

Universidade de Brasília – UnB
Faculdade UnB Gama – FGA
Engenharia de Software

**IDENTIDADE PRIVILEGIADA DE DADOS PARA
SEGURANÇA CIBERNÉTICA**

**Autores: Sávio Cunha de Carvalho e
Luis Gustavo Ferreira Marques**
Orientadora: Profa. Dra. Luiza Yoko Taneguti

Brasília, DF
2023



Sávio Cunha de Carvalho e
Luis Gustavo Ferreira Marques

**IDENTIDADE PRIVILEGIADA DE DADOS PARA SEGURANÇA
CIBERNÉTICA**

Monografia submetida ao curso de graduação em
Engenharia de Software da Universidade de Brasília,
como requisito parcial para obtenção do Título de
Bacharel em Engenharia de Software.

Universidade de Brasília – UnB

Faculdade UnB Gama – FGA

Orientadora: Profa. Dra. Luiza Yoko Taneguti

Brasília, DF

2023

Cunha de Carvalho, Sávio
CC331 Identidade privilegiada de dados para Segurança Cibernética / Sávio Cunha de Carvalho,
Luis Gustavo Ferreira Marques; orientador Luiza Yoko Taneguti. 66 p. Brasília, 2023.

Monografia (Graduação Engenharia de Software) Universidade de Brasília, 2023.

1. Desenvolvimento de práticas de segurança aplicadas ao desenvolvimento web 2.
Gerenciamento de identidade no contexto da segurança cibernética. 3. Autenticação
multifatorial. 4. Comunicação via HTTP. I. Ferreira Marques, Luis Gustavo. II. Yoko
Taneguti, Luiza, orient. III. Título.

CDU 02:141:005.

Sávio Cunha de Carvalho e
Luis Gustavo Ferreira Marques

**IDENTIDADE PRIVILEGIADA DE DADOS PARA SEGURANÇA
CIBERNÉTICA**

Monografia submetida ao curso de graduação em Engenharia de Software da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Software.

Trabalho aprovado. Brasília, DF, 15 de dezembro de 2023:

Profa. Dra. Luiza Yoko Taneguti
Orientadora

Prof. Dr. Tiago Alves da Fonseca
Convidado 1

Profa. Dra. Tatiane da Silva
Evangelista
Convidado 2

Brasília, DF

2023

Este trabalho é dedicado à todas as crianças,
grandes e pequenas, que sonham em construir
um mundo melhor através da tecnologia.

AGRADECIMENTOS

Gostaríamos de agradecer primeiramente a Deus, que nos concedeu discernimento e força ao longo de todos os anos de estudo e dedicação necessários para alcançarmos nossos objetivos. Aos funcionários, docentes e toda a equipe acadêmica da Universidade de Brasília, nossa mais sincera gratidão. O comprometimento e a dedicação de vocês profissionais foram cruciais para moldar nosso percurso acadêmico. Gostaríamos ainda, de agradecer a cada amigo que construímos e nos apoiaram até o aqui, vocês foram necessários.

Além disso, expressamos nossa profunda gratidão à Universidade de Brasília (UnB), pela oportunidade de formação e pela promoção de um ambiente acadêmico propício à aquisição de conhecimento. O apoio contínuo e os recursos oferecidos pela instituição foram fundamentais para a compreensão e conclusão desta graduação. A UnB desempenhou um papel crucial no enriquecimento da nossa jornada acadêmica, fornecendo não apenas conhecimento teórico, mas também oportunidades significativas para aplicar e aprimorar essas práticas inovadoras. Essas experiências, aliada à educação de qualidade, com bolsas concedidas ao longo do curso apresentou-se como um alicerce sólido para compreensão do real sentido da Engenharia de Software.

Neste sentido, eu, Luis Gustavo Ferreira Marques, gostaria de agradecer a todos os meus familiares, minha esposa Fernanda Oliveira Rezende Rocha e meus pais Joaquim e Valdezy, que me apoiaram integralmente ao longo dessa jornada, tanto dentro quanto fora da universidade. Seu constante incentivo e apoio foram fundamentais para que me tornasse um profissional e um ser humano melhor a cada dia.

Eu, Sávio Cunha de Carvalho, gostaria de expressar minha profunda gratidão aos meus pais, Jerônimo Pinheiro e Carmem Célia por me permitirem chegar até aqui, aos irmãos, Thablo Cunha e Otávio Cunha, gostaria de agradecer por todo o amor, apoio e incentivo que me deram ao longo desta jornada. A minha orientadora, professora Dra. Luiza Yoko, minha imensa gratidão pela sua orientação, paciência e sabedoria ao longo deste processo. Seu conhecimento e dedicação foram fundamentais para o desenvolvimento deste trabalho, e sou muito grato por todo o tempo e esforço que dedicou a mim. Ao meu amigo 'D.F.', agradeço por todo apoio e conhecimento compartilhado, você é um ser humano que inspira.

RESUMO

A segurança cibernética desempenha um papel fundamental na proteção de dados em sistemas digitais. Em particular, destaca-se a gestão da identidade privilegiada de acesso como uma ferramenta adicional para garantir a integridade e confidencialidade das informações. Esta monografia explora as diversas etapas envolvidas no desenvolvimento de um sistema para uma loja fictícia, desde a fase inicial de levantamento de requisitos até a efetiva implementação da solução, com o objetivo de apresentar a importância da identidade privilegiada nessas etapas de desenvolvimento e apresentar os conceitos fundamentais para a construção de um ambiente digital mais protegido. Ademais, o sistema desenvolvido demonstrou os conceitos de segurança cibernética, gerenciamento de acesso e identidade privilegiada de dados, a fim de indicar um caminho viável para a aplicação de práticas mais seguras no desenvolvimento e utilização de software, contribuindo para o avanço contínuo da segurança da informação em ambientes digitais dinâmicos.

Palavras-chave: segurança cibernética; identidade privilegiada; proteção de dados; desenvolvimento de sistema.

ABSTRACT

Cybersecurity plays a key role in protecting data in digital systems. In particular, the management of privileged access identity stands out as a crucial additional tool to ensure the integrity and confidentiality of information. This monograph explores the various stages involved in the development of an abstract store system, from the initial requirements gathering phase until the effective implementation of the solution, with the aim of presenting the importance of privileged identity in these stages of development and present the fundamental concepts to build a robust and more protected digital environment. Furthermore, the developed system demonstrated the concepts of cybersecurity, security management access and privileged identity of data, in order to indicate a viable path for the application cation of safer practices in the development and use of software, contributing for the continuous advancement of information security in dynamic digital environments.

Keywords: cybersecurity; privileged identity; data protection; system development.

LISTA DE FIGURAS

Figura 1 - CERT.br, quantidade de incidentes 2012-2022.....	21
Figura 2 - CERT.br, tipos de incidentes em 2021	21
Figura 3 - Fluxograma do Processo de Desenvolvimento	29
Figura 4 - Captura do Quadro TCC, na plataforma Trello	35
Figura 5 - Diagrama Entidade Relacionamento, sistema Spay v1.0.0.	43
Figura 6 - Diagrama de Entidade Relacionamento, Módulo de Pagamentos, Sistema Spay v1.0.0.	44
Figura 7 - Logs em arquivo na aplicação Spay, v1.1.0.....	45
Figura 8 - Novos Módulos Aplicação Spay, v1.2.0.	46
Figura 9 - Novos Módulos Aplicação Spay, v1.2.0	47
Figura 10 - Diagrama de autorização da listagem de pagamentos,v1.3.0.	48
Figura 11 - Diagrama de autorização da criação de pagamentos,v1.3.0.	48
Figura 12 - Login no sistema do Django admin,v1.4.0	49
Figura 13 - Login no sistema do Django admin,v1.4.0.	50
Figura 14 - Login no sistema do Django admin,v1.3.0.	51
Figura 15 - QR code com segredo para geração de códigos. v1.4.0.	52
Figura 16 - Tela de verificação nos demais logins,v1.4.0.	53
Figura 17 - Requests realizados via https para os endpoints Spay	54
Figura 18 - Pagina de Logs Spay	54
Figura 19 - Script para tentativa de quebra de senha por força bruta.....	57
Figura 20 - Intercepção de comunicações por HTTP	57

LISTA DE QUADROS

Quadro 1 - Tipos de usuários sistema Spay	35
Quadro 2 - Requisitos não funcionais.....	37
Quadro 3 - Requisitos funcionais não priorizados.....	38
Quadro 4 - Requisitos funcionais priorizados	39
Quadro 5 - Ataques e aspectos do sistema.....	55

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CPF	Cadastro de Pessoa Física
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IAM	<i>Identity and Access Management</i>
ID	Identificador Único
LGPD	Lei Geral de Proteção de Dados
MFA	Multi-factor Authentication
MVP	<i>Minimum Viable Product</i>
NIST	<i>National Institute of Standards and Technology</i>
PAM	<i>Privileged Access Management</i>
PIM	<i>Privileged Identity Management</i>
RBAC	<i>Role-Based Access Control</i>
RG	Registro Geral
TCC	Trabalho de Conclusão de Curso
UI	<i>User Interface</i>
UnB	Universidade de Brasília
UX	<i>User Experience</i>
API	<i>Application Programming Interface</i>

SUMÁRIO

1 INTRODUÇÃO	14
1.1 JUSTIFICATIVA	15
1.2 OBJETIVOS	16
1.2.1 Objetivo Geral	16
1.2.2 Objetivos Específicos	16
2 REFERENCIAL TEÓRICO	17
2.1 SEGURANÇA DA INFORMAÇÃO.....	17
2.1.1 Segurança da Informação nas Comunicações	19
2.2 SITUAÇÃO BRASILEIRA NA SEGURANÇA CIBERNÉTICA	20
2.3 CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO	22
2.3.1 Identidade	22
2.3.2 Autenticação	23
2.3.3 Autorização	23
2.3.4 Monitoramento	23
2.3.5 Auditoria	23
2.4 IDENTIDADE PRIVILEGIADA DE ACESSO	24
2.4.1 Definição de Identidade Privilegiada de Acesso	24
2.4.2 Desafios e Boas Práticas para a Gestão da Identidade Privilegiada de Acesso	25
2.4.3 Plataformas de gerenciamento de acesso privilegiada.	26
2.5 PRINCIPAIS AMEAÇAS E RISCOS	27
2.5.1 Ataques Cibernéticos Voltados para Identidades Privilegiadas	27
2.5.2 Potenciais Consequências da Exploração de Identidades Privilegiadas	28
3 METODOLOGIA	29
4 DESENVOLVIMENTO	31
4.1 PROBLEMÁTICA FICTÍCIA E SOLUÇÃO	31
4.1.1 Proto-persona	31
4.1.2 Brainstorm	33
4.1.3 Solução	33
4.2 GESTÃO DO PROJETO DE DESENVOLVIMENTO DO SISTEMA BASE DA LOJA FICTÍCIA	33
4.3 CICLOS DE DESENVOLVIMENTO.....	33
4.4 FLEXIBILIDADE E ADAPTABILIDADE	34

4.5 INTEGRAÇÃO ENTRE PESQUISA ACADÊMICA E DESENVOLVIMENTO PRÁTICO	34
4.6 KANBAN	34
4.7 PERFIL DE USUÁRIOS	35
4.8 REQUISITOS	36
4.8.1 Requisitos Não Funcionais	36
4.8.2 Requisitos Funcionais	36
4.8.3 Requisitos Funcionais Priorizados	36
4.9 FLUXO DE DESENVOLVIMENTO E TECNOLOGIAS DO SISTEMA BASE	37
4.10 TECNOLOGIAS	38
4.10.1 Python	38
4.10.2 Django	39
4.10.3 PostgreSQL	39
4.10.4 Django REST framework	40
4.10.5 HTTPS (Hypertext Transfer Protocol Secure)	40
4.10.6 OAuth2 (Open Authorization)	40
4.10.7 Google MFA (Multi-Factor Authentication)	40
4.10.8 Docker	41
4.10.9 Docker Compose	41
4.10.10 Swagger	41
4.10.11 NGINX	41
4.11 APLICAÇÃO BASE	42
4.11.1 Diagramas	42
4.11.1.1 Diagramação do projeto completo	42
4.11.1.2 Diagramação do Módulo de Pagamentos	44
4.12 VERSÕES DESENVOLVIDAS	44
4.12.1 v1.0.0 - Sem Implementações específicas de segurança	45
4.12.2 v1.1.0 - Implementação do sistema de logs	45
4.12.3 v1.2.0 - Implementação de novos recursos e integrações de pacotes	45
4.12.4 v1.3.0 - Implementação de funções de autorização	46
4.12.4.1 Mudanças nas Funções de Autorização da PaymentCreateView	47
4.12.4.2 Mudanças nas Funções de Autorização da PaymentListView	48
4.12.5 v1.4.0 - Implementação de autenticação multifatorial	49
4.12.6 v1.5.0 - Implementação de HTTPS	53

4.12.7 v1.6.0 - Implementação de visualização de logs	53
5 RESULTADOS E DISCUSSÃO	55
6 CONCLUSÃO.....	59
6.1 TRABALHOS FUTUROS	60
REFERÊNCIAS.....	62

1 INTRODUÇÃO

Antes da existência da internet, as preocupações com a segurança da informação eram abordadas de maneiras distintas. As organizações e indivíduos confiavam principalmente em dispositivos de armazenamento físico, como arquivos em papel, para proteger suas informações valiosas (Monteiro, 2001). Medidas de segurança física, como trancas, cofres e salas de arquivos restritas, eram implementadas para assegurar a confidencialidade e proteção dos dados. No entanto, com as revoluções tecnológicas do século XX e a ascensão da internet, o cenário da segurança da informação passou por transformações significativas (Carvalho, 2006). A conectividade global proporcionada pela internet trouxe novos desafios e demandas por estratégias mais avançadas e tecnologicamente sofisticadas de proteção de dados em um ambiente digital cada vez mais complexo.

Com a crescente penetração da internet em diferentes setores da sociedade, desde empresas até indivíduos, surgiram novas oportunidades e desafios relacionados à segurança, privacidade e governança digital. Esses avanços tecnológicos proporcionaram uma maior conveniência e eficiência para a sociedade, permitindo a realização de transações comerciais entre indivíduos geograficamente distantes e a troca de conhecimento com uma conexão global (Joseph; Norman, 2019). No entanto, essa expansão também ampliou a superfície de ataque, tornando os sistemas digitais mais vulneráveis a possíveis ameaças cibernéticas.

Segundo Vieira (2003), a internet facilitou a comunicação mundialmente, pois as pessoas se adaptaram com o uso, aproximando assim os ambientes on-line e off-line. A interconectividade global proporcionada pelo avanço da internet permitiu que indivíduos acessem sistemas digitais, compartilhem e recebam informações em tempo real. Junto à facilidade de acesso, surge a necessidade de proteger as informações do seu usuário contra fraudes no ambiente on-line, a fim de garantir a privacidade e a segurança dos dados pessoais. Nesse contexto, (Hosang, 2011) destaca-se a importância de adotar medidas de segurança cibernética, como *firewalls*, criptografia e autenticação de usuários, a fim de proteger as informações sensíveis contra ameaças cibernéticas cada vez mais sofisticadas.

A segurança cibernética abrange a proteção de redes, sistemas, dispositivos e dados contra ameaças virtuais, como ataques cibernéticos, invasões, roubo de identidade e outros tipos de atividades maliciosas (Canêdo, 2006). Neste contexto, Chapple (2018) afirma que a segurança cibernética não é apenas uma preocupação técnica, mas também um desafio contínuo que requer uma abordagem holística, envolvendo aspectos tecnológicos, processuais e educacionais. Além disso, a colaboração entre setores público e privado, compartilhando

informações e coordenando esforços, desempenha um papel fundamental na proteção dos sistemas digitais e na mitigação de riscos cibernéticos.

A segurança da informação, no contexto da identidade privilegiada de acesso, é um aspecto crucial na proteção dos sistemas digitais. Conforme destacado por Santos e Soares (2015), a identidade privilegiada refere-se a contas de usuário com privilégios administrativos ou de alto nível que possuem acesso a informações e recursos sensíveis. Essas contas são altamente visadas por atacantes, uma vez que comprometê-las permite acesso amplo e desautorizado a dados confidenciais.

O roubo de credenciais, por sua vez, é uma ameaça cada vez mais comum e sofisticada enfrentada pelas organizações. Segundo Johnson (2005), essa ação ocorre quando os atacantes obtêm ilegalmente informações de login e senha de usuários, permitindo acesso não autorizado a sistemas e dados sensíveis. Essas informações podem ser adquiridas por meio de técnicas como *phishing*, *malware* ou um ataque de força bruta.

Diante dessas ameaças, é imprescindível adotar medidas robustas de segurança cibernética para proteger a identidade privilegiada e evitar o roubo de credenciais. A implementação de soluções de autenticação multifator (MFA) é uma prática recomendada, conforme sugerido por Wangham *et al.* (2018). A utilização de MFA requer a validação de múltiplos fatores de autenticação, como algo que o usuário sabe (senha), algo que o usuário possui (token) ou algo que o usuário é (biometria), reduzindo significativamente o risco de acesso não autorizado, mesmo no caso de roubo de credenciais.

Além disso, é fundamental promover a conscientização e a educação dos usuários sobre boas práticas de segurança, como a criação de senhas fortes e únicas, o cuidado ao clicar em links suspeitos e a utilização de autenticação de dois fatores sempre que possível. A combinação dessas medidas de segurança cibernética e conscientização pode ajudar a mitigar os riscos relacionados à identidade privilegiada e ao roubo de credenciais, fortalecendo a segurança da informação e protegendo efetivamente os sistemas digitais.

1.1 JUSTIFICATIVA

A segurança da informação é um tema de extrema relevância na era digital, à medida que a dependência de sistemas tecnológicos aumenta significativamente (Souza; Fernandes, 2016). Com a crescente conectividade global e o avanço das ameaças cibernéticas, torna-se imprescindível compreender e abordar, de forma efetiva, as questões relacionadas à proteção de dados, privacidade e governança digital.

Uma abordagem importante neste trabalho, é compreender a necessidade de autenticação forte para a construção de uma identidade mais segura, pois é através dela que é verificada a identidade do usuário, permitindo ou negando o acesso a sistemas e informações sensíveis. Dessa maneira, a criação de uma identidade privilegiada única para cada usuário contribui significadamente para a segurança dos sistemas, impedindo o acesso não autorizado a recursos restritos.

Dessa forma, a elaboração desta monografia desempenha um papel crucial no progresso do entendimento no âmbito da segurança cibernética e identidade privilegiada.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo principal desse TCC é realizar o desenvolvimento de práticas de segurança aplicadas ao desenvolvimento web de um sistema de gerenciamento de pagamentos para uma loja fictícia, tendo como ênfase o gerenciamento de identidade e níveis de permissão.

1.2.2 Objetivos Específicos

1. Desenvolver um sistema para uma loja fictícia que realize a gravação e listagem de pagamentos.
2. Realizar o desenvolvimento incremental de práticas de segurança.
3. Exemplificar a importância do gerenciamento seguro em aplicações digitais, utilizando a prova de conceito desenvolvida para a loja fictícia como caso prático.
4. Demonstrar a importância da proteção de identidades no contexto da segurança cibernética.
5. Evidenciar que identidades com senhas de maior complexidade de combinações apresentam uma resistência maior em comparação a senhas mais simples.
6. Prover o acesso ao sistema com autenticação multifatorial e comunicação via HTTP seguro, a fim de garantir uma segurança robusta e eficaz.
7. Realizar a integração da equipe de TCC, entre os alunos e a orientadora, para desenvolvimento eficaz do grupo, além de promover a integração de todos os envolvidos.

2 REFERENCIAL TEÓRICO

Neste capítulo, será apresentada uma revisão sistemática da literatura existente sobre o tema de estudo, situando o trabalho em relação às pesquisas anteriores e estabelecendo as bases teóricas para a investigação.

2.1 SEGURANÇA DA INFORMAÇÃO

A informação em um sistema digital é um conjunto de bytes armazenados em disco rígido, conhecido como HD (oriundo do inglês *Hard disk drive*) ou disco de estado sólido, mas os bytes sem contextos ou transformações são inúteis para os humanos, não passando de um conjunto de dígitos binários que, a primeira vista, podem parecer não representativo, sem sentido, bytes armazenados que para a maioria da população simplesmente não podem ser utilizados. “Informação é muito mais que um conjunto de dados, transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional.” (Fontes, 2012, p. 22).

As informações transmitidas por meios digitais têm um grau de relevância bastante diverso na vida das pessoas, variando desde algo que pode ser considerado inútil para a maioria, como o registro de acesso a um site, até algo de extrema relevância, como a senha de acesso ao *Internet banking*.

A segurança da informação é essencial na era digital em que vivemos. À medida que a tecnologia avança e a dependência de sistemas de informação aumenta, a proteção adequada das informações torna-se uma preocupação fundamental para indivíduos, empresas e governos. A segurança não se estende somente a ações eletrônicas de defesa, como um firewall, senhas e criptografias, mas também deve ser uma cultura organizacional para os indivíduos ou empresas.

Junto a isto, nas empresas do mercado existe ainda pouca preocupação das organizações com os riscos cibernéticos em comparação com a cobertura de riscos tradicionais, mesmo que seja de extrema importância, a segurança da informação para a maioria das empresas ainda tem uma subvalorização, por mais que exista uma crescente preocupação com a segurança das informações, segredos industriais e acessos a sistemas sensíveis (Gomes *et al.*, 2011).

A segurança da informação possui alguns princípios que devem ser respeitados.

Apresentaremos os principais, segundo Gomes *et al.*, (2011).

Confidencialidade: este princípio informa que somente pessoas autorizadas e credenciadas devem acessar e atualizar as informações, cabendo normalmente ao profissional

ou departamento de segurança da informação utilizar mecanismos e ferramentas para impedir este acesso não autorizado, seja por descoberta acidental de uma informação publicada erroneamente, ou por má-fé por parte dos indivíduos, usuários ou não, de um sistema. (Gomes *et al.*, 2011)

As organizações estão constantemente expostas a ameaças cibernéticas, sendo a violação do sigilo dos dados um dos principais riscos enfrentados (Pinheiro, 2020). Desta forma, adotando medidas para garantir que somente indivíduos autorizados possam acessar informações sensíveis, as empresas reduzem significativamente o potencial de ataques maliciosos, como tentativas de invasão, roubo de informações ou sabotagem interna.

Integridade: este princípio é a garantia, por parte dos usuários, gerentes e demais, que a informação previamente armazenada no sistema, será disponibilizada sem a perda de parte da informação ou alterações, ou, ainda, deleções indevidas destes dados (Gomes *et al.*, 2011). Neste viés, é importante estabelecer políticas e procedimentos adequados, a fim de evitar acesso não autorizado ou ações maliciosas que possam comprometer a integridade dos dados.

Segundo Pinheiro (2020), existem diversos desafios associados à garantia da integridade dos dados, desta forma, é de fundamental importância que as organizações estejam cientes desses desafios e adotem medidas proativas para enfrentá-los. Isso pode envolver auditorias regulares, backups frequentes, monitoramento constante do ambiente de armazenamento utilizado e a aplicação de práticas recomendadas de segurança de dados. Essas medidas asseguram a confiança nos dados e na informação disponível, tanto para a organização quanto para seus usuários e é uma parte vital para a construção de um ambiente seguro e resiliente no cenário digital atual.

Disponibilidade: o princípio da disponibilidade é um dos pilares fundamentais da segurança da informação, assegurando que os dados e informações estejam prontamente acessíveis sempre que necessários, independentemente do local ou momento acessado (Gomes *et al.*, 2011). A garantia de disponibilidade é de extrema importância, de acordo com (Machado, 2014), a falta de acesso a informações críticas pode acarretar sérias consequências para uma organização, afetando sua produtividade, capacidade de tomada de decisões e abalando a confiança de clientes e parceiros.

Autenticidade: com a crescente sofisticação dos ataques cibernéticos e das técnicas de manipulação de dados, destaca-se a importância de adotar medidas avançadas de autenticação para proteger a integridade e a veracidade das informações. Deste modo, a fim de garantir que as informações existentes sejam autênticas, não tenham sido adulteradas ou falsificadas e

possam ser confiáveis para os usuários e sistemas, é aplicado o princípio da autenticidade que garante a confiabilidade das informações, bem como sua origem legítima (Freitas, 2012).

Neste sentido, ter recursos por meio de registros aprimorados para gerenciar o acesso de quais foram os usuários que realizaram os acessos, as atualizações e exclusões de informações, é indispensável para ser possível confirmar sua autoria e originalidade (Gomes *et al.*, 2011).

2.1.1 Segurança da Informação nas Comunicações

As três grandes revoluções que marcaram a história da humanidade – a agrícola, a industrial e a tecnológica – protagonizaram o gradativo crescimento da importância da informação como insumo básico do processo decisório, culminando com o seu alinhamento entre os fatores clássicos de produção (terra, trabalho e capital), vindo mesmo a superá-los em relevância no cenário econômico mundial. (Gomes *et al.*, 2011)

Em tempos mais recentes, a informação foi alçada à categoria de ativo estratégico para organizações e Estados-Nação, conferindo àqueles que a detêm e dela se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais. (Gomes *et al.*, 2011, p. 15).

Os avanços tecnológicos e a globalização digital desempenham um papel fundamental na integração e troca de conhecimento e informações entre indivíduos geograficamente distantes. Hoje em dia, é possível realizar transações comerciais e trabalhar para empresas remotamente. No entanto, esses avanços também apresentam novos desafios no que diz respeito à segurança da informação.

Antes da era digital os problemas relacionados à segurança da informação podiam ser gerenciados armazenando-se documentos importantes em data centers separados ou utilizando-se dispositivos físicos acessados somente off-line. No entanto, com os novos modelos de trabalho e a necessidade de acesso remoto a arquivos restritos de corporações específicas, torna-se essencial o uso de ferramentas de segurança adicionais que antes não eram necessárias diante das antigas regras e necessidades comerciais.

A segurança da informação nas comunicações é uma preocupação crescente diante da interconexão global e da natureza digital das transações e comunicações atualmente.

Segundo Anderson *et al.* (2018, p. 24), “a disseminação de tecnologias de informação e comunicação permitiu a conexão de pessoas, empresas e organizações de maneiras sem

precedentes”. No entanto, esse cenário também expõe as informações a novas ameaças e vulnerabilidades.

A proteção dos dados e informações sensíveis torna-se especialmente crítica em ambientes de trabalho remoto. De acordo com (Johnson, 2020, p. 4), “com a expansão do trabalho remoto, as organizações precisam implementar medidas de segurança apropriadas para garantir a integridade, confidencialidade e disponibilidade das informações transmitidas e armazenadas”. Isso requer a adoção de medidas para prevenir o acesso não autorizado e a exposição de informações confidenciais.

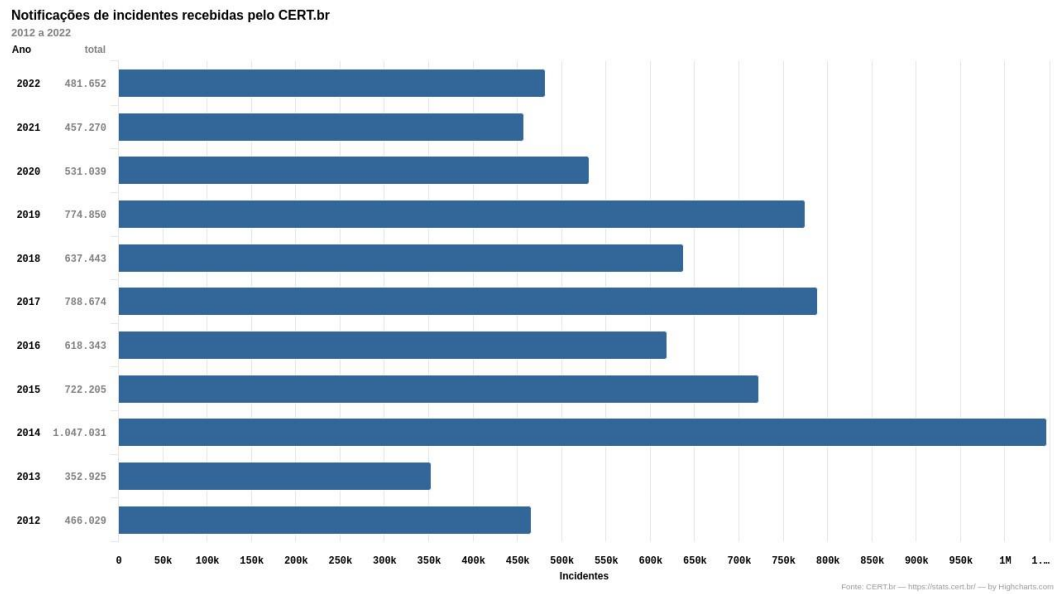
Além disso, a evolução das comunicações digitais trouxe consigo desafios específicos para a proteção da privacidade. De acordo com Li; Liang; Sarathy (2019, p. 24), “a crescente interconectividade digital levanta preocupações sobre a privacidade dos dados pessoais e a vigilância em massa”. É necessário, portanto, o desenvolvimento de políticas e regulamentações adequadas para equilibrar a necessidade de segurança da informação com a proteção da privacidade dos indivíduos envolvidos.

Em suma, a globalização digital e os avanços tecnológicos revolucionaram o modo como as informações são compartilhadas e as atividades comerciais são conduzidas. No entanto, essas mudanças também introduziram novos desafios para a segurança da informação. É crucial que as organizações adotem medidas proativas relacionada à segurança da informação nas comunicações, garantindo a proteção dos dados, a privacidade dos indivíduos envolvidos e a integridade das transações comerciais.

2.2 SITUAÇÃO BRASILEIRA NA SEGURANÇA CIBERNÉTICA

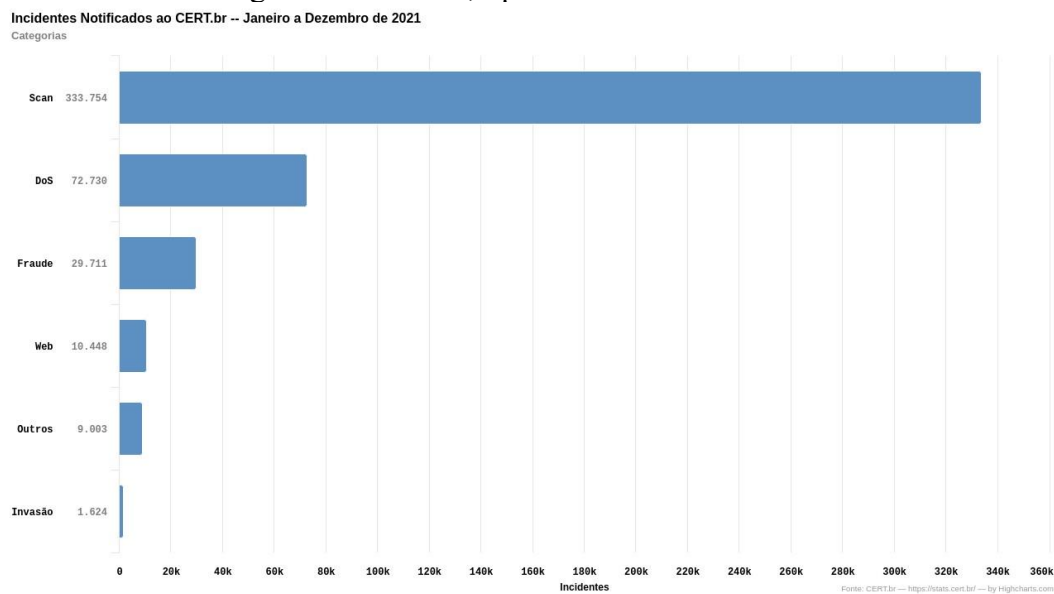
A situação brasileira em relação à segurança cibernética tem apresentado melhorias ao longo dos anos, mas ainda enfrenta desafios significativos, como prejuízos financeiros, vazamento de dados e tentativas de invasões. As notificações voluntárias de incidentes reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [CERT.br](https://www.cert.br) (2023), mostrou que os incidentes enfrentados pelo Brasil no ano de 2021 tiveram 457 mil incidentes totais, conforme mostra a Figura 1. No tocante aos tipos de ataques mais comuns, é visível que no ano de 2021 a quantidade de invasões, quando um indivíduo mal-intencionado consegue acesso não autorizado a um sistema, foi de 0.36% do total de *reports* realizados, esse número pode ser obtido realizando a divisão entre a quantidade de invasões com a somatória de todos os incidentes informados, conforme pode ser observado na Figura 2 ([CERT.br](https://www.cert.br), 2023).

Figura 1 - CERT.br, quantidade de incidentes 2012-2022



Fonte: [CERT.br](https://stats.cert.br/) (2023).

Figura 2 - CERT.br, tipos de incidentes em 2021



Fonte: [CERT.br](https://stats.cert.br/) (2023).

Paralelamente ao incremento de ataques mostrados acima, temos a implementação de leis específicas para tratamento de dados, a Lei Geral de Proteção de dados (LGPD) promulgada na data de 14 de agosto de 2018 implementando mais restrições e responsabilidades legais das empresas perante os dados armazenados de terceiros, sendo legalmente obrigadas a adotarem políticas de segurança, proteção dos dados. (Brasil, 2018).

Com a lei número 13709/2018 (LGPD), foi também realizada a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar e aplicar as

penalidades previstas na lei em caso de descumprimento das medidas legais previstas. ([Brasil, 2018](#)).

2.3 CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um campo vital e em constante evolução que desempenha um papel fundamental em proteger dados sensíveis e sistemas contra ameaças cibernéticas. Os conceitos básicos de segurança da informação fornecem a base sólida sobre a qual estratégias e medidas de proteção mais avançadas são construídas. Esses princípios essenciais abrangem uma variedade de aspectos, desde a confidencialidade e a integridade dos dados até a disponibilidade de sistemas críticos.

2.3.1 Identidade

A identidade é o primeiro princípio para o reconhecimento de um indivíduo em um sistema de informação. É essencial que uma identidade seja única entre os usuários do sistema, para evitar conflitos e ambiguidades. Além disso, a identidade deve ser persistente, ou seja, associada ao mesmo usuário ao longo do ciclo de vida do sistema. No entanto, a manutenção da privacidade da identidade é um desafio, uma vez que informações pessoais podem ser utilizadas por indivíduos mal-intencionados para obter acesso indevido. Portanto, é importante estabelecer mecanismos de proteção e conscientização dos usuários para evitar a divulgação irresponsável de identidades ([Harvard, 2015](#)).

Uma identidade forte deve respeitar ao menos dois principais pilares que devem ser respeitados.

1. A identidade deve ser única entre os possíveis usuários/portadores de identidade do sistema.
2. A identidade é algo persistente, ou seja, uma mesma identidade será sempre designada a um mesmo usuário durante o ciclo de vida de uso do sistema.

Além dos desafios de manutenção da privacidade provenientes de usuários e entidades desonestas que podem possuir direta ou indiretamente informações que facilitem a obtenção dessa identidade, o próprio usuário, por sua vez, pode acabar passando a sua identidade para terceiros, seja por interesse próprio ou por descuido em disponibilizar sua identidade publicamente na rede.

2.3.2 Autenticação

De acordo com [Stallings \(2017\)](#), a autenticação envolve a apresentação de uma prova de identidade, como senha, chave criptográfica ou até mesmo características biométricas únicas. [Whitman e Mattord \(2019\)](#) destaca que existem três principais fatores de autenticação reconhecidos: algo que o usuário sabe (senhas), algo que o usuário possui (tokens de segurança) e algo que o usuário é (autenticação biométrica). Essas técnicas de autenticação são amplamente discutidas na literatura de segurança da informação, fornecendo níveis variados de segurança e conveniência ([Pfleeger; Pfleeger; Margulies, 2015](#)).

2.3.3 Autorização

A autorização é um processo que visa controlar os privilégios concedidos a identidades privilegiadas, determinando quais ações e recursos um usuário autenticado pode acessar. A autorização baseia-se em políticas e diretrizes definidas pela organização, que estabelecem os níveis de acesso a serem concedidos com base nas funções e responsabilidades dos usuários. Uma abordagem comum para a autorização é o Controle de Acesso Baseado em Funções RBAC (Role-Based Access Control), onde os privilégios são atribuídos conforme as funções desempenhadas pelos usuários. A autorização adequada é fundamental para garantir que apenas as identidades privilegiadas autorizadas tenham acesso aos recursos críticos do sistema, reduzindo o risco de violações de segurança e abuso de privilégios ([Whitman; Mattord, 2019](#)).

2.3.4 Monitoramento

O monitoramento do sistema por meio de um sistema de registro de eventos, mais conhecido pelo seu termo em inglês *logging*, é uma das principais ferramentas para detecção de um possível acesso não autorizado ao sistema, realizando a detecção de atividades incomuns que precisam ser tratadas no sistema, além da possível geração de um relatório de ações realizadas no sistema para uma possível correção dos problemas ([Fontes, 2012](#)).

2.3.5 Auditoria

Através da auditoria, é possível rastrear e analisar as ações executadas por essas identidades, identificar comportamentos suspeitos e detectar possíveis violações de segurança.

A importância da auditoria de atividades de identidades privilegiadas é destacada por sua capacidade de fornecer evidências forenses em caso de incidentes, auxiliar na conformidade regulatória e aprimorar a eficácia das políticas de segurança. Para realizar uma auditoria eficaz, são utilizadas ferramentas e tecnologias especializadas que permitem o registro detalhado das atividades, além de técnicas de análise e investigação para a detecção de anomalias e ameaças (Stallings, 2017).

2.4 IDENTIDADE PRIVILEGIADA DE ACESSO

2.4.1 Definição de Identidade Privilegiada de Acesso

A gestão de identidades privilegiadas é um conceito crítico no campo da segurança e privacidade de dados. Conforme o NIST (2020), uma identidade privilegiada de acesso refere-se a uma conta de usuário que possui privilégios elevados em um sistema de informação. Indivíduos com essas identidades conseguem acessar recursos e executar ações que não estão disponíveis para usuários regulares. Elas são frequentemente associadas a funções administrativas, como administradores de sistemas, administradores de banco de dados e administradores de rede.

A importância da identidade privilegiada de acesso reside na sua capacidade de proteger as transações contra atividades fraudulentas e garantir que apenas indivíduos autorizados possam acessar informações sensíveis. Conforme mencionado por (Schneier, 2015), as identidades privilegiadas têm amplo acesso e controle sobre os recursos do sistema, o que as torna um alvo atraente para atacantes em potencial. O comprometimento de uma identidade privilegiada pode resultar em graves violações de segurança, como vazamento de dados, manipulação de sistemas e interrupção dos serviços.

A gestão eficiente da identidade privilegiada de acesso é fundamental para garantir a segurança e a integridade dos sistemas de informação. Segundo o (NIST, 2020), isso envolve a implementação de políticas e procedimentos robustos para a concessão, monitoramento e revogação de privilégios. Além disso, é necessário adotar soluções tecnológicas, como sistemas de gerenciamento de identidades e controle de acesso, para garantir uma administração adequada das identidades privilegiadas. É importante ressaltar que a gestão da identidade privilegiada de acesso é um desafio contínuo, exigindo a revisão regular das permissões concedidas e a adoção de medidas de proteção, como autenticação multifator e criptografia de dados.

2.4.2 Desafios e Boas Práticas para a Gestão da Identidade Privilegiada de Acesso

A gestão da identidade privilegiada de acesso apresenta alguns desafios significativos. Um dos principais desafios é garantir a segregação de funções, ou seja, evitar que uma única identidade tenha privilégios excessivos que comprometam a segurança. Para lidar com esse desafio, a adoção de modelos de Controle de Acesso Baseado em Funções, conforme descrito por (Sandhu *et al.*, 1996), é uma prática recomendada. O RBAC permite que os privilégios sejam atribuídos com base nas funções desempenhadas pelos usuários, garantindo que cada identidade privilegiada tenha apenas os privilégios necessários para realizar suas atividades.

Outro desafio importante na gestão da identidade privilegiada de acesso é a garantia da conformidade regulatória. Muitos setores, como serviços financeiros e saúde, possuem requisitos regulatórios rigorosos para o controle e monitoramento das identidades privilegiadas. A implementação de auditorias regulares e a geração de relatórios de atividades são práticas essenciais para demonstrar a conformidade com essas regulamentações (Fischer; Argon, 2014).

Além disso, a conscientização e o treinamento dos usuários desempenham um papel crucial na gestão da identidade privilegiada de acesso. Os usuários devem ser instruídos sobre a importância da segurança da informação, os riscos associados a identidades privilegiadas comprometidas e as melhores práticas para proteger suas credenciais de acesso. Isso inclui a adoção de senhas fortes, a não divulgação de informações confidenciais e a utilização de autenticação multifator sempre que possível (NIST, 2020).

Neste sentido, boas práticas sobre o gerenciamento de uma identidade privilegiada segura está relacionada a cinco fundamentos principais, que podem ser seguidos para aumentar a segurança de uma identidade privilegiada (CyberArk, 2022).

1. Catalogar todas as identidades humanas e de máquinas com acesso a recursos.

Só se pode identificar algo que se conhece e pode ser diferenciado. Por isso, é de suma importância que todos os usuários e máquinas que estejam utilizando o sistema tenham uma identidade separada. Essas identidades únicas devem ser catalogadas e armazenadas para uma possível verificação do log de erros ou acesso de indivíduos.

2. Autenticar usuários com acesso adaptativo baseado no contexto.

Imaginando um sistema que o fluxo de trabalho exige que o usuário realize o *login*, acesse uma tela intermediária onde são inseridas algumas informações e por fim acesse a página que contenham dados sensíveis, é essencial implementar medidas de autenticação e segurança para proteger essas informações críticas. Esse fundamento impede que, por exemplo, um usuário malicioso consiga acessar o *endpoint* com os dados sensíveis diretamente, pois será

necessário seguir todo o fluxo, algo que pode não ser possível. Porém o usuário que possui o acesso legítimo, conseguirá acessar o *endpoint* sem problemas, pois o mesmo já realizou o *login* e possui as credenciais necessárias para acessar o sistema.

3. Utilizar autorização dinâmica, aplicando o acesso sob demanda.

Quanto maior o tempo que uma determinada chave de acesso (seja ela um *token*, ou um *cookie* com a sessão de navegação salvas no navegador do usuário) maior o tempo que a identidade desse usuário pode ser utilizada sem o seu consentimento para roubo de dados no sistema. Por mais que manter a sessão de uso seja uma prática extremamente útil para o usuário, já que o mesmo não irá precisar digitar os dados de autenticação novamente, esta prática vai contra o fundamento de que a identidade deve ser removida quando não estiver sendo utilizada.

4. Tornar todo o processo seguro para aprimorar a segurança.

A segurança de um sistema não está exclusivamente nas mãos do desenvolvedor, do gerente ou do analista de segurança. A segurança da informação compete a todo o ciclo de vida de um *software*, inclusive para os não usuários diretos do sistema. Toda cadeia da organização deve estar atenta a manter hábitos seguros a fim de aprimorar a segurança. Com isso, deve-se evitar os atritos que possam acabar afetando a experiência do usuário final, garantindo assim a integridade, confidencialidade e disponibilidade dos dados, bem como a estabilidade e confiabilidade do sistema na totalidade.

5. Realizar auditoria unificada em toda a paisagem corporativa

Assim como no meio acadêmico, onde é realizada a verificação por pares de um artigo, no campo da segurança a auditoria assegura a qualidade e eficácia das medidas que estejam sendo adotadas pelas organizações. Com essa auditoria externa e unificada, pode-se detectar falhas que antes não eram observadas, além de garantir o cumprimento das políticas empresariais de segurança e da regulamentação vigente.

2.4.3 Plataformas de gerenciamento de acesso privilegiada.

Segundo Fisher (2023), Plataformas de Gerenciamento de Acesso Privilegiado (PAM) são controles críticos de cibersegurança que lidam com os riscos de segurança associados ao acesso privilegiado em organizações e empresas. Estima-se que a maioria dos ataques cibernéticos bem-sucedidos envolva o uso indevido de contas privilegiadas. E esse uso indevido é facilitado pela má gestão do acesso privilegiado por meio de software PAM desatualizado ou inadequado, políticas ou processos internos. Um relatório da RSA Conference de 2020, afirma que o acesso privilegiado potencialmente malicioso de um host desconhecido representou 74%

de todas as detecções de comportamentos anômalos relacionados ao acesso privilegiado (Jarecki, 2020). A mensagem é clara: os hackers estão mirando ativamente contas privilegiadas, como a melhor maneira de entrar em uma organização.

Mesmo que as plataformas de PAM existam há cerca de 20 anos, as demandas da transformação digital e as mudanças estruturais no ambiente de TI intensificaram o interesse por *software* e aplicativos de Gerenciamento de Acesso Privilegiado em todos os setores de mercado. Os fornecedores, tanto tradicionais quanto novos, têm respondido à demanda e à necessidade crítica por soluções avançadas de PAM que enfrentem os desafios da era da computação. Entre os principais problemas de segurança enfrentados pelo PAM, estão o abuso de credenciais compartilhadas, o tempo excessivo que os acessos privilegiados são mantidos no sistema, o uso indevido de privilégios elevados por usuários não autorizados, o roubo de credenciais privilegiadas por cibercriminosos e o abuso de privilégios em infraestrutura de nuvem.

Pesquisas da Kuppinger (2014) mostram que o mercado de PAM está respondendo e crescendo devido a esses desafios, vivendo um período vigoroso de inovação. Parte disso é a flexibilidade nas opções de compra, muito em consequência do aumento dos modelos de assinatura e opções de *software* como serviço (SaaS), que retira a obrigatoriedade de adquirir servidores e *hardwares* físicos para a operação de serviços exclusivos para a empresa, sendo necessário realizar o pagamento somente dos recursos que estejam utilizando de um servidor compartilhado. Com a evolução do PAM, de um modelo operacional estático para um modelo mais dinâmico para lidar com arquiteturas de TI igualmente dinâmicas, as opções de SaaS e de compras flexíveis tornam-se cada vez mais populares entre os clientes que não desejam ficar presos a uma tecnologia que não evolua rápido o suficiente para atender às suas demandas em constante mudança (Kuppinger, 2014).

2.5 PRINCIPAIS AMEAÇAS E RISCOS

2.5.1 Ataques Cibernéticos Voltados para Identidades Privilegiadas

Os ataques cibernéticos voltados para identidades privilegiadas representam uma das maiores ameaças à segurança da informação. Esses ataques visam obter acesso não autorizado a contas e credenciais de usuários com privilégios elevados, como administradores de sistemas ou usuários com acesso a informações sensíveis. Segundo Carroll; Smith; Johnson (2019), os invasores buscam explorar vulnerabilidades nas políticas de segurança, fraquezas em sistemas

de autenticação e autorização, ou ainda técnicas de engenharia social para enganar os usuários e obter acesso às suas credenciais.

Um exemplo comum de ataque cibernético voltado para identidades privilegiadas é o *phishing* direcionado a indivíduos com privilégios elevados. Nesse tipo de ataque, os invasores enviam e-mails falsos ou mensagens de texto que se passam por fontes confiáveis, solicitando que os usuários forneçam suas credenciais de acesso. Caso os invasores obtenham essas informações, eles podem se passar pelo usuário legítimo e realizar atividades maliciosas no sistema (Cai; Wang; Wei, 2018).

2.5.2 Potenciais Consequências da Exploração de Identidades Privilegiadas

A exploração de identidades privilegiadas pode ter consequências devastadoras para as organizações e indivíduos envolvidos. Uma vez que um invasor obtém acesso a uma identidade privilegiada, ele pode explorar essa posição para realizar uma série de atividades maliciosas, como acesso não autorizado a informações confidenciais, modificação ou exclusão de dados críticos, interrupção de serviços essenciais ou até mesmo o comprometimento de sistemas inteiros (Khalil; Khreishah; Azeem, 2014).

Por exemplo, um caixa eletrônico requer um cartão e uma senha numérica para acesso à conta bancária e informações, caso estas informações sejam interceptadas ou descobertas por um agente malicioso interno, ou por injeção de código-fonte maliciosa, resultaria em acessos não autorizados, podendo provocar danos financeiros aos clientes e as instituições que sofreram o ataque (Khalil; Khreishah; Azeem, 2014).

Além disso, a exploração de identidades privilegiadas também pode levar a violações de conformidade regulatória, resultando em consequências legais e financeiras significativas para as organizações. Por exemplo, em setores altamente regulamentados, como serviços financeiros e saúde, a exposição de informações protegidas por lei pode resultar em multas substanciais e danos à reputação da empresa (Khalil; Khreishah; Azeem, 2014).

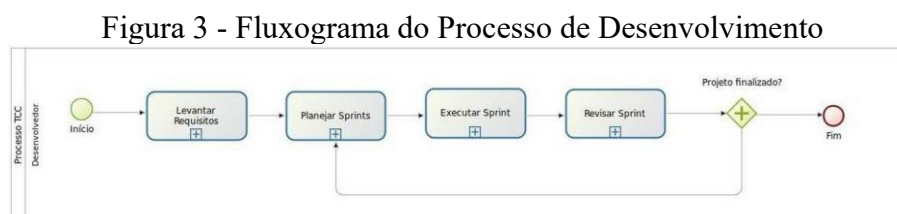
3 METODOLOGIA

Para o desenvolvimento do trabalho foi realizado inicialmente uma procura por temas, assuntos, fontes, bases bibliográficas e recursos disponíveis para sua realização. Essa busca abrangeu as bases de dados acadêmicas disponibilizadas pela UnB, a utilização do *Google scholar* e outras fontes confiáveis para a identificação dos recursos bibliográficos relevantes relacionados a identidade privilegiada de dados.

Para o desenvolvimento do sistema para sustentação deste trabalho, optou-se pelo desenvolvimento de software ágil, com ênfase na metodologia Scrum. O desenvolvimento ágil, comumente referido como *Agile*, é uma abordagem de desenvolvimento que prioriza a flexibilidade e aplica um pragmatismo significativo à entrega do produto final. Uma das vantagens notáveis de utilização da metodologia ágil é a sua capacidade de apoiar equipes em ambientes em constante evolução, garantindo que o foco permaneça na entrega eficaz do produto final (Dingsøyr *et al.*, 2012).

O Scrum é um framework ágil de natureza leve, utilizado por gestores de projeto para supervisionar uma variedade de projetos iterativos e incrementais. Dentro do contexto do Scrum, o proprietário do produto desempenha um papel essencial ao criar um backlog do produto. Essa lista permite que ele colabore com sua equipe no processo de identificação e priorização da funcionalidade do sistema (Dingsøyr *et al.*, 2012). O backlog do produto é uma compilação abrangente de todas as tarefas necessárias para a entrega bem-sucedida de um sistema de software funcional, abrangendo desde correções de bugs até recursos e requisitos não funcionais.

A Figura 3, sob a forma de fluxograma, ilustra a ordem de planejamento para realização das atividades necessárias para a realização da aplicação.



Fonte: Autores.

Conforme os quadros da Figura 3, para a entrega bem-sucedida, foi seguida a ordem do fluxograma. O processo iniciou-se com a etapa de levantamento de requisitos, seguido pelo

desenvolvimento de um produto de qualidade e a prática da entrega contínua de software. Essa abordagem sequencial e estruturada permitiu uma compreensão abrangente das necessidades do projeto e a definição clara de objetivos.

4 Desenvolvimento

O desenvolvimento deste trabalho foi projetado para incorporar práticas de segurança em um sistema exclusivo para a pesquisa. Este capítulo apresenta os métodos de gerenciamento, planejamento, técnicas de levantamento de requisitos, estrutura organizacional do projeto e a metodologia de gerenciamento de projetos.

Foi criado um problema fictício envolvendo múltiplas lojas para aplicar os conceitos da revisão teórica.

4.1 PROBLEMÁTICA FICTÍCIA E SOLUÇÃO

Para implementar os conceitos discutidos na revisão teórica, elaboramos um cenário fictício que envolve diversas lojas localizadas em diferentes cidades. Diante da necessidade de coletar manualmente dados financeiros diários de todas essas lojas para o fechamento do caixa, identificou-se um desafio significativo que demanda um tempo considerável por parte dos gerentes. Estes são obrigados a realizar a catalogação minuciosa de diversos comprovantes de pagamento.

Visando resolver essa problemática, propusemos a integração de uma API Django, projetada para simplificar e automatizar esse processo. A proposta da API é facilitar a recepção de pagamentos, além de fornecer uma listagem organizada dos mesmos. Para garantir a segurança e a eficácia do sistema, seria implementado um robusto sistema de gerenciamento de identidades, incluindo a definição de identidades privilegiadas com acesso especial.

4.1.1 Proto-persona

No contexto de engenharia de desenvolvimento de produto, personas são personagens fictícios baseados em dados demográficos reais do grupo de usuários a ser retratado e são comumente representados por uma imagem e um texto descritivo (Billestrup *et al.*, 2014). Poderosas ferramentas empáticas para se discutir os valores do usuário e adicionar diversidade de características durante o desenvolvimento, as personas são embasadas na capacidade humana de tentar prever o comportamento de outras pessoas, criando para isso modelos mentais com as características destas pessoas (Grudin, 2006).

A chamada proto-persona, proposta por Gothelf (2012), surgiu na Indústria de desenvolvimento de software como uma variação da persona clássica. Diferenciando-se principalmente pelo modo de concepção artefato, ao invés de se basear em extensas pesquisas demográficas como as personas clássicas, a proto-persona se embasa no conhecimento específico de especialistas. A proposta de Gothelf (2012) considera que integrantes do time de desenvolvimento possuem um conhecimento prévio sobre o usuário final para construir o protótipo de uma persona.

A técnica de proto-persona foi adotada no projeto devido à sua capacidade de reduzir os custos associados à pesquisa demográfica, proporcionando uma definição mais rápida e eficiente de personas. Em contraste com as personas tradicionais, que demandam coleta extensiva de dados demográficos, as proto-personas se baseiam no conhecimento prévio da equipe de desenvolvimento, eliminando a necessidade de pesquisas dispendiosas. Além disso, essa abordagem agiliza o processo de criação de personas, sendo particularmente valiosa em projetos com prazos restritos, onde a eficiência na compreensão do usuário é crucial. A escolha da proto-persona reflete a busca por eficiência e economia de recursos sem comprometer a qualidade da compreensão do usuário final.

Nome: Alberto Fernandes

Idade: 48 anos

Profissão: Empresário

Alberto é um empresário bem-sucedido que possui uma loja. Ele é casado e tem dois filhos adolescentes. Alberto está constantemente preocupado com a eficiência operacional de sua loja e está sempre em busca de maneiras de otimizar seus processos de negócios. Ele valoriza muito seu tempo e deseja simplificar a tarefa de coletar e gerenciar os dados financeiros de sua loja.

Necessidades e Expectativas

- Alberto deseja uma solução que economize tempo e esforço na coleta de dados financeiros de sua loja.
- Ele está interessado em uma plataforma que permita o acompanhamento em tempo real do faturamento de cada loja, facilitando a tomada de decisões.
- Alberto valoriza soluções tecnológicas que automatizem tarefas repetitivas e reduzam a necessidade de inserção manual de dados.
- Ele está em busca de uma maneira eficiente de consolidar as informações financeiras de sua loja em um só lugar.

4.1.2 Brainstorm

Tendo o problema listado acima, foi realizado um *brainstorm* sobre as possíveis funcionalidades desse sistema, levantando como os pontos principais.

- Deve ser possível listar todos os pagamentos.
- Deve ser possível listar os pagamentos.
- Deve possuir um sistema de gerenciamento de usuários.
- Deve existir um sistema de logs com identificação das ações de cada usuário.
- O login do usuário deve ser feito por uma autenticação multifator.
- Os dados devem ser transmitidos seguramente.

4.1.3 Solução

Com base no texto apresentado, uma solução viável é a implementação de uma plataforma de Gerenciamento de Identidade Privilegiada (*Privileged Identity Management-PIM*) e aprimoramento da segurança de dados. Essa plataforma automatizaria a coleta e a consolidação dos dados financeiros de todas as lojas em tempo real, garantindo um acesso seguro e privilegiado apenas para os responsáveis autorizados. Isso proporcionaria ao Sr. Alberto Fernandes uma visão transparente do faturamento de cada loja, ao mesmo tempo, em que fortalece as medidas de segurança de dados sensíveis. Essa abordagem está consoante aos conceitos estudados no referencial teórico, que podem ser aplicados para aprimorar a gestão de identidades privilegiadas e proteger os dados críticos do negócio de Alberto.

4.2 GESTÃO DO PROJETO DE DESENVOLVIMENTO DO SISTEMA BASE DA LOJA FICTÍCIA

Visando alcançar um aprimoramento constante e progressivo deste documento e do sistema que ele propõe, a metodologia de gestão adotada envolve o desenvolvimento simultâneo da aplicação e desta monografia.

4.3 CICLOS DE DESENVOLVIMENTO

Os ciclos de desenvolvimento foram estabelecidos com uma duração fixa de 7 (sete) dias, abrangendo a implementação de funcionalidades completas, incluindo a documentação, o *Back-End* e o *Front-End*. Essa abordagem visa assegurar uma entrega contínua e significativa de valor para a conclusão do projeto.

4.4 FLEXIBILIDADE E ADAPTABILIDADE

A abordagem de desenvolvimento em ciclos curtos e simultâneos oferece vantagens ao permitir maior flexibilidade e adaptabilidade no processo. Completar os ciclos em curto prazo possibilita responder rapidamente a mudanças nas prioridades dos requisitos elicitados. Assim, se surgir uma nova necessidade ou oportunidade de melhoria, ela pode ser incorporada no próximo ciclo, garantindo uma resposta ágil às demandas propostas.

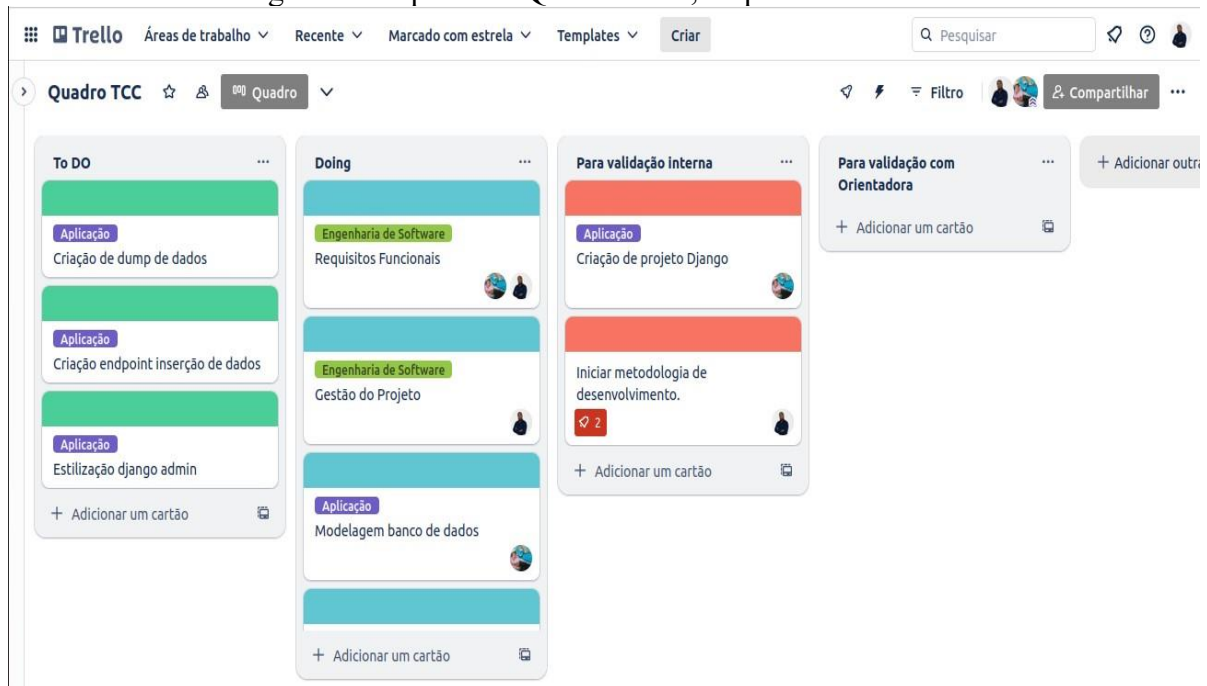
4.5 INTEGRAÇÃO ENTRE PESQUISA ACADÊMICA E DESENVOLVIMENTO PRÁTICO

Outro ponto importante é a integração natural entre a pesquisa acadêmica e o desenvolvimento prático. A monografia é atualizada a cada ciclo de desenvolvimento para refletir o estado atual do sistema, abordando os desafios enfrentados, as soluções implementadas e os resultados obtidos, proporcionando uma narrativa mais rica e fundamentada.

4.6 KANBAN

O Kanban é baseado na ideia de que o trabalho é visualizado como tarefas em cartões, movidos por meio de etapas específicas do processo à medida que são concluídas.

Figura 4 - Captura do Quadro TCC, na plataforma Trello



Fonte: Autores.

4.7 PERFIL DE USUÁRIOS

O gerenciamento e permissão de usuário são passos de extrema importância para a segurança do sistema, pois é através deles que é definido o nível de acesso de cada usuário, e quais ações ele pode realizar dentro do sistema, para exemplificar, foi criado perfis de usuário, com suas respectivas permissões, conforme o Quadro 1.

Quadro 1 - Tipos de usuários sistema Spay

Perfil	Descrição
Administrador	O administrador é o usuário com o maior nível de acesso, podendo realizar todas as ações dentro do sistema. Possuindo permissão para acesso total a página de administração.
Auditor	O auditor é o usuário responsável por auditar as ações realizadas dentro do sistema, podendo visualizar os logs de ações realizadas por todos os usuários. Tendo Acesso somente aos registros de logs no painel de administração.
Contador	O contador é o usuário responsável por gerenciar os pagamentos, podendo visualizar todos os pagamentos realizados.
Diretor	O diretor é o usuários responsável por adicionar os pagamentos, não permitindo a esse usuário visualizar os pagamentos.
Sócio	O sócio é o usuário que possui permissão tanto de criação quando te visualização dos pagamentos.

Fonte: Autores.

4.8 REQUISITOS

4.8.1 Requisitos Não Funcionais

Os requisitos não funcionais são elementos críticos que afetam o desempenho, a segurança e a eficácia geral do sistema. Eles abrangem várias áreas, desde segurança e eficiência até escalabilidade e conformidade com regulamentações. Esses requisitos garantem que o sistema não apenas funcione corretamente, mas também atenda a padrões de qualidade e desempenho. No Quadro 2, listamos os principais requisitos não funcionais do sistema.

4.8.2 Requisitos Funcionais

Primeira Introspecção

Durante a primeira introspecção do software, foi realizada a listagem dos requisitos funcionais do projeto, conforme apresentado no Quadro 3.

4.8.3 Requisitos Funcionais Priorizados

Após a segunda passagem nos requisitos elicitados, foi realizada a priorização dos requisitos funcionais, resultando na seguinte ordem. Os detalhes podem ser encontrados no Quadro 4.

Essas tabelas fornecem uma visão detalhada dos requisitos funcionais identificados e priorizados durante o processo de introspecção do software. Elas servem como base para o desenvolvimento do sistema e a priorização ajuda a determinar quais funcionalidades são mais críticas e devem ser implementadas primeiro.

Quadro 2 - Requisitos não funcionais

Código	Descrição
RNF-01	O sistema deve atender a padrões de segurança rigorosos para proteger as informações de pagamento, incluindo autenticação de dois fatores, criptografia de dados e proteção contra ataques como injeção SQL.
RNF-02	O sistema deve conseguir lidar com um grande volume de informações de pagamento e relatórios eficientemente, garantindo tempos de resposta aceitáveis.
RNF-03	Deve ser possível dimensionar o sistema para acomodar um aumento no número de lojas e usuários sem perda significativa de desempenho.
RNF-04	O sistema deve estar disponível 24/7, com um tempo de inatividade planejado mínimo para manutenção.
RNF-05	O sistema deve estar conforme as regulamentações de privacidade de dados, como o Lei Geral de Proteção de Dados (LGPD) e leis locais de proteção de dados.
RNF-06	A interface do usuário do sistema deve ser amigável e intuitiva para garantir que os usuários possam realizar suas tarefas facilmente.
RNF-07	O sistema deve conseguir registrar atividades de usuário e transações para fins de auditoria e conformidade.
RNF-08	O sistema deve ter um plano de recuperação de desastres em vigor para garantir a disponibilidade contínua dos dados em caso de falha do sistema.
RNF-09	Deve haver um plano de manutenção regular e suporte técnico para resolver problemas e garantir que o sistema esteja sempre atualizado.

Fonte: Autores.

4.9 FLUXO DE DESENVOLVIMENTO E TECNOLOGIAS DO SISTEMA BASE

O fluxo de desenvolvimento do projeto foi dividido utilizando o modelo incremental. O modelo de desenvolvimento incremental pode ser adotado como estrutura metodológica para a execução de projetos. O processo de desenvolvimento será estruturado em incrementos, representados por versões do produto. Cada incremento corresponderá a um conjunto de funcionalidades específicas a serem desenvolvidas, e essas funcionalidades serão detalhadas em *issues* ou tarefas individuais. À medida que cada incremento é concluído, ele será incorporado ao produto, representando uma nova versão. Esse modelo de trabalho permitirá uma abordagem iterativa, na qual aprimoramentos contínuos e ajustes podem ser realizados à medida que o projeto avança. Além disso, a documentação e análise detalhada serão fornecidas para cada incremento, demonstrando o progresso e as decisões tomadas ao longo do desenvolvimento.

Quadro 3 - Requisitos funcionais não priorizados

Código	Nome	Descrição
RF-01	Registro de Pagamentos	O sistema deve permitir o registro de informações de pagamento recebidas por meio da API REST.
RF-02	Comunicação Segura	O sistema deve garantir uma comunicação segura com a API REST, usando protocolos de segurança, como HTTPS, para evitar a interceptação de informações sensíveis.
RF-03	Armazenamento de Dados	O sistema deve armazenar as informações de pagamento de forma segura e organizada em um banco de dados.
RF-04	Relatórios	O sistema deve conseguir gerar relatórios com base nas informações de pagamento, permitindo que os usuários visualizem esses dados de maneira compreensível.
RF-05	Gerenciamento de Lojas	Deve haver funcionalidades para adicionar, editar e excluir informações relacionadas a várias lojas que utilizam o sistema.
RF-06	Gerenciamento de Usuários	O sistema deve permitir o cadastro de usuários com diferentes níveis de acesso, como administradores e funcionários. Cada usuário deve ter acesso apenas às informações relacionadas da loja que gerencia.
RF-07	Autenticação segura	O sistema deve implementar uma autenticação segura, para verificar a identidade dos usuários durante o login.
RF-08	Controle de Acesso	O sistema deve garantir que apenas os usuários autorizados tenham acesso às informações específicas relacionadas às lojas que gerenciam.

Fonte: Autores.

4.10 TECNOLOGIAS

4.10.1 Python

Python é uma linguagem de programação versátil amplamente usada no desenvolvimento de aplicativos web. Sua sintaxe simples e legibilidade tornam-na uma escolha popular entre desenvolvedores ([Python Software Foundation, 2023](#)). Além disso, Python possui uma vasta biblioteca padrão que abrange desde processamento de texto até aprendizado de máquina, facilitando o desenvolvimento eficiente de aplicativos.

Quadro 4 - Requisitos funcionais priorizados

Posição	Código	Descrição
1	RF-02	O sistema deve garantir uma comunicação segura com a API REST, usando protocolos de segurança, como o TLS, para evitar a interceptação de informações sensíveis.
2	RF-08	O sistema deve garantir que apenas os usuários autorizados tenham acesso às informações específicas relacionadas às lojas que gerenciam.
3	RF-07	O sistema deve implementar uma autenticação segura, para verificar a identidade dos usuários durante o login.
4	RF-06	O sistema deve permitir o cadastro de usuários com diferentes níveis de acesso, como administradores e funcionários. Cada usuário deve ter acesso apenas às informações relacionadas à(s) loja(s) que gerenciam.
5	RF-03	O sistema deve armazenar as informações de pagamento de forma segura e organizada em um banco de dados.
6	RF-05	Deve haver funcionalidades para adicionar, editar e excluir informações relacionadas a várias lojas que utilizam o sistema.
7	RF-01	O sistema deve permitir o registro de informações de pagamento recebidas por meio da API REST.
8	RF-04	O sistema deve conseguir gerar relatórios com base nas informações de pagamento, permitindo que os usuários visualizem esses dados de maneira compreensível.

Fonte: Autores.

4.10.2 Django

Django é um framework de desenvolvimento web em Python que simplifica a criação de aplicativos robustos e escaláveis ([Django Software Foundation, 2023](#)). Ele segue o princípio *batteries-included*, fornecendo um conjunto abrangente de funcionalidades que aceleram o desenvolvimento. Com recursos como o sistema de administração automática, autenticação de usuário e roteamento de URL, Django é uma escolha poderosa para desenvolvedores que desejam construir aplicativos web de alta qualidade.

4.10.3 PostgreSQL

A escolha do PostgreSQL para o projeto é respaldada por sua sólida reputação de confiabilidade e pelos recursos avançados que oferece ([PostgreSQL, 2023](#)). Este sistema de gerenciamento de banco de dados relacional de código aberto é conhecido por sua capacidade de fornecer armazenamento robusto, transações ACID (Atômicas, Consistentes, isoladas e duráveis) e suporte à replicação. Esses atributos, além de justificarem a escolha de tal banco para o projeto, garantem eficiência, segurança e escalabilidade, aspectos cruciais para atender

às necessidades de armazenamento e recuperação de dados em um projeto de aplicativo web de alta qualidade.

4.10.4 Django REST framework

O Django REST framework é uma extensão do Django que simplifica a criação de APIs RESTful (Django REST framework, 2023). Ele fornece suporte para serialização de dados, autenticação, autorização e muito mais. Com a facilidade de integração com o Django, ele é amplamente utilizado no desenvolvimento de serviços web escaláveis e orientados a recursos.

4.10.5 HTTPS (Hypertext Transfer Protocol Secure)

O protocolo HTTPS é essencial para garantir a segurança de comunicações na web. Ele fornece criptografia de dados entre o cliente e o servidor, protegendo informações confidenciais de ataques. Além disso, HTTPS é uma parte fundamental na garantia da privacidade e integridade das transações on-line. Informações detalhadas sobre HTTPS podem ser encontradas no site oficial do Let's Encrypt (Let's Encrypt, 2023).

4.10.6 OAuth2 (Open Authorization)

OAuth2 é um protocolo de autorização amplamente utilizado para garantir a segurança de aplicativos web e APIs. Ele permite que aplicativos solicitem acesso a recursos em nome de um usuário, sem a necessidade de compartilhar credenciais. A especificação oficial do OAuth2 pode ser encontrada no RFC 6749 (OAuth [...], 2012), fornecendo as diretrizes essenciais para a implementação de autorização segura.

4.10.7 Google MFA (Multi-Factor Authentication)

A autenticação de vários fatores desempenha um papel crítico na proteção da identidade dos usuários. O Google MFA é uma implementação de autenticação de dois fatores (2FA) fornecida pelo Google. Ele adiciona uma camada adicional de segurança exigindo uma segunda forma de autenticação, como um código gerado por um aplicativo móvel, juntamente com a senha. Essa abordagem é eficaz na prevenção de acessos não autorizados (Google, 2023).

4.10.8 Docker

Docker é uma plataforma de código aberto que permite o desenvolvimento, implantação e execução de aplicativos em contêineres (Docker [...], 2023b). Os contêineres são unidades de empacotamento que incluem o código, as bibliotecas e todas as dependências necessárias para a execução de um aplicativo. A escolha do Docker oferece diversos benefícios, incluindo a padronização do ambiente de desenvolvimento e implantação, a portabilidade entre diferentes sistemas e a capacidade de escalar aplicativos com facilidade.

4.10.9 Docker Compose

O Docker Compose é uma ferramenta que simplifica a definição e o gerenciamento de aplicativos Docker multi-contêiner em um único arquivo (Docker [...], 2023a). Ele permite a especificação de todos os serviços, redes e volumes necessários para um aplicativo em um único arquivo YAML. Com o Docker Compose, é possível iniciar e interligar vários contêineres com um único comando, simplificando o desenvolvimento, a execução e a escalabilidade de aplicativos complexos.

4.10.10 Swagger

Swagger é uma estrutura para descrição, documentação e geração de código de APIs RESTful (Swagger, 2023). Ele fornece uma maneira padronizada de definir a estrutura de uma API, incluindo os endpoints, parâmetros, respostas e modelos de dados. A documentação gerada automaticamente a partir de especificações Swagger facilita a compreensão e o uso das APIs, tornando-as mais acessíveis para desenvolvedores e equipes de desenvolvimento. A escolha de integrar o Swagger no projeto visa melhorar a documentação e a compreensão da API desenvolvida.

4.10.11 NGINX

NGINX é um servidor web de código aberto amplamente reconhecido pelo seu desempenho, escalabilidade e flexibilidade. Ele atua como servidor web, proxy reverso e balanceador de carga, sendo uma escolha popular para hospedar sites e aplicativos da web. Sua configuração baseada em arquivos de texto simples permite uma personalização avançada, e o

suporte a SSL/TLS garante comunicações seguras. O NGINX é uma solução confiável para melhorar a velocidade e a disponibilidade de serviços on-line, sendo uma opção poderosa para a infraestrutura de hospedagem. Para mais detalhes, consulte a documentação oficial em ([NGINX, 2023](#)).

4.11 APLICAÇÃO BASE

Para fins de validação e testes, foi desenvolvida a aplicação denominada Spay. Esse projeto adotou a metodologia de desenvolvimento incremental para sua construção, sendo utilizada a linguagem de programação Python, juntamente com o framework Django para a codificação. Além de outras diversas bibliotecas para a implementação de uma API, autenticação multifator, autorização e testes automatizados.

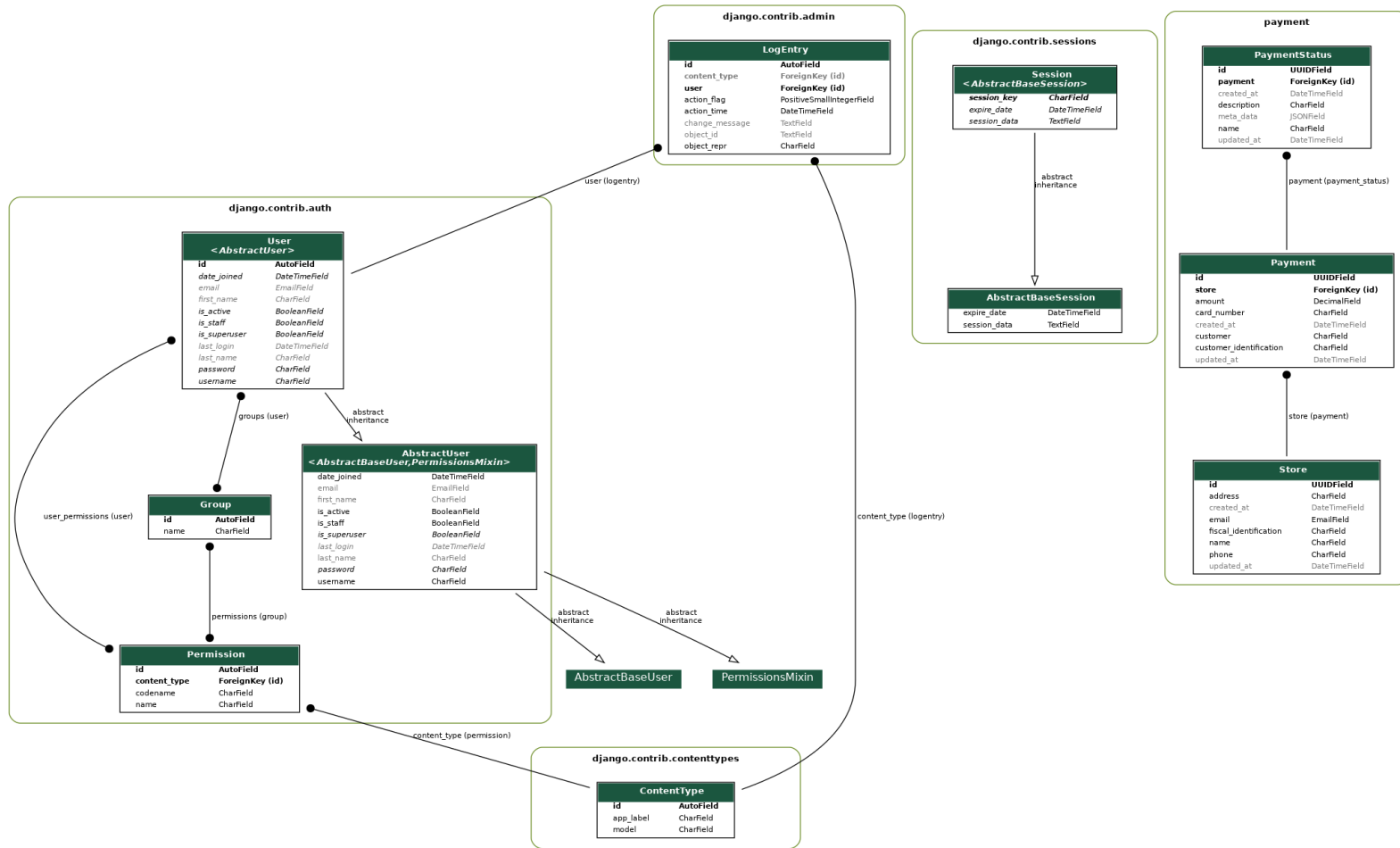
As escolhas das linguagens, frameworks e tecnologias utilizadas durante o desenvolvimento se deu pelo amplo uso na indústria de tais ferramentas, pela facilidade e robustez, e pela ampla documentação disponível publicamente.

4.11.1 Diagramas

4.11.1.1 Diagramação do projeto completo

Para a Diagramação da aplicação foi utilizado o pacote *pygraphviz* do Python, com este pacote foi realizado a criação de duas figuras: a Figura 5 representa o diagrama de toda a aplicação, incluindo os módulos criados pelo Django para realizar o gerenciamento de usuário e demais subsistemas.

Figura 5 - Diagrama Entidade Relacionamento, sistema Spay v1.0.0.



Fonte: Autores.

4.11.1.2 Diagramação do Módulo de Pagamentos

A Figura 6 representa o diagrama de entidade relacionamento do módulo de Pagamentos do sistema Spay v1.0.0, criado em 26 de setembro de 2023.

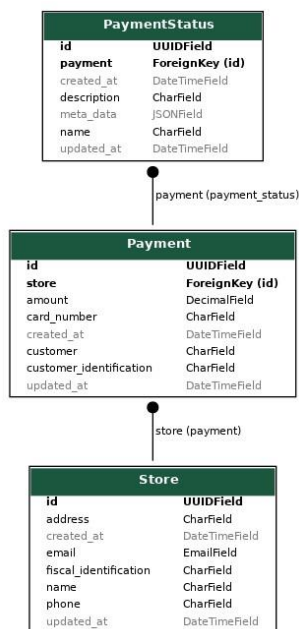
Neste diagrama, é possível observar a estrutura e as relações entre as principais entidades que compõem o módulo de Pagamentos do sistema Spay. O diagrama oferece uma representação visual das tabelas e seus atributos, bem como as conexões entre elas. As entidades representadas no diagrama incluem:

Store (Loja): Esta entidade contém informações sobre as lojas, incluindo um identificador único, nome, identificação fiscal, data de criação, data de atualização, número de telefone, endereço e endereço de e-mail. Cada loja é associada a vários pagamentos por meio de um relacionamento de chave estrangeira.

Payment (Pagamento): Esta entidade registra informações sobre os pagamentos.

PaymentStatus (Status do Pagamento): Esta entidade rastreia o status de cada pagamento registrado no sistema.

Figura 6 - Diagrama de Entidade Relacionamento, Módulo de Pagamentos, Sistema Spay v1.0.0.



Fonte: Autores.

4.12 VERSÕES DESENVOLVIDAS

Durante o desenvolvimento do projeto, optou-se por adotar uma abordagem incremental, resultando na criação de versões sucessivas. Cada versão representa um ciclo de desenvolvimento, incorporando funcionalidades e/ou melhorias no sistema.

4.12.1 v1.0.0 - Sem Implementações específicas de segurança

A versão 1.0.0 marcou o estágio inicial do projeto, durante o qual um aplicativo Django básico foi desenvolvido. Este protótipo tinha o propósito de destacar as vulnerabilidades comuns encontradas em projetos Django, focando em segurança e controle de identidade.

4.12.2 v1.1.0 - Implementação do sistema de logs

Na versão 1.1.0, o foco principal foi aprimorar o monitoramento da aplicação. Foram implementadas melhorias significativas, incluindo a introdução de um sistema de registro de logs. Isso permitiu o rastreamento de eventos cruciais no sistema, como acessos de usuários e erros, proporcionando aos administradores uma visão detalhada das atividades.

A Figura 7 apresenta o arquivo de logs criado, enquanto a Figura reffig08 apresenta os logs registrados pela aplicação Spay na versão 1.1.0.

Figura 7 - Logs em arquivo na aplicação Spay, v1.1.0.

```
luismarques@Spay:~/SPay/logs/backend$ tail -20 debug.log
raise DisallowedHost(msg)
django.core.exceptions.DisallowedHost: Invalid HTTP_HOST header: '20.84.59.116'. You may need to add '20.84.59.116' to ALLOWED_HOSTS.
2023-11-24 07:45:17.925 WARNING log 10 140184100267712 Bad Request: /.well-known/security.txt
2023-11-24 07:45:17.926 WARNING basehttp 10 140184100267712 "GET /.well-known/security.txt HTTP/1.0" 400 63281
2023-11-24 07:45:20.100 ERROR exception 10 140184100267712 Invalid HTTP_HOST header: '20.84.59.116'. You may need to add '20.84.59.116' to ALLOWED_HOSTS.
Traceback (most recent call last):
  File "/usr/local/lib/python3.11/site-packages/django/core/handlers/exception.py", line 55, in inner
    response = get_response(request)
               ~~~~~^
  File "/usr/local/lib/python3.11/site-packages/django/utils/deprecation.py", line 133, in __call__
    response = self.process_request(request)
               ~~~~~^
  File "/usr/local/lib/python3.11/site-packages/django/middleware/common.py", line 48, in process_request
    host = request.get_host()
           ~~~~~^
  File "/usr/local/lib/python3.11/site-packages/django/http/request.py", line 150, in get_host
    raise DisallowedHost(msg)
django.core.exceptions.DisallowedHost: Invalid HTTP_HOST header: '20.84.59.116'. You may need to add '20.84.59.116' to ALLOWED_HOSTS.
2023-11-24 07:45:28.198 WARNING log 10 140184100267712 Bad Request: /favicon.ico
2023-11-24 07:45:28.199 WARNING basehttp 10 140184100267712 "GET /favicon.ico HTTP/1.0" 400 63662
luismarques@Spay:~/SPay/logs/backend$ ls
debug.log
luismarques@Spay:~/SPay/logs/backend$
```

Fonte: Autores

4.12.3 v1.2.0 - Implementação de novos recursos e integrações de pacotes

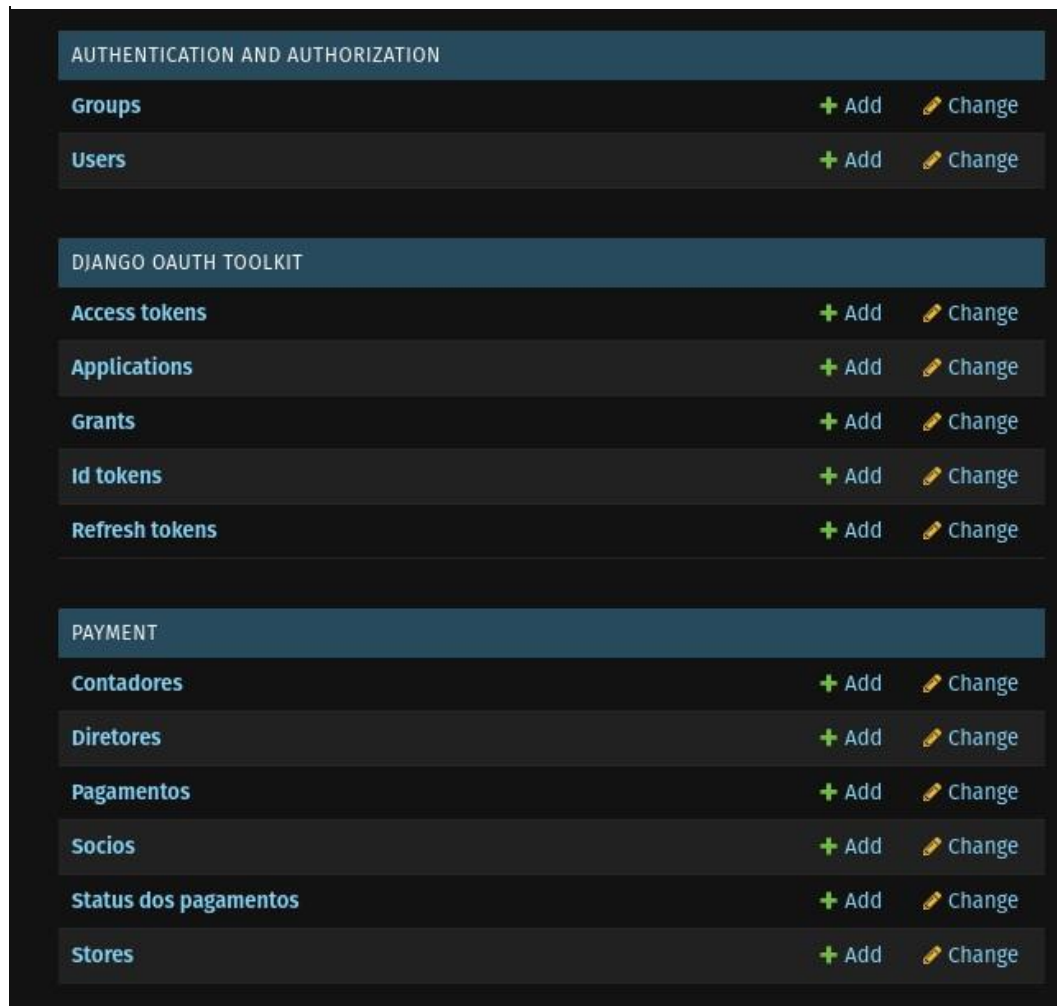
A versão 1.2.0 concentrou-se na implementação de novos recursos e integrações de pacotes para aprimorar a funcionalidade e a segurança da aplicação. Destaques incluem a integração do pacote oauth2provider para aprimorar a autenticação, a integração do pacote corsheaders para lidar com problemas de CORS, refinamentos na interface do usuário, correção de bugs e ajustes gerais.

A Figura 9 apresenta os novos módulos adicionados à aplicação Spay na versão 1.2.0.

4.12.4 v1.3.0 - Implementação de funções de autorização

Na versão 1.3.0, foram implementadas mudanças substanciais nas funções de autorização para as vistas *PaymentCreateView* e *PaymentListView*. Isso visava aprimorar a segurança e o controle de acesso, adaptando-se eficazmente às diferentes funções de usuário.

Figura 8 - Novos Módulos Aplicação Spay, v1.2.0.



AUTHENTICATION AND AUTHORIZATION		
Groups	+ Add	Change
Users	+ Add	Change
DJANGO OAUTH TOOLKIT		
Access tokens	+ Add	Change
Applications	+ Add	Change
Grants	+ Add	Change
Id tokens	+ Add	Change
Refresh tokens	+ Add	Change
PAYMENT		
Contadores	+ Add	Change
Diretores	+ Add	Change
Pagamentos	+ Add	Change
Socios	+ Add	Change
Status dos pagamentos	+ Add	Change
Stores	+ Add	Change

Fonte: Autores.

As Figuras 10 e 11 apresentam os diagramas de autorização para as vistas *PaymentCreateView* e *PaymentListView*.

4.12.4.1 Mudanças nas Funções de Autorização da PaymentCreateView

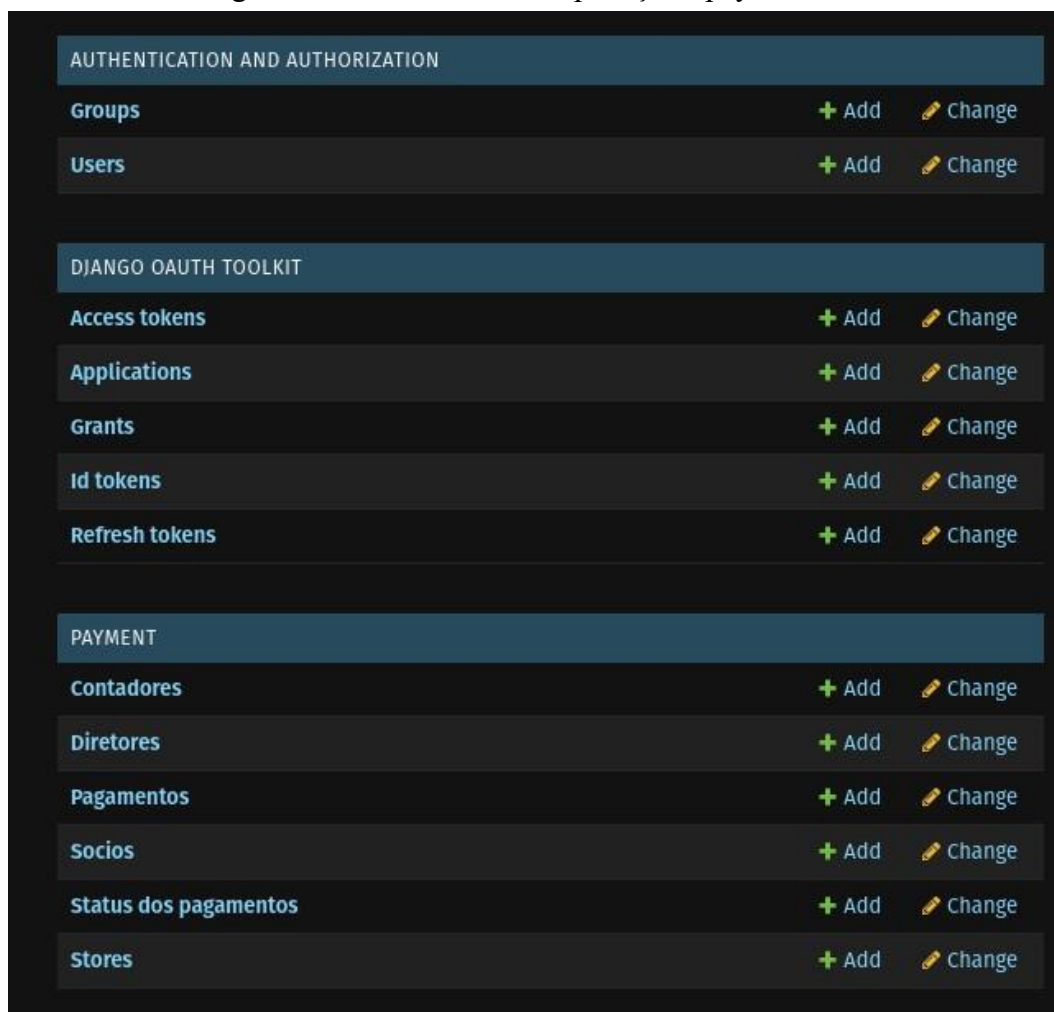
Fluxo de Autorização:

1. Quando uma solicitação é feita ao endpoint `/payment/create`, o sistema inicia verificando se o usuário está autenticado.

2. Se o usuário estiver autenticado, o sistema avança para a próxima etapa, onde verifica se o usuário possui a função de "Parceiro" ou "Diretor". Se o usuário detiver uma dessas funções, o acesso é permitido.

3. Com o acesso concedido, a view `PaymentCreateView` continua o processo de criação de um pagamento. Após a conclusão bem-sucedida da operação, uma resposta de sucesso (HTTP 200) é gerada.

Figura 9 - Novos Módulos Aplicação Spay, v1.2.0



Fonte: Autores.

4. Além disso, detalhes sobre os dados da solicitação e da resposta são registrados para fins de auditoria, e a resposta é então enviada ao usuário.

4.12.4.2 Mudanças nas Funções de Autorização da PaymentListView

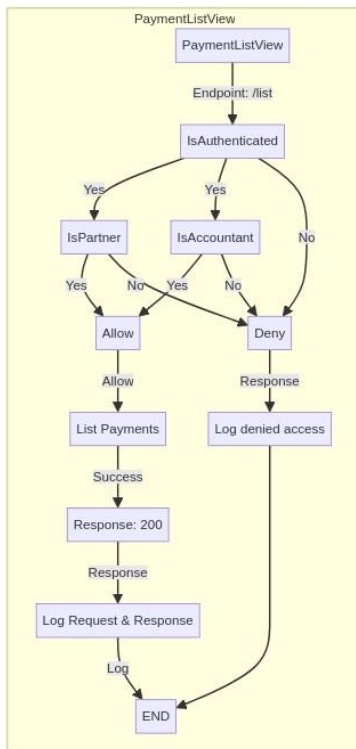
Fluxo de Autorização:

1. Quando uma solicitação é feita ao endpoint `/payment/list`, o sistema segue o mesmo protocolo de verificação inicial, onde verifica se o usuário está autenticado.

2. Se o usuário estiver autenticado, o sistema passa para a próxima fase, onde verifica se o usuário possui a função de "Parceiro" ou "Contador". Se o usuário detiver uma dessas funções, o acesso é autorizado.

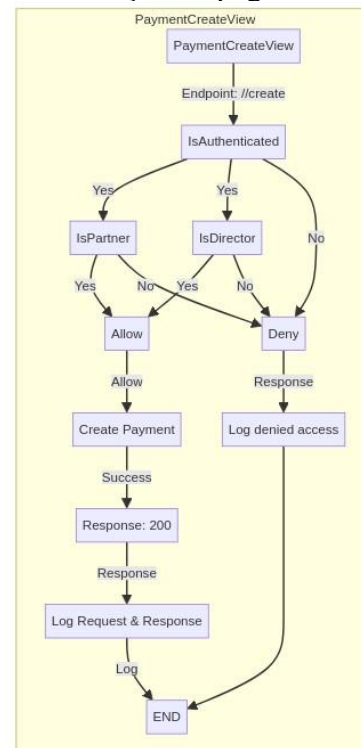
3. Uma vez concedido o acesso, a view `PaymentListView` prossegue para listar os pagamentos disponíveis no sistema. Após a conclusão da operação, uma resposta de sucesso (HTTP 200) é retornada ao usuário.

Figura 10 - Diagrama de autorização da listagem de pagamentos, v1.3.0.



Fonte: Autores.

Figura 11 - Diagrama de autorização da criação de pagamentos, v1.3.0.



Fonte: Autores

4. Da mesma forma, os dados da solicitação e da resposta são registrados para fins de auditoria, garantindo a conformidade e a rastreabilidade das operações.

4.12.5 v1.4.0 - Implementação de autenticação multifatorial

A versão 1.4.0 introduziu um sistema de autenticação multifatorial para a página de administração do site, considerada a área com maior quantidade de recursos e, portanto, restrita ao administrador do sistema. Esse novo sistema adiciona uma camada a mais de segurança ao login, exigindo a criação de senhas seguras e implementando a autenticação TOTP.

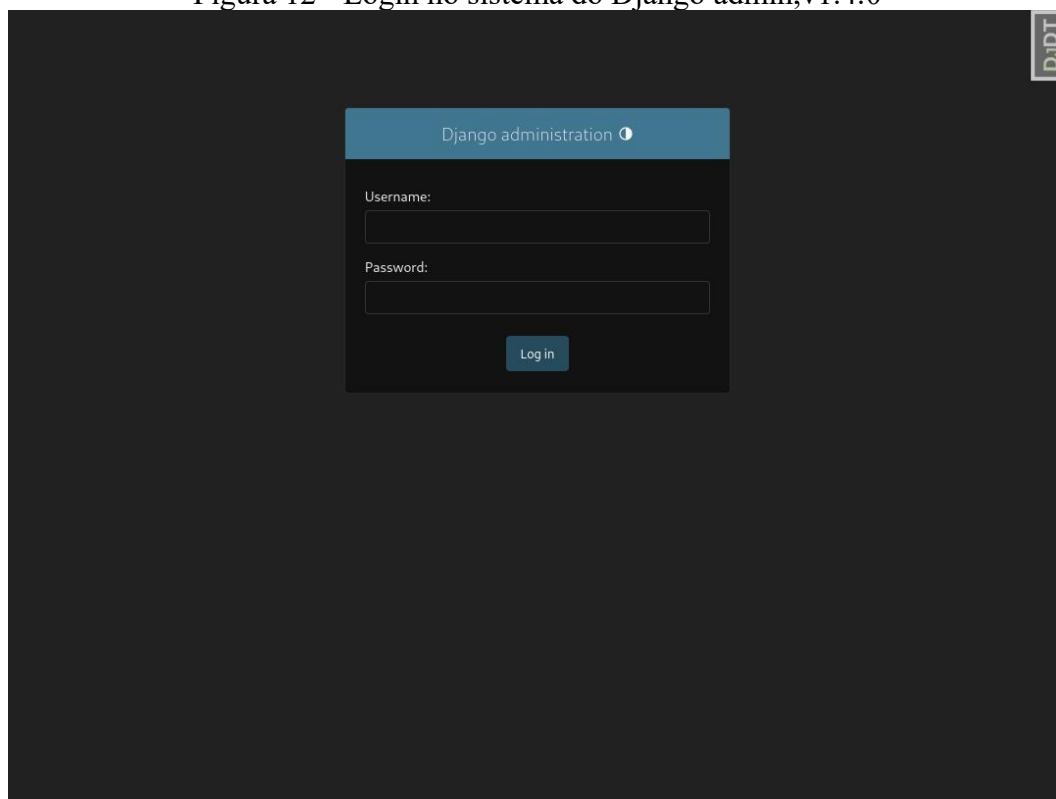
passo 1. Login

O primeiro passo consiste na realização do login padrão, com usuário e senha, a fim de incrementar a segurança do sistema é exigência ao usuário que seja realizada o cadastro de uma senha segura, os requisitos de senha são:

- A senha não pode ser muito semelhante às outras informações pessoais do usuário.
- A senha deve conter pelo menos 8 caracteres.
- A senha não pode ser uma senha comumente usada.
- A senha não pode ser completamente numérica.

As telas de login podem ser vistas nas figuras 12 e 13.

Figura 12 - Login no sistema do Django admin,v1.4.0



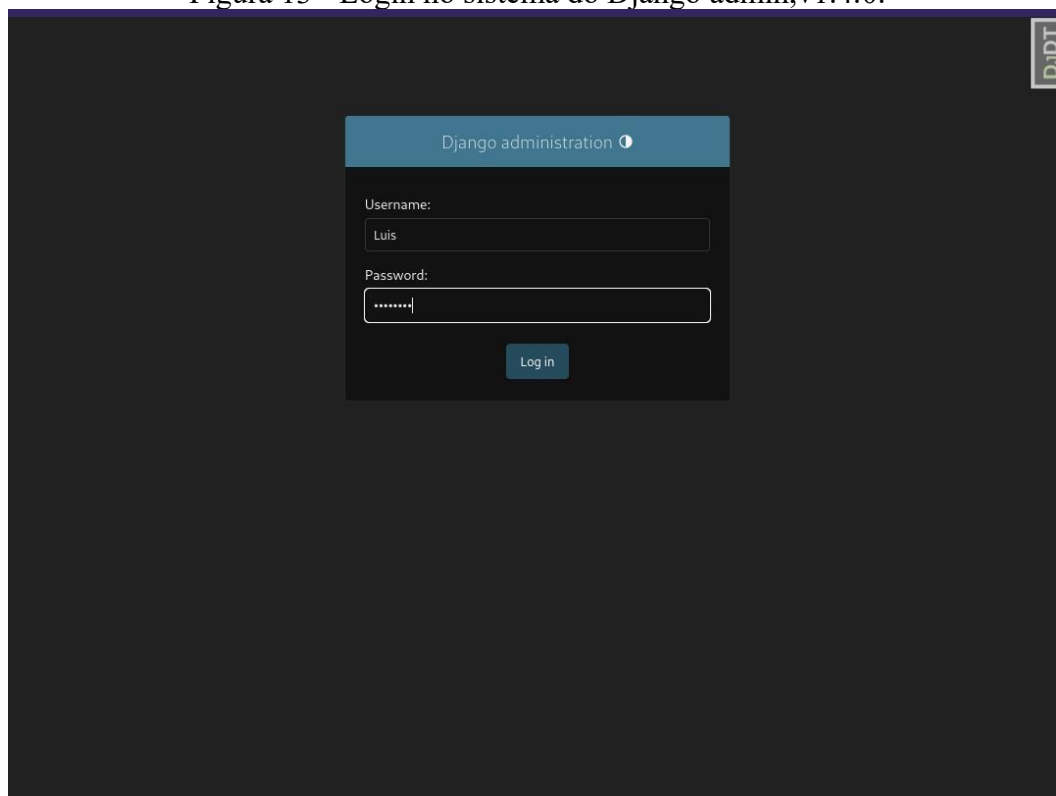
Fonte: Autores.

passo 2. Cadastramento MFA

Após o login, se o usuário não tiver um sistema de Autenticação Multifator (MFA) registrado, é solicitado que escolha um método, com destaque para a autenticação TOTP. A Autenticação TOTP no sistema funciona da seguinte forma:

1. O usuário instala um aplicativo de autenticação em seu dispositivo, como o Google Authenticator ou o Authy.
2. Quando o usuário configura a autenticação TOTP, o sistema gera um segredo compartilhado entre o usuário e o sistema.

Figura 13 - Login no sistema do Django admin, v1.4.0.



Fonte: Autores.

3. Esse segredo é usado para gerar códigos de autenticação de uso único. Esses códigos têm uma validade de 1 minuto.
4. Quando o usuário tenta fazer login, o sistema solicita um código TOTP.
5. O usuário gera o código atual no aplicativo de autenticação.
6. O código TOTP gerado é baseado no segredo compartilhado e no tempo atual.
7. O código é inserido pelo usuário, sendo verificado pelo sistema. Se for válido, o usuário é autenticado.

A principal vantagem da autenticação TOTP é que os códigos de uso único têm uma validade limitada, tornando-os eficazes na proteção das contas do usuário. Além disso, como

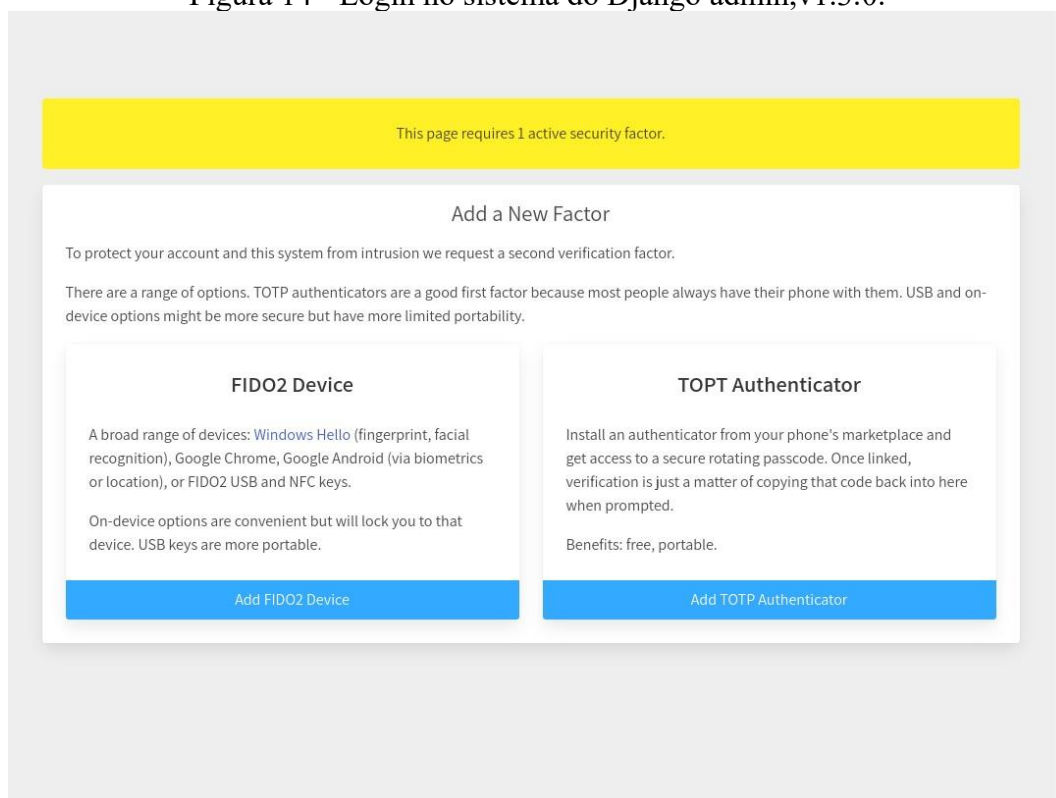
os códigos são baseados no tempo, eles são gerados automaticamente e não requerem o uso de redes de comunicação, tornando a autenticação mais segura.

A Figura 14 mostra a tela de escolha do sistema de autenticação multifator.

Escolhido o sistema TOTP, ira aparecer um QR code onde é possível realizar o scanner utilizando um aplicativo TOTP no smartphone (como exemplo foi utilizado o Google *authenticator*).

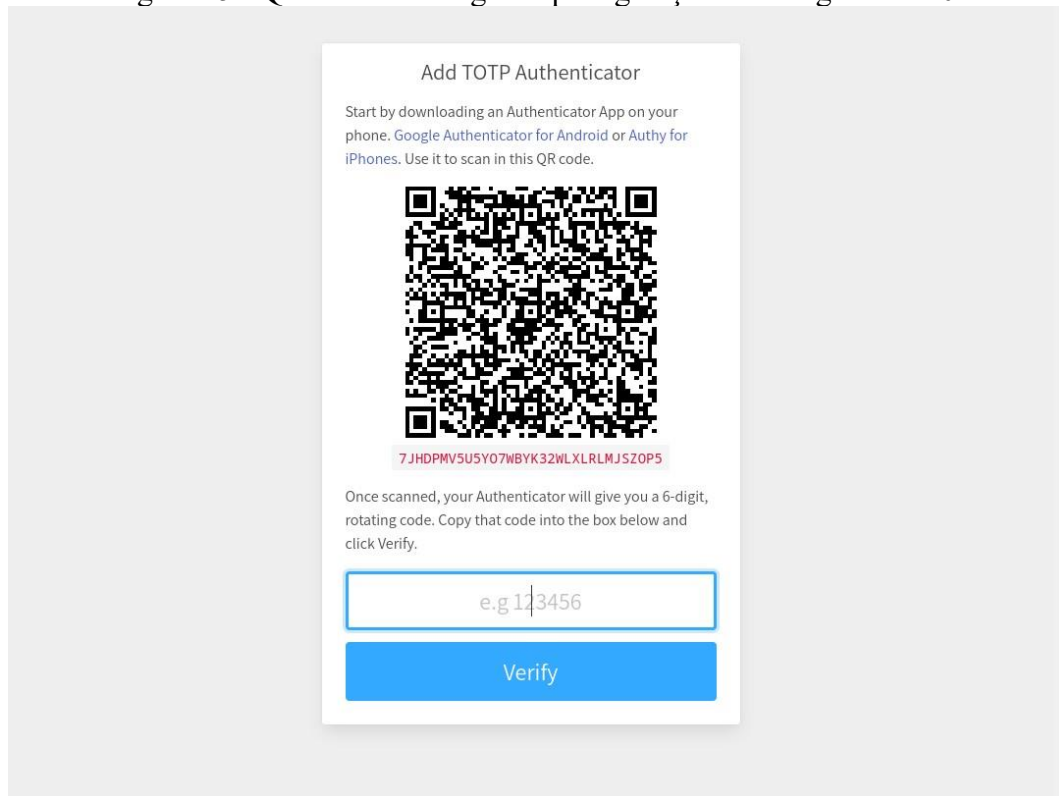
A Figura 15 mostra o QR code gerado pelo sistema.

Figura 14 - Login no sistema do Django admin,v1.3.0.



Fonte: Autores.

Figura 15 - QR code com segredo para geração de códigos. v1.4.0.

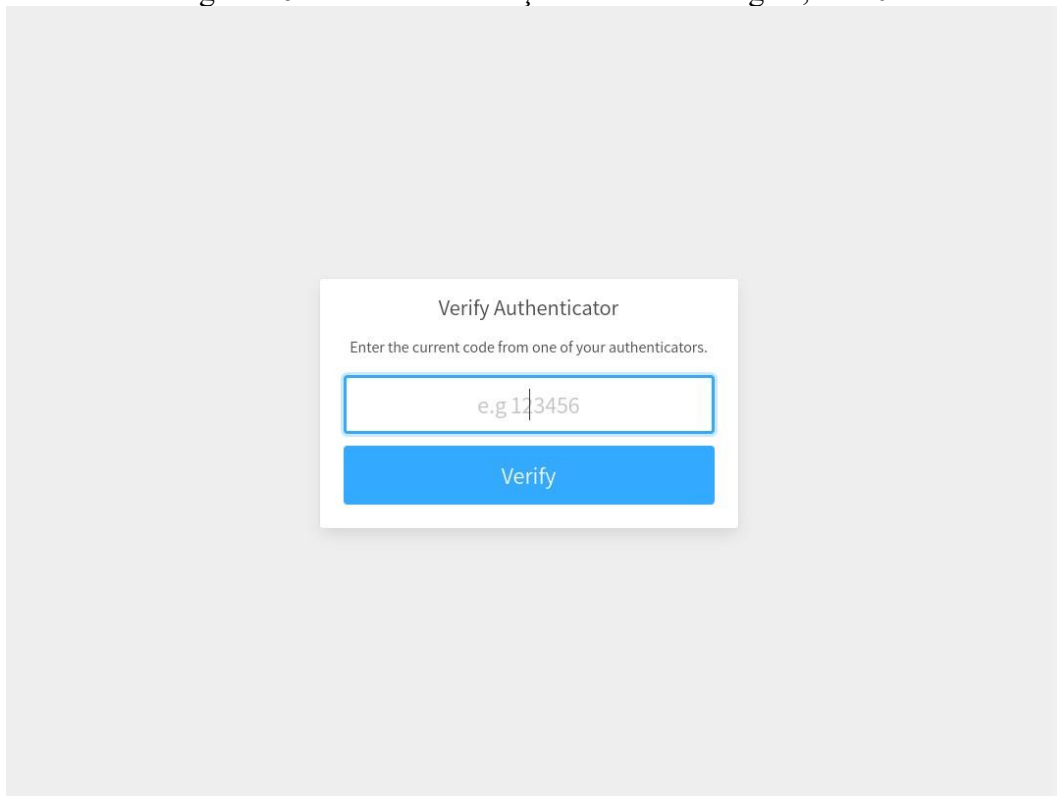


Fonte: Autores.

passo 3. Utilização do MFA

Após este primeiro cadastro, os demais logins no sistema, após a digitação da senha do usuário, irá solicitar o código de autenticação de 6 números que será fornecido pelo aplicativo, sendo mais uma camada de segurança para garantia da autenticidade do usuário. Esse processo pode ser visto na Figura 16.

Figura 16 - Tela de verificação nos demais logins,v1.4.0.



Fonte: Autores

4.12.6 v1.5.0 - Implementação de HTTPS

A versão 1.5.0 priorizou a segurança nas comunicações, implementando o protocolo HTTPS para criptografar os dados transmitidos entre o usuário e o servidor.

A Figura 17 mostra os requests realizados via https para os endpoints Spay.

4.12.7 v1.6.0 - Implementação de visualização de logs

A versão 1.6.0 visou facilitar a análise e o monitoramento do sistema, introduzindo uma página dedicada para visualização de logs. Isso proporciona uma maneira eficiente de analisar registros de acesso, erros e outras informações, sem a necessidade de acesso direto ao servidor.

A Figura 18 mostra a página de logs do sistema, onde é possível visualizar os logs de acesso, erros e ações realizadas pelos usuários.

5 RESULTADOS E DISCUSSÃO

Durante o desenvolvimento desse trabalho, foi possível identificar diversas vulnerabilidades de segurança, como a falta de validação de autenticação, comunicações inseguras por HTTP e falta de controle de acesso. Essas vulnerabilidades foram tratadas durante as versões desenvolvidas.

A fim de facilitar a obtenção de métricas e comparação entre as versões desenvolvidas, tendo em vista que cada versão foi desenvolvida com o objetivo de corrigir as vulnerabilidades identificadas na versão anterior, foi criado um roteiro de testes a ser executado em cada versão desenvolvida. Esse roteiro de testes foi desenvolvido com o objetivo de identificar as vulnerabilidades de segurança presentes em cada versão, além de verificar se as vulnerabilidades identificadas nas versões anteriores foram corrigidas nas versões subsequentes. Esse roteiro de testes foi desenvolvido com base nas vulnerabilidades identificadas durante o desenvolvimento do projeto, sendo que cada vulnerabilidade identificada foi associada a um ou mais testes. Os testes foram desenvolvidos com base nas vulnerabilidades identificadas, sendo que cada teste foi associado a uma ou mais vulnerabilidades.

Os testes foram escolhidas a fim de demonstrar as vulnerabilidades mais comuns em sistemas web, sendo que cada ataque foi associado a uma ou mais vulnerabilidades.

Quadro 5 - Ataques e aspectos do sistema

1. Ataques	<ul style="list-style-type: none"> • Tentativa de quebra de senha por força bruta • Interceptação de comunicações por HTTP
2. Aspectos do Sistema	<ul style="list-style-type: none"> • Possibilidades de auditoria do sistema • Organização de informações privadas do sistema (dados de acesso, dados financeiros, etc.) • Facilidade de acesso aos logs do sistema • Tipos possíveis de usuários no sistema • Política de senha do sistema

Fonte: Autores.

O sistema de tentativa de quebra de senha por força bruta consiste em um usuário, que está tentando realizar obter acesso à identidade privilegiada, tentar realizar o login na plataforma com todas as combinações de letras possíveis, para exemplificação desse ataque foi

utilizado um pequeno script em python que realiza a tentativa de login com todas as combinações de letras possíveis, sendo que o script pode ser encontrado na Figura 19.

Realizando esse teste em uma máquina com processador Intel Core i7-7700 , 16GB de memória RAM e sistema operacional Pop-OS 20.04 LTS, foi possível quebrar uma senha de cinco caracteres em aproximadamente 1 hora. A senha que foi quebrada foi a senha "admin", senha padrão para o usuário administrador do sistema, que possui acesso privilegiado a todas as configurações do mesmo. Cabe ressaltar porém que o algoritmo utilizado apresenta limitações devido a capacidade de processamento da máquina utilizada, e o caso de testes tem vantagem nessa abordagem pois as 2 primeiras letras correspondem respectivamente ao primeiro e ao quarto caso de teste executado pelo algoritmo para aquelas respectivas posições. Com isso em mente é possível observar que com um hardware ainda é possível utilizar uma abordagem simples e descobrir em um tempo praticável a senha de um usuário, sendo que quanto mais complexa e longa for a senha, mais tempo será necessário para quebrar a senha.

O sistema base não possui nenhum tipo de auditoria, sendo que não é possível identificar quem realizou determinada ação no sistema, como por exemplo, quem criou um novo usuário ou quem realizou um novo pagamento.

Durante o desenvolvimento da versão v1.3.0 foi possível observar que o gerenciamento de identidades, a depender dos casos de uso da aplicação, torna-se um ponto crítico de segurança, pois a identidade de um usuário pode ser utilizada para realizar ações que podem comprometer a segurança do sistema, vazamento de dados ou pratica de crimes, como por exemplo, a criação de um novo pagamento com um valor muito alto ou até mesmo a exclusão de um usuário ou pagamento.

A versão v1.4.0 realizou a implementação de um sistema de autenticação multifator. Esta autenticação contribui para uma identidade mais segura dentro do sistema pois para realizar o login do usuário na aplicação, faz necessário realizar a utilização de 2 senhas, uma considerante a senha escolhida pelo usuário, e outra senha sendo um código numérico de seis dígitos gerado por um aplicativo de autenticação, sendo que esse código é gerado a cada sessenta segundos e é único para cada usuário. Essa etapa a mais de autenticação torna o ataque por força bruta muito mais difícil, pois o atacante teria que descobrir a senha do usuário e o código gerado pelo aplicativo de autenticação, sendo que o código gerado pelo aplicativo de autenticação expira em pouco tempo. somando isso a complexidade mínima de 6 caracteres, com caracteres especiais, para a senha do usuário, o ataque por força bruta se torna muito mais difícil de ser realizado, a depender do hardware utilizado inviável pela quantidade de combinações possíveis de senhas.

Figura 19 - Script para tentativa de quebra de senha por força bruta

```

1 import requests
2 from bs4 import BeautifulSoup
3 import itertools
4 import random
5 import time
6 import asyncio
7
8 async def test_login(username, password):
9     login_url = 'http://localhost:8000/admin/login/'
10    session = requests.Session()
11
12    response = await loop.run_in_executor(None, session.get, login_url)
13    soup = BeautifulSoup(response.text, 'html.parser')
14    csrf_token = soup.find('input', {'name': 'csrfmiddlewaretoken'}).get('value')
15
16    payload = {
17        'username': username,
18        'password': password,
19        'csrfmiddlewaretoken': csrf_token,
20    }
21
22    response = await loop.run_in_executor(None, session.post, login_url, payload)
23
24    return 'Bem-vindo' in response.text
25
26 async def brute_force_password(password_set, password_length, num_parallel_attempts):
27    start_time = time.time()
28
29    tasks = []
30    for password in itertools.product(password_set, repeat=password_length):
31        attempted_password = "".join(password)
32        print("attempted-password:", attempted_password)
33
34        task = asyncio.ensure_future(test_login("admin", attempted_password))
35        tasks.append(task)
36
37        # Se atingir o número desejado de tentativas paralelas, espera por todas
38        if len(tasks) >= num_parallel_attempts:
39            await asyncio.gather(*tasks)
40            tasks = []
41
42    # Aguarda as tentativas finais, se houverem
43    if tasks:
44        await asyncio.gather(*tasks)
45
46    end_time = time.time()
47    tempo_necessario = end_time - start_time
48    print("Tempo total necessário para quebrar é:", tempo_necessario)
49
50 loop = asyncio.get_event_loop()
51 loop.run_until_complete(brute_force_password("abcdefghijklmnopqrstuvwxyz", 5, num_parallel_attempts=30))

```

Fonte: Autores.

Figura 20 - Intercepção de comunicações por HTTP

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of packets. Packet 84 is highlighted, showing an HTTP GET request. The details pane for this packet shows the following information:

- Accept-Language: en-US,en;q=0.9
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?
- Referer: http://localhost:8000/admin/login/?next=/admin/login/
- Accept-Encoding: gzip, deflate, br
- Host: localhost:8000
- URI: /admin/login/?next=/admin/login/
- Method: GET

The raw packet bytes pane shows the hex and ASCII representation of the request, including the HTTP version, status code, and headers.

Fonte: Autores.

Ao decorrer das versões foram implementados mecanismos que impossibilitaram a interceptação de comunicações por HTTP, sendo que na versão 1.5.0 foi implementado o protocolo HTTPS em toda a aplicação, garantindo a criptografia dos dados transmitidos entre o cliente e o servidor, impedindo interceptações por terceiros. O uso do HTTPS contribui para uma experiência mais segura e confiável para os usuários, protegendo contra ataques de injeção de código e reforçando a integridade da aplicação. Além de proteger os dados de identidade privilegiadas do sistema contra interceptação, o uso do HTTPS também protege os dados financeiros dos usuários, como por exemplo, os dados do cartão de crédito, impedindo que um usuário mal intencionado intercepte esses dados e realize compras com o cartão de crédito de outro usuário.

Em nossa versão 1.6.0, foi implementado um facilitador para o sistema de auditoria, que realiza o registro todas as ações realizadas nele, e disponibiliza esse dado na plataforma web somente para os usuários autorizados. Esse sistema de auditoria é importante para que seja possível identificar possíveis erros no sistema e monitorar acessos de usuários mal intencionados.

Como um todo, o projeto apresenta um maior grau de segurança. A aplicação possui sistema de identidade privilegiada com autenticação multifatorial, comunicação segura via HTTPS, sistema de auditoria e controle de acesso, sendo que esses mecanismos de segurança são importantes para garantir a segurança da aplicação e dos dados dos usuários.

Foi observado, entretanto, a possibilidade de aumentar ainda mais a segurança no gerenciamento de identidade ao colocar uma autenticação por sistema biométrico ou geolocalização associada ao smartphone do usuário, sendo que esses sistemas são mais difíceis de serem burlados, pois é necessário que o usuário esteja presente no local onde o acesso está sendo realizado, e que o usuário esteja com o smartphone em mãos, sendo esse um dispositivo pessoal e dificilmente será compartilhado com outras pessoas.

6 CONCLUSÃO

A partir da realização desta monografia, os objetivos delineados foram atingidos, consolidando um conjunto de práticas de segurança implementadas no desenvolvimento web de um sistema de gerenciamento de pagamentos para uma loja fictícia. A ênfase primordial deste trabalho foi direcionada ao fortalecimento do gerenciamento de identidade e níveis de permissão, a fim de estabelecer um ambiente digital mais seguro e confiável. No contexto dos objetivos gerais, dedicou-se especial atenção à criação de um sistema para uma loja fictícia, capaz de realizar a gravação e listagem de pagamentos. Simultaneamente, procedeu-se ao desenvolvimento incremental de práticas de segurança, sublinhando a importância dessa abordagem contínua na salvaguarda da integridade e confidencialidade dos dados.

Os objetivos específicos também foram alcançados. A prova de conceito desenvolvida para a loja fictícia não só demonstrou a eficácia das práticas implementadas, mas também exemplificou a relevância do gerenciamento seguro em aplicações digitais. Destacou-se, sobretudo, a importância crucial da proteção de identidades no contexto da segurança cibernética, evidenciando que senhas de maior complexidade são fundamentais para resistir a ameaças em comparação a senhas mais simples.

Adicionalmente, a implementação de autenticação multifatorial e a comunicação segura via HTTP, utilizando o TLS para implementação de criptografia nas comunicações, foram elementos fundamentais para garantir uma segurança mais forte e eficaz no acesso e comunicações do sistema.

A proteção de identidade de um sistema garante a confiabilidade e a segurança do mesmo, pois é através dela que é verificada a identidade do usuário, permitindo ou negando o acesso a sistemas e informações sensíveis. Dessa maneira, a criação de uma identidade privilegiada única para cada usuário contribui significativamente para a segurança dos sistemas, impedindo o acesso não autorizado a recursos restritos.

Por mais que o sistema em sua versão final possua uma segurança no quesito técnico maior que as versões anteriores, a maior parte dos ataques sofridos por empresas e negócios são focados em obter acesso a identidades privilegiadas dentro de sistemas por ferramentas de engenharia social ou phishing de dados. Tais problemas não podem ser plenamente resolvidos por um software interno da empresa, por abranger ações dos usuários que possuam identidade privilegiada e estão fora do escopo do software. Por conta disso conclui-se que a segurança de um sistema não depende apenas de mecanismos de segurança nele implementados, mas também

de uma política de segurança bem definida e de uma filosofia organizacional que conscientize a todos dos riscos associados ao vazamento ou roubo identidades privilegiadas.

Com a utilização cada vez mais disseminada de dispositivos eletrônicos e softwares na indústria e no cotidiano pessoal, além da evolução natural e o uso da tecnologia cada vez mais disseminado no planeta, a segurança da identidade privilegiada de dados tem se tornado cada vez menos um problema exclusivamente da indústria de engenharia de software e gerenciamento de sistemas, e se tornando cada vez mais um problema de segurança nacional, organizacional e pessoal. A identidade de uma pessoa em sistemas digitais tem se tornado por vezes mais importantes que a identidade física, pois é através dos dados desta pessoa contidas no sistema, que se tem acesso não somente a informações pessoais, mas também financeiras e de saúde. Por conta disso, a segurança da identidade privilegiada de dados tem se tornado cada vez mais um problema de segurança individual.

Além dos problemas legais e pessoais que o vazamento de identidades privilegiadas podem causar, o vazamento de dados de uma empresa, também podem causar danos financeiros e de imagem para a empresa. Por conta disso, a segurança da identidade privilegiada de dados tem se tornado igualmente um problema de segurança empresarial.

Para além dos aspectos técnicos, a integração da equipe de TCC entre os alunos e a orientadora desempenharam um importante papel no desenvolvimento eficaz do trabalho. A promoção da integração de todos os envolvidos não apenas enriqueceu o processo, mas também evidenciou a importância da colaboração e sinergia na consecução de objetivos complexos.

Por fim, conclui-se que este trabalho oferece uma contribuição à área de segurança da informação, destacando de forma enfática a necessidade de proteger as identidades privilegiadas de acesso e de conscientizar sobre os riscos associados. Através de uma análise bibliográfica detalhada e do sistema proposto desenvolvido, foi possível obter uma compreensão profunda das ameaças cibernéticas direcionadas a essas identidades, enfatizando as graves consequências que a exploração delas pode acarretar para as organizações. Além disso, ao demonstrar de maneira concreta a aplicação prática de medidas de segurança em um contexto de gerenciamento de dados financeiros, oferecemos uma referência para profissionais e organizações que buscam fortalecer sua postura de segurança em ambientes críticos.

6.1 TRABALHOS FUTUROS

Com base na análise bibliográfica realizada, surgem sugestões para pesquisas futuras na área de segurança da informação:

1. Avaliação da eficácia das medidas de segurança: realizar estudos que avaliem a eficácia das medidas de segurança adotadas pelas empresas para proteger as identidades privilegiadas de acesso (análises de casos reais e a comparação dos resultados obtidos por diferentes organizações).

2. Análise de novas ameaças e técnicas de ataque: com o avanço tecnológico e a evolução do cenário cibernético, é importante investigar e analisar novas ameaças e técnicas de ataque direcionadas às identidades privilegiadas. Isso permitiria o desenvolvimento de estratégias defensivas mais eficazes.

3. Implementação de boas práticas de segurança discutida na monografia em um sistema real.

REFERÊNCIAS

- ANDERSON, R. *et al.* Measuring the cost of cybercrime. **Proceedings of the 2018 Workshop on Economics of Information Security (WEIS)**. [S.l.: s.n.], 2018.p. 4-7.
- BILLESTRUP, J. *et al.* Persona usage in software development: advantages and obstacles. **The Seventh International Conference on Advances in Computer-Human Interactions, ACHI**. [S.l.: s.n.], 2014. p. 359–364.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Planalto, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 nov. 2023.
- CAI, M.; WANG, Y.; WEI, L. Insider threat detection based on deep learning in privileged access management. **International Journal of Machine Learning and Cybernetics**, Springer, v. 9, n. 7, p. 1217–1231, 2018.
- CANÊDO, D. R. **Um ambiente experimental para análise de ataques de negação de serviço**. 2006. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de Brasília, Brasília, 2006.
- CARROLL, J.; SMITH, J.; JOHNSON, D. Privileged identity management: A comprehensive review of current research. **Journal of Information Security**, Springer, v. 12, n. 3, p. 123–145, 2019.
- CARVALHO, M. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. 2006. Dissertação (Mestrado em Engenharia) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.
- CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas Mantidas pelo CERT.br**. [s. l.]: CERT.br, 2023. Disponível em: <https://stats.cert.br/>. Acesso em: 6 nov. 2023.
- CHAPPLE, M.; M, S. J.; D., G. Managing identity and authentication. **(ISC)2-CISSP® Certified Information Systems Security Professional**. John Wiley & Sons, Ltd, 2018. p. 579–621. ISBN 9781119549567. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119549567.ch13>. Acesso em: 3 de dezembro de 2023.
- DINGSØYR, T. *et al.* A decade of agile methodologies: Towards explaining agile software development. **Journal of Systems and Software**, [s. l.], v. 85, n. 6, p. 1213-1221, 2012. ISSN 0164-1212. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0164121212000532>. Acesso em: 6 nov. 2023.
- DJANGO SOFTWARE FOUNDATION. **Django REST framework Documentation**. Django Rest Framework, 2023.
- Disponível em: <https://www.django-rest-framework.org/>. Acesso em: 6 nov. 2023.

Django Software Foundation. **Django Documentation**. Django Project, 2023. Disponível em: <https://docs.djangoproject.com/>. Acesso em: 6 nov. 2023.

DOCKER. **Compose Documentation**. Docker, 2023. <https://docs.docker.com/compose/>. Acesso em: 6 nov. 2023.

DOCKER. **Documentation**. Docker, 2023. Disponível em: <https://docs.docker.com/>. Acesso em: 20 out. 2023.

FISCHER, J.; ARGON, N. T. **Identity Management: Concepts, Technologies, and Systems**. [s. l.]: Springer, 2014.

FISHER, P. **Privileged access management**. Kuppingercole Analysts AG January 2023. Disponível em: <https://assets.beyondtrust.com/assets/documents/KCPAMLeadershipCompass2022.pdf>. Acesso em: 6 nov. 2023.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. Brasport, 2012. E-book. ISBN 9788574525150. Disponível em: https://books.google.com.br/books?id=X61rbEWwJ__UC. Acesso em: 6 nov. 2023.

FREITAS, C. Garantir a autenticidade e o acesso continuado à informação digital: os desafios da preservação digital em arquivos. **Associação Portuguesa de Bibliotecários, Arquivistas e Documentalistas**, [s. l.], 2012. Disponível em: http://eprints.rclis.org/17866/1/Artigo_11%C2%BAcongresso_BAD.pdf Acesso em: 6 nov. 2023.

GOMES, U. d. M. *et al.* **Desafios estratégicos para segurança e defesa cibernética**. Presidencia da Republica, 2011.

GOOGLE. Identity Platform - Multi-Factor Authentication. **Google**, [California], 2023. Disponível em: <https://developers.google.com/identity/gsi>. Acesso em: 6 nov. 2023.

GOTHELF, J. Using proto-personas for executive alignment. **UX Magazine**, [s. l.], v. 1, p. 26–29, 2012.

GRUDIN, J. Why personas work: The psychological evidence. **The persona lifecycle**, Elsevier, v. 12, p. 642–664, 2006.

HAVARD. An Introduction to Identifiers. **Harvard University**, Massachusetts, 2015. Disponível em: <https://iam.harvard.edu/resources/introduction-identifiers>. Acesso em: 6 nov. 2023.

HOSANG, A. Política nacional de segurança cibernética: uma necessidade para o Brasil. **Escola Superior de Guerra**, Rio de Janeiro, 2011. Disponível em: <https://abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf>. Acesso em: 6 nov. 2023.

CYBERARK. Identity Security: Why it Matters and Why Now₂₀₂₂. [s. l.]: CyberArk, 2022. Disponível em: <https://www.cyberark.com/resources/ebooks/identity-security> . Acesso em: 6 nov. 2023.

JARECKI, S. Topics in Cryptology—CT-RSA 2020. *In: The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24–28, 2020. Proceedings [...]. [s. l.]: Springer Nature, 2020. v. 12006.*

JOHNSON, R. Security challenges for remote work. **Network Security**, [s. l.], v. 2020, n. 4, p. 4–7, 2020.

JOHNSON, V. R. Cybersecurity, identity theft, and the limits of tort liability. **ScL REv., HeinOnline**, [s. l.], v. 57, p. 255, 2005.

JOSEPH, D. P.; NORMAN, J. An analysis of digital forensics in cyber security. *In: First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018. Anais [...]. [s. l.]: Springer, 2019. p. 701-708.*

KHALIL, I.; KHREISHAH, A.; AZEEM, M. Consolidated identity management system for secure mobile cloud computing. **Computer Networks**, [s. l.], v. 65, p. 99–110, 2014. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S1389128614001194>. Acesso em: 6 nov. 2023.

KUPPINGER, M. Cloud user and access management. **KuppingerCole Leadership Compass Report**, [s. l.], v. 70969, 2014. Citado na página 31.

LET'S ENCRYPT. **Documentation**. San Francisco: Let's Encrypt, 2023. Disponível em: <https://letsencrypt.org/docs/>. Acesso em: 6 nov. 2023.

LI, Q.; LIANG, H.; SARATHY, R. Privacy protection in the digital age: An overview of information privacy research. **Information & Management**, [s. l.], v. 56, n. 6, p. 801–809, 2019.

MACHADO, F. N. R. **Segurança da informação: princípios e controle de ameaças**. [S.l.]: Saraiva Educação SA, 2014.

MONTEIRO, L. A internet como meio de comunicação: possibilidades e limitações. *In: Congresso Brasileiro de Comunicação, 24, 2001, Campo Grande. Anais [...]. Campo Grande: INTERCOM, 2001.*

NGINX. **NGINX Documentation**. NGINX, 2023. Disponível em: <https://nginx.org/en/docs/>. Acesso em: 6 nov. 2023.

NIST. **NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations**. NIST, 2020. <https://nvlpubs.nist.gov>. Acesso em: 6 nov. 2023.

OAUTH 2.0 Authorization Framework. RFC 6749. [s. l.: s. n.], 2012. Disponível em: <https://oauth.net/2/>. Acesso em: 6 nov. 2023.

PFLEEGER, C. P.; PFLEEGER, S. L.; MARGULIES, J. A. **Security in Computing**, 5. ed. [s. l.]: Prentice Hall, 2015.

PINHEIRO, P. P. **Segurança digital: Proteção de dados nas empresas**. 1. ed. São Paulo, SP: Grupo GEN, 2020.

POSTGRESQL. **Documentation**. PostgreSQL, 2023. <https://www.postgresql.org/docs/>. Acesso em: 6 nov. 2023.

PYTHON. **Python Documentation**. [s. l.]: Python Software Foundation, 2023. Disponível em: <https://www.python.org/doc/>. Acesso em: 6 nov. 2023.

SANDHU, R. *et al.* Role-based access control models. **IEEE Computer**, [s. l.], v. 29, n. 2, p. 38–47, 1996.

SANTOS, E. E.; SOARES, T. M. M. K. **Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações**, 2018.

SCHNEIER, B. **Secrets and Lies: Digital Security in a Networked World**. [s. l.]: John Wiley & Sons, 2015.

SOUZA, R. C.; FERNANDES, J. H. C. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Science**, São Paulo, v. 10, n. 1, p. 63–75, 2016.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6. ed. [s. l.]: Pearson, 2017.

SWAGGER. **Documentation**. Swagger, 2023. Disponível em: <https://swagger.io/docs/>. Acesso em: 6 nov. 2023.

VIEIRA, E. **Os bastidores da Internet no Brasil**. [s. l.]: Editora Manole Ltda, 2003.

WANGHAM, M. S. *et al.* O futuro da gestão de identidades digitais. *In: SBC XVIII SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS*, 18, 2018, [s. l.]. **Anais Estendidos**. [s. l.: s. n.], 2018. p. 146–166.

WHITMAN, M. E.; MATTORD, H. J. **Princípios de Segurança da Informação e Gerenciamento de Riscos**. [s. l.]: Cengage Learning, 2019.