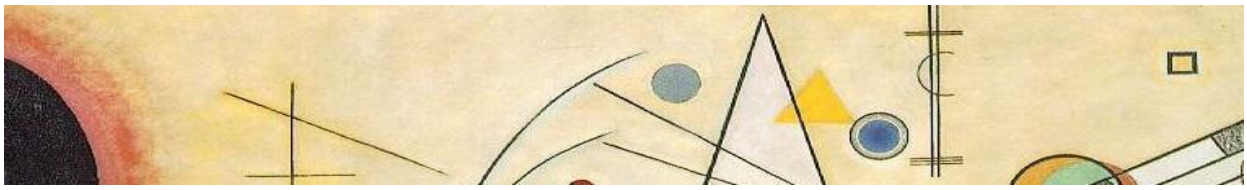


Contemporânea
Contemporary Journal
Vol. 5 N°. 6: p. 01-13, 2025
ISSN: 2447-0961

Artigo

A IMPORTÂNCIA DOS CONTROLADORES DE DOMÍNIO EM AMBIENTES UNIVERSITÁRIOS: UMA ANÁLISE TÉCNICA E ESTRATÉGICA

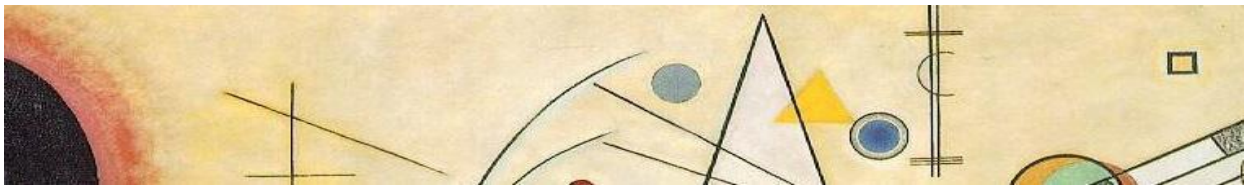
THE IMPORTANCE OF DOMAIN CONTROLLERS IN UNIVERSITY ENVIRONMENTS: A TECHNICAL AND STRATEGIC ANALYSIS

LA IMPORTANCIA DE LOS CONTROLADORES DE DOMINIO EN ENTORNOS UNIVERSITARIOS: UN ANÁLISIS TÉCNICO Y ESTRATÉGICO

DOI: 10.56083/RCV5N6-075
Receipt of originals: 5/16/2025
Acceptance for publication: 6/6/2025

Guilherme Henrique Cândido de Moraes
Graduando em Sistemas de Informação, Tecnologia da Informação
Instituição: Instituto Federal Goiano - campus Ceres
Endereço: Goiânia, Goiás, Brasil
E-mail: guilhermehenriqueif@gmail.com

RESUMO: A crescente complexidade da infraestrutura da tecnologia da informação nas universidades públicas brasileiras tem demandado soluções eficientes para o gerenciamento de usuários, dispositivos e recursos de rede. Nesse contexto, a ausência de controle centralizado pode comprometer a segurança, a padronização e a governança dos sistemas institucionais. Diante desse cenário, este trabalho tem como objetivo analisar a importância dos controladores de domínio, com ênfase no Active Directory (AD), em ambientes universitários. A metodologia adotada baseou-se em uma pesquisa exploratória e descritiva de caráter qualitativo, fundamentada em revisão bibliográfica e análise documental de fontes técnicas, acadêmicas e normativas. Foram examinadas as funcionalidades, aplicações e benefícios da adoção de um controlador de domínio, destacando-se aspectos como a centralização da autenticação, aplicação de políticas de segurança, automação de tarefas administrativas e melhoria da gestão de recursos. A análise evidenciou que o uso de controladores de domínio, quando bem planejado e mantido, contribui significativamente para a eficiência



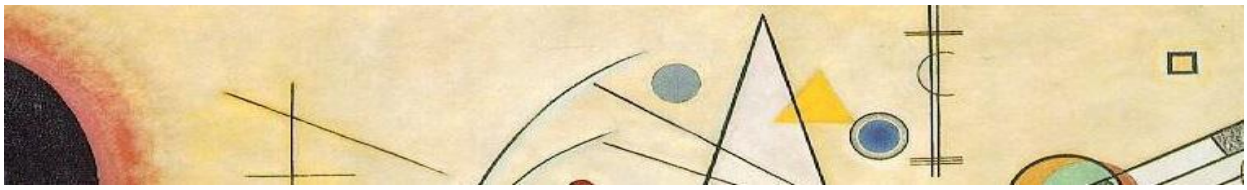
operacional, a integridade dos dados institucionais e a conformidade com as legislações vigentes como a Lei Geral de Proteção de Dados (LGPD). Conclui-se que a adoção dessa tecnologia é estratégica para instituições de ensino superior, especialmente aquelas com ambientes amplos e distribuídos. É notória a necessidade de políticas institucionais de TI que incentivem a implementação e o uso adequado de soluções de gerenciamento centralizado, alinhando infraestrutura, segurança e qualidade dos serviços prestados.

PALAVRAS-CHAVE: active directory, ambientes universitários, controladores de domínio, governança de TI.

ABSTRACT: The increasing complexity of information technology infrastructure in Brazilian public universities has demanded efficient solutions for managing users, devices, and network resources. In this context, the absence of centralized control can compromise the security, standardization, and governance of institutional systems. Given this scenario, this study aims to analyze the importance of domain controllers, with an emphasis on Active Directory (AD), in university environments. The methodology adopted was based on an exploratory and descriptive qualitative research approach, grounded in a literature review and documentary analysis of technical, academic, and regulatory sources. The study examined the functionalities, applications, and benefits of adopting a domain controller, highlighting aspects such as centralized authentication, enforcement of security policies, automation of administrative tasks, and improved resource management. The analysis showed that the use of domain controllers, when properly planned and maintained, significantly contributes to operational efficiency, the integrity of institutional data, and compliance with current regulations such as the Brazilian General Data Protection Law (LGPD). It is concluded that the adoption of this technology is strategic for higher education institutions, especially those with broad and distributed environments. The need for institutional IT policies that encourage the implementation and proper use of centralized management solutions is evident, aligning infrastructure, security, and quality of services provided.

KEYWORDS: active directory, university environments, domain controllers, IT governance.

RESUMEN: La creciente complejidad de la infraestructura de tecnología de la información en las universidades públicas brasileñas ha exigido soluciones eficientes para la gestión de usuarios, dispositivos y recursos de red. En este contexto, la ausencia de un control centralizado puede comprometer la seguridad, la estandarización y la gobernanza de los sistemas institucionales. Ante este escenario, el presente trabajo tiene como objetivo analizar la

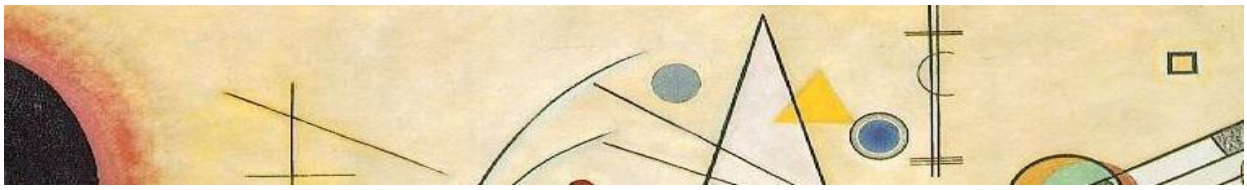


importancia de los controladores de dominio, con énfasis en Active Directory (AD), en entornos universitarios. La metodología adoptada se basó en una investigación exploratoria y descriptiva de carácter cualitativo, fundamentada en una revisión bibliográfica y análisis documental de fuentes técnicas, académicas y normativas. Se examinaron las funcionalidades, aplicaciones y beneficios de la adopción de un controlador de dominio, destacándose aspectos como la centralización de la autenticación, la aplicación de políticas de seguridad, la automatización de tareas administrativas y la mejora en la gestión de recursos. El análisis evidenció que el uso de controladores de dominio, cuando están bien planificados y mantenidos, contribuye significativamente a la eficiencia operativa, a la integridad de los datos institucionales y al cumplimiento de las legislaciones vigentes, como la Ley General de Protección de Datos (LGPD). Se concluye que la adopción de esta tecnología es estratégica para las instituciones de educación superior, especialmente aquellas con entornos amplios y distribuidos. Es notoria la necesidad de políticas institucionales de TI que fomenten la implementación y el uso adecuado de soluciones de gestión centralizada, alineando infraestructura, seguridad y calidad de los servicios prestados.

PALABRAS CLAVE: active directory, entornos universitarios, controladores de dominio, gobernanza de TI.

1. Introdução

O avanço da transformação digital nas instituições de ensino superior brasileiras tem ampliado consideravelmente a complexidade da gestão de infraestrutura tecnológica. Ambientes universitários, especialmente em instituições públicas multicampi, demandam soluções eficazes para lidar com uma grande quantidade de usuários, dispositivos e serviços independentes. A descentralização na administração de identidades e acessos compromete não apenas a eficiência operacional, mas também a segurança da informação, o controle de recursos computacionais e a conformidade com marcos legais como a Lei Geral de Proteção de Dados (LGPD).



Nesse cenário, os controladores de domínio despontam como componentes estratégicos de infraestrutura de TI. Dentre as soluções mais consolidadas nesse campo, o *Active Directory (AD)*, desenvolvido pela *Microsoft*, se destaca por permitir a centralização da autenticação de usuários, o gerenciamento de estações e servidores, além da aplicação padronizada de políticas de segurança por meio das chamadas *Group Policy Objects* (GPOs). Apesar de sua ampla adoção no setor corporativo, o uso do AD em universidades ainda é um tema pouco discutido na literatura técnica e acadêmica, especialmente no que diz respeito à sua contribuição para a governança institucional, a padronização dos processos de TI e a redução de vulnerabilidades em ambientes amplamente distribuídos.

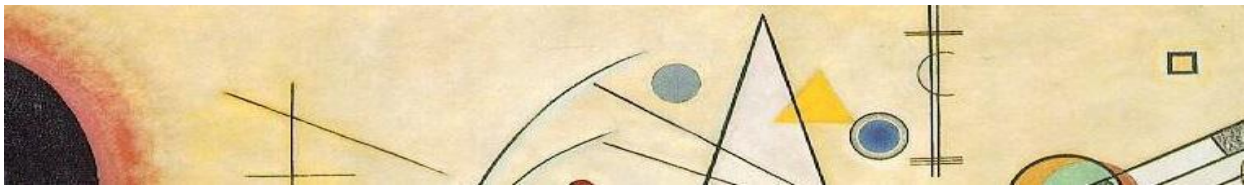
Diante do exposto, este trabalho tem como objetivo analisar, com base em referencial técnico e acadêmico, a importância dos controladores de domínio em ambientes universitários, com ênfase no Active Directory, destacando seus benefícios operacionais, desafios de implementação e implicações para a segurança e a gestão estratégica da tecnologia da informação em instituições públicas de ensino superior.

2. Referencial Teórico

2.1 Infraestrutura de TI em Ambientes Universitários

As universidades públicas brasileiras, especialmente as federais, possuem uma infraestrutura tecnológica heterogênea e distribuída, muitas vezes segmentada entre campi, centros acadêmicos, departamentos administrativos e unidades especializadas. Essa descentralização física e organizacional apresenta desafios significativos à gestão de redes, à segurança da informação e à manutenção da integridade dos dados institucionais.

De acordo com Pöhn e Hommel (2023), a gestão de identidade em



instituições como universidades enfrenta desafios impostos pela grande diversidade de perfis de usuários, como alunos, professores, técnicos e colaboradores externos, além da alta rotatividade desses públicos. Essa complexidade torna o ambiente acadêmico particularmente suscetível a inconsistências no gerenciamento de credenciais e a falhas no controle de acesso. Nesse contexto, a adoção de políticas estruturadas de TI, baseadas em padronização e automação, torna-se indispensável para garantir a continuidade operacional e a segurança dos serviços tecnológicos oferecidos.

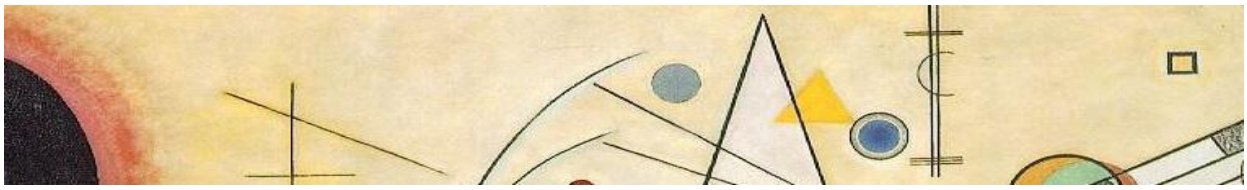
Nesse sentido, a crescente adoção de sistemas integrados de gestão acadêmica, bibliotecas digitais, plataformas de ensino remoto, ambientes de laboratório virtual e serviços em nuvem requerem uma base sólida de autenticação e controle de identidade, sob pena de exposição a vulnerabilidades críticas.

2.2 Gerenciamento de Identidade e Controle de Acesso

O gerenciamento de identidade (*Identity Management*) é o conjunto de processos e tecnologias que visam identificar, autenticar e autorizar indivíduos ou grupos dentro de um sistema, controlando seu acesso aos recursos e serviços de uma organização. Em ambientes universitários, a falta de padronização desses processos pode levar a acessos indevidos, duplicação de contas, perda de rastreabilidade e sobrecarga das equipes de suporte.

Segundo Stallings (2015), um sistema robusto de gerenciamento de identidade deve garantir os princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Além disso, deve assegurar a rastreabilidade das ações dos usuários e permitir a aplicação uniforme de políticas de segurança, reduzindo a margem para erros humanos.

Com o advento de legislações como a LGPD (Lei nº 13.709/2018), a preocupação com a proteção de dados sensíveis nas instituições tornou-se ainda mais relevante. O uso de soluções que permitam o controle



centralizado de identidade e acesso passou a ser não apenas uma boa prática, mas também uma exigência normativa e jurídica.

2.3 Controladores de Domínio: Definição e Funcionalidades

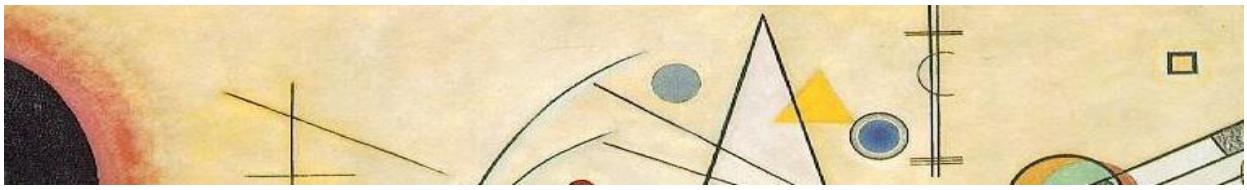
Controladores de domínio são servidores responsáveis por autenticar e autorizar usuários e dispositivos em uma rede, além de aplicar políticas administrativas de forma centralizada. Esses servidores utilizam protocolos como o LDAP (*Lightweight Directory Access Protocol*), DNS (*Domain Name System*) e Kerberos para permitir que os usuários acessem recursos com segurança e praticidade.

O *Active Directory* (AD), desenvolvido pela Microsoft, é a solução de diretório mais amplamente utilizada no mundo corporativo e institucional. Ele permite a criação de um domínio lógico, onde usuários, computadores, grupos e recursos são gerenciados por meio de uma estrutura hierárquica. A administração do AD é facilitada por ferramentas como a *Organizational Units* (OUs), que permitem segmentar políticas conforme setores ou perfis, e as *Group Policy Objects* (GPOs), que automatizam e padronizam configurações de segurança, permissões, scripts de login, entre outros.

A adoção de um controlador de domínio como o AD permite que o suporte de TI otimize o tempo de resposta, minimize erros de configuração manual e amplie o controle sobre o ambiente de rede. Além disso, facilita a auditoria e o monitoramento de atividades, contribuindo para a conformidade institucional com políticas internas e normativas externas.

2.4 Aplicações do *Active Directory* em Instituições Públicas

Em órgãos públicos e instituições federais de ensino, o uso do *Active Directory* tem se consolidado como uma estratégia para garantir segurança, integridade de dados e eficiência administrativa. Segundo o Guia de Boas



Práticas em Segurança da Informação para Instituições Públicas, publicado pela Secretaria de Governo Digital (2020), a adoção de soluções centralizadas de autenticação é fundamental para a conformidade com a política de segurança cibernética da administração pública.

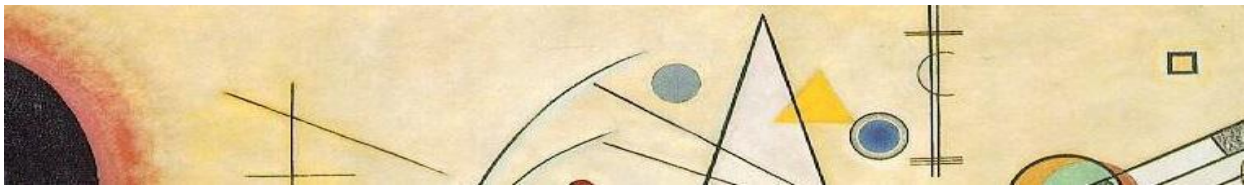
Nas universidades, o AD é particularmente útil para lidar com cenários complexos, como o provisionamento e desativação automatizada de contas conforme a matrícula ou desligamento de alunos, a integração com sistemas de autenticação única (*Single Sign-On – SSO*) e a aplicação de políticas diferenciadas para laboratórios, setores administrativos e docentes. Além disso, o AD pode ser integrado a serviços em nuvem, como o *Azure AD*, permitindo que instituições operem em modelos híbridos, mantendo a segurança e flexibilidade.

Estudos de caso documentados, como aplicações na Universidade de Brasília (UnB) e da Universidade Federal do Rio Grande do Sul (UFRGS, indicam que a adoção planejada e alinhada às políticas institucionais de TI resulta em ganhos expressivos em produtividade, segurança da informação e governança, além de promover a padronização de procedimentos e a melhoria da experiência do usuário final. Dessa forma, o *Active Directory* não apenas atende a requisitos técnicos, mas também fortalece a capacidade institucional de adaptação às exigências tecnológicas e regulatórias dentro do panorama atual.

3. Metodologia

Esta pesquisa caracteriza-se como um estudo de natureza qualitativa e abordagem exploratória e descritiva, com foco na análise teórica sobre a importância e os impactos da adoção de controladores de domínio em ambientes universitários, especialmente por meio do uso do *Active Directory*.

Optou-se pela realização de uma revisão bibliográfica e documental, considerando publicações acadêmicas, livros técnicos, manuais de



fabricantes, guias de boas práticas, legislações e normativas aplicáveis à gestão de tecnologia da informação com foco no âmbito universitário. As fontes foram selecionadas a partir de bases como *Google Scholar*, *Scielo*, *IEEE Xplore*, além de documentos institucionais disponíveis em repositórios de universidades federais e órgãos governamentais, como o Ministério da Economia e a Secretaria de Governo Digital.

A seleção dos materiais foi orientada pelos seguintes critérios:

I - relevância do conteúdo para o tema de controladores de domínio e *Active Directory*;

II - aplicabilidade em contextos públicos e educacionais;

III - atualização dos dados (com prioridade para fontes dos últimos dez anos);

IV - confiabilidade técnica e científica das publicações.

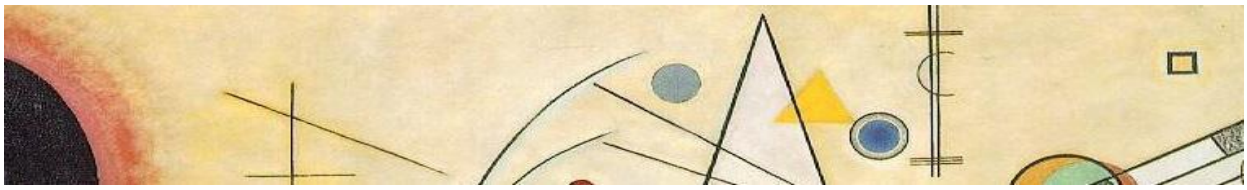
V - conformidade com as legislações vigentes.

Os dados foram organizados e analisados de forma qualitativa, com base em categorias temáticas previamente definidas: infraestrutura de TI, gestão de identidade e acesso, segurança da informação, benefícios operacionais e desafios de implementação. A análise buscou identificar padrões, boas práticas e implicações estratégicas da adoção de controladores de domínio em universidades públicas, permitindo uma compreensão ampliada do papel dessa tecnologia na gestão institucional da informação.

Ressalta-se que a implementação de políticas e ações voltadas à segurança da informação e dados sensíveis está relacionada diretamente a uma conduta institucional e não diretamente ligada a situações-problema exclusivamente no âmbito de TI.

4. Resultados e Discussões

A análise desenvolvida a partir da literatura técnica, estudos de caso institucionais e documentação oficial permitiu identificar aspectos técnicos e



estratégicos essenciais sobre o uso de controladores de domínio em ambientes universitários. A partir da comparação das soluções mais amplamente adotadas, destacam-se vantagens, limitações e critérios decisivos para a seleção da tecnologia mais adequada a esse contexto.

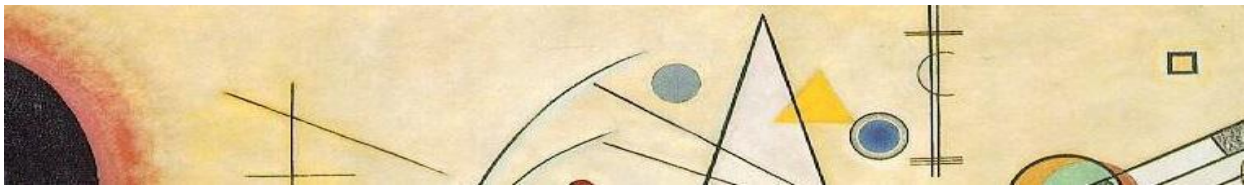
4.1 Características e alternativas dos Controladores de Domínio

Tabela 1. Soluções e características dos controladores de domínio

Nº	Solução	Fabricante	Licença	Integração com SSO	Suporte a GPO	Compatibilidade com Nuvem	Custo Estimado
1	Active Directory (AD)	Microsoft	Proprietária	Nativa com Microsoft Azure	Amplo	Forte	Elevado
2	Samba AD	Comunidade	Livre	Limitada	Parcial	Limitada	Baixo
3	FreeIPA	Red Hat / Comunidade	Livre	Linux	Não nativo	Baixo	Baixo
4	OpenLDAP com Kerberos	Comunidade	Livre	Exige customizações	Não nativo	Baixo	Baixo

Fonte: Própria, a partir dos dados coletados.

A partir desta comparação é possível evidenciar que, embora existam opções de código aberto viáveis como o Samba AD e o FreeIPA, o *Active Directory* da *Microsoft* se destaca por oferecer recursos mais maduros, suporte técnico especializado, integração nativa com ambientes híbridos (*on-premise e cloud*), e mecanismos avançados de *Group Policy Object* (GPO), aspecto crítico para instituições que buscam padronizar a experiência dos usuários e manter políticas de segurança centralizadas.

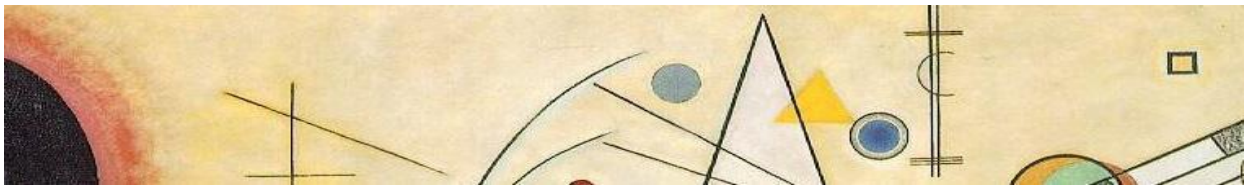


4.2 Adoção do Active Directory em Universidades Públicas

Estudos de caso analisados da Universidade de Brasília (UnB) e da Universidade Federal do Rio Grande do Sul (UFRGS) demonstram que a adoção do Active Directory tem promovido avanços significativos na gestão de tecnologia da informação. A centralização da administração de usuários e permissões tem contribuído diretamente para a redução do retrabalho das equipes de suporte técnico, otimizando processos e minimizando falhas humanas. Além disso, a aplicação padronizada de políticas de segurança, por meio do uso de objetos de diretiva de grupo (GPOs), tem possibilitado um controle mais granular dos acessos, alinhando a infraestrutura às exigências atuais de proteção da informação. Outro ponto evidenciado nos estudos é a aderência mais efetiva à Lei Geral de Proteção de Dados (LGPD), viabilizada pelo registro automatizado de atividades, pela definição de privilégios com base em identidade e função, e pelo fortalecimento dos mecanismos de auditoria. Por fim, as instituições que adotaram o *Active Directory* relatam ganhos significativos de integração com serviços em nuvem, especialmente com redes VPN e sistemas acadêmicos internos, ampliando a interoperabilidade e a flexibilidade da infraestrutura tecnológica no ambiente universitário.

4.3 Desafios e Considerações Técnicas

Apesar das vantagens evidenciadas na adoção do Active Directory em ambiente universitário, sua implementação também impõe desafios técnicos e estratégicos relevantes. O custo de licenciamento e manutenção representa um dos principais obstáculos, sobretudo para instituições com orçamentos restritos e dependência de recursos públicos. Além disso, a exigência de uma infraestrutura mínima, como a presença de controladores



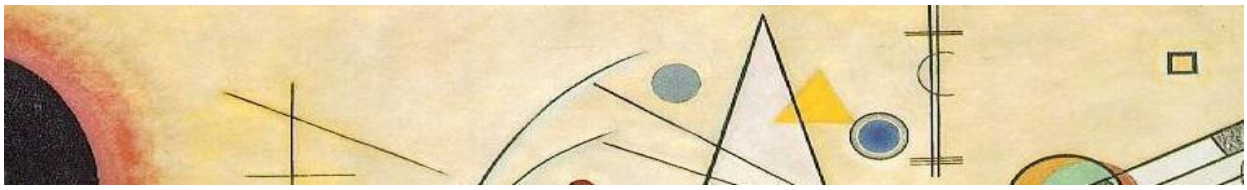
de domínio redundantes, conectividade estável e servidores dedicados demanda investimento prévio e planejamento adequado.

Junto a isso, a dependência tecnológica da *Microsoft*, que pode restringir a interoperabilidade com sistemas baseados em software livre, ainda comuns em muitas instituições de ensino superior. Para mitigar esses entraves, algumas universidades têm adotado abordagens alternativas, como o uso do *Azure* AD *Free*, que permite integração com serviços em nuvem sem custos adicionais, e a criação de ambientes híbridos, que combinam controladores locais com sincronização via *Azure* AD *Connect*, garantindo flexibilidade e continuidade operacional.

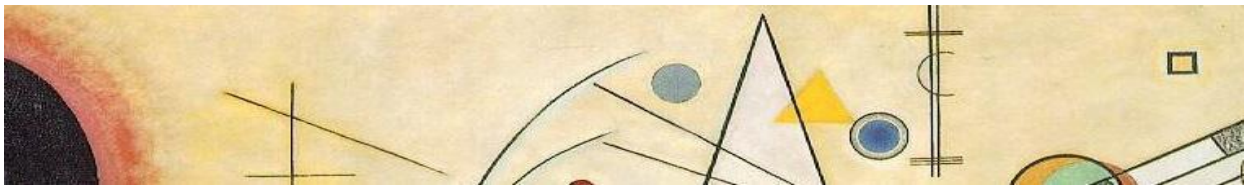
Com base na análise comparativa entre as principais soluções de controladores de domínio, infere-se que o Active Directory, quando implantado com planejamento técnico e por equipes qualificadas, constitui a alternativa mais robusta e alinhada às demandas de instituições que buscam maior conformidade, segurança, automação de processos e escalabilidade de infraestrutura. Ainda que soluções como o Samba AD e o FreeIPA se apresentem como alternativas viáveis em cenários de menor complexidade ou em instituições com forte adesão ao software livre, elas tendem a exigir maior esforço de customização e oferecem recursos mais limitados. Assim, a escolha da melhor solução deve considerar o porte institucional, os objetivos estratégicos de TI e o grau de maturidade da gestão tecnológica.

5. Conclusão

A escolha de um controlador de domínio deve considerar múltiplos fatores, como o nível de exigência em segurança, necessidade de integração com sistemas legados e em nuvem, a disponibilidade de equipe técnica, além da capacidade orçamentária. Após a análise das soluções, é possível inferir que o Active Directory, embora proprietário e com custos associados, é a alternativa mais alinhada com os requisitos operacionais, normativos e



estratégicos de ambientes universitários que demandam alta confiabilidade e governança de TI.



Referências

Brasil. (2018). **Lei Geral de Proteção de Dados Pessoais – LGPD** (Lei nº 13.709/2018). Presidência da República.

FreeIPA - **Identity, Policy, Audit**. Disponível em <https://www.freeipa.org/>

Microsoft. (2022). **Active Directory Domain Services Overview.** Microsoft Learn. Disponível em: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

PÖHN, D; HOMMEL, W. **An Overview of Limitations and Approaches in Identity Management**. arXiv, 2023.

SAMBA. **Samba Active Directory Domain Controller**. Samba Wiki, 2025. Disponível em: <https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller>.

Secretaria de Governo Digital – SGD. (2020). **Guia de Boas Práticas em Segurança da Informação para Instituições Públicas.** Disponível em: https://www.gov.br/governodigital

Stallings, W. (2015). **Criptografia e Segurança de redes: princípios e práticas.** 6. ed. São Paulo: Pearson.

UNIVERSIDADE DE BRASÍLIA. **Active Directory**. Brasília. Disponível em: <https://sti.unb.br/active-directory/>

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. **Manual de Procedimentos para Acesso à Rede com Autenticação no AD**. Porto Alegre: UFRGS, 2022.