# Desenvolvimento de Infraestrutura Segura com Aplicação de Boas Práticas de Segurança da Informação

**Cibelle Araújo de Magalhães[1], Fábio Castro Araújo[1]**

[1]Centro Universitário Luterano de Palmas - (CEULP/ULBRA)
Palmas – TO – Brasil

cibelle.magalhaes@rede.ulbra.br, fabio.araujo@ulbra.br

***Resumo.*** *Este artigo descreve a implementação de melhorias na infraestrutura de Tecnologia da Informação (TI) de uma empresa no setor alimentício, visando segurança, organização e eficiência operacional. O projeto incluiu a estruturação do departamento de TI, mapeamento da infraestrutura, implementação de firewall, segmentação de rede com VLANs e integração de filiais. Foram adotadas práticas de segurança e atualização de equipamentos. Os resultados demonstraram redução de custos, aumento da segurança e melhoria na disponibilidade dos sistemas.*

## 1. Introdução

A Tecnologia da Informação (TI) tem se tornado um pilar essencial para o funcionamento das organizações, garantindo a disponibilidade, integridade e confidencialidade dos sistemas e dados. Nesse contexto, a segurança da informação é fundamental para prevenir riscos e preservar os ativos digitais, sendo considerada um dos principais desafios da atualidade [COSTA, 2020]. Em um cenário de expansão acelerada e crescente dependência de recursos tecnológicos, a falta de uma infraestrutura de TI adequada pode resultar em ineficiências operacionais, vulnerabilidades de segurança e impactos financeiros significativos.

O objetivo principal do projeto foi modernizar a infraestrutura de TI, assegurando a segurança dos dados, a eficiência operacional e a conformidade com as melhores práticas de mercado. Para alcançar esses objetivos, foram executadas diversas etapas. Inicialmente, estruturou-se o departamento de TI com a contratação de uma equipe especializada em infraestrutura e segurança. Em seguida, realizou-se o mapeamento da infraestrutura existente, utilizando Google Planilhas para o inventário dos equipamentos e Draw.io para a elaboração dos diagramas físico e lógico da rede.

Para fortalecer a segurança perimetral, foi implementado um firewall Cisco Meraki MX64, enquanto a segmentação de rede com VLANs foi configurada em switches gerenciáveis TP-Link SG-3428, com auxílio do Notepad++ para edição e organização dos scripts. A integração das filiais foi realizada por meio de VPNs, utilizando IPSec para conexões *site-to-site* e SSL VPN para acesso remoto de colaboradores. Adicionalmente, adotaram-se práticas de segurança da informação alinhadas a *frameworks* reconhecidos no mercado.

Para garantir a continuidade dos negócios, foram implementados sistemas de backup em nuvem com o Veeam, além da configuração de um ambiente de Active

Directory para centralizar a gestão de usuários e políticas de grupo. Por fim, os equipamentos e servidores foram atualizados, assegurando a conformidade com os padrões de segurança e a modernização necessária para suportar as demandas atuais.

A justificativa para este trabalho reside na necessidade de demonstrar como a modernização da infraestrutura de TI pode impactar positivamente a operação de uma empresa, especialmente em setores críticos, onde a disponibilidade e a segurança dos sistemas são fundamentais. Este artigo apresenta um estudo de caso sobre a implementação de melhorias na infraestrutura de TI de uma empresa real, que operava sem um departamento de TI estruturado e enfrentava desafios como a falta de gerenciamento de rede, ausência de políticas de segurança e equipamentos obsoletos.

## 2. Referencial Teórico

A infraestrutura de Tecnologia da Informação (TI) é um componente crítico para o funcionamento eficiente de organizações modernas. Ela engloba sistemas, redes, hardware e software que, quando bem gerenciados, garantem a disponibilidade, integridade e confidencialidade dos dados. Segundo a InvGate (2024), uma infraestrutura de TI bem estruturada é essencial para sustentar as operações de negócios, oferecendo suporte à continuidade, segurança e eficiência operacional. Neste referencial teórico, serão abordados conceitos essenciais como Firewall, VLANs, Backup, Active Directory (AD) e IPSec, que são fundamentais para a segurança e operação de redes corporativas, especialmente em ambientes com múltiplas filiais.

### 2.1 Firewall

O Firewall é um sistema de segurança que atua como uma barreira entre redes confiáveis e não confiáveis, filtrando o tráfego de dados com base em regras predefinidas. Ele é um equipamento de borda essencial para prevenir ataques cibernéticos, como negação de serviço (DDoS) e tentativas de acesso não autorizado (Brute Force). Existem diferentes tipos de firewalls, como os de filtragem de pacotes, os de estado e os de aplicação, cada um com suas particularidades.

Segundo Tanenbaum (2021, p.486) relata que

> O critério de filtragem normalmente é dado como regras ou em tabelas que listam as origens e os destinos aceitáveis, as origens ou destinos bloqueados e as regras padrão que orientam o que deve ser feito com os pacotes recebidos de outras máquinas ou destinados a elas.

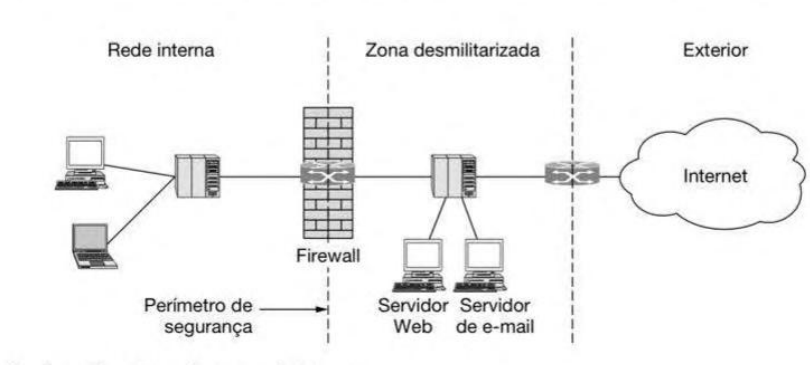



**Figura 1 – Exemplo de firewall protegendo uma rede interna**

*[Fonte: TANENBAUM, 2021, p. 486.]*

Além disso, os firewalls modernos evoluíram para atuar em múltiplas camadas do modelo OSI, oferecendo recursos que vão além da filtragem básica. Os chamados firewalls de próxima geração (*Next-Generation Firewall* – NGFW) incorporam funcionalidades como inspeção profunda de pacotes (*Deep Packet Inspection* – DPI), prevenção contra intrusões (IPS) e controle de aplicações, permitindo políticas de segurança mais detalhadas e adaptadas às necessidades das organizações. De acordo com a Clavis (2023), os firewalls modernos combinam a inspeção de pacotes com a filtragem por aplicação e análise de comportamento, permitindo um controle mais eficaz contra ameaças dinâmicas e persistentes.

Portanto, observa-se que a implementação de firewalls é um componente indispensável na arquitetura de segurança de redes computacionais dentro de uma empresa. Sua ausência torna os sistemas significativamente mais expostos a ataques maliciosos, especialmente em ambientes críticos. A ocorrência de tais ataques pode comprometer a disponibilidade dos serviços, ocasionando prejuízos financeiros diretos, custos com mitigação de danos e perda de confiabilidade por parte dos usuários. Assim, o firewall se consolida como uma ferramenta essencial na prevenção de acessos indevidos e na garantia da continuidade operacional das redes.

## 2.2 VLANs (*Virtual Local Area Networks*)

As VLANs (*Virtual Local Area Networks*) são redes virtuais criadas dentro de uma rede física, permitindo a segmentação lógica de dispositivos. Elas melhoram a segurança, o desempenho e a gestão da rede ao isolar grupos de dispositivos em sub-redes distintas. Conforme explica a Columbia TI (2022), esse tipo de segmentação lógica contribui para um ambiente de rede mais seguro e organizado, facilitando o controle e a administração dos recursos de forma eficiente. Elas aumentam a segurança ao reduzir riscos de ataques internos e vazamentos, utilizando ACLs (*Access Control Lists*) e firewalls para controlar comunicações entre VLANs. Além disso, melhoram o desempenho ao reduzir domínios de broadcast e permitir priorização de tráfego via QoS (*Quality of Service*).

Segundo Frinhani (2005, P.45), “Uma VLAN é a união de dispositivos de uma rede local em um agrupamento lógico que tem a intenção de segmentar a rede em pequenos domínios de difusão”. Elas facilitam a escalabilidade, permitindo expansão sem grandes reconfigurações físicas, e suportam a mobilidade de usuários. Integram-se a tecnologias como virtualização, *cloud*, IoT e dispositivos móveis, estendendo a segmentação e isolando dispositivos para maior segurança.

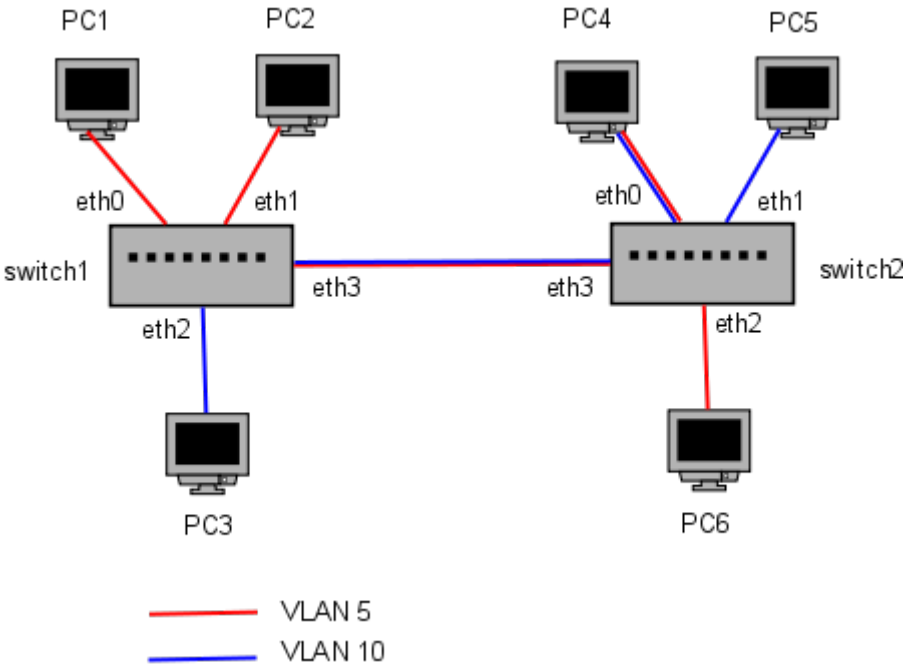



**Figura 2: Exemplo de funcionamento de VLANs**

As identificações das VLANs são feitas por meio do VID (VLAN ID), composto por números. Segundo a Huawei (2024), “as IDs de VLAN variam de 0 a 4095. Os valores 0 e 4095 são reservados e, portanto, as IDs VLAN válidas variam de 1 a 4094”. Além do VID, as VLANs funcionam com base em dois modos de operação nas portas: *tagged* (*trunk*) e *untagged* (acesso), e a forma de parametrização dependerá da topologia implementada na rede. As VLANs do tipo *tagged* exigem que cada pacote transmitido inclua a identificação da VLAN à qual pertence, permitindo o transporte de múltiplas VLANs em uma mesma porta. Já as VLANs *untagged* não exigem que os pacotes contenham informações sobre a VLAN de origem, sendo normalmente utilizadas na conexão com dispositivos finais que não reconhecem VLAN.

O sucesso da implementação depende de planejamento, documentação detalhada e padronização de nomenclatura, alinhados às melhores práticas de rede, nesse quesito, as VLANs são uma estratégia eficaz para alinhar recursos de rede aos objetivos operacionais e de segurança da empresa.

## 2.3 VPN (*Virtual Private Network*)

As Redes Privadas Virtuais (VPNs) representam uma solução tecnológica ideal para estabelecer comunicações seguras em infraestruturas públicas não confiáveis. "Em vez de alugar linhas de transmissão dedicadas, uma empresa pode conectar seus escritórios à Internet. Isso permite que as conexões sejam feitas entre os escritórios como enlaces virtuais que usam a capacidade de infraestrutura da Internet." [TANENBAUM; WETHERALL; FEAMSTER, 2021, p. 15].

A VPN é amplamente utilizada em ambientes corporativos, permitindo que funcionários acessem remotamente a rede interna da organização como se estivessem fisicamente presentes. Isso se dá por meio da criação de um túnel virtual entre o dispositivo do usuário e a rede corporativa, no qual os dados trafegam de forma criptografada, dificultando a interceptação por terceiros. Essa prática é viabilizada pelo uso de redes públicas, como a Internet, que interconectam diferentes locais da organização com redução de custos e maior flexibilidade de acesso, inclusive para profissionais que trabalham em campo ou em *home office* [STALLINGS, 2014]. Existem diferentes tipos de VPNs, entre elas:

### 2.3.1 VPN de Acesso Remoto

A VPN de acesso remoto permite que um usuário estabeleça uma conexão segura com a rede interna da empresa utilizando a internet pública como meio de transporte. Essa modalidade é amplamente adotada por empresas que oferecem modelos de trabalho remoto, garantindo que seus colaboradores tenham acesso aos recursos corporativos de forma segura, mesmo estando fora do ambiente físico da empresa. Para a implementação dessa conexão, são utilizados protocolos específicos que garantem a integridade, autenticidade e confidencialidade dos dados. Dentre os protocolos modernos, destaca-se o IKEv2/IPSec, que oferece excelente desempenho e é especialmente eficiente por sua capacidade de reconectar automaticamente após quedas de conexão, sendo ideal para dispositivos móveis.

Além disso, é recomendável o uso de softwares que utilizam os protocolos SSL/TLS para criptografia, uma vez que oferecem um alto nível de segurança e flexibilidade, sem exigir investimentos em infraestrutura adicional. Entre algumas soluções mais utilizadas no mercado, destacam-se, por exemplo, o OpenVPN, NetExtender e o Cisco AnyConnect, que estabelecem a conexão segura diretamente com dispositivos de borda da rede, como os firewalls. Ainda de acordo com Stallings (2014), o uso de VPNs é uma estratégia eficaz para reduzir custos com infraestrutura de rede dedicada, ao mesmo tempo em que garante segurança através de protocolos criptográficos aplicados nos dispositivos de borda, como firewalls ou roteadores, capazes de realizar autenticação e cifração de dados sem que isso seja perceptível às estações de trabalho na LAN.

### 2.3.2 VPN de *Site-to-Site*

A VPN do tipo *site-to-site* é uma tecnologia que permite conectar duas ou mais redes locais (LANs) situadas em diferentes locais geográficos por meio de túneis criptografados sobre a internet. Essa modalidade é amplamente utilizada por empresas com filiais ou unidades remotas, garantindo a integração segura e contínua das redes internas. Nessa

configuração, a comunicação ocorre diretamente entre os dispositivos de borda das redes, como roteadores ou firewalls, sem a necessidade de intervenção dos usuários finais. O tráfego entre os sites é roteado automaticamente pela VPN, fazendo com que as redes atuem como se estivessem fisicamente conectadas [FORTINET, [s.d.]].

O protocolo mais utilizado para a implementação de VPNs *site-to-site* é o IPSec *(Internet Protocol Security*), que garante os principais atributos da segurança da informação dos dados transmitidos entre os pontos. O IPSec é um conjunto de protocolos que atua na camada 3 do modelo OSI e pode operar em dois modos: modo transporte, que protege apenas o conteúdo do pacote IP, e modo túnel, que encapsula o pacote IP inteiro, sendo este último o mais comum em conexões entre redes corporativas. Para oferecer segurança de ponta a ponta, o IPSec utiliza dois subprotocolos principais: o AH (*Authentication Header*), responsável por autenticação e integridade, e o ESP (*Encapsulating Security Payload*), que, além disso, também realiza a criptografia dos dados. Em ambientes VPN, o ESP é amplamente preferido por proporcionar proteção completa aos pacotes transmitidos. Segundo o autor Stallings (2014), o uso do AH tem se tornado obsoleto nas aplicações modernas, uma vez que as funcionalidades de autenticação e integridade já são providas pelo próprio ESP, tornando-o a escolha mais indicada para cenários que exigem confidencialidade e autenticação simultâneas.

A negociação das chaves criptográficas e dos parâmetros de segurança é feita por meio do protocolo IKE (*Internet Key Exchange),* geralmente em sua versão mais atual, o IKEv2, que automatiza e protege o processo de criação dos túneis IPSec. Essa combinação garante alto desempenho na comunicação entre redes remotas, sendo compatível com firewalls, roteadores e *appliances* de segurança modernos. Em alguns cenários, o protocolo GRE (*Generic Routing Encapsulation*) pode ser utilizado em conjunto com o IPSec para encapsular diferentes protocolos de roteamento, ampliando a flexibilidade da solução.

### 2.3.4 VPN por Camada (Layer 2 e Layer 3)

Segundo a Cato Networks ([s.d])**,** as VPNs também podem ser classificadas de acordo com a camada do modelo OSI em que operam, sendo elas: camada 2 (enlace) e camada 3 (rede). As VPNs de camada 2 operam no nível do enlace de dados, encapsulando quadros (*frames*) completos. Essa abordagem permite o transporte de protocolos não-IP, como *Ethernet*, e é frequentemente utilizada em ambientes que exigem comunicação em nível de broadcast ou configurações específicas de rede local. O protocolo L2TP (*Layer 2 Tunneling Protocol*) é um dos principais representantes dessa categoria, frequentemente utilizado em conjunto com IPSec para fornecer segurança adicional.

Já as VPNs de camada 3 atuam na camada de rede, manipulando pacotes IP diretamente. Esse tipo de VPN é mais comum em ambientes corporativos e utiliza protocolos como o IPSec para criar túneis seguros. As VPNs de camada 3 oferecem maior escalabilidade e desempenho, sendo indicadas para conexões entre redes IP padronizadas e com maior necessidade de roteamento.

**Quadro 1 – Comparação entre os principais tipos de VPN**

| **Tipo de VPN** | **Finalidade Principal** | **Protocolos Utilizados** | **Características** |
|---|---|---|---|
| Acesso Remoto | Conectar usuários externos à rede corporativa | IKEv2/IPSec, L2TP/IPSec, OpenVPN, SSL | Ideal para trabalho remoto. Fácil de configurar. Requer software cliente. |
| Site-to-Site | Interligar redes locais de diferentes localidades | IPSec, GRE/IPSec | Comunicação automática entre redes. Não requer ação do usuário final. |
| Camada 2 (Enlace) | Transportar protocolos de enlace (ex: *Ethernet*) | L2TP, MPLS | Suporta protocolos não-IP. Útil para simular redes locais ampliadas. |
| Camada 3 (Rede) | Encapsular pacotes IP para comunicação entre redes. | IPSec, OpenVPN | Alta escalabilidade. Roteamento eficiente entre redes IP. |

*Fonte: Elaborado pelo autor com base em Stallings (2014) e Tanenbaum e Wetherall (2011).*

Embora a VPN seja uma ferramenta essencial para garantir a comunicação segura entre usuários externos e a rede corporativa, ela, por si só, não é suficiente para assegurar a proteção integral dos recursos organizacionais. É ideal que seu uso esteja inserido em uma estrutura mais ampla de segurança, composta por firewalls bem configurados, sistemas de detecção e prevenção de intrusões (IDS/IPS), e, sobretudo, uma política de segurança da informação bem definida, atualizada e alinhada às necessidades da empresa e em cultura com os colaboradores.

Além disso, recomenda-se que as organizações adotem *frameworks* de segurança consolidados, como a ISO/IEC 27001, o NIST Cybersecurity Framework ou o COBIT, que orientam na criação de controles, diretrizes e procedimentos voltados à gestão de riscos, ao controle de acessos, e à proteção de dados sensíveis. Esses *frameworks* auxiliam na estruturação de ambientes seguros, garantindo não apenas a proteção técnica, mas também organizacional e comportamental, essenciais para prevenir vulnerabilidades decorrentes de erros humanos ou falhas de processo.

## 2.4 Backup

O Backup é uma prática essencial para garantir a recuperação de dados em caso de falhas, ataques cibernéticos ou desastres. Ele consiste na criação de cópias de segurança dos dados, que podem ser armazenadas em diferentes mídias, como discos locais, fitas ou na nuvem. Uma das estratégias mais eficazes atualmente é o backup híbrido, que combina armazenamento local e em nuvem, oferecendo maior flexibilidade e segurança.

Diferentemente do simples armazenamento em nuvem, o backup em nuvem é projetado para proteger automaticamente os dados, permitindo sua restauração em caso de perda [DROPBOX, 2025]. O backup híbrido permite que as organizações mantenham uma cópia dos dados localmente, para recuperação rápida em caso de pequenos incidentes, e outra na nuvem, para proteção contra desastres de grande escala, como incêndios ou inundações. Essa abordagem segue a regra 3-2-1, que recomenda manter três cópias dos dados, em dois tipos de mídia diferentes, com uma cópia *off-site*.

O backup nas empresas é extremamente importante, pois garante muita segurança a todo tipo de informação da empresa. Com ele é possível recuperar os danos de algum problema ocorrido com os servidores ou as máquinas dos funcionários [SCOPEL et al., 2018]. Além disso, a nuvem oferece vantagens como escalabilidade, redução de custos com infraestrutura física e acesso remoto aos dados. No entanto, é fundamental garantir que a conexão com a nuvem seja segura e que os dados sejam criptografados durante o transporte e o armazenamento.

## 2.5 *Active Directory*

O Active Directory (AD) é um serviço de diretório da Microsoft utilizado para gerenciar usuários, computadores e permissões em uma rede corporativa. Ele organiza os recursos da rede em domínios, árvores e florestas, facilitando a administração centralizada [MICROSOFT, 2023]. A implementação do AD permite a aplicação de políticas de segurança, políticas de grupo (GPOs), como a restrição de privilégios administrativos e o controle de acesso a pastas e arquivos. A remoção de privilégios administrativos das máquinas dos usuários é uma medida importante para aumentar a segurança do ambiente.

Segundo a Quest (2025), o Active Directory simplifica a vida dos administradores e usuários finais, ao mesmo tempo que aumenta a segurança das organizações. Os administradores se beneficiam do gerenciamento centralizado de usuários e direitos, assim como do controle centralizado sobre as configurações do computador e do usuário por meio do recurso Diretiva de grupo do AD. Além disso, a segmentação de pastas por departamento permite uma gestão mais eficiente dos dados, garantindo que apenas os usuários autorizados tivessem acesso às informações relevantes.

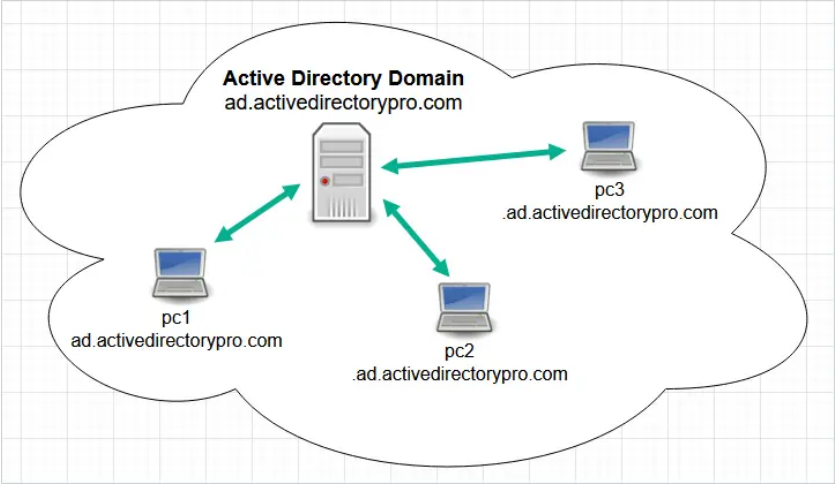



**Figura 3: Exemplo de funcionamento do Active Directory**

**Quadro 2 – Principais Componentes do Active Directory**

| Componente | Função |
|---|---|
| Domínio (*Domain*) | É a base lógica do AD. Agrupa objetos como usuários, PCs e grupos. |
| Controlador de Domínio (DC) | Servidor responsável por autenticar usuários e aplicar políticas. |
| Unidade Organizacional (OU) | Subdivisão lógica dentro de um domínio, usada para organizar objetos. |
| GPO (*Group Policy Object*) | Conjunto de regras aplicadas a usuários e PCs para padronizar configurações. |
| LDAP (*Lightweight Directory Access Protocol*) | Protocolo usado para consultar e modificar dados no AD. |

| | |
|---|---|
| Kerberos | Protocolo padrão para autenticação segura no Windows. |

*Fonte: Elaborado pelo autor com base em documentação da Microsoft*

De acordo com a Microsoft (2025), o Active Directory é um serviço de diretório que oferece uma maneira estruturada de armazenar informações sobre objetos da rede e facilita a autenticação e o controle de acesso em ambientes corporativos. Ele organiza e controla objetos como usuários, computadores, grupos e políticas de segurança dentro de um ambiente de domínio. Por meio de componentes como o Controlador de Domínio (DC), Unidades Organizacionais (OU) e Políticas de Grupo (GPO), o AD permite a autenticação de usuários, aplicação de regras e controle de permissões para acesso a recursos de rede. Sua arquitetura baseada em protocolos como o LDAP e Kerberos proporciona segurança, escalabilidade e eficiência no gerenciamento de ambientes corporativos. A centralização promovida pelo Active Directory é essencial para empresas que precisam de controle rigoroso sobre seus recursos de TI.

## 2.6 Políticas da Segurança da Informação

Diante do aumento dos ataques cibernéticos, é essencial estabelecer políticas de segurança da informação nas empresas, que estipulem regras, normas e procedimentos para o uso seguro dos recursos tecnológicos e a proteção dos ativos digitais. Essas políticas ajudam a mitigar vulnerabilidades, orientam ações corretivas em caso de incidentes e promovem a conscientização dos colaboradores sobre as melhores práticas de segurança [SECURITY BUSINESS, 2024]. A proteção dos ativos digitais depende também da implementação de políticas de segurança da informação bem estruturadas, que estabeleçam regras, normas e diretrizes para o uso seguro dos recursos tecnológicos.

Segundo a norma ABNT NBR ISO/IEC 27001:2022, política de segurança da informação é definida como um conjunto de diretrizes formalmente documentadas que orientam o comportamento corporativo, com o objetivo de proteger a confidencialidade, a integridade e a disponibilidade das informações. Essas políticas abrangem aspectos como controle de acessos, uso de senhas, classificação da informação, gestão de incidentes e riscos, matriz de riscos e conscientização de usuários.

Além disso, a utilização de *frameworks* de cibersegurança reconhecidas internacionalmente contribui para a consolidação de uma governança eficiente em segurança da informação.

### 2.6.1 ISO/IEC 27001

De acordo com o portal 27001.pt (2025), a ISO/IEC 27001 é uma norma internacional amplamente utilizada para padronizar e fortalecer os processos de segurança da informação nas organizações, sendo referência na definição de práticas seguras e no gerenciamento de riscos. Seu objetivo é proteger a confidencialidade, integridade e disponibilidade das informações dentro de uma organização. A norma propõe uma

abordagem baseada em riscos, exigindo que as empresas identifiquem, avaliem e tratem ameaças potenciais à informação. Ela também especifica a adoção de controles de segurança, auditorias internas, ações corretivas e melhoria contínua. Define requisitos para um sistema de gestão da segurança da informação (SGSI), com foco na gestão de riscos e melhoria contínua.

> A adoção da norma ISO 27001 serve para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação. A norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigar e gerir adequadamente o risco da organização, promovendo uma abordagem completa para a segurança da informação: avaliando pessoas, políticas e tecnologias. [27001.PT, 2025]


**Figura 4: Anexo A ISO 27001**

*Fonte: QFS Management System LLP*

Segundo o relatório publicado pela ISMS.online, a certificação ISO 27001 é uma das mais adotadas mundialmente no campo da segurança da informação, com um aumento significativo nas últimas décadas:

> As certificações na ISO 27001 aumentaram 450% nos últimos dez anos.
>
> (tradução livre do autor)
>
> (ISMS.ONLINE, 2022, p. 5).

A norma também se alinha a sete dos nove princípios de segurança da informação definidos pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), como: conscientização, responsabilidade, resposta a incidentes, avaliação de riscos, arquitetura de segurança, gestão contínua e ética.

A avaliação de desempenho se concretiza por meio da realização de auditorias internas, que analisam o cumprimento dos objetivos do SGSI e os requisitos da norma, sendo obrigatória a revisão por auditores independentes durante o processo de certificação. Em caso de não conformidades identificadas, a organização deve adotar ações corretivas baseadas em análises de causa, documentando os procedimentos e assegurando que as falhas não se repitam. Por fim, a norma também inclui anexos e diretrizes complementares que abordam temas como análise de riscos, controle de segurança, avaliação de conformidade, capacitação das equipes, documentação e auditoria do SGSI, fortalecendo a aplicação prática dos princípios previstos.

### 2.6.2 *NIST Cybersecurity Framework*

O *National Institute of Standards and Technology* (NIST) é uma agência federal norte-americana, não reguladora, vinculada ao Departamento de Comércio dos Estados Unidos, cuja missão é promover a inovação e a competitividade industrial por meio do avanço da ciência, da normalização e da tecnologia de medição [NIST, 2024]. No campo da segurança da informação, o NIST destaca-se pelo desenvolvimento do *Cybersecurity Framework* (NIST CSF), uma estrutura de referência composta por padrões, diretrizes e boas práticas destinadas a apoiar as organizações na gestão eficaz dos riscos de segurança cibernética. Ainda de acordo com o NIST, foi lançado oficialmente em 2014, após a publicação da Ordem Executiva 13636, o NIST CSF tornou-se uma das ferramentas mais utilizadas nos Estados Unidos para fortalecer a segurança de infraestruturas críticas e ambientes corporativos, especialmente no setor privado.

> O Framework concentra-se no uso de direcionadores de negócios para orientar as atividades de segurança cibernética e na consideração dos riscos de segurança cibernética como parte dos processos de gestão de riscos da organização. O Framework consiste em três partes: o Framework Core, os Framework Implementation Tiers e os Framework Profiles.
>
> (tradução livre do autor) (NIST, 2014, p. 1).

O NIST CSF foi concebido para ser flexível e adaptável a organizações de diferentes portes e setores, permitindo sua integração com outros *frameworks* e sistemas de gestão já existentes. A estrutura é composta por quatro elementos principais: funções, categorias, subcategorias e referências informativas. As funções que representam os pilares do *framework* são: Identificar, Proteger, Detectar, Responder e Recuperar. Segundo a IBM (2024), essas funções não são etapas sequenciais, mas sim componentes operacionais que atuam de maneira simultânea e contínua, estabelecendo uma cultura de segurança cibernética sólida e resiliente.

Cada função é subdividida em categorias, que agrupam objetivos de segurança relacionados a áreas específicas, como governança, controle de acesso, detecção de incidentes, mitigação de danos e continuidade operacional. Conforme explicado pela IBM (2024), as subcategorias detalham atividades que ajudam a implementar essas categorias,

enquanto as referências informativas conectam as ações a outras normas, como ISO/IEC 27001:2013, COBIT 5, CIS Controls e NIST SP 800-53.


**Figura 5: Funções da CSF**

*Fonte: NIST*

A estrutura também define quatro níveis de implementação que permitem avaliar o grau de maturidade da organização em relação à segurança cibernética:

- Nível 1 – Parcial: práticas reativas e pouco padronizadas;
- Nível 2 – Risco Informado: maior consciência dos riscos, porém sem integração formal de processos;
- Nível 3 – Repetido: gestão sistemática dos riscos com participação da liderança;
- Nível 4 – Adaptativo: aprendizado contínuo, análises preditivas e resiliência organizacional consolidada, como descrito pela IBM (2024).

O NIST CSF também propõe um ciclo estruturado de implementação, composto pelas seguintes etapas: definição de escopo e prioridades, orientação por regulamentos e ameaças, criação de um perfil atual da organização, realização de avaliação de riscos, construção de um perfil de destino, identificação e priorização de lacunas entre os perfis e, por fim, execução de um plano de ação baseado em marcos, recursos e metas definidas. Essas diretrizes, conforme descritas no portal da IBM (2024), orientam o fortalecimento da governança e a continuidade dos negócios frente a incidentes. Em suma, o *framework* representa uma abordagem prática e escalável para o desenvolvimento de políticas de segurança da informação alinhadas ao contexto organizacional, à legislação vigente e às melhores práticas do setor

## 3. Materiais e Métodos

Para assegurar a aplicabilidade dessa prática, foi adotado uma abordagem sistemática na seleção e aquisição das novas ferramentas e para a documentação de todos os componentes tecnológicos utilizados. A seleção dos equipamentos e softwares considerou critérios como desempenho, segurança e conformidade com os padrões do setor, assegurando que a implementação das soluções de VPN e redes seguissem as melhores práticas de mercado.

### 3.1 Materiais

#### 3.1.1 Firewall Cisco Meraki MX64

O equipamento foi selecionado como solução central de segurança devido à sua capacidade de gerenciamento unificado via *cloud* e proteção integrada contra ameaças, substituindo o antigo roteador MikroTik que operava sem políticas de segurança adequadas. Segundo a documentação técnica do fabricante [CISCO MERAKI, 2023], o MX64 possui um processador quad-core de 1.4 GHz e 4GB de memória DDR4, capaz de gerenciar até 50 túneis VPN simultâneos com throughput de 250 Mbps quando o IPsec está ativado. Na implementação, configuramos políticas de segurança hierárquicas, criando zonas separadas para WAN, LAN e DMZ, além de ativar todos os recursos de IPS/IDS integrados.

Foram configuradas regras de firewall com granularidade, baseadas em aplicações, usuários e dispositivos. Por exemplo, foram bloqueadas portas como HTTP (80) e HTTPS (443) e demais portas, para serviços não autorizados, permitindo apenas o tráfego necessário para aplicações específicas, como o sistema interno da empresa e o acesso remoto via VPN.

**Figura 6: Modelo de referência (Cisco Meraki MX64)**

*Fonte: Datasheet do fabricante Cisco*

A funcionalidade de VPN *Site-to-Site* foi ativada com criptografia AES-256 e autenticação por IKEv2, garantindo a integridade e a confidencialidade dos dados trafegados entre unidades remotas. A opção de *Perfect Forward Secrecy* (PFS) foi habilitada para reforçar ainda mais a proteção dos túneis criptografados, prevenindo que chaves de sessão antigas sejam reutilizadas em caso de comprometimento.

O monitoramento foi realizado por meio do Meraki Dashboard, uma plataforma centralizada em nuvem que permite visualizar o tráfego em tempo real, gerar relatórios automáticos e emitir alertas para atividades suspeitas, como tentativas de acesso não autorizado e picos de tráfego fora do padrão.

### 3.1.2 Switches Gerenciáveis TP-Link TL-SG3428

Estes switches foram fundamentais para a segmentação lógica da rede através de VLANs. Conforme a documentação técnica do fabricante [TP-LINK, 2023], esses switches oferecem de 24 portas Gigabit RJ45 e 4 portas SFP, com capacidade para gerenciar até 4.000 VLANs simultâneas através do padrão IEEE 802.1Q, além de throughput não-bloqueante de 56 Gbps. Na prática, foi configurado portas *trunk* para interligação dos equipamentos principais e portas *access* para conexão dos dispositivos finais. A configuração de QoS garantiu prioridade para o tráfego de voz e dos principais sistemas da empresa. Os switches foram implementados como solução central para a rede interna, substituindo os dispositivos não gerenciáveis que causavam conflitos e instabilidade na infraestrutura anterior.


**Figura 6: Modelo de referência (Switch TP Link 3428)**

*Fonte: DataSheet do fabricante TPLINK.*

Foram criadas VLANs específicas para diferentes setores da empresa, como TI, corporativo, colaboradores e visitantes, promovendo o isolamento de tráfego e aumentando a segurança da rede. Essa segmentação reduziu consideravelmente o risco de broadcast storms e possibilitou a aplicação de regras distintas para cada grupo de usuários. As portas *trunk* foram configuradas para interligar os equipamentos principais da infraestrutura (como o firewall e outros switches), enquanto as portas *access* foram atribuídas aos dispositivos finais, como estações de trabalhos e impressoras. Foi utilizado o recurso de *Quality of Service* (QoS) para garantir a priorização do tráfego de dados críticos, como chamadas de voz por IP (VoIP), acesso ao sistema ERP e ao servidor de

arquivos em nuvem. Essa configuração resultou em maior desempenho e estabilidade nos serviços sensíveis à latência.

### 3.1.3 TP-Link EAP Outdoor 225 e 610

Para a cobertura wireless em áreas externas e internas, os access points da série EAP foram instalados seguindo as especificações de resistência ambiental descritas no datasheet. Segundo o fabricante (TP-LINK, 2023), o modelo EAP610 suporta o padrão Wi-Fi 6 (IEEE 802.11ax), operando com múltiplos fluxos simultâneos e oferecendo velocidades superiores, além de melhor eficiência em ambientes com muitos dispositivos conectados. Por esse motivo, foi posicionado em locais com maior concentração de usuários, como salas de reunião e áreas administrativas. Já o EAP225 Outdoor [TP-LINK, 2021], com suporte ao padrão 802.11ac (Wi-Fi 5), foi alocado em áreas internas de menor demanda, complementando a cobertura e com melhor eficiência em ambientes com maior concentração de umidade. Foi configurado 4 SSIDs distintos segregados por VLANs (Corporativo, Coletores, Colaboradores e Visitantes). Essa separação lógica permitiu aplicar políticas de acesso diferenciadas, garantindo maior segurança e controle do tráfego.

**Figura 7: Modelo de referência (TP-Link EAP Outdoor 225)**

*Fonte: DataSheet do fabricante TPLINK.*

***Figura 8: Modelo de referência (STP-Link EAP 610)***

*Fonte: DataSheet do fabricante TPLINK.*

Foram ajustados manualmente os canais de operação e os níveis de potência de transmissão, minimizando interferências entre os dispositivos. Foi também ativado o balanceamento de carga entre os *access points,* permitindo uma distribuição equilibrada dos clientes conectados e evitando sobrecarga em um único AP. Nos modelos EAP 610, o recurso *Fast Roaming* (*Zero-Roaming*) foi habilitado, possibilitando a transição suave de conexão entre pontos de acesso com latência inferior a 50 milissegundos, algo essencial para dispositivos móveis, como nos casos dos coletores de dados e aplicações de tempo real.

As VLANs definidas no switch foram propagadas corretamente até os *access points*, garantindo a coerência do isolamento de tráfego desde a borda da rede até os dispositivos finais.

### 3.1.4 Mikrotik RB 2011

Os roteadores MikroTik RB2011 foram mantidos nas unidades filiais da empresa como parte da estratégia de redundância de conectividade e continuidade operacional. Embora tenham sido substituídos na matriz por um firewall dedicado, nas filiais os equipamentos ainda demonstram desempenho adequado quando corretamente configurados. Segundo a documentação técnica do fabricante [MIKROTIK, 2023], o modelo conta com processador ARM de 600 MHz e 256 MB de RAM, sendo capaz de sustentar até cinco túneis IPSec simultâneos com throughput médio de 87 Mbps. Esses dispositivos foram configurados para operar como roteadores de borda, otimizados para duas funcionalidades principais: gerenciamento de *failover* e estabelecimento de túneis criptografados IPSec com a matriz.


**Figura 9: Modelo de referência (Mikrotik Routerboard RB2011UIAS-RM)**

*Fonte: DataSheet do fabricante Mikrotik*

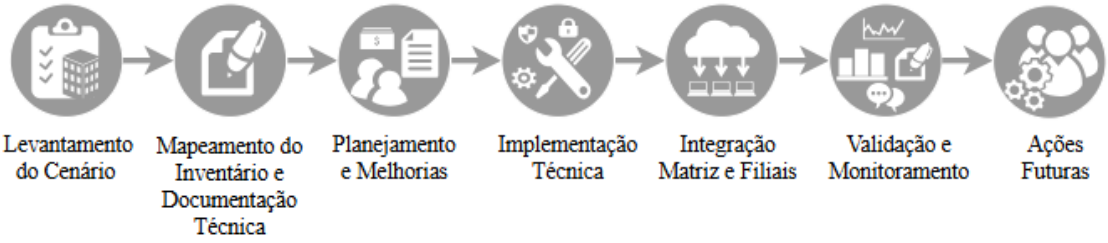
O *failover* foi implementado com testes de conectividade (ping) realizados a cada dois segundos nos gateways dos provedores de internet. Paralelamente, o roteador realiza análises de qualidade de conexão por meio de métricas de jitter (inferior a 30 ms) e perda de pacotes (menor que 5%). Quando há falha no link principal, o roteador ativa automaticamente o link secundário em menos de três segundos. Uma vez estabilizada a conexão original por um período contínuo de cinco minutos, o roteador realiza o retorno automático ao link primário. Foram configurados túneis IPSec utilizando criptografia forte com algoritmos como AES-256, autenticação via SHA-256 e estabelecimento de chaves com DH Group 14, para garantir a segurança na comunicação entre matriz e filiais. O parâmetro de *Perfect Forward Secrecy* (PFS) também foi habilitado, garantindo que cada sessão possua chaves únicas e não reaproveitáveis.

O Mikrotik também desempenha a função de servidor DHCP, realizando reservas de endereços IP para dispositivos específicos e distribuindo faixas de IP para os diferentes segmentos de rede interna das filiais. Foi configurado um firewall stateful, com regras para detecção e bloqueio de varreduras de portas (*port scanning*) e aplicação de *rate limiting* em serviços de gerenciamento como SSH e Winbox, mitigando o risco de ataques por força bruta e negação de serviço.

## 3.2 Métodos

Para a execução deste trabalho, foi necessário seguir uma sequência de etapas práticas no ambiente real de uma empresa do ramo alimentício, com foco na reestruturação da infraestrutura de TI e segurança da informação. A figura 10 apresenta o fluxo do trabalho realizado, seguido de uma breve explicação de cada etapa a seguir:

**Figura 10: Fluxo de trabalho**




*Fonte: Autoria própria*

Foi realizado um diagnóstico completo da infraestrutura de TI, contemplando aspectos físicos e lógicos. Esse processo incluiu mapeamento de equipamentos ativos e passivos, levantamento de inventário com apoio do setor contábil, patrimônio e análise de conectividade, segurança e disponibilidade dos serviços. Utilizaram-se ferramentas como Google Planilhas para inventário, Draw.io para modelagem da topologia de rede e Google Docs para documentação de processos e políticas. A partir do diagnóstico, foi possível identificar falhas críticas, como ausência de segmentação de rede, inexistência de controle de acesso, falta de políticas de segurança e equipamentos obsoletos. Essa documentação serviu de base para as próximas fases do projeto.

A seguir, as atividades foram divididas em blocos de execução, conforme as prioridades definidas com a gerência executiva e o conselho da empresa. Foi elaborado um documento RFP (*Request for Proposal*) com propostas com o objetivo de selecionar empresas especializadas para atuar em etapas críticas do projeto, especialmente nas frentes de segurança da informação, certificações e *frameworks* de segurança como ISO/IEC 27001:2013, ITIL, COBIT 5, CIS Controls e NIST SP 800-53, backup em nuvem, implantação do Active Directory e locação de notebooks e demais ativos de TI.

A partir das propostas recebidas, foram selecionadas as empresas parceiras que melhor atenderam aos requisitos técnicos, operacionais e financeiros do projeto. As soluções implementadas incluíram a instalação de firewall perimetral [Cisco Meraki MX64], segmentação da rede com VLANs em switches gerenciáveis TP-Link, implantação do Active Directory com políticas de segurança e servidor de arquivos, backup em nuvem com retenção mínima de 30 dias, além da integração entre matriz e filiais via VPN Site-to-Site com criptografia IPSec.

As melhorias foram implementadas de forma sequencial. Foram adotadas VLANs para segmentação da rede, substituição de switches não-gerenciáveis por gerenciáveis, instalação de firewall, e reconfiguração dos *access points*. O Active Directory foi implantado com restrições de acesso, mapeamento de pastas e políticas de segurança.

Foram criados túneis de VPN entre matriz e filiais, permitindo acesso remoto seguro aos dispositivos e sistemas. Isso melhorou o controle do ponto eletrônico, impressoras, roteadores e reduziu o tempo de resposta da TI. Durante a execução, foram utilizados critérios técnicos baseados em desempenho, segurança, escalabilidade e compatibilidade com padrões do setor. A metodologia também incluiu a adoção de

*frameworks* de segurança, como ISO/IEC 27001 e NIST Cybersecurity Framework, utilizados como referência para definição de políticas e controles internos.

Além da parte técnica, o projeto foi acompanhado de um processo de gestão de mudanças, incluindo comunicação e aprovação junto à diretoria, elaboração de orçamentos OPEX e CAPEX, e validação contínua das etapas por meio de reuniões com *stakeholders*. Cada uma dessas etapas foi conduzida visando a redução de custos, reaproveitamento de recursos existentes e alinhamento com as melhores práticas de segurança da informação. A metodologia adotada permitiu alinhar as melhorias de infraestrutura às necessidades operacionais da empresa, promovendo um ambiente seguro, eficiente e preparado para futuras expansões.

## 4. Desenvolvimento

O desenvolvimento deste projeto teve início com uma análise da infraestrutura de tecnologia da informação existente na empresa, cuja operação vinha se sustentando, até então, sem um departamento de TI estruturado. O ambiente apresentava sérias fragilidades tanto no aspecto físico quanto lógico, que comprometem diretamente a segurança, a disponibilidade dos serviços e a eficiência dos processos operacionais.

Diante desse cenário, tornou-se imprescindível realizar um levantamento de todos os ativos tecnológicos, bem como mapear os principais pontos críticos, de forma a elaborar um plano de ação estruturado, capaz de atender às demandas atuais e, principalmente, preparar o ambiente para suportar o crescimento da organização nos próximos anos.

### 4.1. Parte Lógica

O primeiro passo foi construir do zero a base operacional do setor de TI. Esse processo envolveu não apenas a definição da estrutura organizacional, mas também o desenvolvimento de metodologias, processos e práticas que garantem a governança da infraestrutura tecnológica. Para isso, foi conduzido um levantamento completo do parque tecnológico, no qual foram inventariados computadores, notebooks, servidores, ativos de rede, dispositivos de conectividade e demais elementos que compunham a infraestrutura existente.

#### 4.1.1 Levantamento e Diagnóstico

Inicialmente, foi realizado um levantamento técnico detalhado da infraestrutura existente. Esse levantamento identificou uma série de problemas críticos, como ausência de gerenciamento de rede, inexistência de segmentação lógica, vulnerabilidades de segurança e falta de controle sobre usuários e acessos. Ferramentas como Google Planilhas e Draw.io foram utilizadas para documentar os ativos, desenhar diagramas da topologia física e lógica e planejar as intervenções necessárias.

### 4.1.2 Modelagem da Topologia de Rede

A partir desse diagnóstico, foi possível elaborar a modelagem da nova topologia da rede, considerando tanto os aspectos físicos quanto os lógicos. A definição da arquitetura priorizou uma abordagem segmentada, baseada na criação de VLANs, que permitiram isolar setores como administrativo, comercial, TI, antecâmara e visitantes. Essa segmentação não só elevou o nível de segurança, como também otimizou o desempenho da rede, reduzindo o domínio de broadcast e promovendo maior controle sobre o tráfego interno. Essa arquitetura lógica foi desenhada levando em consideração as melhores práticas de segurança da informação, além dos princípios de alta disponibilidade e escalabilidade.

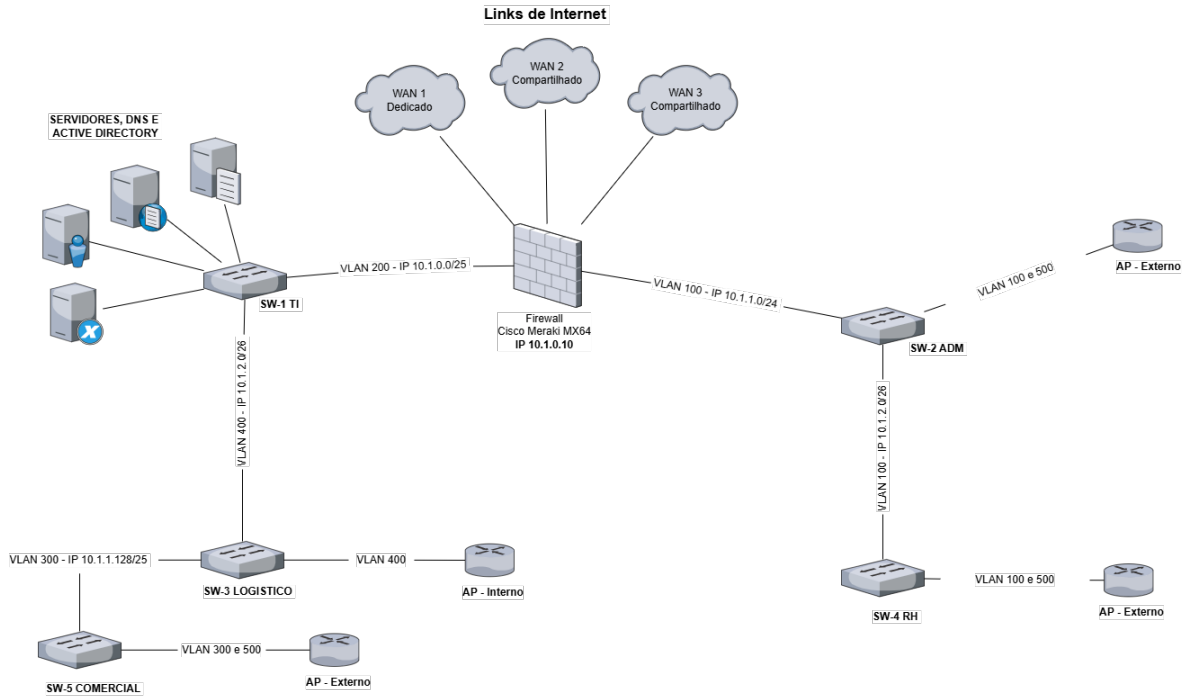



**Figura 11: Topologia Lógica atual da Matriz**

*Fonte: Autoria própria*

As VLANs foram distribuídas conforme a necessidade de cada setor da empresa: a VLAN 100 - Administrativa atende aos departamentos administrativo, financeiro, de recursos humanos e contabilidade; a VLAN 200 - TI concentra os dispositivos e serviços da área de Tecnologia da Informação; a VLAN 300 - Comercial cobre o anexo destinado às operações comerciais; a VLAN 400 - Logística contempla as antecâmaras utilizadas por coletores de dados, impressoras de etiquetas, impressoras convencionais e estações de trabalho da área logística; e, por fim, a VLAN 500 - Visitantes configura uma rede isolada, com acesso restrito ao restante da rede e somente para navegação na internet, garantindo a integridade da rede corporativa. Essa divisão lógica reforça o controle e a eficiência da infraestrutura, contribuindo diretamente para a segurança e o gerenciamento eficaz da rede.

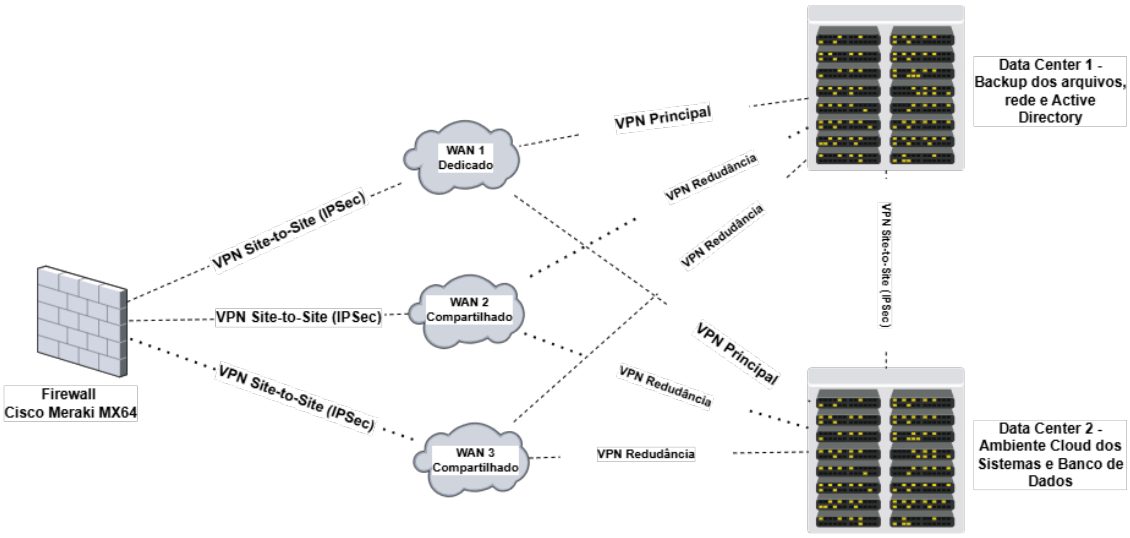



**Figura 12: Topologia lógica atual da comunicação entre Matriz e os Data Centers**

*Fonte: Autoria própria*

A matriz se comunica com dois data centers que desempenham papéis distintos e complementares na infraestrutura da organização. O Data Center 1 é responsável pelos backups dos servidores de arquivos, da rede e do Active Directory, garantindo a preservação e a recuperação de dados críticos. Já o Data Center 2 hospeda o ambiente em nuvem onde estão localizados os sistemas corporativos e o banco de dados, assegurando alta disponibilidade e escalabilidade dos serviços. Ambos os data centers estão interligados à matriz por meio de túneis VPN Site-to-Site utilizando o protocolo IPSec, além de possuírem conectividade entre si, permitindo o redirecionamento de rotas em caso de falhas nos links principais. A WAN 1, uma conexão dedicada à internet, concentra o tráfego principal e as VPNs primárias. Já as WAN 2 e WAN 3 são conexões compartilhadas, configuradas como redundâncias automáticas via failover, garantindo a continuidade das operações em situações de indisponibilidade da WAN principal.

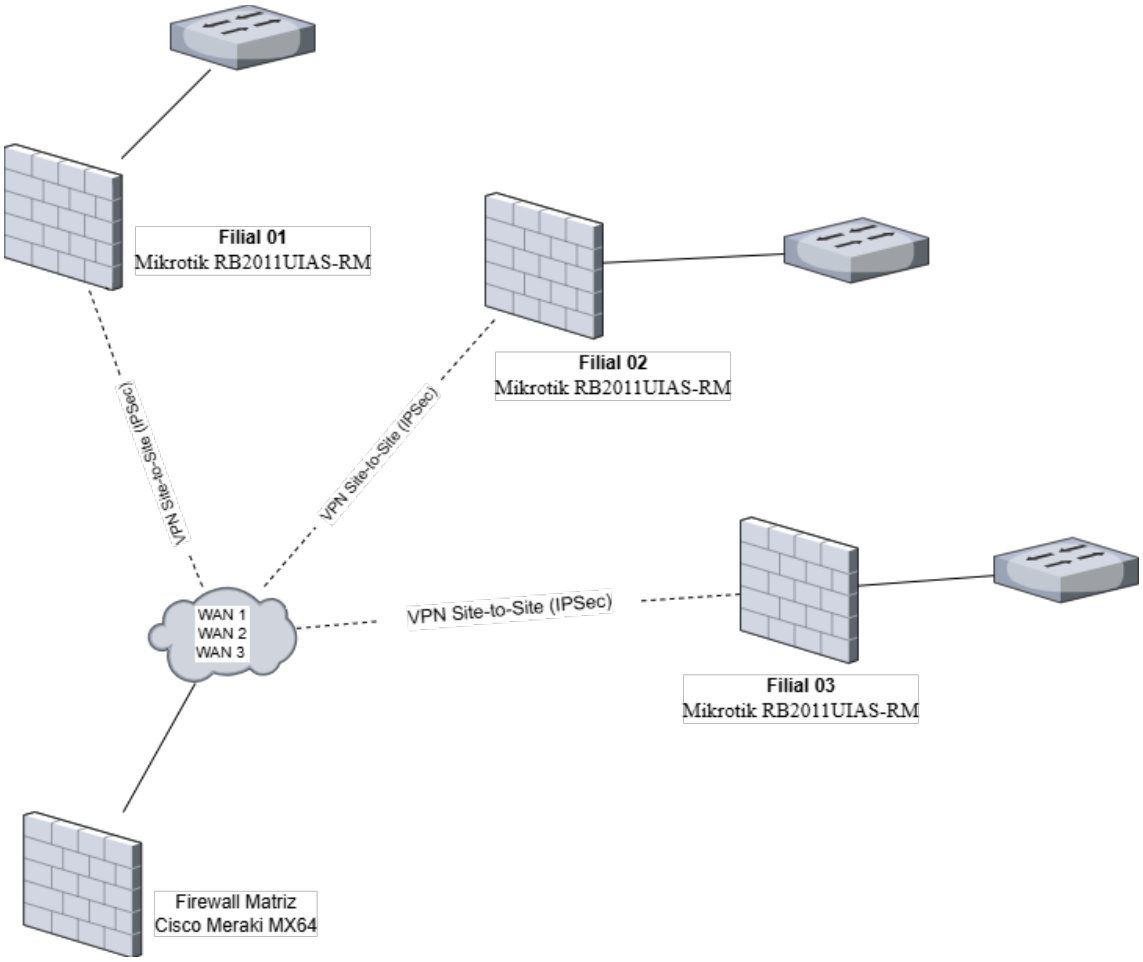



**Figura 13: Topologia lógica atual da comunicação entre Matriz e Filiais**

*Fonte: Autoria própria*

A comunicação entre a matriz e as filiais é realizada por meio de túneis VPN Site-to-Site utilizando o protocolo IPSec, com suporte a múltiplos links e configuração de redundância para garantir a disponibilidade da conexão em caso de falhas. Cada filial utiliza equipamentos padrão Mikrotik RB2011UiAS-RM e segue a mesma estrutura lógica de segmentação de VLANs adotada na matriz. Embora atualmente não haja operação ativa nas filiais, essa padronização foi mantida com o objetivo de garantir organização e facilitar futuras expansões, permitindo a integração imediata de novos dispositivos ou setores conforme necessário. Essa uniformidade na arquitetura de rede contribui para a escalabilidade e facilita o gerenciamento centralizado dos recursos de TI.

### 4.1.3 Arquitetura de Segurança

Foram definidos os parâmetros que nortearam as regras de segurança, incluindo a criação de políticas de firewall, controle de acesso, restrições de serviços, roteamento interno e externo, além do planejamento de redundância de links e conexões seguras com as filiais. A definição da arquitetura de segurança envolveu ainda a estruturação de túneis VPN site-to-site, com aplicação de criptografia e autenticação avançada, garantindo que a comunicação entre as unidades da empresa fosse realizada de forma segura, íntegra e

eficiente. Foi definida uma arquitetura de segurança composta pelos seguintes elementos principais:

- **Firewall Perimetral:** Controle de tráfego externo e interno, com bloqueio de portas e protocolos não autorizados;
- **Segmentação via VLANs:** Isolamento de setores, dispositivos críticos e rede de colaboradores e visitantes;
- **VPN Site-to-Site e Acesso Remoto:** Implementação de túneis criptografados entre matriz e filiais e acesso seguro para colaboradores externos;
- **Políticas de Controle de Acesso:** Definindo permissões baseadas em perfis, utilizando Active Directory;
- **Plano de Backup e Recuperação de Desastres:** Com retenção de 30 dias e recuperação em até 6 horas;
- **Matriz de Riscos e Plano de Contingência:** Avaliação dos principais riscos operacionais e definição de ações mitigatórias.

### 4.1.4 Definição de Processos e Políticas

Foram elaboradas diretrizes de segurança da informação, ainda em construção, mas já aplicando os seguintes controles:

- Controle de Acesso e Autenticação Fortalecida;
- Bloqueio de portas USB e dispositivos não autorizados;
- Restrição de navegação por conteúdo;
- Aplicação de criptografia para dados em trânsito e em repouso;
- Política de senhas e renovação periódica.
- Políticas de instalações de programas.

Essas definições foram alinhadas às normas e *frameworks* como ISO/IEC 27001 e NIST Cybersecurity Framework, além de estarem em conformidade com a LGPD (Lei Geral de Proteção de Dados).

Por meio desse processo de modelagem lógica, consolidou-se um ambiente capaz de oferecer não apenas mais segurança, mas também uma base sólida para suportar a operação atual e a expansão futura da empresa. A combinação de uma arquitetura lógica bem estruturada, aliada a processos de governança e segurança, garantiu a mitigação dos principais riscos operacionais apresentados durante o diagnóstico, preparando o cenário para a implementação física da nova infraestrutura.

## 4.2 Parte Física

A etapa física foi dedicada à execução prática de todo o planejamento elaborado na fase lógica, envolvendo tanto a aquisição de novos equipamentos quanto a reconfiguração dos recursos existentes.

### 4.2.1 Infraestrutura de Rede

Este processo teve início com a substituição dos switches não gerenciáveis por modelos gerenciáveis de alta performance, que passaram a desempenhar um papel central na infraestrutura, permitindo a aplicação efetiva das VLANs, o controle de tráfego, a implementação de políticas de QoS (*Quality of Service*) e o monitoramento contínuo da rede. A implementação do firewall Cisco Meraki representou um dos marcos mais significativos deste projeto. Esse equipamento passou a concentrar funções essenciais como controle de tráfego de entrada e saída, filtragem de pacotes, aplicação de políticas de segurança, além de ser o responsável pela gestão dos túneis VPN que conectam a matriz às filiais.

A adoção desse firewall não só fortaleceu a segurança perimetral, como também possibilitou uma administração mais eficiente e centralizada, graças à sua interface de gerenciamento em nuvem, que oferece visibilidade total do ambiente e permite a detecção e resposta rápida a incidentes.

### 4.2.2 Servidores e Serviços Críticos

Outro avanço importante foi a reestruturação do ambiente dos servidores. Foram configurados servidores Dell PowerEdge para hospedar serviços essenciais como Active Directory, servidor de arquivos e sistema de backup. A implantação do Active Directory permitiu centralizar a gestão de usuários, grupos e permissões, aplicando diretivas de segurança via GPOs e restringindo acessos de acordo com os níveis hierárquicos e necessidades operacionais de cada departamento.

Complementarmente, a solução de backup foi concebida no modelo híbrido, com cópias locais e em nuvem hospedado em datacenter terceiro, onde também há responsabilidades legais quanto às informações e dados armazenados e serviços prestados, assegurando a integridade e disponibilidade dos dados, além de permitir uma recuperação ágil em caso de falhas, conforme demonstrado durante um incidente em que foi possível restaurar um servidor comprometido em menos de duas horas.

### 4.2.3 Rede Sem Fio

No âmbito da conectividade, foi realizada a expansão e otimização da rede sem fio, com a instalação de *access points* corporativos, modelos TP-Link EAP225 Outdoor e EAP610, estrategicamente posicionados para garantir cobertura em todas as áreas internas e externas da empresa. A configuração desses dispositivos incluiu a criação de múltiplos SSIDs, cada um vinculado a uma VLAN específica, garantindo o isolamento adequado dos diferentes tipos de tráfego, como dados corporativos, dispositivos móveis, coletores de dados e acesso de visitantes. Adicionalmente, foram aplicadas otimizações de canais, balanceamento de carga e habilitação do *fast roaming*, proporcionando uma experiência de conexão estável, segura e com baixa latência, mesmo em ambientes críticos como antecâmaras e setores operacionais.

### 4.2.4 Filiais e Redundância

Os roteadores de borda Mikrotik RB2011, que anteriormente desempenhavam um papel central na infraestrutura, foram mantidos nas unidades filiais, porém, com uma nova

configuração, voltada para funções específicas de roteamento, gerenciamento de *failover* e estabelecimento de túneis VPN IPSec com a matriz. Essa configuração não apenas garantiu a continuidade dos serviços em caso de falhas nos links principais, como também proporcionou uma comunicação segura e estável entre os diferentes pontos da organização, como mostra a figura 11.

Por fim, foram implementados processos de monitoramento e gestão de processos, utilizando a plataforma Meraki Dashboard, que oferece visibilidade em tempo real do desempenho da rede, permite a geração de relatórios, envio de alertas automáticos e facilita o diagnóstico de problemas, e também a implementação do GLPI, ferramenta de código aberto disponibilizada na internet para customização conforme a necessidade da organização, utilizado para gerir as demandas pertinentes ao departamento para atendimento e resolução das demandas dos colaboradores em tempo hábil, padronizado SLAs e OLAs conforme urgência de cada processo e operação.

## 5. Considerações Finais

Este trabalho teve como objetivo modernizar a infraestrutura de TI de uma empresa do setor alimentício, com foco em segurança, desempenho e organização dos recursos tecnológicos. A proposta foi atender às demandas atuais da empresa e preparar o ambiente para seu crescimento, promovendo melhorias técnicas e estruturais na rede, nos servidores e nos serviços de TI.

A execução das atividades permitiu corrigir diversos problemas que impactavam diretamente a operação da empresa, como lentidão na rede, ausência de controle centralizado, falta de backup confiável e dificuldades de acesso remoto. As soluções aplicadas incluíram a implantação de firewall perimetral, segmentação da rede com VLANs, Active Directory com controle de usuários, servidor de arquivos, backup em nuvem com retenção de 30 dias e integração via VPN entre matriz e filiais. Parte dessas soluções foram implementadas com o apoio de empresas especializadas, contratadas por meio de RFP, garantindo mais qualidade e segurança na execução dos serviços.

Do ponto de vista prático, os resultados foram bastante positivos. A área logística teve a lentidão solucionada, o suporte técnico passou a ser mais eficiente, e os chamados fora do horário, principalmente por problemas de conexão ou acesso ao ambiente *cloud*, praticamente desapareceram. O ambiente de TI ficou mais estável e confiável, e as mudanças foram reconhecidas positivamente pelo conselho consultivo da empresa.

Com isso, conclui-se que o objetivo do trabalho foi alcançado. A nova infraestrutura atendeu às necessidades da empresa e proporcionou um ambiente mais seguro, escalável e alinhado com as boas práticas da área. Além dos benefícios técnicos, o projeto contribuiu para o fortalecimento da cultura organizacional voltada à segurança da informação e ao uso estratégico da tecnologia.

Como próximos passos, estão previstos: a implementação de monitoramento completo de servidores, links e dispositivos; a substituição do firewall atual por um modelo de próxima geração; a replicação da nova estrutura nas demais filiais; a troca dos nobreaks por modelos de maior capacidade (10KVA); e a adoção de uma solução SD-WAN para melhorar a gestão da conectividade entre unidades.

Essas futuras melhorias visam dar continuidade à evolução do ambiente de TI, ampliando os resultados obtidos e mantendo a infraestrutura preparada para os próximos desafios da organização.

## 6. Referências


FRINHANI, Rafael de Magalhães Dias. **Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras**. 2005. 80 f. Monografia (Graduação em Ciência da Computação) – Universidade Federal de Lavras, Lavras, 2005.

TANENBAUM, A.; WETHERALL, D.; FEAMSTER, K. **Redes de computadores**. 6. ed. São Paulo: Pearson, 2021.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. Tradução da 2. ed. Rio de Janeiro: Elsevier, 2014.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

SCOPEL, Eduardo Longhi et al. **Importância da segurança da informação e backup**. In: MOSTRA DE INICIAÇÃO CIENTÍFICA, 18., 2018, Caxias do Sul. Anais [...]. Caxias do Sul: Universidade de Caxias do Sul, 2018. p. 10.

QUEST. **O que é Active Directory?** Disponível em: https://www.quest.com/br-pt/solutions/active-directory/what-is-active-directory.aspx. Acesso em: 20 jun. 2025.

MICROSOFT. **Active Directory Domain Services – learning path**. Disponível em: https://learn.microsoft.com/pt-br/training/paths/active-directory-domain-services/. Acesso em: 16 jun. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2022 – Tecnologia da informação – Segurança da informação, cibersegurança e proteção da privacidade – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2022.

QMS BRASIL. **ISO 27001:2013 ISO 27701:2020 – Sistema de Gestão da Segurança da Informação e Sistema de Gestão de Informação Privada**. São Paulo: QMS Brasil, 2021. Disponível em: https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf. Acesso em: 16 jun. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (EUA). **Framework for improving critical infrastructure cybersecurity**. Version 1.1. Gaithersburg, MD: NIST, 2018. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 1 abr. 2025.

COSTA, Juliana. **O que é ISO 27001? Entendendo o padrão de segurança da informação**. Blog Clicksign, 22 abr. 2024. Disponível em: https://www.clicksign.com/blog/o-que-e-iso-27001. Acesso em: 20 jun. 2025.

IBM BRASIL. **O que é o NIST Cybersecurity Framework?** Disponível em: https://www.ibm.com/br-pt/topics/nist. Acesso em: 20 jun. 2025.

CISCO MERAKI. **MX64 and MX65 overview and specifications**. Disponível em: https://documentation.meraki.com/MX/MX_Overviews_and_Specifications/MX64_and_MX65_Overview_and_Specifications. Acesso em: 20 jun. 2025.

TP-LINK. **TL-SG3428 – JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots: especificações técnicas**. Disponível em: https://www.tp-link.com/br/business-networking/managed-switch/tl-sg3428/#specifications. Acesso em: 20 jun. 2025.

TP-LINK. **EAP610 – Access Point Wi-Fi 6 Dual Band AX1800 de montagem no teto: especificações técnicas**. Disponível em: https://www.omadanetworks.com/br/business-networking/omada-wifi-ceiling-mount/eap610/#specifications. Acesso em: 20 jun. 2025.

TP-LINK. **EAP225-Outdoor – AC1200 Wireless Dual-Band 802.11ac Wave 2 Outdoor Access Point: especificações técnicas**. Disponível em: https://www.omadanetworks.com/br/business-networking/omada-wifi-outdoor/eap225-outdoor/#specifications. Acesso em: 20 jun. 2025.

MIKROTIK. **RB2011UiAS-RM – RouterBOARD 2011UiAS-RM: 1U rackmount router: especificações técnicas**. Disponível em: https://mikrotik.com/product/RB2011UiAS-RM. Acesso em: 20 jun. 2025.

INVGATE. **Infraestrutura de TI: o que é e por que é importante?** InvGate, 2024. Disponível em: https://invgate.com/pt/itsm/it-operations/it-infrastructure. Acesso em: 24 jun. 2025.

CLAVIS. **Entenda o que é um firewall de próxima geração (NGFW).** Clavis Segurança da Informação, 2023. Disponível em: https://clavis.com.br/entenda-firewall-proxima-geracao-ngfw/. Acesso em: 24 jun. 2025.

COLUMBIA TI. **O que é VLAN?** Columbia Tecnologia da Informação, 2022. Disponível em: https://columbiati.com/o-que-e-vlan/. Acesso em: 25 jun. 2025.

HUAWEI. **Basic concepts of VLAN.** Atualizado em 4 nov. 2024. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1000089036/60b1f2f0/basic-concepts-of-vlan. Acesso em: 25 jun. 2025.

FORTINET. **What is site-to-site VPN?** Disponível em: https://www.fortinet.com/br/resources/cyberglossary/what-is-site-to-site-vpn. Acesso em: 25 jun. 2025.

CATO NETWORKS. **MPLS vs VPN: what are the key differences?** Disponível em: https://www.catonetworks.com/what-is-mpls/mpls-vs-vpn-what-are-the-key-differences/. Acesso em: 25 jun. 2025.

DROPBOX. **Armazenamento em nuvem versus backup em nuvem: qual é a diferença?** 21 jan. 2025. Disponível em: https://www.dropbox.com/pt_BR/resources/cloud-storage-vs-cloud-backup. Acesso em: 25 jun. 2025.

MICROSOFT. **Visão geral dos serviços de domínio do Active Directory.** 6 jul. 2023. Disponível em: https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. Acesso em: 25 jun. 2025.

SECURITY BUSINESS. **Saiba a importância da segurança da informação nas organizações.** 2024. Disponível em: https://securitybusiness.com.br/saiba-a-importancia-da-seguranca-da-informacao-nas-organizacoes/. Acesso em: 25 jun. 2025.

27001.PT. **O que é a ISO/IEC 27001.** 2025. Disponível em: https://www.27001.pt/. Acesso em: 25 jun. 2025.

ISMS.ONLINE. **The proven path to ISO 27001 success.** v. 3.0. 2022. Disponível em: https://www.scribd.com/document/686958487. Acesso em: 26 jun. 2025.

NIST. **Cybersecurity Framework.** Gaithersburg, MD: National Institute of Standards and Technology, 2014. (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0). Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf. Acesso em: 26 jun. 2025.

IBM. **NIST Cybersecurity Framework (CSF).** 2024. Disponível em: https://www.ibm.com/br-pt/topics/nist. Acesso em: 26 jun. 2025.

COSTA, Juliana. **Segurança da informação e TI. Administradores.com**, 2020. Disponível em: ttps://www.administradores.com.br/artigos/seguranca-da-informacao-ti. Acesso em: 24 jun. 2025.