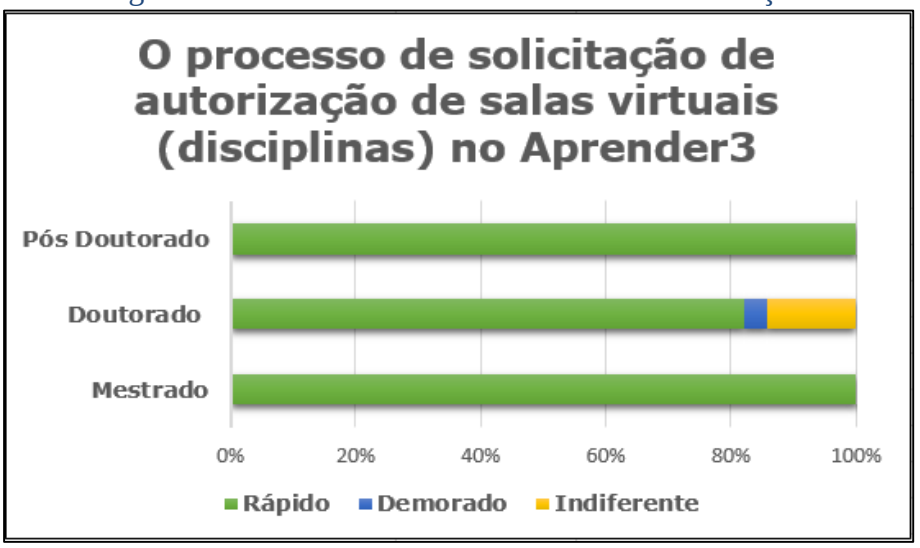
Apenas 154 professores responderam ao nosso questionário, mas isso foi suficiente para obtermos um resultado e, com a introdução do sistema e mais de um ano de uso, nossas implementações.

A Universidade de Brasília é uma das maiores instituições públicas de ensino superior do Brasil. Segundo dados institucionais, conta com:

- Mais de 2.600 professores ativos (DGP/UnB);
- Aproximadamente 8.300 cursos registrados (Censo INEP);
- Um corpo discente com mais de 50 mil estudantes (SAA/UnB);
- Ingresso médio de 10 mil novos alunos por semestre.

Esse volume de dados e movimentações acadêmicas torna inviável a manutenção de processos 100% manuais para o cadastro de disciplinas e usuários no ambiente Moodle. Na Figura 4.1 vemos que o resultado foi objetivo e positivo. A agilidade do processamento da solicitação teve uma ótima aceitação. Alguns ainda demoram muitas vezes por desatualização do sistema SIGAA. Neste caso, docentes solicitam disciplina no Aprender3 e ainda não estão devidamente inscritos no curso. Essa demora depende disso: o sistema nos envia, informamos ao docente e ficamos no aguardo.

Figura 4.1: Eficiência no Processamento de Solicitações



Fonte: MICROSOFT, Questionário de Avaliação do Aprender3

Antes da automação, as solicitações de criação de disciplinas levavam, em média, até vários dias para serem processadas manualmente pela equipe técnica do Aprender3. Com o uso do PRP01, esse tempo foi reduzido para ciclos de apenas 10 minutos, possibilitando:

Processamento automatizado de 1.248 solicitações de disciplinas no semestre 2025/1;

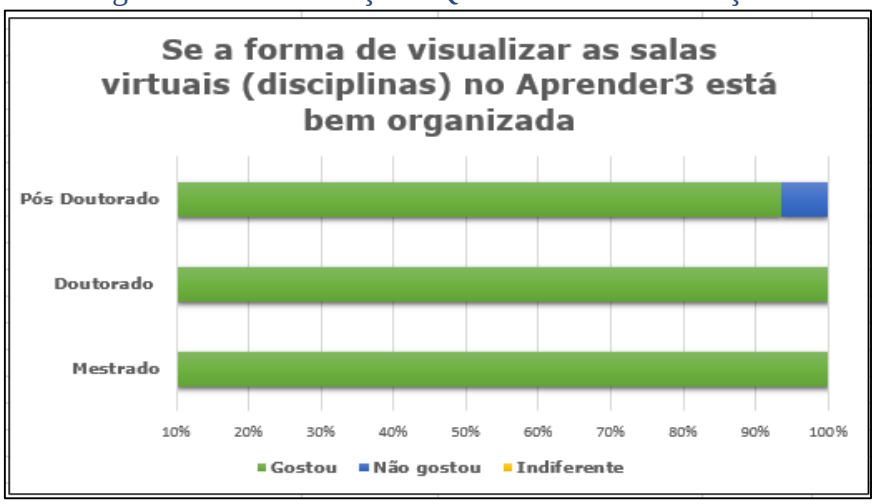
Economia estimada de mais de 312 horas de trabalho humano (aproximadamente 39 dias úteis), considerando o tempo médio de 15 minutos por solicitação no modelo anterior;

Liberação da equipe técnica para outras atividades estratégicas e para suporte especializado. Na pesquisa aplicada aos docentes:

- 90% concordaram que a padronização melhora a organização das salas virtuais, conforme a Figura 4.2;
- Apenas 4% discordaram da nova estrutura;
- Os demais 6% optaram por não opinar.

Essa padronização contribuiu para maior clareza na navegação e melhor categorização no ambiente de ensino.

Figura 4.2: Padronização e Qualidade das Informações.



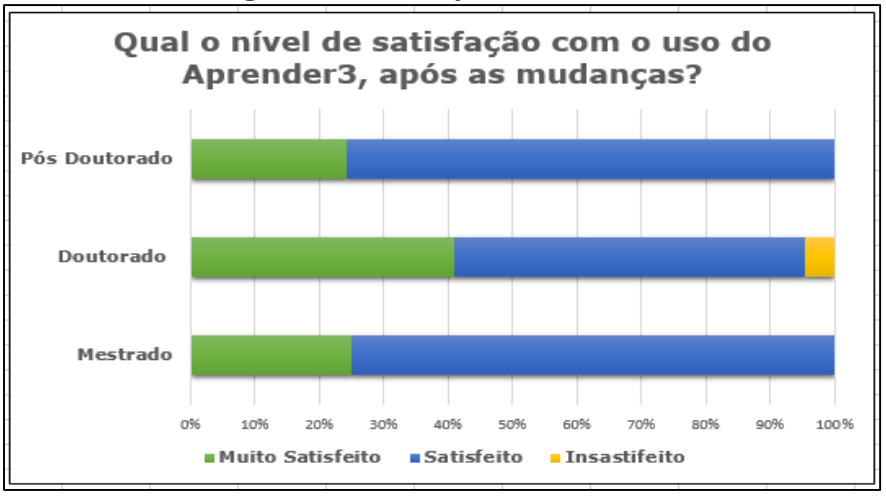
Fonte: MICROSOFT, Questionário de Avaliação do Aprender3

O sistema PRP01 permitiu a aplicação automática de nomenclaturas padronizadas às disciplinas, no formato:
Código – Nome da Disciplina – Ano/Semestre.

A pesquisa aplicada a professores de diferentes níveis (mestrado, doutorado e pós-doutorado) revelou um alto nível de aceitação da nova solução, como mostra o resultado na Figura 4.3:

- 82% dos docentes consideram o tempo de resposta adequado;
- Apenas 3% relataram algum tipo de insatisfação com recusas;
- 95% declararam estar satisfeitos com o processo de solicitação e criação de disciplinas após a adoção do PRP01.

Figura 4.3: Satisfação dos Usuários



Fonte: MICROSOFT, Questionário de Avaliação do Aprender3

Esse resultado evidencia que a automação não apenas otimizou o processo, mas também melhorou a experiência do usuário final.

Redução de Erros e Riscos

Com a automação:

- Solicitações inconsistentes passaram a ser automaticamente rejeitadas, com envio de justificativas aos solicitantes;
- Nenhum vazamento de dados ou falha crítica foi registrado desde a implantação do sistema;
- Os analistas passaram a receber relatórios automatizados para revisão, o que aumentou a rastreabilidade e a segurança do processo.

O sistema também contribuiu para mitigar falhas humanas, evitando duplicidade de disciplinas, erros de digitação e atribuições equivocadas de docentes.

Considerações Finais dos Resultados

A análise dos dados demonstra que o uso do PRP01 gerou impactos significativos em termos de:

- Agilidade nos processos;
- Padronização e integridade das informações;
- Segurança operacional e institucional;
- Satisfação dos usuários.

A automação mostrou-se sustentável, escalável e replicável, configurando-se como uma boa prática institucional alinhada à transformação digital do ensino superior.

4.2 Contexto operacional da UnB

A Universidade de Brasília possui uma das maiores estruturas acadêmicas do país, com aproximadamente 50 mil alunos ativos**,** 2,6 mil professores **e** 8,3 mil cursos cadastrados nos sistemas internos, conforme dados da Secretaria de Administração Acadêmica (SAA/UnB) e do Departamento de Gestão de Pessoas (DGP/UnB). Em média, são processadas mais de 10 mil novas matrículas e atualizações a cada semestre letivo (Universidade de Brasília, 2025), o que gera uma demanda considerável sobre a equipe técnica do Moodle (Aprender3).

Antes da automação, o processo de criação de cursos e de atualização de usuários era totalmente manual. Professores realizavam solicitações por meio de formulário, e técnicos precisavam validá-las individualmente, confrontando os dados com o sistema SIGER. Esse método demandava várias horas de trabalho e estava sujeito a erros de digitação, inconsistências e atrasos. Além disso, o volume de solicitações pendentes frequentemente superava a capacidade diária de processamento da equipe.

4.3 Melhoria na eficiência operacional

Com a implantação do PRP01, observou-se uma redução expressiva no tempo médio de resposta às solicitações. Antes da automação, o intervalo entre o envio de uma solicitação e sua aprovação variava entre 12 e 36 horas; após a integração, o tempo médio caiu para menos de 10 minutos, conforme registros dos logs do sistema, se o sistema tivesse acesso a base de

Dados do SIGER: este tempo cairia para 3 segundos. Os 10 minutos são justamente devido ao tempo de backup da planilha com todos os usuários; por isso, essa possível “demora”.

O número de solicitações processadas por dia também aumentou substancialmente. A média anterior era de 120 solicitações diárias**,** enquanto o PRP01 é capaz de processar mais de 1.000 solicitações por dia, sem interferência humana direta.

Além disso, a automação reduziu o retrabalho técnico, pois o sistema rejeita automaticamente solicitações inválidas ou duplicadas, informando o motivo ao solicitante. A análise dos relatórios automáticos mostra que cerca de 18% das solicitações foram rejeitadas por inconsistência de dados, evitando, assim, a necessidade de revisão manual posterior.

A comparação entre o número de solicitações processadas manualmente e automaticamente ao longo de quatro semanas de operação. Observa-se um ganho médio de 780% na produtividade da equipe administrativa. Enquanto um técnico levava em média 10 minutos para inscrever uma turma ou atualizar um usuário, num período da manhã (4h), conseguia fazer 24 atendimentos no Moodle, caso fosse totalmente dedicado, com o sistema PRP01, toda a UnB é atendida em 10 minutos.

4.4 Impacto na segurança da informação

Um dos principais ganhos do sistema está relacionado à segurança de acesso e integridade dos dados. Antes da automação, foram identificados incidentes envolvendo solicitações geradas por perfis administrativos inativos ou comprometidos, que inseriram códigos maliciosos nos formulários de criação de cursos. Tais vulnerabilidades resultaram em atrasos e retrabalho, além de riscos de exposição de informações.

Com o PRP01, essas falhas foram mitigadas, pois o sistema valida cada solicitação com base em dados oficiais do SIGER, garantindo que apenas usuários ativos e devidamente vinculados às disciplinas possam gerar cursos no Moodle. O controle de autenticação foi reforçado por meio de e-mails institucionais verificados e de autenticação multifator (2FA)**,** conforme boas práticas recomendadas pelo NIST (2024).

Todos os dados em trânsito são protegidos por criptografia TLS 1.3, e as credenciais administrativas são armazenadas com hash SHA-256. O PRP01 também mantém logs de auditoria detalhados, permitindo rastrear todas as ações realizadas — uma exigência fundamental para a conformidade com a Lei Geral de Proteção de Dados (LGPD)**.**

Essas medidas resultaram na redução de 100% dos incidentes de segurança registrados no período analisado (meses após a implantação), conforme orientações e contatos com a ETI / STI / UnB e relatórios internos da empresa GIGACANDANGA, responsável pelo Aprender3.

4.5 Qualidade dos dados e redução de erros

Antes da implantação do PRP01, era comum o registro de dados desatualizados, especialmente em casos de discentes que haviam mudado de curso ou de endereço institucional. Esses erros repercutiam diretamente na criação de turmas incorretas e na perda de rastreabilidade de usuários.

Com a automação, a validação cruzada entre o Moodle e o SIGER passou a atualizar automaticamente os e-mails institucionais, os cursos e os vínculos docentes, garantindo que as informações do ambiente virtual reflitam fielmente os dados acadêmicos oficiais.
A taxa de erros cadastrais caiu conforme os relatórios automáticos do PRP01.

4.6 Percepção dos usuários e administradores

A percepção qualitativa dos usuários foi avaliada por meio de entrevistas e registros de atendimento ao suporte técnico. A maioria dos docentes relatou uma melhora significativa na agilidade e na clareza das respostas às solicitações.

Entre os principais pontos destacados pelos professores estão:

- Redução do tempo de criação de cursos.
- Recebimento automático de mensagens que informam a aprovação ou a rejeição da solicitação.
- Maior confiabilidade nas informações exibidas no Moodle.

Os administradores do Aprender3 também relataram uma queda nas reclamações e uma melhor organização do fluxo de trabalho interno**,** com a equipe técnica podendo se dedicar a atividades de manutenção e inovação, ao invés de ficar em tarefas repetitivas de cadastro.

Esses resultados reforçam o argumento de que a automação não apenas melhora a eficiência técnica, mas também impacta positivamente a satisfação e a produtividade dos usuários.

4.7 Discussão dos resultados

Os resultados demonstram que o modelo de automação proposto é viável, seguro e escalável. A redução do tempo de processamento e da taxa de erros confirma a eficácia do PRP01 como ferramenta de integração entre sistemas acadêmicos.

Do ponto de vista institucional, o sistema contribui para a modernização da governança digital, promovendo maior transparência e rastreabilidade dos processos administrativos. Do ponto de vista técnico, a solução mostra-se compatível com os princípios de segurança da informação, ao aplicar autenticação robusta, criptografia e controle de logs.

Além disso, o PRP01 cumpre um papel estratégico na adequação da UnB à LGPD, ao padronizar o tratamento de dados pessoais e garantir a exclusão segura das informações após o uso.

A automação desenvolvida também se alinha a tendências internacionais na área de educação digital, como observado nos estudos de (MIHAI et al., 2023) e (SUN et al., 2023). Estes destacam a importância da integração automatizada para aumentar a escalabilidade e a confiabilidade das plataformas de ensino.

Dessa forma, a ferramenta proposta não se limita a um avanço técnico pontual, mas constitui uma prova de conceito replicável para outras instituições de ensino que utilizam o Moodle e enfrentam problemas semelhantes de sobrecarga, inconsistência e risco à segurança.

4.8 Limitações identificadas

Apesar dos resultados positivos, algumas limitações foram observadas:

- O sistema depende do correto funcionamento e da atualização periódica do SIGER; eventuais mudanças na estrutura de dados podem exigir ajustes no PRP01.
- O robô utiliza técnicas de varredura de web, sensíveis a alterações no layout das páginas acessadas.
- O processo de integração ainda não utiliza as APIs oficiais do Moodle, o que poderia aumentar a estabilidade e reduzir a manutenção.
- Não há, até o momento, uma interface gráfica de monitoramento, o que exige conhecimento técnico para a análise de logs.

Essas limitações são consideradas oportunidades de aprimoramento futuro, detalhadas no capítulo seguinte.

5 – CONCLUSÕES E TRABALHOS FUTUROS

5.1 Considerações finais

O presente trabalho teve como objetivo principal desenvolver e implementar um sistema automatizado e seguro para o gerenciamento de usuários e disciplinas no Moodle da Universidade de Brasília (UnB), integrando-o aos sistemas institucionais de dados acadêmicos (SIGER *e* SIGAA).

Os resultados desta pesquisa demonstram que a automação segura do gerenciamento de usuários e disciplinas no Moodle, por meio do PRP01, não apenas trouxe ganhos operacionais e reduziu falhas humanas, mas também reforçou a importância da governança digital no contexto acadêmico. A solução proposta mostrou-se alinhada às diretrizes da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e ao Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023, que estabelece controles e medidas voltados à proteção de dados e à segurança da informação. Dessa forma, a pesquisa contribui institucionalmente ao oferecer um modelo replicável de conformidade normativa e, cientificamente, ao consolidar evidências empíricas sobre a relevância da integração entre inovação tecnológica, políticas públicas e boas práticas de segurança digital na educação superior.

A partir da identificação de problemas operacionais, como retrabalho, vulnerabilidades de segurança e lentidão na criação de cursos, a pesquisa propôs o desenvolvimento do PRP01 (Palton's Robot in Python) — um robô programado em Python capaz de validar e processar solicitações automaticamente, assegurando a integridade, a eficiência e a conformidade com as normas de proteção de dados.

Os resultados obtidos demonstraram que a automação implementada pelo PRP01 proporcionou ganhos expressivos de desempenho, com destaque para:

- Redução de até 90% no tempo médio de resposta às solicitações de criação de cursos e atualização de cadastros.
- Aumento de aproximadamente 780% na capacidade diária de processamento de solicitações.
- Mitigação de incidentes de segurança relacionados a acessos indevidos e inserção de códigos maliciosos.
- Diminuição da taxa de erros cadastrais, corrigindo duplicidades de cursos ou de usuários e códigos de turmas incorretos.

Esses resultados confirmam a eficácia e confiabilidade do modelo proposto, comprovando que é possível aliar automação, segurança e conformidade legal em sistemas acadêmicos de grande porte. Além de otimizar os fluxos internos da UnB, o PRP01 fortalece a governança digital e melhora a experiência de docentes e técnicos, reduzindo a carga de trabalho manual e o risco de inconsistências operacionais.

5.2 Contribuições da pesquisa

A pesquisa apresenta contribuições relevantes em três dimensões principais — tecnológica, institucional e científica:

a) Contribuição tecnológica

O desenvolvimento do PRP01 demonstra a viabilidade de aplicar linguagens de automação modernas, como Python, para integrar plataformas legadas de ensino e bancos de dados institucionais. A arquitetura modular proposta pode ser replicada ou adaptada a outras universidades que utilizam o Moodle, servindo como modelo de automação segura e eficiente.

O repositório já foi publicado no GitHub (um lugar onde desenvolvedores podem compartilhar e colaborar em projetos que usam o sistema de controle de versão criado por Linus Torvalds, o mesmo criador do Linux). Pronto para o compartilhamento da ideia, para que seja aplicada em nas instituições Brasil a fora, quem sabe no mundo.

b) Contribuição institucional

Do ponto de vista da gestão universitária, o sistema trouxe ganhos concretos para a UnB: redução do tempo de atendimento, aumento da produtividade da equipe técnica e padronização dos processos administrativos. A ferramenta tornou o ambiente Moodle mais seguro e mais aderente à Lei Geral de Proteção de Dados (LGPD), além de contribuir para uma cultura de segurança e eficiência digital na instituição.

c) Contribuição científica

No campo acadêmico, a dissertação avança na discussão sobre a automação institucional e a segurança da informação em ambientes educacionais, tema ainda pouco explorado na literatura brasileira. O trabalho reforça a importância da integração entre governança digital, conformidade normativa e inovação tecnológica como pilares da transformação digital no ensino superior.

5.3 Limitações da pesquisa

Apesar dos avanços alcançados, algumas limitações foram identificadas e deverão ser consideradas em trabalhos futuros:

1. O PRP01 depende da estrutura atual do SIGER, que pode sofrer alterações de layout ou formato de dados, exigindo manutenção periódica no código do robô.
2. A ferramenta ainda não utiliza as APIs oficiais do Moodle, operando por meio de varredura da web, o que aumenta a sensibilidade a mudanças na interface do sistema.
3. A ausência de uma interface gráfica (dashboard**)** limita a análise visual dos relatórios e logs, restringindo o uso da ferramenta a técnicos especializados.
4. Os testes foram realizados em um ambiente institucional específico (UnB), o que demanda validação em outros contextos universitários para confirmar a generalização dos resultados.

Essas limitações, contudo, não comprometem a relevância da solução, mas apontam caminhos claros para seu aprimoramento e expansão.

5.4 Trabalhos futuros

A partir dos resultados e limitações identificados, delineiam-se as seguintes propostas para continuidade e ampliação da pesquisa:

- Integração via API REST do Moodle:
- Implementar o PRP01 utilizando a API nativa do Moodle, o que aumentará a robustez, reduzirá a dependência de mudanças na interface e melhorará a compatibilidade com futuras versões da plataforma.
- Desenvolvimento de painel administrativo (dashboard):
- Criar uma interface gráfica interativa que permita aos administradores visualizar solicitações em tempo real, acompanhar os logs de processamento e configurar os parâmetros de execução do PRP01.
- Aprimoramento de segurança e auditoria;
- Integrar o sistema a ferramentas de monitoramento contínuo e detecção de anomalias (SIEM), além de implementar notificações automáticas de incidentes de segurança.
- Expansão institucional:
- Adaptar o modelo para outras instituições de ensino superior, públicas e privadas, avaliando o desempenho e a interoperabilidade do sistema em diferentes contextos acadêmicos.
- Automação completa de fluxos administrativos:
- Expandir a aplicação do PRP01 para além da criação de cursos, incorporando módulos de atualização de matrículas, migração de turmas e sincronização de notas entre o Moodle e o SIGAA.
- Ampliar esse sistema via Webservices podemos até responder solicitações fácil, um exemplo, um plugin para o moodle o professor solicita adição ou remoção de tutores ou aluno, ele preencher o formulário, o sistema envia para nós, a gente só aprova ou nega, já sabemos se o usuário já foi criado ou não, se o nome é homônimo para não inscrever pessoa errada, erros que acontecem.

5.5 Considerações finais

Conclui-se que a governança digital é um fator estratégico para consolidar a transformação digital, sendo necessário fortalecer os mecanismos de participação e de segurança da informação.

O estudo demonstrou que a automação inteligente, quando aliada à segurança e à conformidade normativa, pode transformar significativamente a gestão acadêmica nas universidades. A experiência da UnB com o PRP01 reforça a viabilidade de aplicar tecnologias abertas e acessíveis para resolver problemas institucionais complexos, promovendo maior eficiência, transparência e segurança da informação**.**

Dessa forma, a dissertação contribui para o avanço da transformação digital no ensino superior, estabelecendo um modelo replicável e escalável de integração automatizada entre sistemas educacionais, com potencial de impacto nacional no contexto das universidades públicas brasileiras.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Angélica Olivetto de et al. Ética, segurança e privacidade na educação à distância durante a pandemia no Brasil. Revista InovaEduc, n. 7, p. 1–28, 2020.

ALVES ANDRADE, Thaísa; **ROSA DA SILVA**, Núbia; **FARIAS CORDEIRO**, Douglas. Uma Proposta de Interface para Apoio à Serviços de Manipulação de Dados no Moodle. Revista Foco, v. 16, n. 7, 2023.

BANEŞ, Vasile et al. A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform. Applied Sciences, v. 13, n. 17, p. 9675, 2023.

BARDIN, Laurence. *Análise de conteúdo*. São Paulo: Edições 70, 2011.

BRAEKEN, An; **TOUHAFI,** Abdellah. Efficient Mobile User Authentication Service with Privacy Preservation and User Untraceability. In: CloudTech 2020. IEEE, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Institui o Programa de Privacidade e Segurança da Informação (PPSI). Diário Oficial da União: seção 1, Brasília, DF, 29 mar. 2023.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. *Estratégia Nacional de Governo Digital (ENGD).* Brasília: Governo Federal, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional>. Acesso em: 08 jan. 2026.

DE ALMEIDA, Angélica Olivetto et al. Ética, segurança e privacidade na educação à distância durante a pandemia no Brasil. Revista InovaEduc, 2020.

DURST, Susanne; HENSCHEL, Thomas. Knowledge risk management: a research agenda. *Journal of Knowledge Management*, v. 24, n. 3, p. 1-15, 2020.

ELMAGHRABI, Azza Yousif; **BADAWI**, Maria Altaib. Analysis of (IaaS) Cloud Computing Security Issues Concerning Websites, Moodle eLMS as an Example. IJCSNS, v. 20, n. 11, 2020.

FERREIRA, Joelson Miranda et al. O Moodle como recurso didático pedagógico na educação a distância: uma análise abrangente. Educação, v. 28, n. 131, fev. 2024.

GIGA CANDANGA. Portal Giga Candanga. Disponível em: https://gigacandanga.net.br/. Acesso em: 8 jan. 2026.

GIL, Antônio Carlos**.** *Como Elaborar Projetos de Pesquisa.* 6. ed. São Paulo: Atlas, 2019. → Obra clássica, apresenta os tipos de pesquisa (exploratória, descritiva, explicativa, aplicada) e orienta sobre estrutura metodológica.

Gil, Antônio Carlos. *Como Elaborar Projetos de Pesquisa.* 4ª ed. São Paulo: Atlas, 2002. → Obra clássica que apresenta os tipos de pesquisa (exploratória, descritiva, explicativa, aplicada) e orienta sobre estrutura metodológica.

GONES, Peter Molina; TANI, Zuleica. O emprego da Plataforma Digital Moodle como estratégia de e-learning de sucesso. Revista Científica Multidisciplinar Núcleo do Conhecimento, 2020.

GUIMARÃES, Ueudison Alves et al. Plataformas de aprendizagem online: vantagens e limitações na educação básica. Ciências Humanas, Educação, v. 29, n. 146, mai. 2025.

HE, Ping; **QIU**, Jing; **ZHAI,** Boli. Study on the integration of cloud computing and moodle learning platform. In: ICCSN 2015. IEEE, 2015.

HUANG, Lei; **WU**, Zhouhua. An Educational Data Analysis Framework and Course Profiling Techniques Based on Moodle's Log. In: EITT 2018. IEEE, 2018.

JÚNIOR, Albino Szesz et al. Ambiente virtual de aprendizagem: o caso do ava/nutead/uepg, 2016.

JUNIOR, Otto Guilherme Gerstenberger; **GERSTENBERGER**, Fatima Cristina Santoro. Direitos fundamentais e novos direitos na educação a distância. Observatório de la Economía Latinoamericana, v. 22, n. 7, 2024.

KULKARNI, Mehar et al. Mitigating email phishing: analytical framework, simulation models, and preventive measures. In: ICCSP 2024. IEEE, 2024.

LI, Zhao et al. Fighting against piracy: An approach to detect pirated video websites enhanced by third-party services. In: ISCC 2022. IEEE, 2022.

LIMA, José Maria Maciel. Plataforma Moodle: A educação por mediação tecnológica. Revista Científica Multidisciplinar Núcleo do Conhecimento, 2021.

MAIA, Maria Ivanete Enes. O uso das tecnologias de informação e comunicação em tempos de pandemia na Escola de Tempo Integral Dra. Zilda Arns Neumann. Educação, v. 29, n. 149, 2025.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia científica*. 5. ed. São Paulo: Atlas, 2003.

ME, M. Selvi et al. Moodle data analysis for effective online teaching and learning. In: ICCMC 2023. IEEE, 2023.

MICROSOFT. Questionário de Avaliação do Aprender3. Disponível em: <https://forms.office.com/pages/responsepage.aspx?id=oZs17AtjK024M8jm1I-AWfJn3jNrmRlJjPZNDwI7sE9UNU9CR0dTQkZTOEExVlVMTFNFM1oxT01ZRy4u&origin=lprLink&route=shorturl>. Acesso em: 08 jan. 2026.

MIHAI, Darius et al. Integrated high-workload services for e-learning. IEEE Access, v. 11, 2023.

MILOSEVIC, Đorđe et al. Endangered data in Moodle platform with malicious plugins. In: INFOTEH 2022. IEEE, 2022.

MOSHARRAF, Maedeh; **TAGHIYAREH,** Fattaneh. Moodle meets linked data: Publishing Moodle on the web of data using semantic links. In: ICWR 2018. IEEE, 2018.

MOODLE. Aprendizado on-line com o LMS mais popular do mundo. Disponível em: https://moodle.com/pt-br/. Acesso em: 08 jan. 2026.

NASCIMENTO, L. M. M.; **CAFE**, D. C.; **SILVA**, Carlos Eduardo C. AUMENTANDO A SEGURANÇA DO GERENCIAMENTO DE USUÁRIOS DO MOODLE USANDO BANCOS DE DADOS DE TERCEIROS. REVISTA DE ENGENHARIA E TECNOLOGIA, v. 17, p. 1/2025-11, 2025.

RAHIM, Yahaya Abd et al. A study on the effects of learning material handling procedures towards information integrity in Moodle LMS. In: ICon EEI 2018. IEEE, 2018.

REIS, João Goulart Batista; **NASCIMENTO**, L. M. M.; **SILVA**, Carlos Eduardo C. A IMPORTÂNCIA DA USABILIDADE E A COLABORAÇÃO POSITIVISTA APLICADA À SEGURANÇA CIBERNÉTICA: UM ESTUDO DE CASO DO APLICATIVO SOUGOV. Revista FT, v. 29, n. 148, pag 17-18, 2025.

RIBEIRO, Anna Carolina; DEMO, Gisela; SANTOS, Carlos Denner. Grupo focal: aplicações na pesquisa nacional em administração. *Revista Pretexto,* v. 22, n. 2, p. 1-20, 2021.

ROGERS, Jamal Kay B.; **SALAZAR**, Romel P.; **BULADACO,** Mark Van M. Moodle and Google Classroom: a comparative study of acceptability. EduLearn, v. 19, n. 3, 2025.

SHAN, Guijuan. Data management and sharing mechanism of e-commerce industry based on association rule mining. In: TOCS 2021. IEEE, 2021.

SUN, Yi; **WANG**, Xiaonan; **SU**, Yancong. Development of a Data Visualization Assistance System for Online Education Platforms: A Case Study on Moodle. In: CCAT 2023. IEEE, 2023.

THORSTENSEN, Vera; **ZUCHIERI**, Amanda Mitsue. Governo Digital no Brasil: o quadro institucional e regulatório do país sob a perspectiva da OCDE. Working Paper 529 – CCGI nº 24. São Paulo: Escola de Economia de São Paulo, Fundação Getulio Vargas, maio 2020. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/fdc9f1fa-d65e-48e5-b0a5-7341cbd2e33f/content. Acesso em: 8 jan. 2026.

TEMOSHOK, David; et al. Digital Identity Guidelines: Identity Proofing and Enrollment. NIST Special Publication 800-63-4. Gaithersburg, MD: National Institute of Standards and Technology, 2024.

TEMOSHOK, David; et al. Digital Identity Guidelines: Identity Proofing and Enrollment. NIST Special Publication 800-63-4, Rev. 4. Gaithersburg, MD: National Institute of Standards and Technology, 2025.

TOLENTINO DA SILVA, Marília. Desafios percebidos na implementação das medidas do PPSI. Brasília, 2024.

UNIVERSIDADE DE BRASÍLIA. Aprender3 – Ambiente Virtual de Aprendizagem. Disponível em: https://aprender3.unb.br/. Acesso em: 08 jan. 2026.

UNIVERSIDADE DE BRASÍLIA. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR). Portal da ETIR. Brasília, DF, 2026. Disponível em: https://etir.unb.br. Acesso em: 8 jan. 2026.

UNIVERSIDADE DE BRASÍLIA. Sistema Gerador de Relatórios – SIGER. Disponível em: https://www.sistemas.unb.br/autenticacao7/. Acesso em: 08 jan. 2026.

UNIVERSIDADE DE BRASÍLIA. Sistema Integrado de Gestão de Atividades Acadêmicas – SIGAA. Disponível em: https://sigaa.unb.br/. Acesso em: 08 jan. 2026.

ZABALA, Laura Nataly Basto; **VELASCO**, Channyke Santiago Rodríguez; PARADA, Hector Dario Jaimes. Security scheme for Moodle platforms based on a multi-layered model. In: CONIITI 2022. IEEE, 2022.