INTERFACE TECNOLÓGICA

SEGURANÇA EM REDES CORPORATIVAS: a importância da segmentação com vlans

SECURITY IN CORPORATE NETWORKS: the importance of segmentation with vlans

Caue D'ambrósio Sicoli - cauesicoli@gmail.com
Faculdade de Tecnologia – FATEC – Taquaritinga- São Paulo- Brasil

Elton Batistão - elton.batistao@fatec.sp.gov.br
Faculdade de Tecnologia – FATEC – Taquaritinga- São Paulo- Brasil

DOI: 10.31510/infa.v22i2.2375
Data de submissão: 26/09/2025
Data do aceite: 02/12/2025
Data da publicação: 20/12/2025

RESUMO

A tecnologia tem adentrado todos os setores da sociedade, e embora os benefícios sejam muitos, ainda existem alguns aspectos a serem observados e que causam preocupação. A segurança em rede é um aspecto que tem pesado no contexto das redes corporativas, quando decidem investir em tecnologia. A segmentação por Virtual Local Area Networks (VLANs) é relevante para promover a segurança das redes corporativas, isso porque o fato de divisão da rede física em várias redes menores, restringe o acesso não autorizado e limita a propagação de ataques. Isso impede o movimento lateral de ameaças, protege dados sensíveis, controla o acesso a recursos e melhora a aplicação de políticas de segurança, reduzindo os riscos de ataques internos e externos. Dentro desse contexto o objetivo deste estudo é evidenciar a relevância do uso dessa segmentação, pontuando as vantagens e desvantagens. A metodologia utilizada foi de Revisão de Narrativa Transparente, onde foram consultados livros, artigos e documentos online que trazem o tema foco deste estudo. Os resultados encontrados mostram que as VLANs apresentam mais vantagens do que desvantagens que fazem parte do contexto da comunicação externa e interna, além de armazenamento de processos, o que agrega grande valor para as redes em questão.

Palavras-chave: Redes. Gestão. VLANs. Segurança.

ABSTRACT

Technology has penetrated all sectors of society, and although the benefits are numerous, there are still some aspects that deserve attention. Network security is a key consideration in corporate networks when deciding to invest in technology. Segmentation by Virtual Local Area Networks (VLANs) is important for promoting corporate network security because dividing the physical network into several smaller networks restricts unauthorized access and limits the spread of attacks. This prevents the lateral movement of threats, protects sensitive

data, controls access to resources, and improves the enforcement of security policies, reducing the risk of internal and external attacks. Within this context, the objective of this study is to highlight the relevance of using this segmentation, highlighting its advantages and disadvantages. The methodology used was a literature review, which consulted books, articles, and online documents addressing the topic of this study. The results show that VLANs, in addition to their advantages and disadvantages, are part of the context of external and internal communication, as well as process storage, which adds significant value to the networks in question.

Keywords: Networks. Management. VLANs. Security.

INTRODUÇÃO

De acordo com Alves e Souza (2022) o mundo tem assistido grandes avanços tecnológicos e dentro dessa realidade crescente complexidade de redes corporativas, movimentada pelo uso de serviços em nuvem, mobilidade institucional e crescentes exigências de conformidade, têm ocasionado também a ocorrência de ataques e a urgência de controles de segurança mais divididos.

A segmentação de rede por Virtual Local Area Networks (VLANs) aparece de forma fundamental para que as exposições sejam menores e assim os ataques reduzidos, sem que para isso a conectividade e produtividade sejam comprometidas (Brown, Larson, 2021).

Como forma de conhecimento, as VLANs são tecnologias que permitem a criação de redes lógicas independentes.

Embora as VLANs apresentem muitas vantagens é preciso evidenciar a simples implementação dessa tecnologia não garante a total segurança, visto que podem acontecer falhas na configuração, trunks mal protegidos e outros que veremos no contexto deste estudo (Dias *et al*., 2020).

O problema norteador para esta investigação é como as VLANs podem trazer segurança para as redes corporativas e se essa segurança realmente é eficiente ou ainda permite a probabilidade de riscos de ataques?

Diante destes fatores o objetivo deste artigo foi evidenciar a relevância do uso dessa segmentação, pontuando as vantagens e desvantagens. Os objetivos específicos configuram: conceituar VLANs e redes corporativas; evidenciar o uso crescente da adoção de VLANs e discutir sobre as vantagens e desvantagens do uso dessa tecnologia, e quais são as perspectivas do mercado da TI sobre essa segmentação como forma de promover segurança.

Fernandes e Moura (2022) descrevem que a correta configuração do roteamento entre VLANs, o uso de listas de controle de acesso (ACLs) restritivas, a implementação de firewalls internos e a gestão de políticas de segmentação tornam-se componentes vitais de uma arquitetura de segurança robusta.

Dentro das modernas tecnologias o uso de VLANs é essencial especialmente para as redes corporativas, o que implica um melhor gerenciamento do tráfego e segurança, além de melhorar o desempenho e trazer uma gestão mais eficiente.

2 A SEGMENTAÇÃO COM VLANS E A SERGURANÇA NAS REDES CORPORATIVAS

2.1 Redes Corporativas

Oliveira (2015) descreve como rede corporativa um sistema de transmissão de dados, onde as informações podem ser compartilhadas com diversos equipamentos de uma mesma corporação como: servidores de documentos e arquivos, impressoras e outros.

A rede corporativa é baseada nos padrões de rede local com switches de hardware, dispositivos roteadores, cabeamento ethernet, conexões Wi-Fi e software de firewall integrado, usados para criar uma rede local. Switches e roteadores tem a finalidade de fazer uma conexão entre uma rede local a Internet Service Provider (ISP) e utilizam uma infraestrutura de rede remota de fibra ótica ou banda larga, e assim permite que dados sejam transferidos em alta velocidade entre máquinas locais (VMWARE, 2021).

De acordo com Oliveira (2015) a rede corporativa é para as empresas que querem aumentar sua produtividade e segurança de seus dados um dos sistemas mais importantes. Tais redes contribuem para a melhor organização e trabalho dos colaboradores, visto que não precisam se deslocar para checar arquivos de outros computadores.

As redes corporativas trazem um conjunto de conectividade, serviços e políticas de segurança e gestão do tráfego, que interligam os ativos de uma organização. Tem como finalidade viabilizar a comunicação, colaboração e operação de negócios, agregando confidencialidade, integridade, disponibilidade e conformidade (segurança e governança). Em locais modernos as redes combinam segmentos internos (LANs/WLANs), conectividade a provedores de serviços, data centers, nuvens híbridas, e mecanismos de controle de acesso e

segmentação para reduzir superfícies de ataque e facilitar a administração centralizada (Alves, Souza, 2022; Oliveira *et al*., 2019).

As empresas que buscam inovação precisam criar soluções exclusivas segundo suas necessidades visando o fluxo de trabalho, etapas de produção, necessidade do consumidor, logística, dentre outros (VMWARE, 2020).

Muitos são os benefícios das redes corporativas, como: aumento da produtividade, oferta de um ambiente de trabalho mais organizado; armazenamento de dados em um único lugar, o que acarreta a liberação de espaço dos computadores dos colaboradores, acesso rápido aos documentos e interação de todas as áreas da empresa. Com o uso de VLANs os softwares ficam mais leves e assim é possível maior eficiência, cuidados na gestão da rede, acesso controlado aos recursos das redes, escalabilidade e agilidade operacional; conformidade e segurança de dados, experiência do usuário final aprimorada e outros (VMWARE, 2020; Eco Telecom, 2019).

2.2 VLANs

Segundo Correio e Correio (2019) para entender o conceito de VLAN é importante entender o conceito de Local Area Network (LAN) e broadcast, que representa a transmissão de uma mensagem emitida por um dispositivo e devido a conectividade pode ser recebida por todos os segmentos.

Sendo assim, a LAN é uma rede de dados tolerante a falhas e de alta velocidade, que promove a cobertura de uma área geográfica pequena, interconecta as estações de trabalho, computadores pessoais, impressoras e outros hardwares (Cisco Systems, 2012).

A VLAN em suma é uma tecnologia que permite que a rede física sofra diversas divisões e ocasionando o surgimento de redes independentes. Tal segmentação é realizada no nível do software, ou seja, dispositivos em diferentes VLANs embora estejam próximas fisicamente podem estar separados por redes, e é essa separação que permite a maior segurança (Mikweb, 2024).

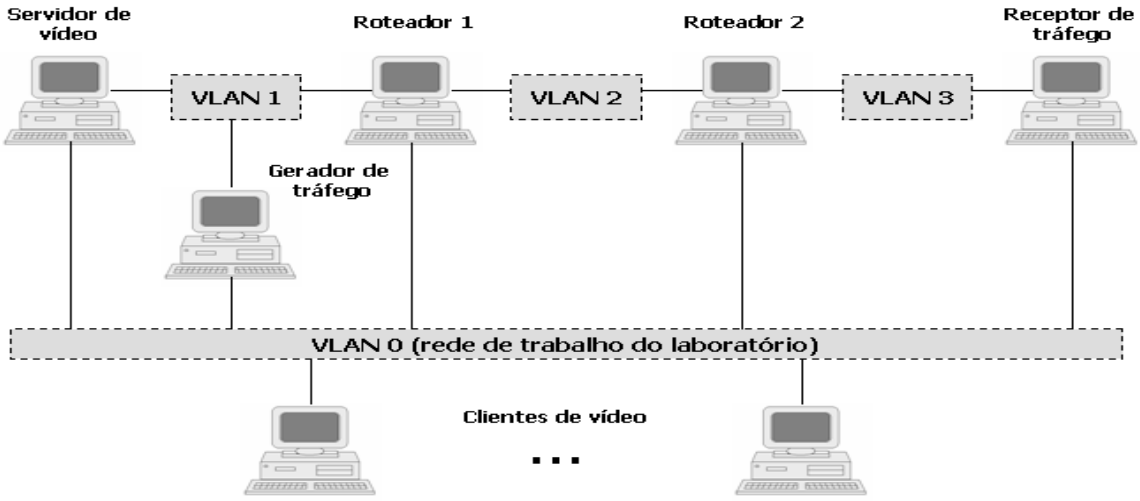
A divisão proporcionada pelas VLANs, permite que diferentes tipos de tráfegos sejam gerenciados com eficiência. Ao gerenciar uma VLAN o switch utiliza um identificador chamado ID da VLAN, cuja função, é garantir que os pacotes de dados pertencentes a uma VLAN não possam sofrer acesso de outra VLAN (Gnew, 2024).

INTERFACE TECNOLÓGICA

O surgimento dessa tecnologia permite que os administradores façam a divisão lógica de diferentes usuários dentro da mesma LAN física, com diferentes domínios de transmissão de acordo com os requisitos reais do aplicativo. Assim, cada VLAN possui um grupo de estações de trabalho do computador, que possuem os mesmos requisitos e os mesmos atributos da LAN física.

A figura 1 traz um exemplo da segmentação das VLANs.

Figura 1: Exemplo de estrutura das VLANs



Fonte: https://www.gta.ufrj.br/grad/02_2/vlans/exemplo.html

Sendo assim é possível que todos os departamentos de uma empresa consigam conectar-se ao mesmo setor, o que traz agilidade na comunicação e produtividade mais eficiente.

É importante descrever que as VLANs se mostram tão importantes que o Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) em 1999 criou o padrão de protocolo 802.1Q como forma de organizar e criar padrões do esquema que implementa as VLANs (Casey, 2023).

2.2.1 Segmentação das VLANs

A segmentação das VLANs pode ser feita da seguinte maneira em uma rede corporativa. Se uma empresa tiver diferentes departamentos como: finanças, recursos humanos, marketing, vendas e utilizar a telefonia IP, as VLANs podem ser assim segmentadas:

- VLAN 1- Tráfego de recursos humanos;
- VLAN 2 – Tráfego de dados do setor de vendas;
- VLAN 3 – Tráfego de dados do departamento de marketing;
- VLAN 4 – Tráfego da telefonia IP e assim sucessivamente.

2.2.2 Tipos de VLANs

- VLAN baseada em Portas
- VLAN baseada em Endereço MAC
- VLAN baseada em Tipo de protocolo
- VLAN baseada em Faixas de IP de subrede
- VLAN baseada em Aplicações ou Serviços

3 METODOLOGIA

O trabalho é fundamentado por meio de Revisão narrativa transparente. O tema foi pensado segundo a necessidade que as redes corporativas têm de segurança. Para o estudo foi delimitado o problema: quais as vantagens e desvantagens da segmentação com VLANs para a segurança de redes corporativas?

A pesquisa foi feita na base de dados Google Acadêmico. A coleta de dados aconteceu entre os meses de janeiro a fevereiro de 2025. Também foram consultados sites que trazem a delimitação do tema foco deste estudo. As palavras-chave utilizadas foram: VLANs, Redes corporativas, VLANs e segurança para as redes corporativas.

Critérios utilizados:

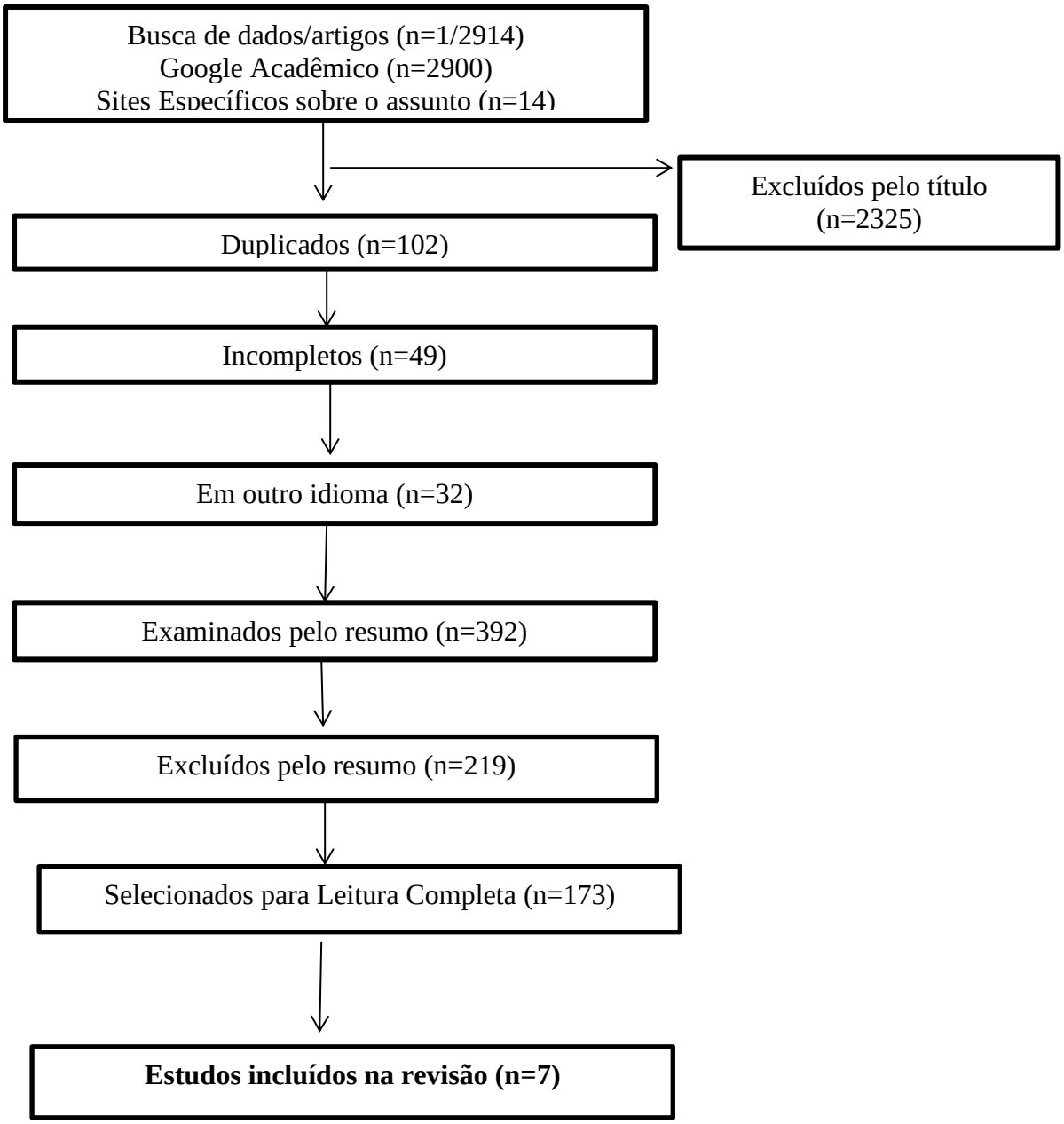
- Inclusão: artigos originais, disponíveis na íntegra, publicados nos últimos 15 anos, no idioma português;

- Exclusão: artigos incompletos, com mais de 15 anos de publicação e em outros idiomas que não o português.

Após usados os critérios de inclusão e exclusão, a pesquisa teve como amostra final o total de 7 artigos e um trabalho de conclusão de curso.

Para um breve entendimento sobre os caminhos da pesquisa realizada até o momento foi elaborado o fluxograma do prisma adaptado.

Fluxograma do Prisma Adaptado



É importante descrever que o PRISMA traz os caminhos apenas para os artigos do Google Acadêmico, pois os sites sobre o tema já eram poucos.

4 RESULTADOS E DISCUSSÃO

Um dos processos vitais da Tecnologia da Informação (TI) é o monitoramento da rede, e esse é feito para trazer maior desempenho, segurança e acessibilidade da rede corporativa. As redes corporativas são na verdade o coração da infraestrutura da tecnologia pois fornece fluxo necessário de informações para que todas as operações da empresa possam funcionar segundo o esperado (Julio, 2020).

É importante descrever que o uso de VLANs trazem muitos benefícios como a redução e propagação de broadcast, limitando o alcance de tráfego entre os segmentos, o que promove melhor desempenho e segurança (Brown, Larson, 2021).

Neto e Almeida (2021) relatam que uma segmentação bem planejada e corretamente configurada, relacionada a controle de acessos dinâmicos e monitoramento constante reduz o risco de compromissos transversais entre departamentos sensíveis e facilita a detecção de atividades suspeitas (Neto, Almeida, 2021).

O quadro 1 apresenta algumas vantagens e desvantagens do uso de Vlans.

Tabela 1: Vantagens e Desvantagens do uso de VLANs

Vantagens	Desvantagens
Segmentação lógica de tráfegos (trazendo maior segurança)	Custo de Hardware – o processo de comunicação entre VLANs diferentes necessita da configuração de um roteador ou switch de Camada 3, o que acaba elevando o custo com a infraestrutura de rede.
Redução da superfície de ataque por função- quando as atividades são agrupadas em VLANs distintas, as políticas de acesso tendem a restringir o movimento lateral de possíveis compromissos.	Complexidade de Configuração – o processo de implementação de VLANs necessita de conhecimento técnicos mais profundos, com isso requer mão de obra qualificada e que nem sempre acessivel.
Contenção de Incidentes – o comprometimento de uma VLANs, devido a sua separação limita o acesso, o que facilita a detecção, contenção e recuperação.	Dependência de Roteadores – a falha de um dispositivo, devido a sua ampla conectividade, pode ocasionar a parada de outros dispositivos.

Controle de acesso entre VLANs (inter-VLAN): é importante evidenciar que o tráfego entre VLANs passa por firewalls/roteadores, os quais têm políticas de acesso restritas, o que exige a autenticação e autorização por usuário/endpoint, inspeção de tráfego, filtragem de aplicações e registro de eventos.	Risco de Congestionamento – se o tráfego não for bem controlado corre-se o risco de congestionamento.
Políticas baseadas em identidade e contexto: o fato de se combinar VLANs com diretórios (AD/LDAP) e políticas de postura (NAC) que permitem acesso apenas a dispositivos e usuários confiáveis	Vazamento de Pacotes – se for feito uma configuração incorreta é possivel que um pacote de uma VLAN vaze para outra
Suporte a Zero Trust estruturado: VLANs oferecem segmentação inicial, a qual é estruturada por verificação contínua de identidade, postura de segurança e monitoramento, reduzindo assim os riscos em locais diversos.	Risco de propagação de ameaças – caso um dispositivo de uma VLAN seja infectado por um vírus essa ameaça pode se espalhar por toda a rede lógica através de configurações inadequadas.
Visibilidade e Governança - logs de tráfego inter-VLAN, métricas de latência e detecção de anomalias ajudam a promover medidas de segurança.	Dificuldade da solução de problemas: a segmentação da rede com VLANs pode dificultar a identificação e redução de problemas.
Facilidade de Conformidade - separação de dados sensíveis facilita atender requisitos regulatórios (LGPD, HIPAA, GDPR).	Acesso a Recursos: empresas que necessitam de acesso a diferentes segmentos podem requerer maior cordenção já que o gerenciamento de acesso pode ser mais complicado.
Compatibilidade com soluções de segurança modernas: VLANs trabalham bem com: firewalls de próxima geração e IDS/IPS entre VLANs.	
Flexibilidade e Escalabilidade- as VLANs permitem a adição de novos dispositivos à rede sem precisar redesenhar toda a infraestrutura.	
Redução da superfície de ataques por meio da segmentação.	

Fonte: Autor segundo dados da pesquisa

Daparé (2020) é categórico em afirmar que a implementação de VLANs tem várias vantagens, e cita a melhoria da performance, visto que a segmentação dos domínios de brodcast o tráfego desnecessário tem redução considerável. O autor cita que os grupos virtuais

criados, oriundos da segmentação, permitem que pessoas e recursos com os mesmos objetivos sejam colocados na mesma VLAN, o que traz uma separação lógica entre departamentos, o que possibilita uma maior segurança na rede local. Dentro desse contexto dados importantes podem ser enviados pelas redes por brodcast, e com VLANs configuradas somente usuários permitidos poderão ter acesso às informações transmitidas.

Diante do que foi exposto é possível perceber que essa tecnologia se faz importante e tende a entrar cada vez mais no contexto das redes. As VLANs trazem mais vantagens do que desvantagens o que mostra e fundamenta sua utilização em redes.

5 CONSIDERAÇÕES FINAIS

Talvez uma das grandes preocupações das empresas, seja adequar redes em seus negócios, tal fato se deve porque é preciso antes de tudo investir em segurança. A divisão das estruturas físicas dentro das redes corporativas é o que define a importância das VLANs no processo de garantia de segurança. Essa tecnologia mostra as suas vantagens e não só pode ser descrita por meio da sua potencialidade em segurança. Diante do exposto é possível definir que o objetivo do estudo foi atingido.

O trabalho traz como contribuição acadêmica o tema proposto neste estudo para conhecimento de futuros profissionais do mercado da tecnologia.

Como contribuição social o trabalho descreve sobre as VLANs que são tecnologias com potencial de gerar segurança, o que é um desejo de empresas que precisam entregar um trabalho eficiente e seguro.

REFERÊNCIAS

ALVES, M. R.; SOUZA, L. A. Segmentação de redes com VLANs: fundamentos, práticas e desafios. **Revista Brasileira de Segurança da Informação**, v. 12, n. 3, p. 45-62, 2022.

CASEY. **VLAN**: o que é e como funciona? 2023. Disponível em: https://www.fibermall.com/pt/blog/what-is-vlan-and-how-it-work.htm?srsltid=AfmBOopLhGS0JJT5j9oZDif2C1ur454sZ1oLh9Srpm9wx0EBaDuVF1q4. Acesso em: 10 jul. 2025.

CISCO SYSTEM. **Virtual LANs/VLAN Trunking Protocol (VLANs/VTP).** 2012. Disponível em: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009441a.shtml. Acesso em: 15 jul. 2025.

CORREIO, C. F. de C. J.; CORREIO, K. R. S. dos A. de C. Aprimorando o desempenho e a segurança das redes locais universitárias com a utilização das técnicas de VLAN. ScientiaTec: **Revista de Educação, Ciência e Tecnologia do IFRS**, v.6, n.1, p: 106-126, Janeiro/Junho 2019. Disponível em:https://d1wqtxts1xzle7.cloudfront.net/75409858/pdf-libre.pdf?1638278707=&response-content disposition=inline%3B+filename%3DAprimorando_o_desempenho_e_a_seguranca_d.pdf&Expires. Acesso em: 2 jan. 2025.

DAPARÉ, C. E**. Uso de VLANs para segurança, segmentação de domínios de broadcast e desempenho da rede**. 2020. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/35476/1/CT_GESER_XI_2020_02.pdf. Acesso em: 2 jul. 2025.

DIAS, K. et al. **Práticas recomendadas de configuração de ACLs e firewalls internos em ambientes segmentados.** IEEE Access Brasil, v. 5, p. 210-225, 2020.

ECOTELECOM. **Benefícios da rede corporativa**. Disponível em: https://ecotelecom.com.br/beneficios-da-rede-corporativa/. Acesso em: 12 jan. 2025.

FERNANDES, R.; MOURA, S. SDN e políticas de identidade na segmentação de VLANs. **Journal of Cloud and Network Security**, v. 4, n. 4, p. 300-316, 2022.

GNEW. **O Que é VLAN e a Importância de Segmentar Redes em Ambientes Corporativos**. 2024. Disponível em: https://gnew.com.br/blog/artigo/segmentacao-rede-vlan-para-empresas/. Acesso em: 2 jan. 2025.

JULIO, C. **Monitoramento de rede**: importância, vantagens e melhores ferramentas. Backup Garantido, 2020. Disponível em: https://backupgarantido.com.br/blog/monitoramento-de-rede/. Acesso em: 30 mar. 2025.

OLIVEIRA, D. R. et al. Boas práticas de governança de redes para conformidade com normas de segurança. **Revista de Governança em TI**, v. 2, n. 1, p. 33-50, 2019.

VMWARE. **Rede Corporativa**. Florianópolis, 2021. Disponível em: https://www.vmware.com/br/topics/glossary/content/enterprise-networking.html. Acesso em: 1 jul. 2025.