



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS  
Instituto de Ciências Exatas e de Informática

**Empresa de manufatura com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km\***

Manufacturing company with offices in the center of a metropolitan region, headquarters in an industrial region and branches in 3 cities approximately 200 km apart.

Bianca Oliveira da Silva<sup>1</sup>  
Davi Perrier Cabral<sup>2</sup>  
Diego da Silva Gomes Barbosa<sup>3</sup>  
Enzo Silva Soares<sup>4</sup>  
Henrique Israel Oliveira<sup>5</sup>  
Fábio L. R. Cordeiro (Orientador)<sup>6</sup>

### Resumo

Esse relatório técnico referente ao quinto eixo temático do curso de Sistemas de Informação da Pontifícia Universidade Católica de Minas Gerais – Projeto de Infraestrutura de Rede, irá abordar sobre a solução tecnológica e desenvolvimento de uma infraestrutura de rede para uma empresa de manufatura de produtos de limpeza com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km. As soluções serão implementadas levando em consideração as necessidades da empresa, incluindo número de usuários, tipos de dispositivos, aplicações utilizadas e localizações das unidades, implementação de um protótipo de rede em ambiente controlado para testar as soluções propostas, criação de um modelo de rede que atenda às necessidades identificadas, utilizando ferramentas de simulação e modelagem, observando as boas práticas de projetos de redes de computadores com o objetivo de garantir uma infraestrutura robusta, segura e escalável para a empresa de produtos de limpeza.

**Palavras-chave:** Infraestrutura de Rede. Solução Tecnológica. Boas Práticas.

\*Relatório Técnico Final Formal referente ao Eixo 5 - Projeto da Infraestrutura de rede.

<sup>1</sup>Aluna do Programa de Graduação em Sistemas de Informação, Brasil – 1395624@sga.pucminas.br.

<sup>2</sup>Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1325706@sga.pucminas.br.

<sup>3</sup>Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1373926@sga.pucminas.br.

<sup>4</sup>Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1389997@sga.pucminas.br.

<sup>5</sup>Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1330553@sga.pucminas.br.

<sup>6</sup>Professor Orientador do Programa de Graduação em Sistemas de Informação, Brasil – fabio@sga.pucminas.br.

## Abstract

This technical report regarding the fifth thematic axis of the Information Systems course at the Pontifical Catholic University of Minas Gerais - Network Infrastructure Project, will address the technological solution and development of a network infrastructure for a cleaning products manufacturing company with offices in the center of a metropolitan region, headquarters in an industrial region, and branches in 3 cities approximately 200 km away. The solutions will be implemented taking into account the company's needs, including the number of users, types of devices, applications used, and locations of the units, implementation of a network prototype in a controlled environment to test the proposed solutions, creation of a network model that meets the identified needs, using simulation and modeling tools, observing best practices in computer network projects with the aim of ensuring a robust, secure, and scalable infrastructure for the cleaning products company.

**Keywords:** Network Infrastructure. Manufacturing. Technological Solution. Best Practices.

## 1 INTRODUÇÃO

A empresa Eco Cleaning teve sua origem em 2010, quando um grupo de ambientalistas e engenheiros químicos se uniu com o objetivo de criar uma linha de produtos de limpeza que fossem eficazes, seguros para o meio ambiente e para as pessoas. Inspirados pela crescente preocupação com a sustentabilidade e o bem-estar, eles fundaram a Eco Cleaning em uma instalação de produção na região industrial, onde começaram a desenvolver fórmulas exclusivas de produtos de limpeza.

Com foco contínuo na inovação e qualidade, a Eco Cleaning rapidamente ganhou reconhecimento por seus produtos que utilizavam ingredientes naturais e biodegradáveis. À medida que a demanda por produtos de limpeza aumentava, especialmente durante a pandemia global, a empresa viu a oportunidade de expandir suas operações investindo na abertura de filiais em três cidades distantes, cada uma estrategicamente localizada a cerca de 200 km de distância da matriz com o objetivo de atender rapidamente clientes em áreas mais distantes, conseguindo atender à crescente demanda e fornecer soluções de limpeza essenciais para uma ampla gama de setores, desde hospitais e instituições de saúde até empresas e residências.

Hoje, a Eco Cleaning é líder no setor de limpeza ecológica, oferecendo uma ampla gama de produtos que não apenas limpam efetivamente, mas também ajudam a proteger o meio ambiente e a saúde das pessoas. Com um compromisso inabalável com a sustentabilidade, inovação e responsabilidade social, a Eco Cleaning continua a ser uma força motriz na transformação da indústria de limpeza para um futuro mais limpo e verde.

## 2 ESTRUTURA

A região industrial de São José dos Campos, localizada no estado de São Paulo, foi escolhida como o local de origem da Eco Cleaning. Com uma infraestrutura industrial bem desenvolvida e acesso a recursos naturais, essa região proporcionou o ambiente ideal para os fundadores da empresa começarem a desenvolver suas fórmulas exclusivas de produtos de limpeza. Suas filiais estão situadas nas cidades de Sorocaba-SP, Piracicaba-SP e Campinas-SP.

## 3 DIFICULDADES ENFRENTADAS

Atualmente a empresa encontra problemas relacionados à:

Gestão financeira: problemas com fluxo de caixa irregular devido à sazonalidade nas vendas e dificuldade em manter o controle de custos devido aos custos mais elevados de produção de produtos ecológicos.

Expansão das vendas de produtos online: dificuldades em alcançar e converter o público-alvo online devido à competição e à necessidade de estratégias eficazes de marketing digital.

Logística e distribuição: desenvolver uma estratégia eficiente de logística para garantir o transporte de matérias-primas da região industrial para as filiais e distribuição dos produtos acabados.

Comunicação e coordenação: implementar tecnologias de comunicação eficazes para garantir uma comunicação regular entre a matriz, filiais e escritórios.

## 4 SERVIÇOS OFERECIDOS

Servidor web: para garantir que os funcionários da empresa tenham acesso controlado e centralizado a banco de dados, permitindo acesso a aplicações e serviços hospedados através da internet.

Servidor DHCP: distribuir endereços IP's e permitir a configuração a máscara de sub-rede, o gateway padrão e as informações do servidor DNS no adaptador de rede.

Servidor de e-mail: gerenciamento de mensagens eletrônicas de modo a garantir que os e-mails enviados cheguem aos destinatários de maneira segura.

Dispositivos de Rede: Utilize dispositivos como switches, roteadores e firewalls para criar uma rede local (LAN) em cada localidade da empresa, incluindo o escritório central na região metropolitana, a matriz na região industrial e as filiais distantes.

Servidor de rede sem fio (Wi-Fi): implementação de pontos de acesso Wi-Fi em cada local para fornecer conectividade sem fio aos dispositivos dos funcionários e visitantes. Configuração de segurança adequada, como autenticação WPA2, para proteger a rede sem fio contra acessos não autorizados.

Conexões WAN: Configure conexões de rede ampla (WAN) entre os diferentes locais da empresa para permitir a comunicação e o compartilhamento de recursos entre eles.

## 5 TOPOLOGIA

A topologia utilizada na infraestrutura de rede foi de barramento visando a implementação de uma rede mais econômica do que outras topologias, como estrela ou malha. Isso é importante para uma empresa com várias filiais, onde os custos de infraestrutura podem se acumular rapidamente. Além disso, um barramento oferece flexibilidade e escalabilidade para expandir a rede. Adicionar novos dispositivos é relativamente fácil, pois eles podem ser conectados diretamente ao barramento existente. Com um barramento, a configuração da rede é simplificada, reduzindo a sobrecarga administrativa e facilita a manutenção da rede. Também é possível destacar a redução de latência em comparação com outras topologias de rede, como malha, isso deve-se ao fato de todos os dispositivos compartilharem o mesmo canal de comunicação. Diante disso, o uso de um barramento na infraestrutura de redes de uma empresa de manufatura com várias filiais pode oferecer vantagens significativas em termos de simplici-

dade, custo, flexibilidade e desempenho, tornando-o uma escolha atraente para esse ambiente específico.

## 6 FAIXA DE IPS, MÁSCARAS E CLASSE

**Figura 1 – Matriz: faixa de IPs, máscaras e classe**

Matriz	Faixa de IPs	Máscara de sub-rede	Lan	Classe
Router Matriz	192.168.0.1/24	255.255.255.0		C
Router Wireless (0)				C
Router Guest Campinas	192.168.0.1/24	255.255.255.0	172.168.0.1/24	C
Pc0	192.168.0.12/24	255.255.255.0		C
Pc4	192.168.0.11/24	255.255.255.0		C
Pc1	192.168.0.10/24	255.255.255.0		C
Laptop 0	192.168.0.15/24	255.255.255.0		C
Laptop 1	192.168.0.13/24	255.255.255.0		C
Servidor DNS	192.168.0.4/24	255.255.255.0		C
Servidor FTP	192.168.0.8/24	255.255.255.0		C
Servidor WEB	192.168.0.7/24	255.255.255.0		C
Servidor Email	192.168.0.3/24	255.255.255.0		C
Servidor DHCP 4	192.168.0.2/24	255.255.255.0		C
Smartphone 0	192.168.0.14/24	255.255.255.0		C
Rede cliente Vlan (10)				
Smartphone 4(3)(6)	172.168.0.103/24	255.255.255.0		B
Smartphone 4(3)(5)	172.168.0.105/24	255.255.255.0		B
Smartphone 4(3)(4)	172.168.0.104/24	255.255.255.0		B
Smartphone 4(3)(3)	172.168.0.106/24	255.255.255.0		B
Smartphone 4(3)(1)	172.168.0.107/24	255.255.255.0		B
Smartphone 4(3)	172.168.0.101/24	255.255.255.0		B

Fonte: Projeto Packet Tracer

**Figura 2 – Filial Campinas: faixa de IPs, máscaras e classe**

Filial Campinas	Faixa de IPs	Máscara de sub-rede	Lan	Classe
Router Campinas	192.168.1.1/24	255.255.255.0		C
Router Wireless (5)	192.168.1.1/24	255.255.255.0		C
Router Guest Campinas	192.168.1.1/24	255.255.255.0	172.168.1.1/24	C
Pc2	192.168.1.14/24	255.255.255.0		C
Pc7(1)	192.168.1.12/24	255.255.255.0		C
Pc7	192.168.1.14/24	255.255.255.0		C
Pc7(4)		255.255.255.0		C
Pc7(7)	192.168.1.10/24	255.255.255.0		C
Pc7(6)	192.168.1.12/24	255.255.255.0		C
Laptop 2(1)	192.168.1.21/24	255.255.255.0		C
Laptop 2(3)	192.168.1.17/24	255.255.0.0		A
Laptop 2(2)	192.168.1.18/24	255.255.255.0		C
Laptop 2(3)	192.168.1.17/24	255.255.0.0		A
Servidor DHCP 2	192.168.1.5/24	255.255.255.0		C
Smartphone 1(3)	192.168.1.15/24	255.255.255.0		C
Smartphone 1(4)	192.168.1.19/24	255.255.255.0		C
Smartphone 1(2)	192.168.1.20/24	255.255.255.0		C
Smartphone 1(1)	192.168.1.16/24	255.255.255.0		C
Rede cliente Vlan (10)				
Smartphone 4(2)(3)(2)	172.168.1.100/24	255.255.255.0		B
Smartphone 4(2)(3)(1)	172.168.1.105/24	255.255.255.0		B
Smartphone 4(2)(3)	172.168.1.104/24	255.255.255.0		B
Smartphone 4(2)(2)	172.168.1.107/24	255.255.255.0		B
Smartphone 4(2)(1)	172.168.1.101/24	255.255.255.0		B
Smartphone 4(2)(2)	172.168.1.106/24	255.255.255.0		B

Fonte: Projeto Packet Tracer

**Figura 3 – Filial Piracicaba: faixa de IPs, máscaras e classe**

Filial Piracicaba	Faixa de IPs	Máscara de sub-rede	Lan	Classe
Router 0	192.168.3.1/24	255.255.255.0		C
Router (1)	192.168.3.1/24	255.255.255.0		C
Router Guest Piracicaba	192.168.3.1/24	255.255.255.0	172.168.3.1/24	C
Pc5	192.168.3.153/24	255.255.255.0		C
Pc5(1)	192.168.3.150/24	255.255.255.0		C
Pc6(3)	192.168.3.156/24	255.255.255.0		C
Pc8	192.168.3.152/24	255.255.255.0		C
Pc6(0)	192.168.3.155/24	255.255.255.0		C
Pc6(1)	192.168.3.154/24	255.255.255.0		C
Pc6(2)	192.168.3.151/24	255.255.255.0		C
Servidor DHCP	192.168.3.2/24	255.255.255.0		C
Laptop 4	169.254.13.172/16	255.255.0.0		A
Laptop 4(1)	192.168.3.158/24	255.255.255.0		C
Smartphone 1(5)	192.168.3.159/24	255.255.255.0		C
Smartphone 4	192.168.3.106/24	255.255.255.0		C
Smartphone 4(5)	192.168.3.104/24	255.255.255.0		C
Rede cliente Vlan (10)				
Smartphone 4(6)	172.168.3.101/24	255.255.255.0		B
Smartphone 4(7)	172.168.3.100/24	255.255.255.0		B
Smartphone 4(8)	172.168.3.107/24	255.255.255.0		B
Smartphone 4(9)	172.168.3.103/24	255.255.255.0		B

Fonte: Projeto Packet Tracer

**Figura 4 – Filial Sorocaba: faixa de IPs, máscaras e classe**

Filial Sorocaba	Faixa de IPs	Máscara de sub-rede	Lan	Classe
Router FilialSorocaba	192.168.2.1/24	255.255.255.0		C
Router Wireless8 (1)	192.168.2.1/24	255.255.255.0		C
Router Guest Sorocaba	192.168.0.1/24	255.255.255.0	172.168.2.1/24	C
Pc3	192.168.2.11/24	255.255.255.0		C
Pc7(2)	192.168.2.105/24	255.255.255.0		C
Pc7(3)	192.168.2.104/24	255.255.255.0		C
Pc7(3)(2)	192.168.2.10/24	255.255.255.0		C
Pc7(3)(4)	192.168.2.104/24	255.255.255.0		C
Pc7(3)(3)	192.168.2.104/24	255.255.255.0		C
Laptop 3	192.168.2.100/24	255.255.255.0		C
Smartphone 2	192.168.2.6/24	255.255.255.0		C
Rede cliente Vlan (10)				
Smartphone 4(1)(6)	172.168.2.107/24	255.255.255.0		B
Smartphone 4(1)(5)	172.168.2.102/24	255.255.255.0		B
Smartphone 4(1)(4)	172.168.2.109/24	255.255.255.0		B
Smartphone 4(1)(3)	172.168.2.100/24	255.255.255.0		B
Smartphone 4(1)(2)	172.168.2.105/24	255.255.255.0		B
Smartphone 4(1)(1)	172.168.2.103/24	255.255.255.0		B
Smartphone 4(1)	172.168.2.110/24	255.255.255.0		B

Fonte: Projeto Packet Tracer

## 6.1 Detalhamento

Os endereços IPs são divididos em diferentes classes, que determinam a faixa de endereços disponíveis e o número de hosts que podem ser conectados a ela. No entanto, o conceito de classes de IP foi substituído pelo CIDR (Classless Inter-Domain Routing), que oferece uma abordagem mais flexível para a alocação de endereços IP.

Os endereços IPs eram divididos em cinco classes: A, B, C, D e E. Cada classe tinha um intervalo específico de endereços que podiam ser atribuídos a dispositivos em uma rede. Aqui está uma definição de cada classe:

Classe A: Os endereços da Classe A são usados para grandes redes, pois oferecem um grande número de hosts (dispositivos) em cada rede. O primeiro octeto é reservado para a rede,

enquanto os três octetos restantes são usados para identificar dispositivos na rede. O intervalo de endereços vai de 0.0.0.0 a 127.255.255.255.

Classe B: Os endereços da Classe B são usados para redes de tamanho médio. Os dois primeiros octetos são usados para a rede, enquanto os dois últimos octetos são usados para identificar dispositivos na rede. O intervalo de endereços vai de 128.0.0.0 a 191.255.255.255.

Classe C: Os endereços da Classe C são usados para pequenas redes. Os três primeiros octetos são usados para a rede, enquanto o último octeto é usado para identificar dispositivos na rede. O intervalo de endereços vai de 192.0.0.0 a 223.255.255.255.

Classe D: Os endereços da Classe D são reservados para multicast, o que significa que são usados para enviar dados para vários destinos simultaneamente. O intervalo de endereços vai de 224.0.0.0 a 239.255.255.255.

Classe E: Os endereços da Classe E são reservados para fins experimentais e não são usados para endereçamento de rede convencional. O intervalo de endereços vai de 240.0.0.0 a 255.255.255.255.

É importante observar que, com a adoção do CIDR (Classless Inter-Domain Routing), as classes de endereço IP deixaram de ser utilizadas para designar endereços IP e agora os endereços IP são atribuídos em blocos variáveis, independentemente da classe.

## 7 SERVIDORES, IPS E ACESSOS

O servidor de banco de dados pode ser acessado através do IP: database-2.cizqrdrzigan.us-east-1.rds.amazonaws.com, User: admin e Senha: 161001dpc. Os demais servidores estão descritos na tabela abaixo.

Servidores, IP's e acessos			
Servidor	IP	User	Senha
DNS	52.70.56.86		
AD	34.193.37.162	Administrator	EgqT1-ZHSS5MEJcQZ-pUEu8eLzNB@I=
Web/Aplicação	34.195.180.39		
FTP	54.145.246.175	aluno	aluno

**Fonte: Produto dos artefatos**

## 8 AMBIENTE DE IMPLANTAÇÃO DOS SERVIÇOS

## 8.1 Serviços On-premises

### 8.1.1 DHCP

## 8.2 Serviços na Nuvem

### 8.2.1 DNS

O serviço de DNS foi instalado na AWS em uma máquina EC2 utilizando o AdGuard Home e fazendo sua configuração por meio de sua interface web. Na máquina EC2 foi configurado no security group a liberação das portas 53(DNS), 80(WEB), 22(SSH) para possibilitar a configuração do servidor tanto via linha de comando quanto via interface web e também para permitir o uso do DNS por outras máquinas. O servidor DNS fica disponível no IP público 52.70.56.86.

Foi configurado no DNS para usar os servidores primários 8.8.8.8 e 1.1.1.1, os servidores de DNS públicos da Google e da CloudFlare, respectivamente.

**Figura 5 – Configuração dos servidores primários de DNS**

The screenshot shows the 'Configurações de DNS' (DNS Settings) page. At the top, there's a header with the AdGuard Home logo, a 'Ligado' (On) status indicator, and navigation links for Painel, Configurações (selected), Filtros, Registro de consultas, Guia de configuração, and Encerrar sessão (Logout). Below the header, the main section is titled 'Servidores DNS primário' (Primary DNS Servers). It contains a text input field with two entries: '8.8.8.8' and '1.1.1.1'. A note above the input field says: 'Insira o endereço de servidor, um por linha. [Saber mais](#) sobre a configuração de servidores DNS primários. Aqui está uma [lista de provedores de DNS conhecidos](#) para escolher.' (Insert the server address, one per line. [Learn more](#) about configuring primary DNS servers. Here is a [list of known DNS providers](#) to choose from.) Below the input field, there are three radio button options under the heading 'Balanceamento de carga' (Load balancing):

- Balanceamento de carga (Load balancing)  
Consulte um servidor DNS primário por vez. O AdGuard Home usa seu algoritmo aleatório ponderado para escolher o servidor para que o servidor mais rápido seja usado com mais frequência.
- Solicitações paralelas (Parallel requests)  
Usar consultas paralelas para acelerar a resolução consultando simultaneamente todos os servidores DNS primário
- Endereço de IP mais rápido (Fastest IP address)  
Consulta todos os servidores DNS e retorna o endereço IP mais rápido entre todas as respostas. Isso torna as consultas DNS mais lentas, pois o AdGuard Home tem que esperar pelas respostas de todos os servidores DNS, mas melhora a conectividade geral.

**Fonte: Servidor DNS na nuvem**

Também foi configurada uma reescrita de DNS para que o domínio *ecocleaning.puc.com* responda com o IP 34.195.180.39, que está atrelado ao servidor Web.

**Figura 6 – Configuração da reescrita de DNS**

The screenshot shows the AdGuard DNS configuration interface. At the top, there are tabs for 'Painel', 'Configurações', 'Filtros', 'Registro de consultas', 'Guia de configuração', and 'Encerrar sessão'. Below the tabs, the title 'Reescritas de DNS' is displayed, with the subtitle 'Permite configurar uma resposta personalizada do DNS para um nome de domínio específico.' A table lists a single rewrite rule:

Domínio	Resposta	Ações
ecocleaning.puc.com	34.195.180.39	

At the bottom of the interface, there are navigation buttons for 'Anterior', 'Próximo', 'Página 1 / 1', and a dropdown for '10 linhas'. A green button labeled 'Adicionar reescrita de DNS' is located at the bottom left.

**Fonte: Servidor DNS na nuvem**

### **8.2.1.1 Teste do servidor**

Para testar o DNS, foi criada uma segunda máquina EC2, com Debian e o systemd foi configurado para utilizar o DNS do AdGuard.

**Figura 7 – Configuração da máquina para teste de DNS**

The screenshot shows a terminal window with the command 'cat /etc/resolved.conf' running. The output displays the contents of the /etc/resolved.conf file, which includes comments about compile-time defaults, a [Resolve] section with various DNS server configurations, and a [Resolve] section with specific examples for Cloudflare, Google, and Quad9. The file also includes sections for FallbackDNS, Domains, and various DNS-related flags like DNSSEC, DNSOverTLS, and MulticastDNS.

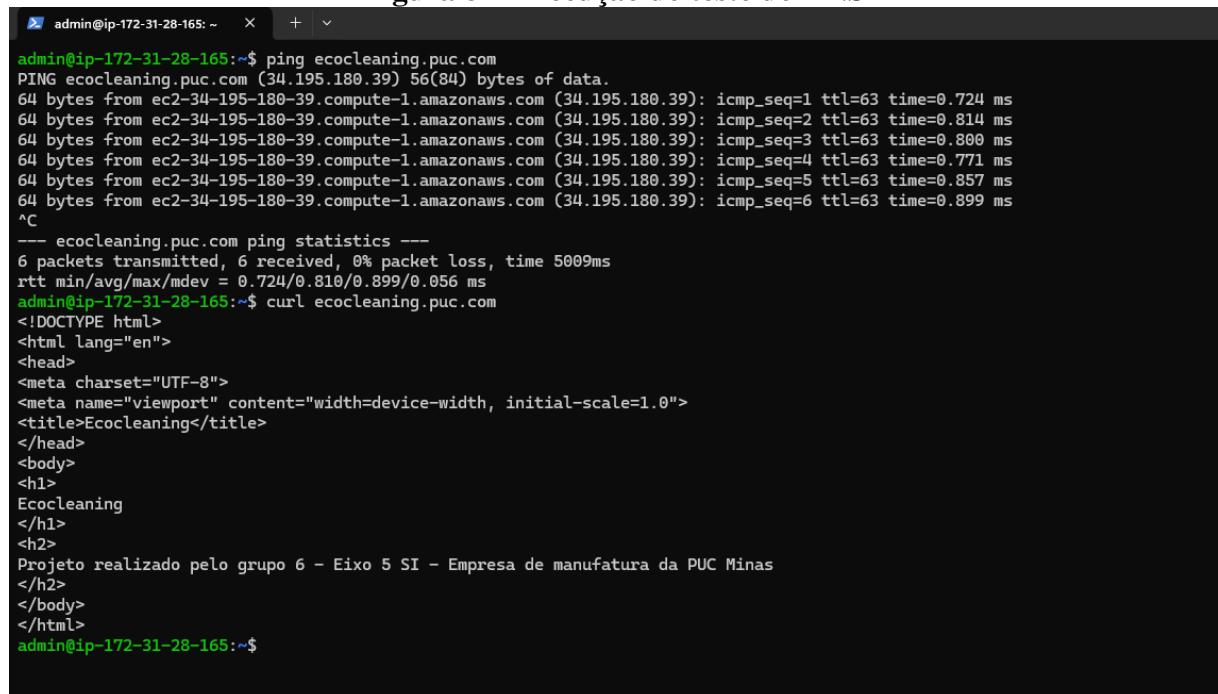
```
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the resolved.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# Use 'systemd-analyze cat-config systemd/resolved.conf' to display the full config.
#
# See resolved.conf(5) for details.

[Resolve]
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1001#cloudflare-dns.com
# Google: 8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:4860:4860::8844#dns.google
# Quad9: 9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.net 2620:fe::9#dns.quad9.net
DNS=52.70.56.86
FallbackDNS=1.1.1.1
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=yes
#LLMNR=yes
#Cache=yes
#CacheFromlocalhost=no
#DNSStubListener=yes
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
admin@ip-172-31-28-165:/$ |
```

**Fonte: Servidor para teste de DNS na nuvem**

A partir desse servidor criado para teste, podemos ver que ao pingar o domínio *ecocleaning.puc.com*, o ping tenta atingir o IP do servidor web, exatamente de acordo com o que foi configurado na reescrita de DNS. Também é interessante notar que ao utilizar um curl no domínio, o retorno é o HTML configurado para ser exibido no servidor web. Esses testes demonstram como o serviço de DNS está configurado e que está funcionando corretamente.

**Figura 8 – Execução do teste do DNS**



```
admin@ip-172-31-28-165:~$ ping ecocleaning.puc.com
PING ecocleaning.puc.com (34.195.180.39) 56(84) bytes of data.
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=1 ttl=63 time=0.724 ms
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=2 ttl=63 time=0.814 ms
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=3 ttl=63 time=0.800 ms
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=4 ttl=63 time=0.771 ms
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=5 ttl=63 time=0.857 ms
64 bytes from ec2-34-195-180-39.compute-1.amazonaws.com (34.195.180.39): icmp_seq=6 ttl=63 time=0.899 ms
^C
--- ecocleaning.puc.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 0.724/0.810/0.899/0.056 ms
admin@ip-172-31-28-165:~$ curl ecocleaning.puc.com
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>EcoCleaning</title>
</head>
<body>
<h1>
EcoCleaning
</h1>
<h2>
Projeto realizado pelo grupo 6 - Eixo 5 SI - Empresa de manufatura da PUC Minas
</h2>
</body>
</html>
admin@ip-172-31-28-165:~$
```

**Fonte:** Servidor para teste de DNS na nuvem

### 8.2.2 *FTP*

### 8.2.3 *Web/Aplicação*

Foi levantada uma maquina EC2 na AWS e instalado o servidor Apache para lidar com requisições HTTP. Na mesma máquina, também foi instalado o PHP para desenvolver a aplicação que roda no servidor. Há um pequeno exemplo do servidor Apache funcionando no arquivo */var/www/html/index.php* que substitui o HTML padrão do Apache e mostra um HTML personalizado com informações da EcoCleaning.

**Figura 9 – Página principal no servidor web**



**Fonte:** Servidor Web na nuvem

Acessando a rota */produtos.php* do servidor é possível ver a aplicação PHP em pleno

funcionamento. A aplicação estabelece uma conexão com o banco de dados MySQL, rodando em um servidor separado de banco de dados e dinamicamente carrega dados de uma tabela de produtos no banco de dados na tabela do HTML apresentado ao usuário.

**Figura 10 – Página de produtos no servidor web**

A screenshot of a web browser window displaying a table of products. The title bar shows the URL as 34.195.180.39/products.php. The page header says "EcoCleaning Company" and "Products". The table has columns for Name, Description, Price, and Stock Quantity. The data includes:

Name	Description	Price	Stock Quantity
Multi-Surface Cleaner	Effective cleaner for multiple surfaces.	R\$9.99	100
Bathroom Cleaner	Specialized cleaner for bathroom surfaces.	R\$7.49	75
Glass Cleaner	Streak-free cleaner for glass surfaces.	R\$5.99	50
Floor Cleaner	Cleans and refreshes all types of floors.	R\$12.99	80
Dishwashing Liquid	Powerful dish soap for sparkling clean dishes.	R\$3.99	120

**Fonte: Servidor Web na nuvem**

### 8.2.4 SMTP

## 9 GERÊNCIA DE REDES DE COMPUTADORES

### 9.1 Monitoramento do ambiente na nuvem

Para monitorar o ambiente na nuvem, foi implementado um servidor Zabbix centralizado para monitoramento. Em cada máquina monitorada, o Zabbix Agent foi instalado para estabelecer comunicação com o servidor de monitoramento. No entanto, o servidor de banco de dados é uma exceção, pois, ao utilizar o AWS RDS, possui monitoramentos nativos da infraestrutura fornecidos pela AWS.

**Figura 11 – Servidores monitorados via Zabbix na nuvem**

A screenshot of the Zabbix interface showing a list of monitored servers. The columns include Name, Interface, Availability, Tags, Status, Latest data, Problems, Graphs, Dashboards, and Web. The data includes:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
AdServer	34.193.37.162:10050	ZBX	class:os target:windows	Enabled	Latest data 111	1	Graphs 11	Dashboards 2	Web
dns-Server	52.70.56.86:10050	ZBX	class:os target:linux	Enabled	Latest data 67	Problems	Graphs 13	Dashboards 2	Web
FtpServer	54.145.248.175:10050	ZBX	class:os target:linux	Enabled	Latest data 67	1	Graphs 13	Dashboards 2	Web
smtp_server	34.193.218.191:10050	ZBX	class:os target:linux	Enabled	Latest data 67	1	Graphs 13	Dashboards 2	Web
webserver	34.195.180.39:10050	ZBX	class:os target:linux	Enabled	Latest data 67	1	Graphs 13	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class:os class:software target:linux ...	Enabled	Latest data 128	Problems	Graphs 24	Dashboards 4	Web

Displaying 6 of 6 found

**Fonte: Monitoramento Zabbix**

### 9.1.1 Métricas monitoradas

Para cada servidor foi utilizado o template padrão do Zabbix de acordo com o sistema operacional da máquina.

### **9.1.1.1 Uso de espaço em disco**

Essa métrica representa a porção do disco rígido que está ocupada em relação ao espaço total.

**Figura 12 – Servidor DNS: Uso de espaço em disco**



**Fonte: Monitoramento Zabbix**

**Figura 13 – Servidor AD: Uso de espaço em disco**



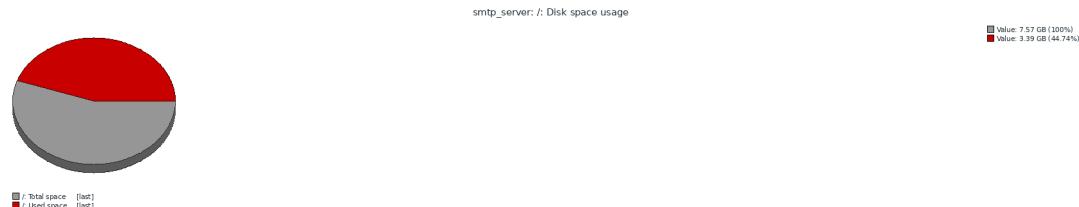
**Fonte: Monitoramento Zabbix**

**Figura 14 – Servidor FTP: Uso de espaço em disco**



**Fonte: Monitoramento Zabbix**

**Figura 15 – Servidor SMTP: Uso de espaço em disco**



Fonte: Monitoramento Zabbix

**Figura 16 – Servidor Web/Aplicação: Uso de espaço em disco**

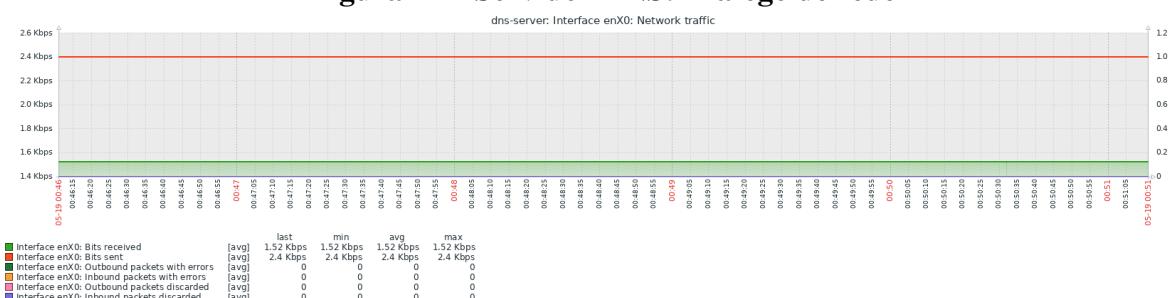


Fonte: Monitoramento Zabbix

### 9.1.1.2 Tráfego de rede

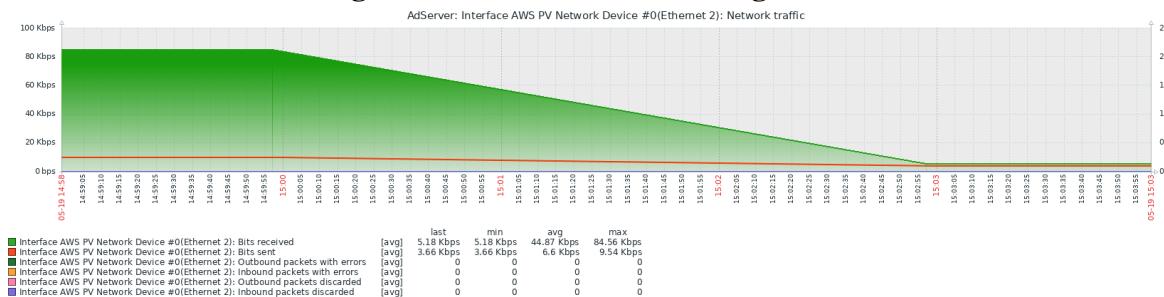
Essa métrica apresenta a quantidade de bits enviados/recebidos na rede. Também traz informações sobre a quantidade de pacotes descartados ou com erros.

**Figura 17 – Servidor DNS: Tráfego de rede**



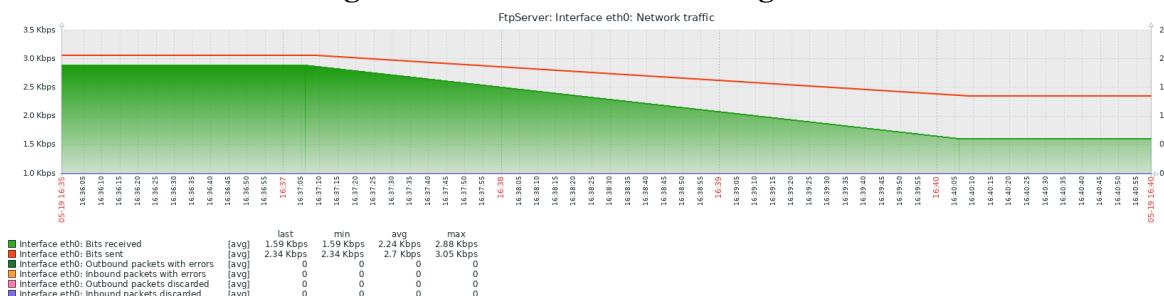
Fonte: Monitoramento Zabbix

**Figura 18 – Servidor AD: Tráfego de rede**



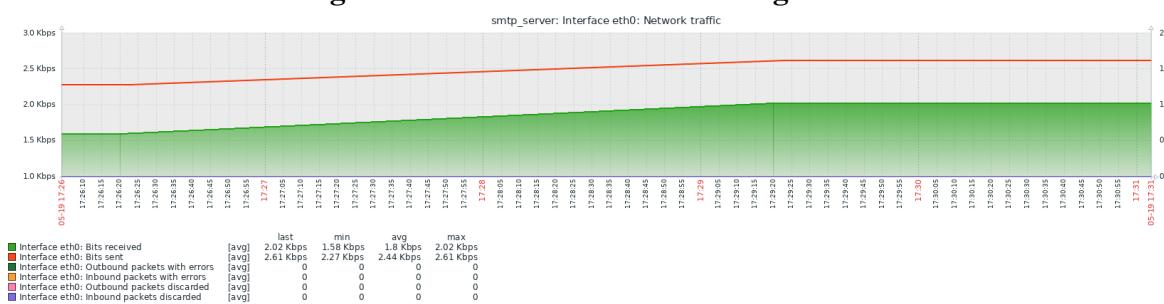
Fonte: Monitoramento Zabbix

**Figura 19 – Servidor FTP: Tráfego de rede**



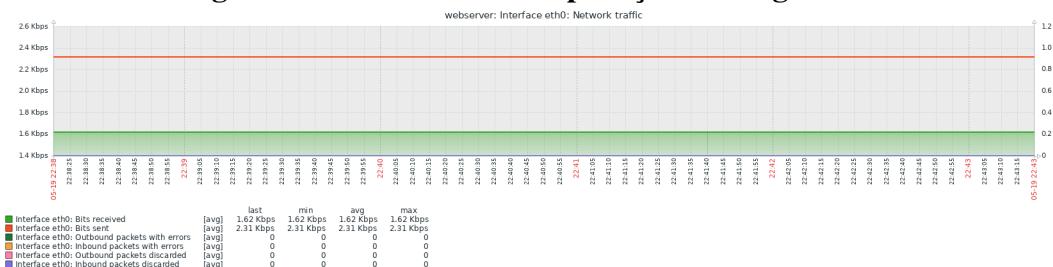
Fonte: Monitoramento Zabbix

**Figura 20 – Servidor SMTP: Tráfego de rede**



Fonte: Monitoramento Zabbix

**Figura 21 – Servidor Web/Aplicação: Tráfego de rede**

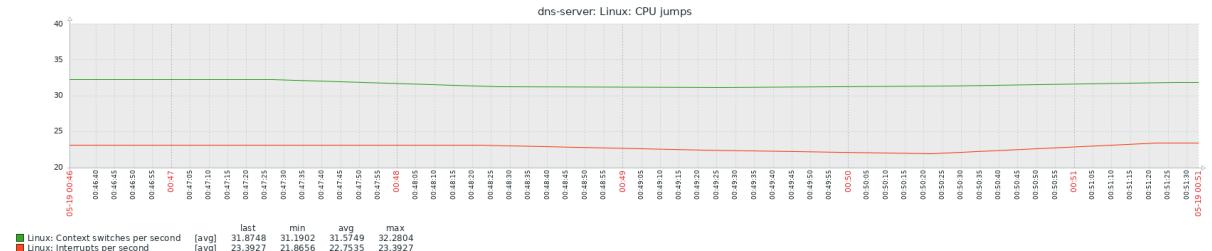


Fonte: Monitoramento Zabbix

### 9.1.1.3 Picos de CPU

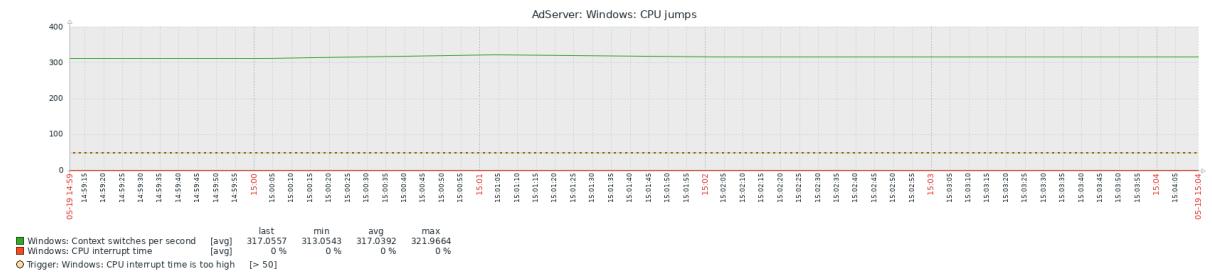
Essa métrica demonstra a quantidade de vezes que o sistema teve aumentos repentinos de processamento (ou picos) ao longo de um determinado período.

**Figura 22 – Servidor DNS: Picos de CPU**



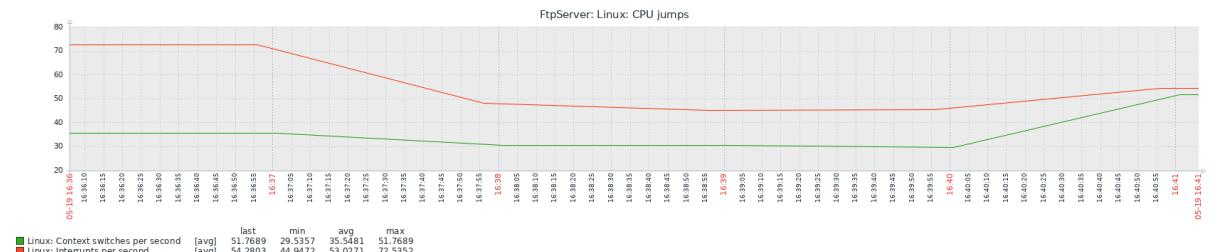
Fonte: Monitoramento Zabbix

**Figura 23 – Servidor AD: Picos de CPU**



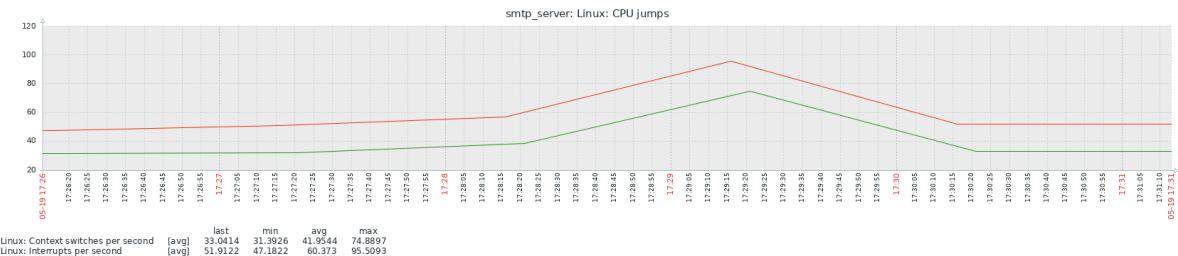
Fonte: Monitoramento Zabbix

**Figura 24 – Servidor FTP: Picos de CPU**



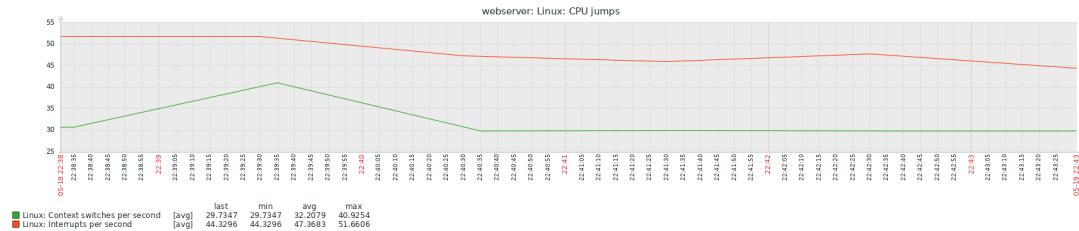
Fonte: Monitoramento Zabbix

**Figura 25 – Servidor SMTP: Picos de CPU**



Fonte: Monitoramento Zabbix

**Figura 26 – Servidor Web/Aplicação: Picos de CPU**

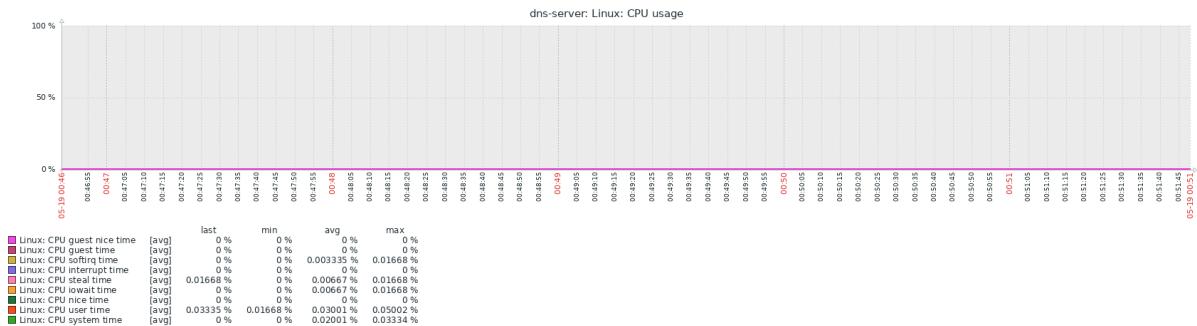


Fonte: Monitoramento Zabbix

#### 9.1.1.4 Uso de CPU

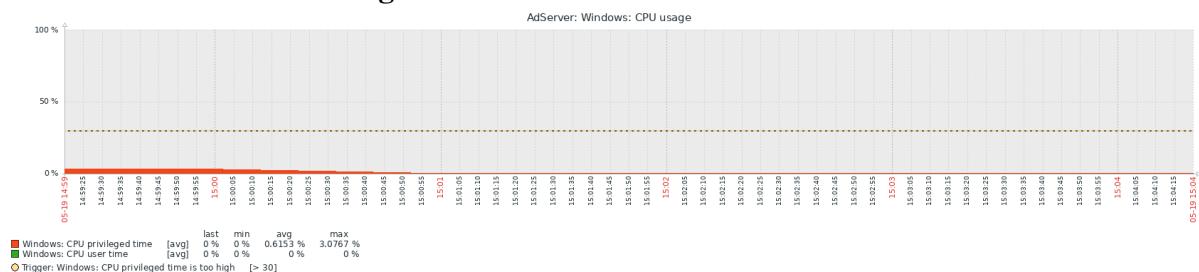
Essa métrica refere-se à quantidade de tempo que a CPU passa executando instruções de um processo.

**Figura 27 – Servidor DNS: Uso de CPU**



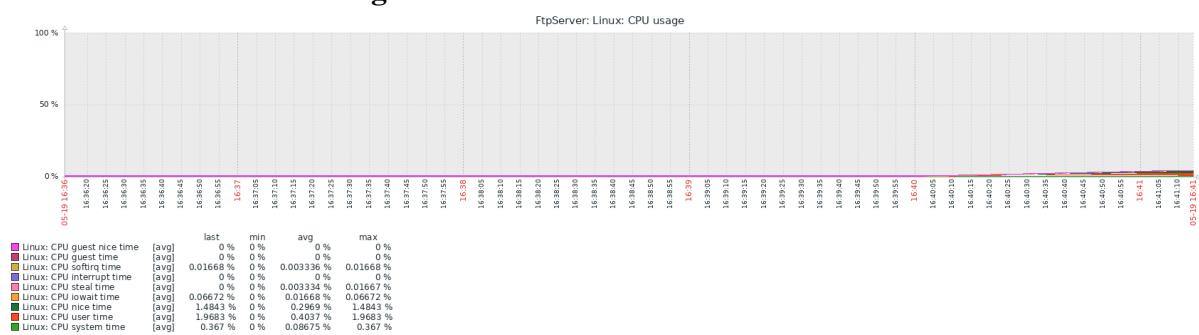
Fonte: Monitoramento Zabbix

**Figura 28 – Servidor AD: Uso de CPU**



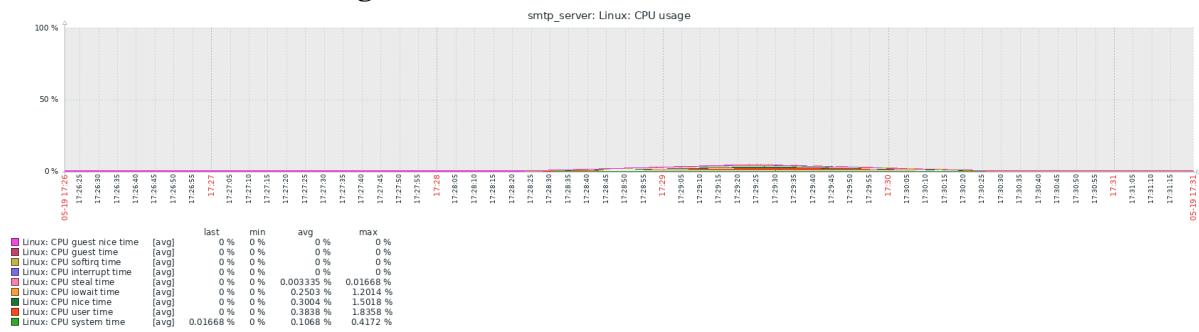
Fonte: Monitoramento Zabbix

**Figura 29 – Servidor FTP: Uso de CPU**



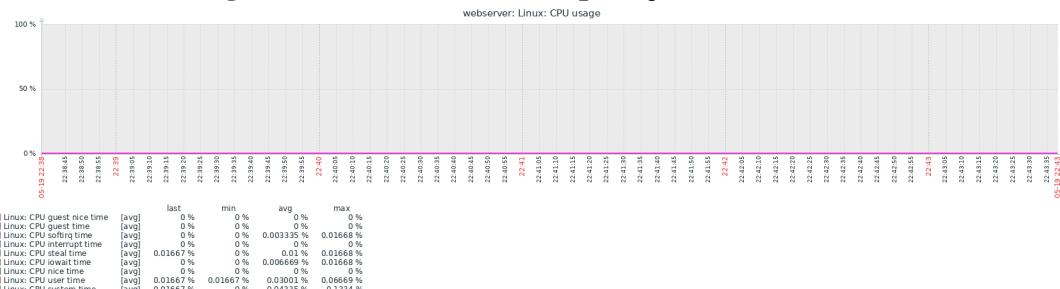
Fonte: Monitoramento Zabbix

**Figura 30 – Servidor SMTP: Uso de CPU**



Fonte: Monitoramento Zabbix

**Figura 31 – Servidor Web/Aplicação: Uso de CPU**

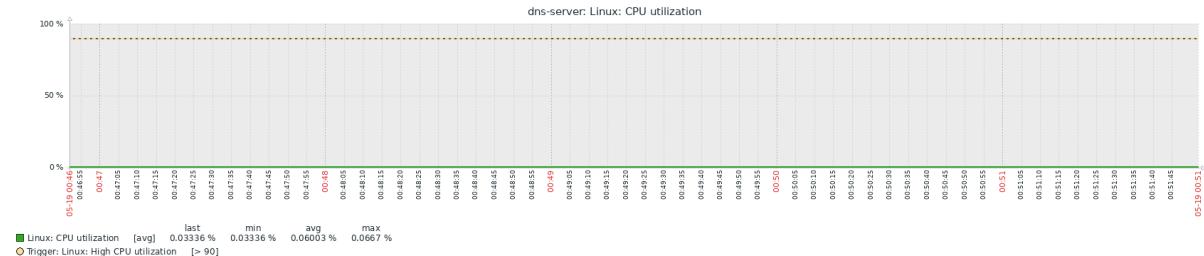


Fonte: Monitoramento Zabbix

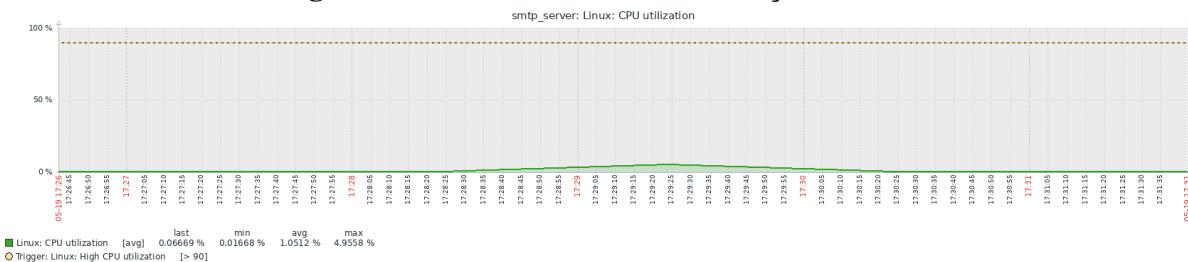
### **9.1.1.5 Utilização de CPU**

Essa métrica refere-se à carga total na CPU, incluindo todas as atividades de processamento do sistema, usuários e interrupções.

**Figura 32 – Servidor DNS: Utilização de CPU**

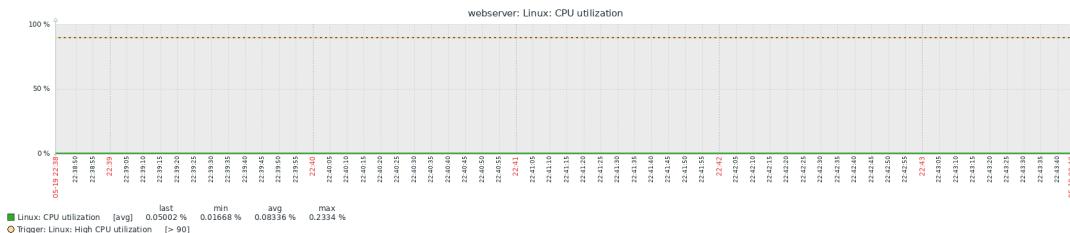


**Figura 35 – Servidor SMTP: Utilização de CPU**



**Fonte:** Monitoramento Zabbix

**Figura 36 – Servidor Web/Aplicação: Utilização de CPU**

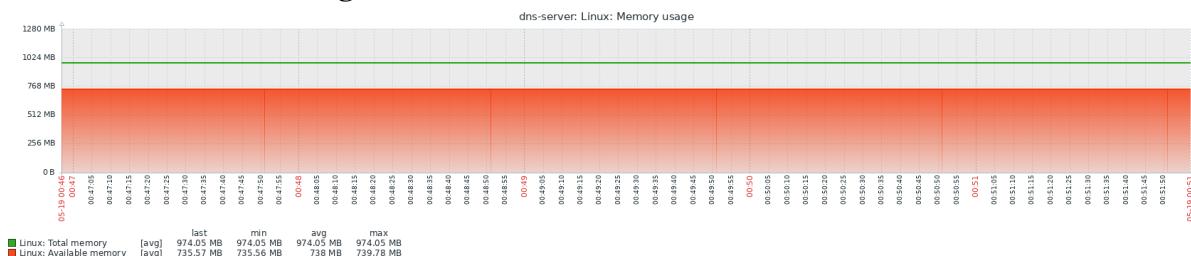


**Fonte:** Monitoramento Zabbix

### **9.1.1.6 Uso de memória**

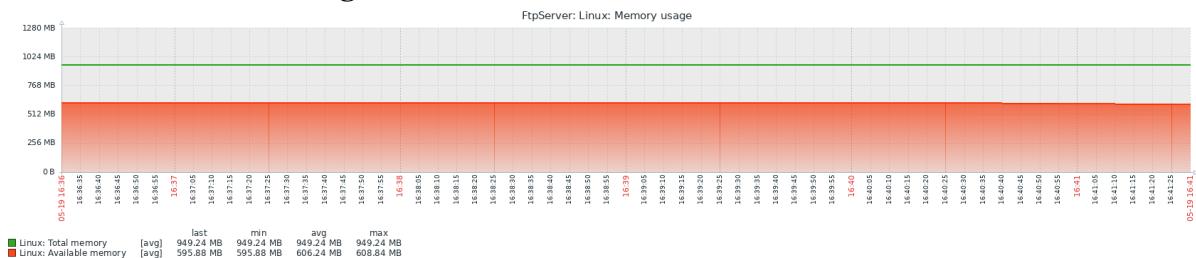
Essa métrica demonstra graficamente a quantidade disponível de memória RAM e a quantidade total de memória RAM do sistema.

**Figura 37 – Servidor DNS: Uso de memória**



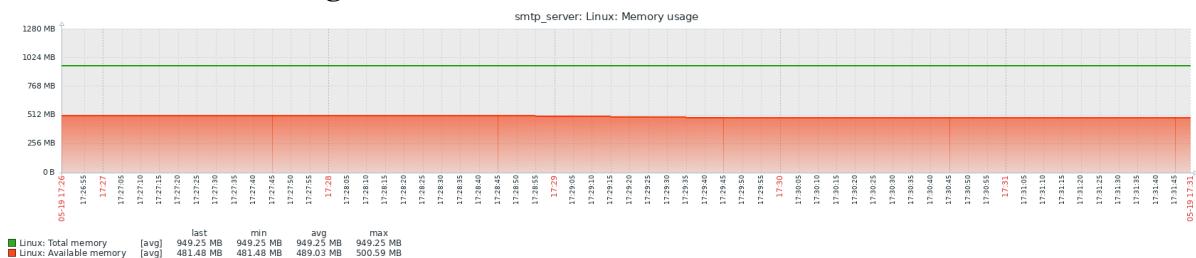
**Fonte:** Monitoramento Zabbix

**Figura 38 – Servidor FTP: Uso de memória**



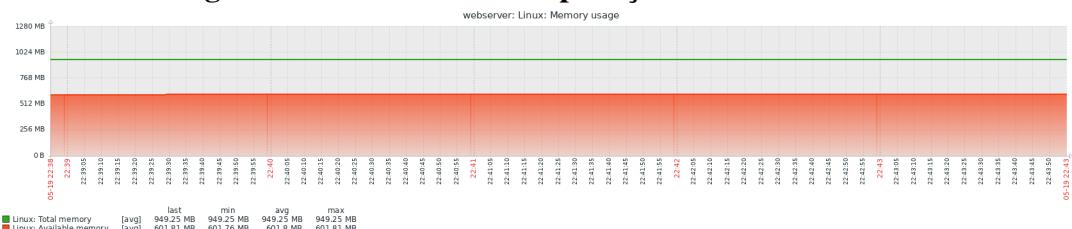
Fonte: Monitoramento Zabbix

**Figura 39 – Servidor SMTP: Uso de memória**



Fonte: Monitoramento Zabbix

**Figura 40 – Servidor Web/Aplicação: Uso de memória**

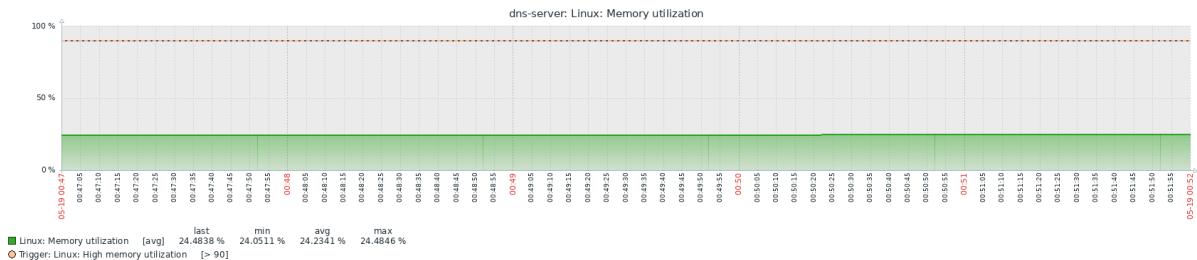


Fonte: Monitoramento Zabbix

### **9.1.1.7 Utilização de memória**

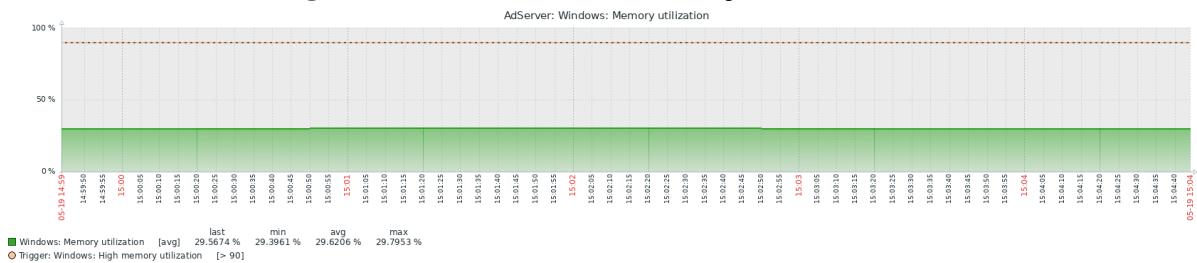
Essa métrica representa a porcentagem de uso de memória RAM do sistema ao longo de um determinado período. Também é demonstrado os números máximos, mínimos e a média desta porcentagem de uso.

**Figura 41 – Servidor DNS: Utilização de memória**



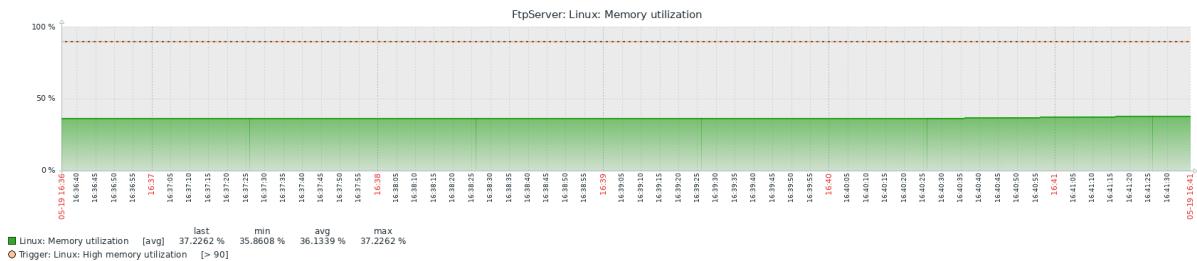
**Fonte: Monitoramento Zabbix**

**Figura 42 – Servidor AD: Utilização de memória**



**Fonte: Monitoramento Zabbix**

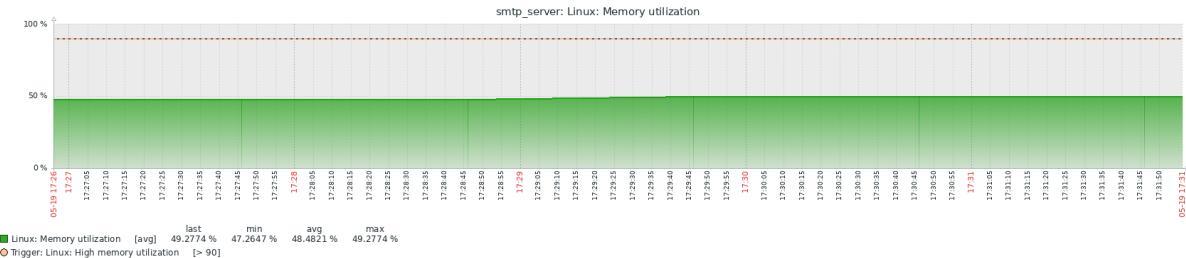
**Figura 43 – Servidor FTP: Utilização de memória**



**Fonte: Monitoramento Zabbix**

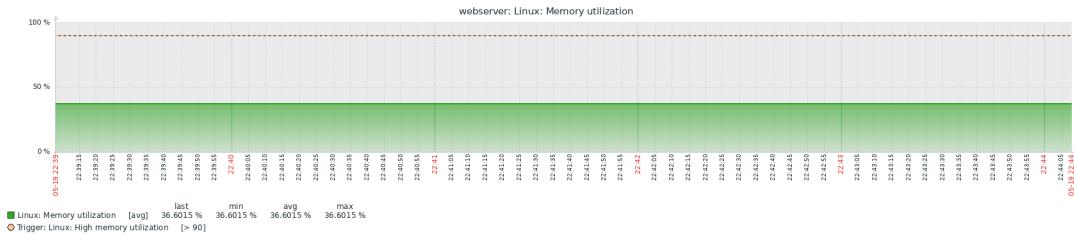
Empresa de manufatura com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km

**Figura 44 – Servidor SMTP: Utilização de memória**



**Fonte:** Monitoramento Zabbix

**Figura 45 – Servidor Web/Aplicação: Utilização de memória**

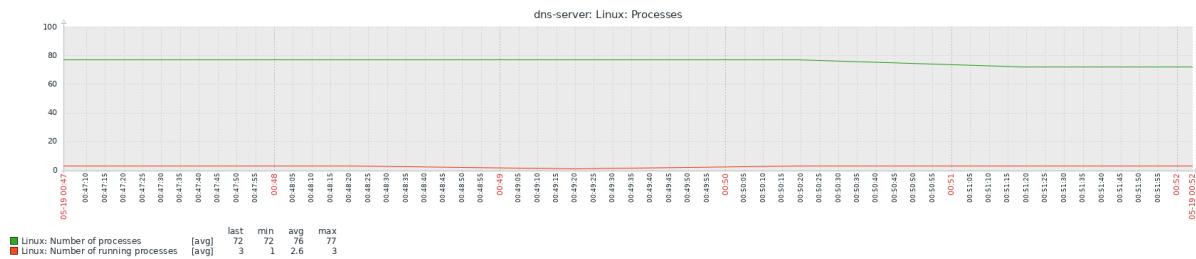


**Fonte:** Monitoramento Zabbix

### **9.1.1.8 Processos**

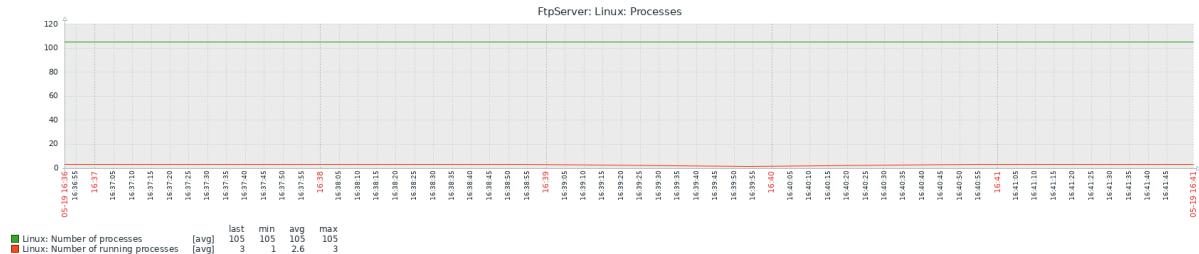
Esta métrica demonstra a quantidade de processos no sistema e a quantidade de processos em execução ao longo de um determinado período.

**Figura 46 – Servidor DNS: Processos**



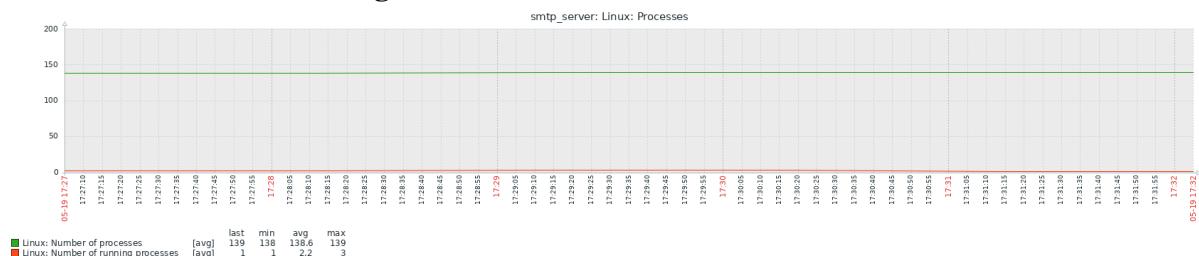
**Fonte:** Monitoramento Zabbix

**Figura 47 – Servidor FTP: Processos**



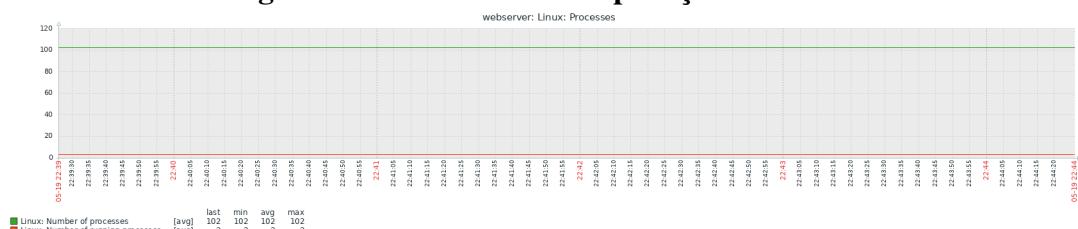
**Fonte:** Monitoramento Zabbix

**Figura 48 – Servidor SMTP: Processos**



Fonte: Monitoramento Zabbix

**Figura 49 – Servidor Web/Aplicação: Processos**

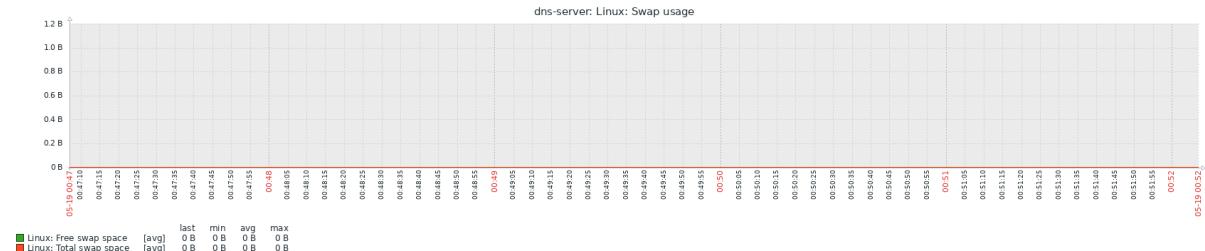


Fonte: Monitoramento Zabbix

### 9.1.1.9 Uso de memória swap

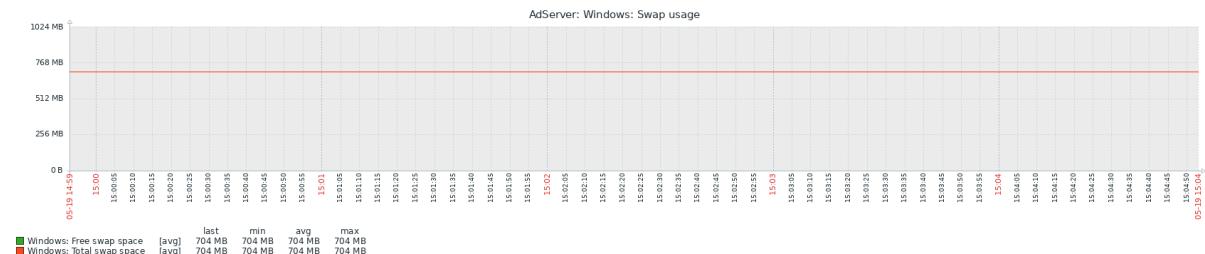
Esta métrica mostra a quantidade de espaço total para memória swap, além da quantidade disponível de memória para swap.

**Figura 50 – Servidor DNS: Uso de memória swap**



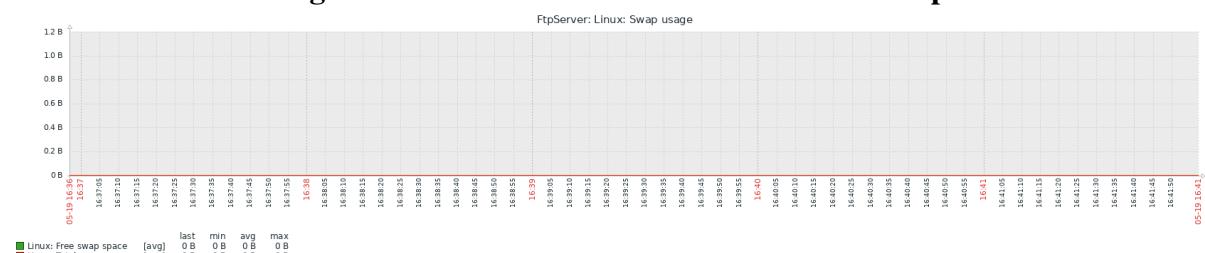
Fonte: Monitoramento Zabbix

**Figura 51 – Servidor AD: Uso de memória swap**



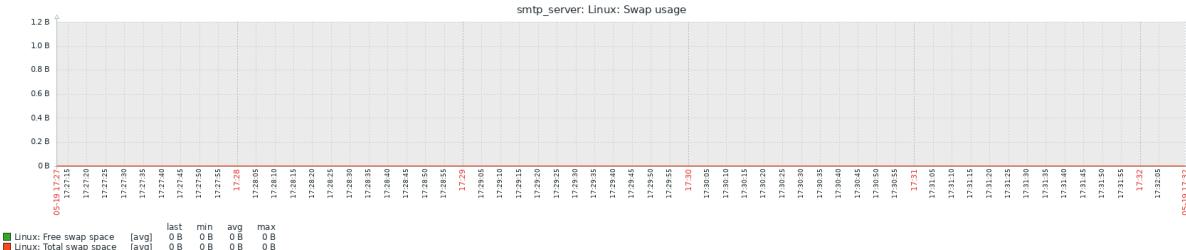
Fonte: Monitoramento Zabbix

**Figura 52 – Servidor FTP: Uso de memória swap**



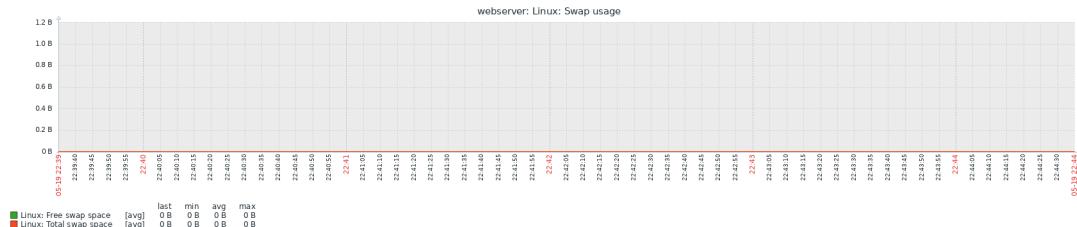
Fonte: Monitoramento Zabbix

**Figura 53 – Servidor SMTP: Uso de memória swap**



**Fonte:** Monitoramento Zabbix

**Figura 54 – Servidor Web/Aplicação: Uso de memória swap**

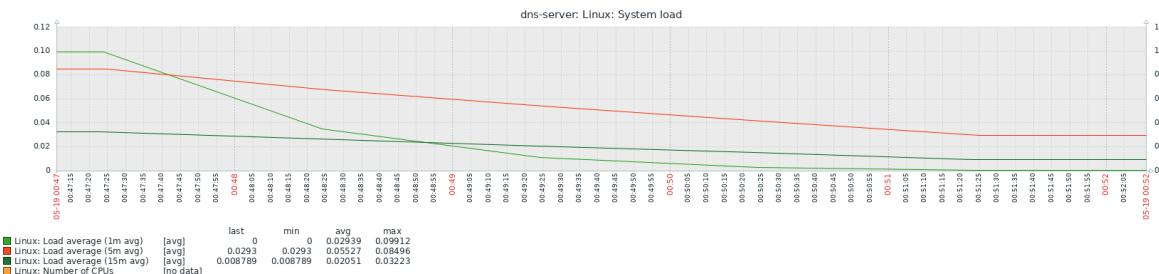


**Fonte:** Monitoramento Zabbix

#### **9.1.1.10 Carga do sistema**

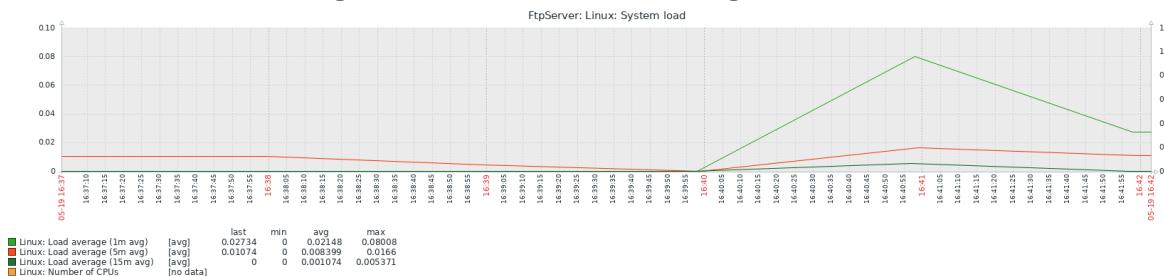
Esta métrica traz a quantidade de carga colocada sobre o sistema ao longo do tempo. Reflete o número de processos na fila de execução ou esperando disponibilidade de recursos de hardware.

**Figura 55 – Servidor DNS: Carga do sistema**



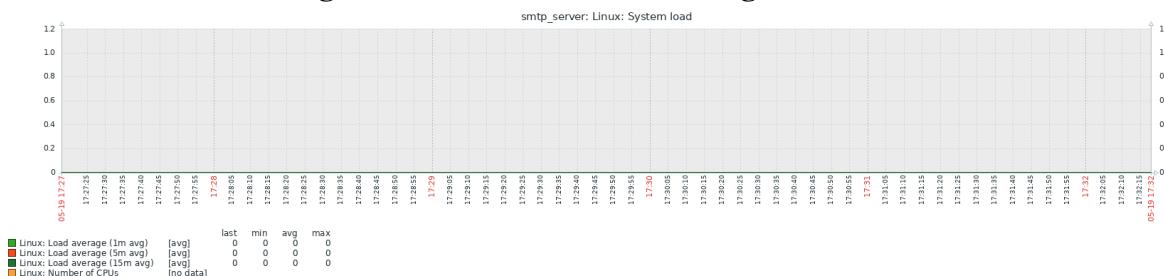
**Fonte:** Monitoramento Zabbix

**Figura 56 – Servidor FTP: Carga do sistema**



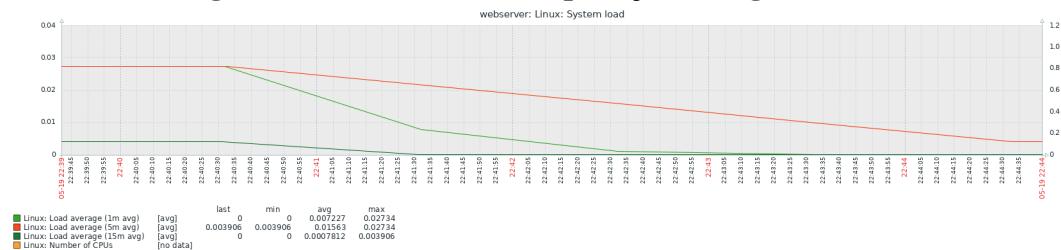
Fonte: Monitoramento Zabbix

**Figura 57 – Servidor SMTP: Carga do sistema**



Fonte: Monitoramento Zabbix

**Figura 58 – Servidor Web/Aplicação: Carga do sistema**



Fonte: Monitoramento Zabbix

## 9.2 Monitoramento do ambiente on-premises

Para monitorar o ambiente on-premises, também foi implementado um servidor Zabbix para gerenciar o monitoramento. Além do servidor Zabbix, também foi instalado o Agente Zabbix no servidor DHCP monitorado.

**Figura 59 – Servidores monitorados via Zabbix On-Premises**

Name ▲	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens	Web
dhcp-server	192.168.15.150:10050	ZBX SNMP [JMX: IPMI]			Enabled	Latest data	Problems	Graphs 6	Screens 2	Web
Zabbix server	127.0.0.1:10050	ZBX SNMP [JMX: IPMI]			Enabled	Latest data	Problems	Graphs 23	Screens 4	Web

Displaying 2 of 2 found

**Fonte: Monitoramento Zabbix Local**

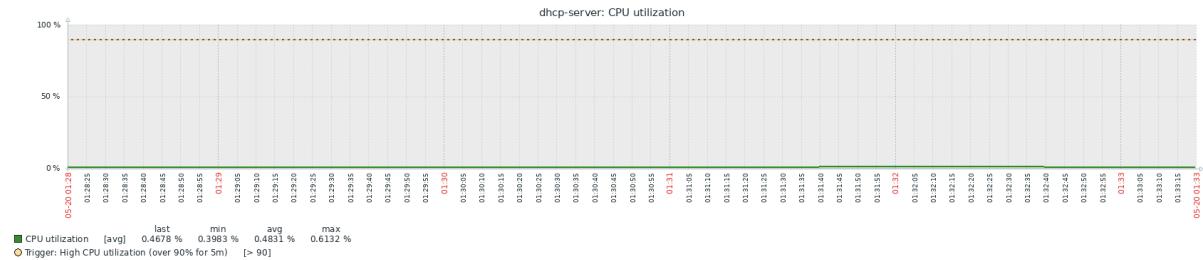
### 9.2.1 Métricas monitoradas

Para definir as métricas monitoradas foi utilizado o template padrão Linux by Zabbix Agent.

#### 9.2.1.1 Utilização de memória

Essa métrica representa a porcentagem de uso de memória RAM do sistema ao longo de um determinado período. Também é demonstrado os números máximos, mínimos e a média desta porcentagem de uso.

**Figura 60 – Servidor DHCP: Utilização de memória**



**Fonte: Monitoramento Zabbix Local**

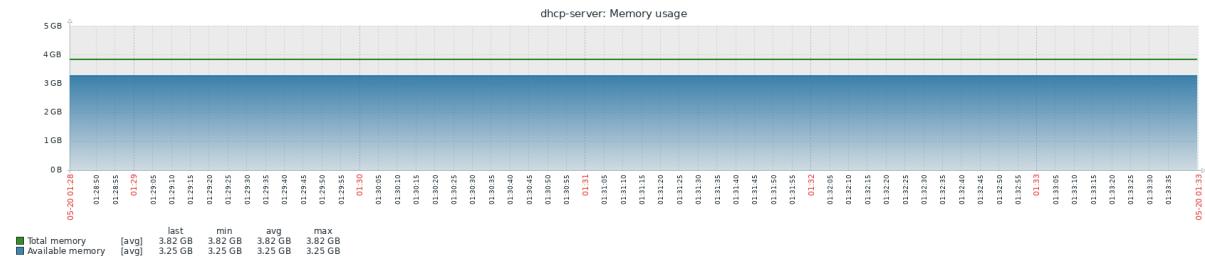
#### 9.2.1.2 Uso de memória

Essa métrica demonstra graficamente a quantidade disponível de memória RAM e a quantidade total de memória RAM do sistema.

#### 9.2.1.3 Uso de memória swap

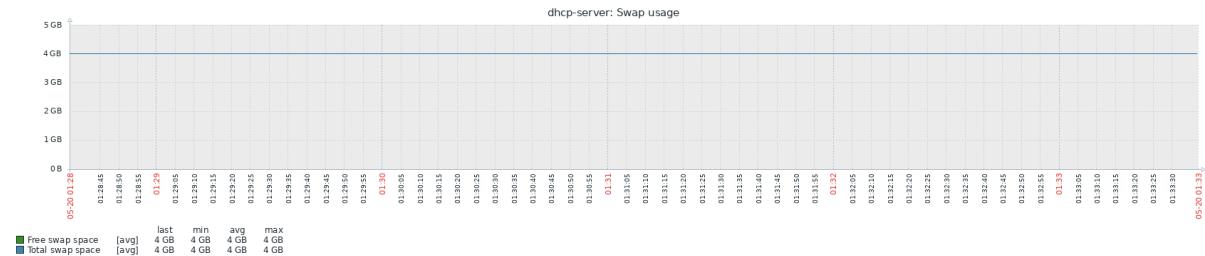
Esta métrica mostra a quantidade de espaço total para memória swap, além da quantidade disponível de memória para swap.

**Figura 61 – Servidor DHCP: Uso de memória**



**Fonte: Monitoramento Zabbix Local**

**Figura 62 – Servidor DHCP: Uso de memória swap**

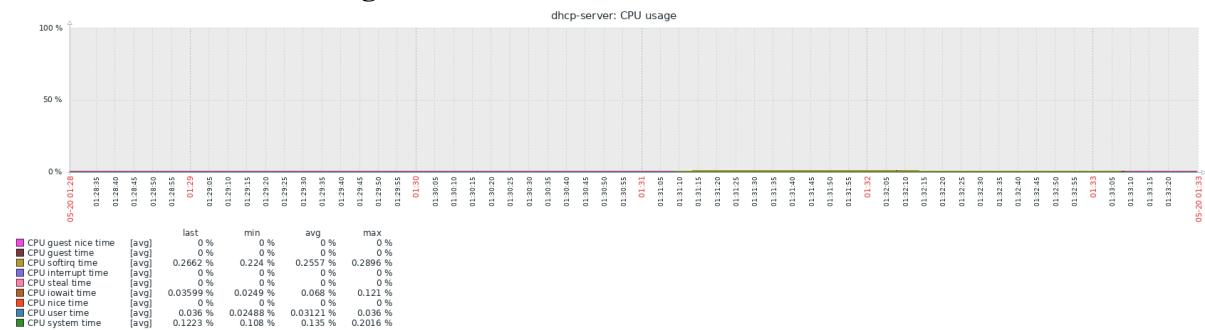


**Fonte: Monitoramento Zabbix Local**

#### 9.2.1.4 Uso de CPU

Essa métrica refere-se à quantidade de tempo que a CPU passa executando instruções de um processo.

**Figura 63 – Servidor DHCP: Uso de CPU**

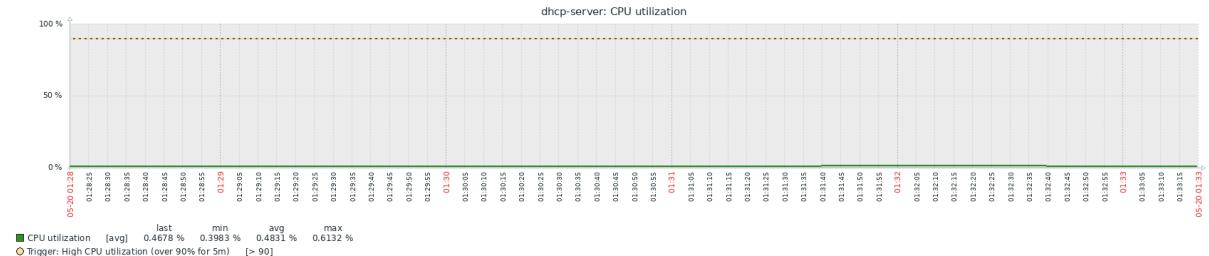


**Fonte: Monitoramento Zabbix Local**

### **9.2.1.5 Utilização de CPU**

Essa métrica refere-se à carga total na CPU, incluindo todas as atividades de processamento do sistema, usuários e interrupções.

**Figura 64 – Servidor DHCP: Utilização de CPU**

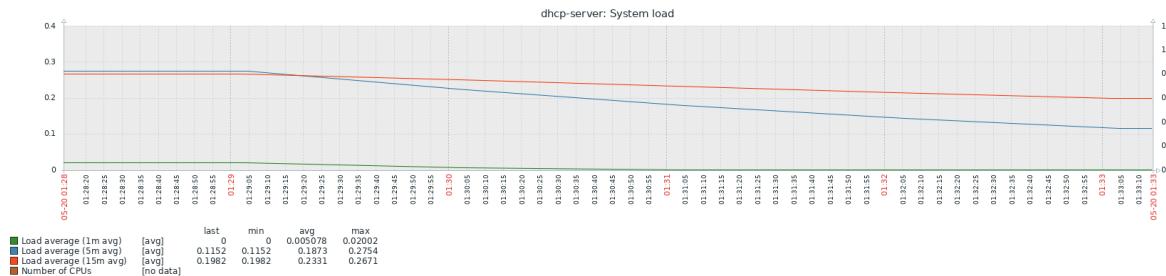


**Fonte: Monitoramento Zabbix Local**

### 9.2.1.6 Carga do sistema

Esta métrica traz a quantidade de carga colocada sobre o sistema ao longo do tempo. Reflete o número de processos na fila de execução ou esperando disponibilidade de recursos de hardware.

**Figura 65 – Servidor DHCP: Carga do sistema**

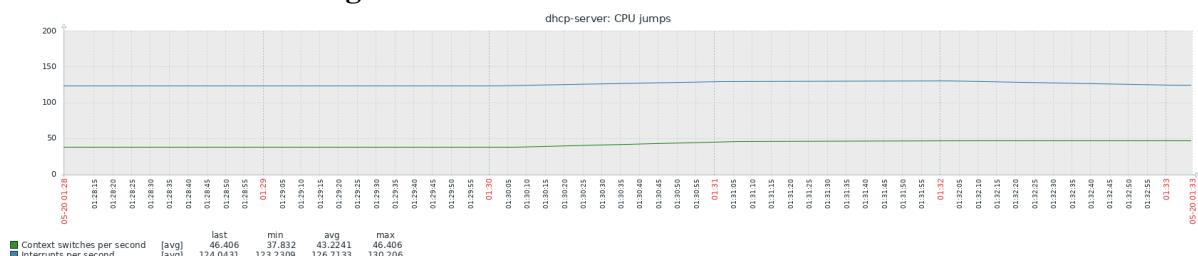


**Fonte: Monitoramento Zabbix Local**

### 9.2.1.7 Picos de CPU

Essa métrica demonstra a quantidade de vezes que o sistema teve aumentos repentinos de processamento (ou picos) ao longo de um determinado período.

**Figura 66 – Servidor DHCP: Picos de CPU**

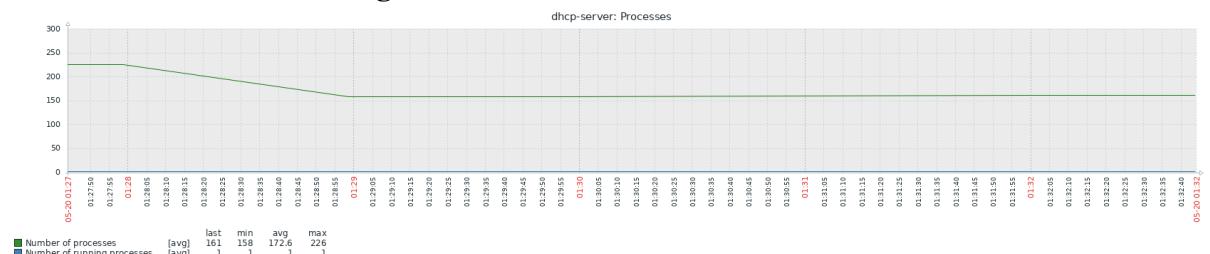


**Fonte: Monitoramento Zabbix Local**

### **9.2.1.8 Processos**

Esta métrica demonstra a quantidade de processos no sistema e a quantidade de processos em execução ao longo de um determinado período.

**Figura 67 – Servidor DHCP: Processos**



**Fonte: Monitoramento Zabbix Local**

## **10 MECANISMOS DE SEGURANÇA**

### **10.1 Política de Segurança da Informação (PSI)**

Uma Política de Segurança da Informação (PSI) é um documento fundamental que estabelece diretrizes e procedimentos para garantir a proteção adequada das informações dentro de uma organização. Inicialmente, ela define uma estrutura clara e concisa que orienta como as informações devem ser protegidas contra acessos não autorizados, uso indevido, modificação não autorizada, ou destruição. Essa política não apenas formaliza as estratégias e abordagens para preservar os ativos da empresa, mas também alinha essas estratégias com os objetivos de negócio, as necessidades regulatórias e as expectativas culturais da organização.

Além disso, a PSI estabelece objetivos claros e um escopo bem definido, fornecendo uma orientação de apoio da direção para a segurança da informação, alinhada aos requisitos específicos do negócio e às regulamentações aplicáveis. Ela abrange desde o manuseio seguro até o descarte adequado das informações, garantindo que todos os processos sejam executados de acordo com padrões estabelecidos. A política não se limita apenas a aspectos tecnológicos, mas também inclui diretrizes para comportamentos e responsabilidades dos colaboradores, tanto em níveis estratégico, tático quanto operacional.

Por fim, a documentação da PSI inclui diretrizes, normas, procedimentos e instruções detalhadas que devem ser seguidas em todos os níveis da organização. Essa estrutura documentada não apenas define as regras gerais e específicas de segurança, como controle de acesso e uso da Internet, mas também estabelece a responsabilidade da alta administração na promoção de uma cultura de segurança. A PSI é um instrumento vital para sensibilizar os colaboradores sobre a importância da segurança da informação e garantir que todos na organização estejam alinhados com os objetivos estratégicos de proteção dos ativos informacionais.

## 10.2 Cartilha de boas práticas de acesso seguro

**Figura 68 – Cartilha de boas práticas de acesso seguro**



**Fonte:** EcoCleaning

**Figura 69 – Cartilha de boas práticas de acesso seguro**

### **ECO CLEANING**

Bem-vindo à cartilha de segurança da informação da Eco Cleaning. A segurança da informação é fundamental para proteger os dados da empresa, dos nossos colaboradores e dos nossos clientes. Esta cartilha visa fornecer orientações claras e práticas para garantir a proteção das informações contra ameaças internas e externas.

### **Pilares da Segurança da Informação**

#### **Confidencialidade**

O que é: Garantir que a informação seja acessada apenas por pessoas autorizadas.

Como garantir: Não compartilhe senhas, utilize criptografia para dados sensíveis e controle rigorosamente quem pode acessar as informações.

#### **Integridade**

O que é: Assegurar que a informação não seja alterada ou destruída de maneira não autorizada.

Como garantir: Use verificações regulares de integridade de dados, mantenha backups atualizados e controle de versão dos documentos.

#### **Disponibilidade**

O que é: Garantir que a informação esteja disponível quando necessário.

Como garantir: Mantenha sistemas atualizados, implemente planos de recuperação de desastres e evite interrupções desnecessárias.



Fonte: EcoCleaning

**Figura 70 – Cartilha de boas práticas de acesso seguro**

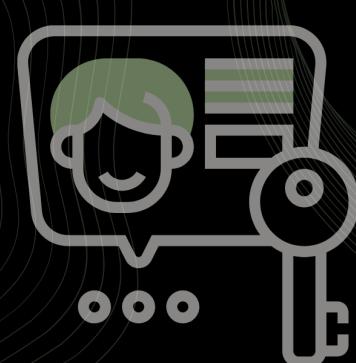
### **Missão**

Garantir a proteção e a confidencialidade das informações e dados da empresa e dos clientes, promovendo um ambiente seguro que permita a continuidade dos negócios e o crescimento sustentável da Eco Cleaning, alinhado com os princípios de limpeza ecológica e responsabilidade ambiental.

### **Visão**

Ser reconhecida como líder em segurança da informação no setor de limpeza ecológica, adotando práticas inovadoras e sustentáveis que protejam os ativos digitais da empresa, assegurando a confiança dos clientes e a integridade dos serviços prestados.

### **Eco Cleaning**



### **Classificação da Informação**

**Pública:** Informações que podem ser divulgadas sem restrições.

**Interna:** Informações que são restritas aos funcionários da empresa.

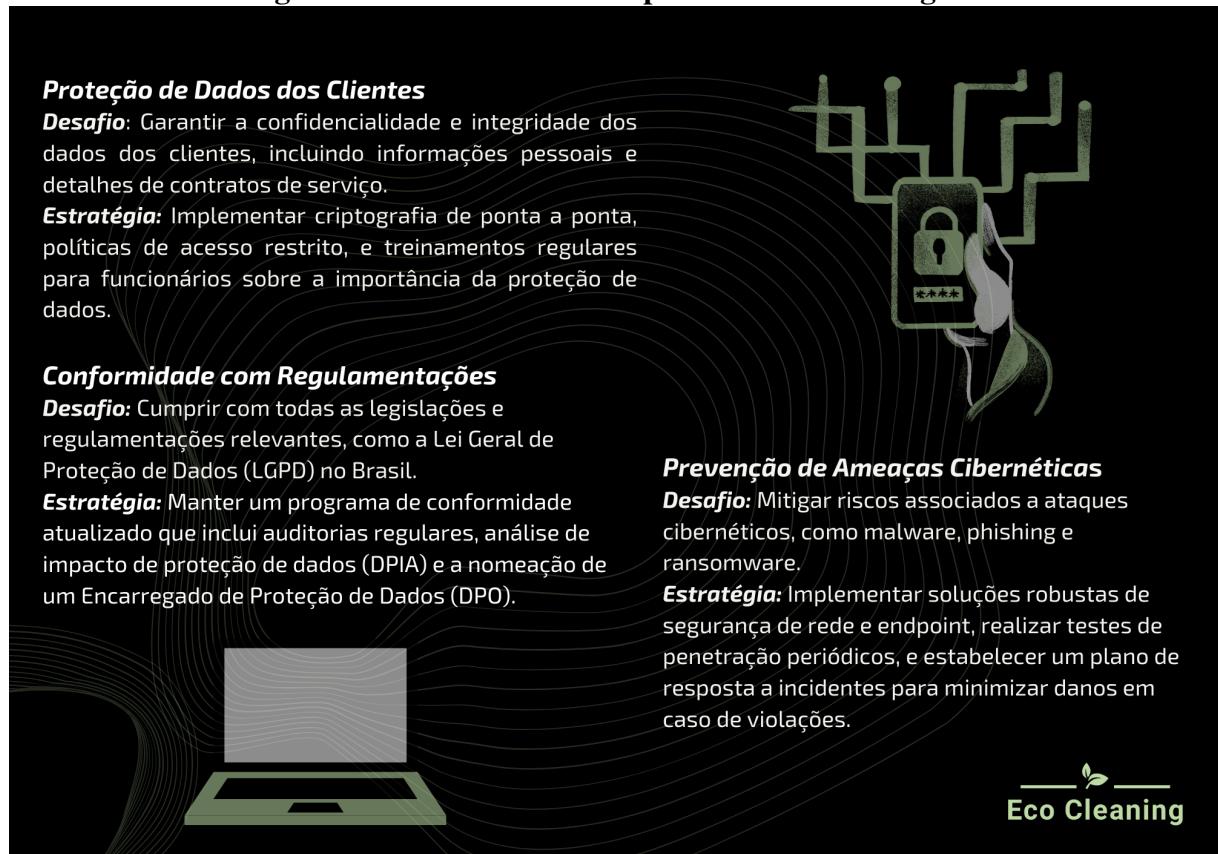
**Confidencial:** Informações sensíveis que requerem proteção contra acesso não autorizado e são acessíveis somente por pessoas autorizadas.

**Secreta:** Informações altamente sensíveis, críticas para a operação da empresa, acessíveis apenas por indivíduos específicos com permissões especiais.



Fonte: EcoCleaning

**Figura 71 – Cartilha de boas práticas de acesso seguro**



**Proteção de Dados dos Clientes**

**Desafio:** Garantir a confidencialidade e integridade dos dados dos clientes, incluindo informações pessoais e detalhes de contratos de serviço.

**Estratégia:** Implementar criptografia de ponta a ponta, políticas de acesso restrito, e treinamentos regulares para funcionários sobre a importância da proteção de dados.

**Conformidade com Regulamentações**

**Desafio:** Cumprir com todas as legislações e regulamentações relevantes, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

**Estratégia:** Manter um programa de conformidade atualizado que inclui auditorias regulares, análise de impacto de proteção de dados (DPIA) e a nomeação de um Encarregado de Proteção de Dados (DPO).

**Prevenção de Ameaças Cibernéticas**

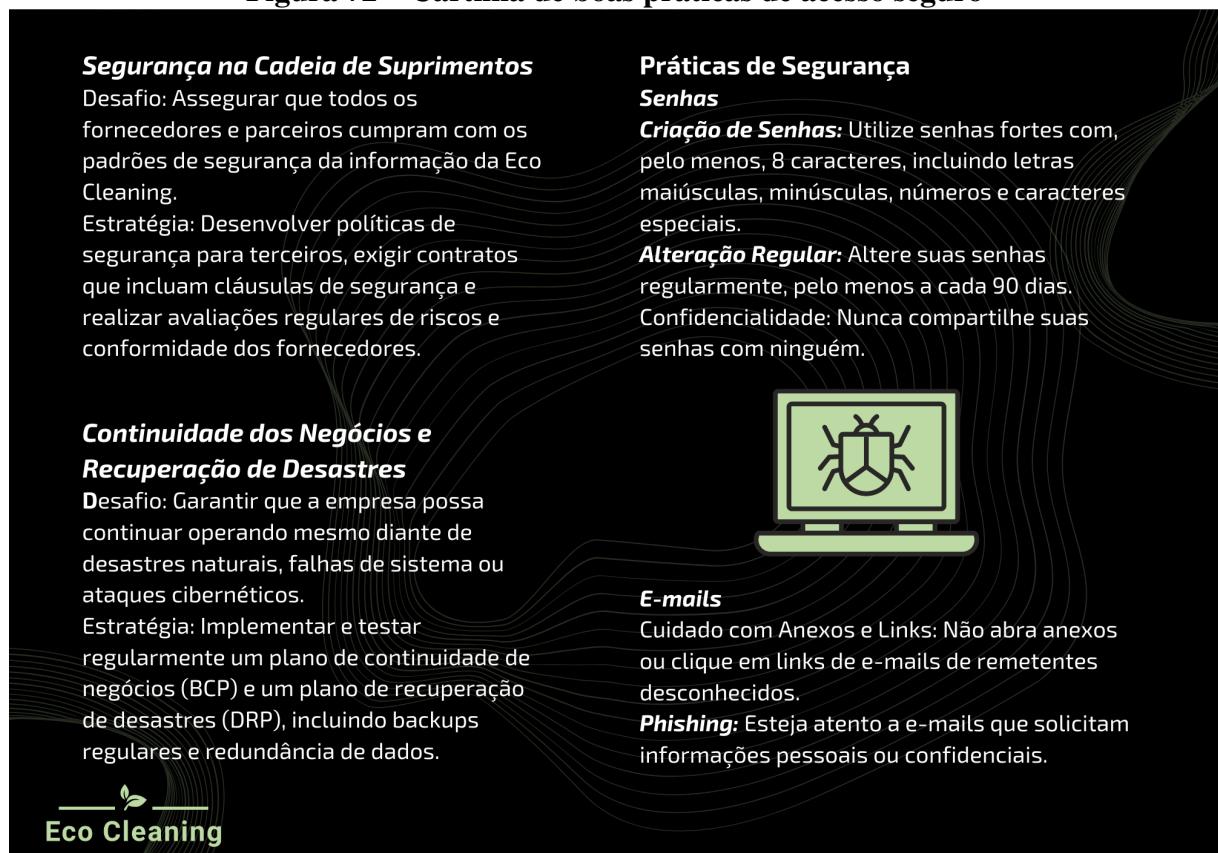
**Desafio:** Mitigar riscos associados a ataques cibernéticos, como malware, phishing e ransomware.

**Estratégia:** Implementar soluções robustas de segurança de rede e endpoint, realizar testes de penetração periódicos, e estabelecer um plano de resposta a incidentes para minimizar danos em caso de violações.

**Eco Cleaning**

Fonte: EcoCleaning

**Figura 72 – Cartilha de boas práticas de acesso seguro**



**Segurança na Cadeia de Suprimentos**

**Desafio:** Assegurar que todos os fornecedores e parceiros cumpram com os padrões de segurança da informação da Eco Cleaning.

**Estratégia:** Desenvolver políticas de segurança para terceiros, exigir contratos que incluam cláusulas de segurança e realizar avaliações regulares de riscos e conformidade dos fornecedores.

**Continuidade dos Negócios e Recuperação de Desastres**

**Desafio:** Garantir que a empresa possa continuar operando mesmo diante de desastres naturais, falhas de sistema ou ataques cibernéticos.

**Estratégia:** Implementar e testar regularmente um plano de continuidade de negócios (BCP) e um plano de recuperação de desastres (DRP), incluindo backups regulares e redundância de dados.

**Práticas de Segurança**

**Senhas**

**Criação de Senhas:** Utilize senhas fortes com, pelo menos, 8 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.

**Alteração Regular:** Altere suas senhas regularmente, pelo menos a cada 90 dias.

**Confidencialidade:** Nunca compartilhe suas senhas com ninguém.

**E-mails**

**Cuidado com Anexos e Links:** Não abra anexos ou clique em links de e-mails de remetentes desconhecidos.

**Phishing:** Esteja atento a e-mails que solicitam informações pessoais ou confidenciais.

**Eco Cleaning**

Fonte: EcoCleaning

**Figura 73 – Cartilha de boas práticas de acesso seguro**

**Dispositivos**

**Uso Seguro de Dispositivos:** Mantenha dispositivos de trabalho seguros, não os deixe desacompanhados e use senhas de bloqueio.

**Atualizações:** Mantenha todos os softwares e sistemas operacionais atualizados com as últimas versões e patches de segurança.

**Acesso Remoto**

**VPN:** Utilize a VPN da empresa para acessar recursos internos de fora do escritório.

**Ambiente Seguro:** Certifique-se de que o ambiente de trabalho remoto é seguro e privado.

**Dados e Documentos**

**Backup Regular:** Realize backups regulares dos dados importantes e armazene-os em local seguro.

**Compartilhamento de Informações:** Compartilhe informações sensíveis somente por meios seguros e com pessoas autorizadas.

**Uso da Internet**

**Sites Confiáveis:** Acesse apenas sites confiáveis e evite downloads de fontes não verificadas.

**Redes Sociais:** Evite compartilhar informações corporativas em redes sociais.

Fonte: EcoCleaning

**Figura 74 – Cartilha de boas práticas de acesso seguro**

**Penalidades e Infrações**

Na Eco Cleaning, levamos a segurança das informações muito a sério. As penalidades para violações incluem:

**Advertência Verbal:** Para infrações menores ou incidentes acidentais.

**Advertência Escrita:** Para reincidências ou infrações mais sérias.

**Suspensão:** Para infrações graves ou contínuas.

**Demissão:** Para violações severas ou repetidas que coloquem a empresa em risco significativo. Todas as penalidades são aplicadas de acordo com a gravidade da infração e o histórico do colaborador.

**Papel dos Colaboradores**

Cada colaborador tem um papel fundamental na proteção das informações da Eco Cleaning:

**Cumprimento das Políticas:** Seguir rigorosamente as políticas e procedimentos de segurança da informação.

**Educação e Treinamento:** Participar ativamente dos programas de treinamento oferecidos pela empresa.

**Relatório de Incidentes:** Reportar imediatamente qualquer suspeita de violação de segurança ou comportamento inadequado.

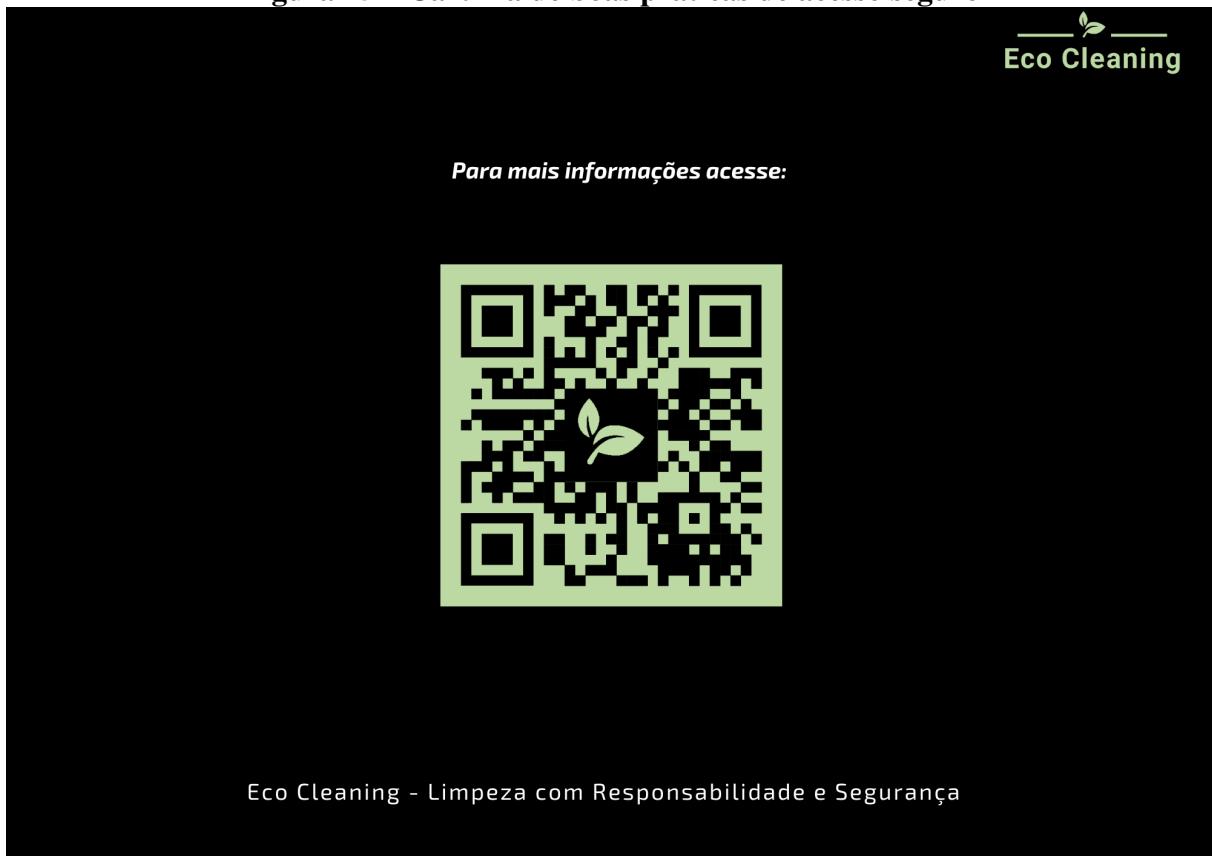
**Confidencialidade:** Manter a confidencialidade das informações e evitar a divulgação não autorizada.

**Conclusão**

A segurança da informação é uma responsabilidade compartilhada. Ao seguir as diretrizes desta cartilha, todos na Eco Cleaning contribuem para um ambiente mais seguro e protegido. Agradecemos sua cooperação e empenho em manter a segurança da informação em nossa empresa.

Fonte: EcoCleaning

**Figura 75 – Cartilha de boas práticas de acesso seguro**



**Fonte:** EcoCleaning

## **11 ELABORAÇÃO DA APRESENTAÇÃO FINAL DO PROJETO**

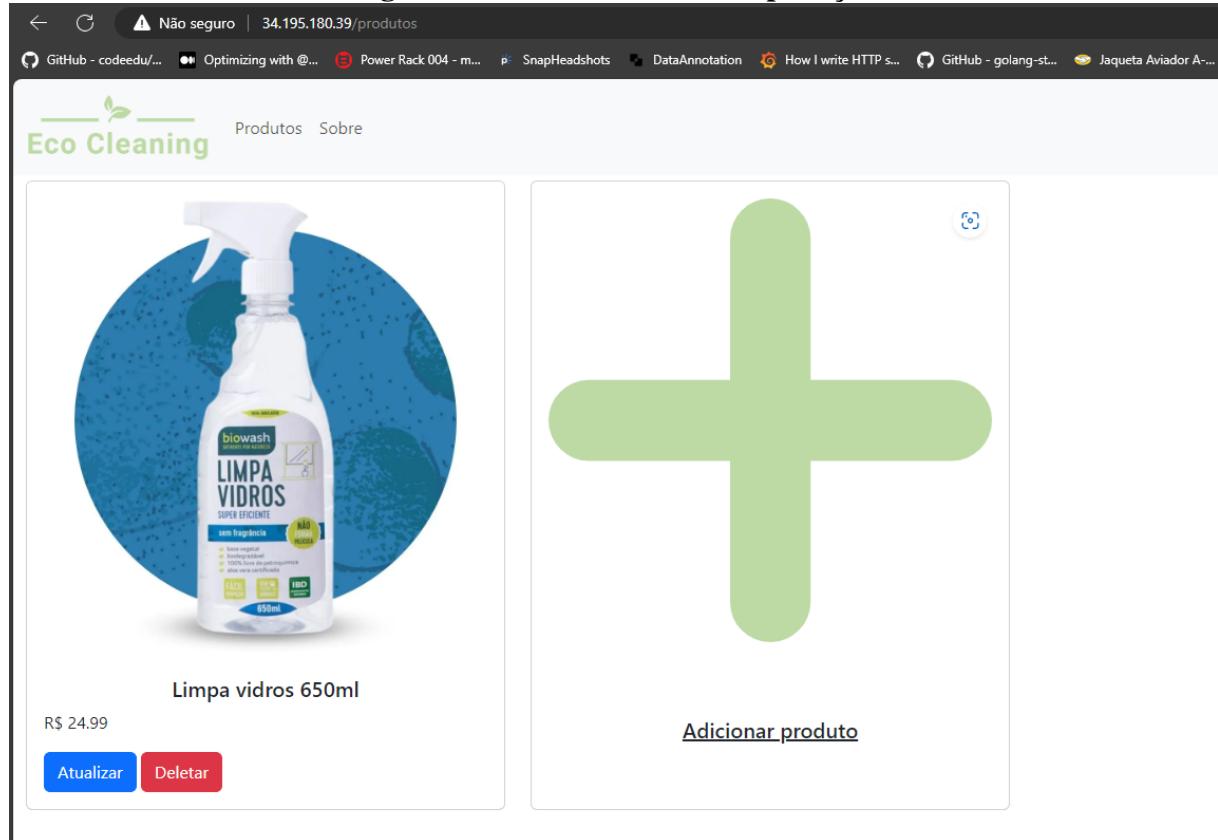
### **11.1 CRUD da Aplicação**

Foi desenvolvida uma aplicação backend em Java 17, utilizando o servidor Tomcat e o framework Spring. É utilizado o Maven para gerenciar as dependências. A aplicação contém um CRUD(Create, Read, Update e Delete) de produtos focando no ramo da empresa que é de produtos de limpeza e este CRUD executa suas operações em um banco MySQL externo.

#### ***11.1.1 Estado inicial da aplicação***

Empresa de manufatura com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km

**Figura 76 – Estado inicial da aplicação**



Fonte: Aplicação Web

**Figura 77 – Estado inicial da aplicação**

The screenshot shows the MySQL Workbench interface. The left sidebar displays the "Navigator" with the "SCHEMAS" section expanded, showing the "ecocleaning" schema with its "Tables" (product), "Views", "Stored Procedures", and "Functions". The main area has a "Query 1" tab with the SQL query `SELECT * FROM ecocleaning.product;` and a "Result Grid" tab showing the following data:

	id	description	image_url	name	price
▶	2	NULL	<a href="https://images.tcdn.com.br/img/img_prod/9111...">https://images.tcdn.com.br/img/img_prod/9111...</a>	Limpa vidros 650ml	24.99
*	NULL	NULL	NULL	NULL	NULL

Fonte: MySQL Workbench

### 11.1.2 Criação de produto

Figura 78 – Criação de produto

The screenshot shows a web-based application for managing products. At the top, there's a navigation bar with links like 'GitHub - codeedu...', 'Optimizing with @...', 'Power Rack 004 - m...', 'SnapHeadshots', 'DataAnnotation', 'How I write HTTP s...', 'GitHub - golang-st...', 'Jaqueta Aviador A...', and 'Jaqueta Masculina...'. Below the navigation, the application has a header with the logo 'Eco Cleaning' and menu items 'Produtos' and 'Sobre'. The main form is titled 'Nome do produto' and contains a text input field with the value 'Limpa pisos 650ml'. Next to it are two input fields for price ('R\$ 24') and quantity ('99'). Below the form is a link 'Link da imagem do produto' with a URL: 'https://images.tcdn.com.br/img/img\_prod/911102/limpa\_pisos\_650ml\_161\_2\_7dd03e4dbc2424f3245cb1aa4383fba3.jpg'. A blue button labeled 'Salvar produto' is visible. A success message 'Produto salvo com sucesso!' is displayed in a green box, along with a link 'Voltar.'

Fonte: Aplicação Web

Figura 79 – Criação de produto

The screenshot shows the MySQL Workbench interface. On the left is a 'Navigator' pane with a tree view of 'SCHEMAS'. Under the 'ecocleaning' schema, there's a 'Tables' node with a 'product' table selected. The main area is a 'Query 1' window containing a SQL query: 'SELECT \* FROM ecocleaning.product;'. Below the query is a 'Result Grid' showing the data from the 'product' table:

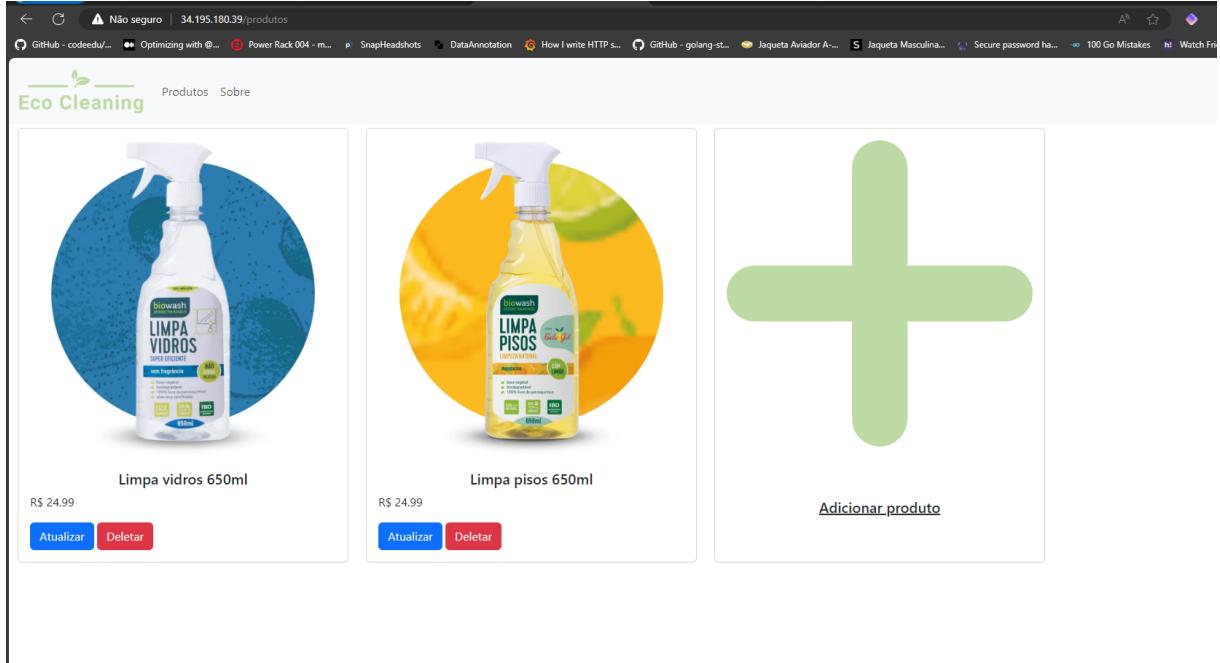
	id	description	image_url	name	price
▶	2	NULL	https://images.tcdn.com.br/img/img_prod/9111...	Limpa vidros 650ml	24.99
▶	4	NULL	https://images.tcdn.com.br/img/img_prod/9111...	Limpa pisos 650ml	24.99
*	NULL	NULL	NULL	NULL	NULL

Fonte: MySQL Workbench

### 11.1.3 Leitura de produtos

O produto criado foi salvo e passa a ser exibido.

**Figura 80 – Leitura de produtos**

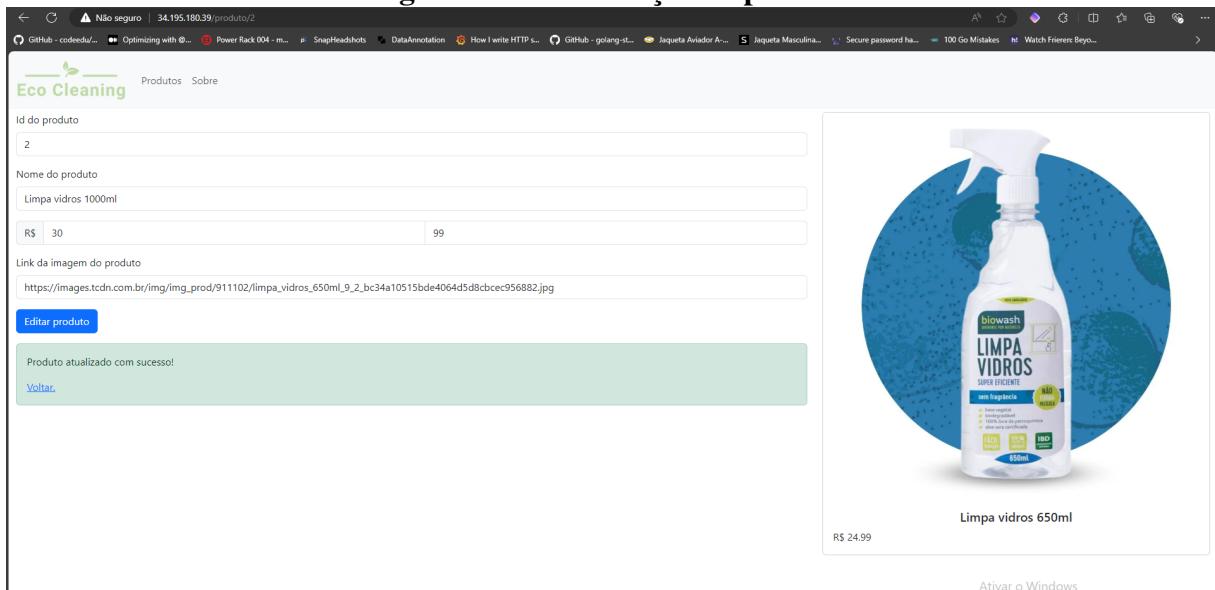


**Fonte: Aplicação Web**

#### 11.1.4 Atualização de produto

O nome do produto é atualizado para limpa vidros 1000ml.

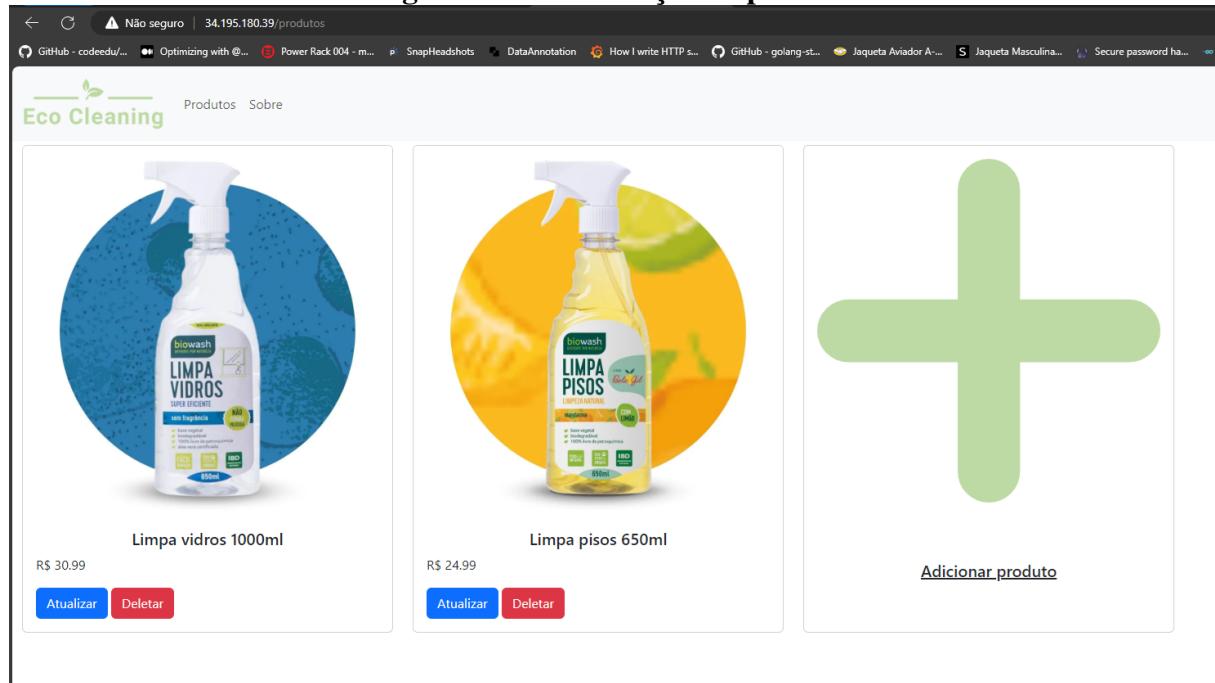
**Figura 81 – Atualização de produto**



**Fonte: Aplicação Web**

O novo nome passa a ser exibido.

**Figura 82 – Atualização de produto**

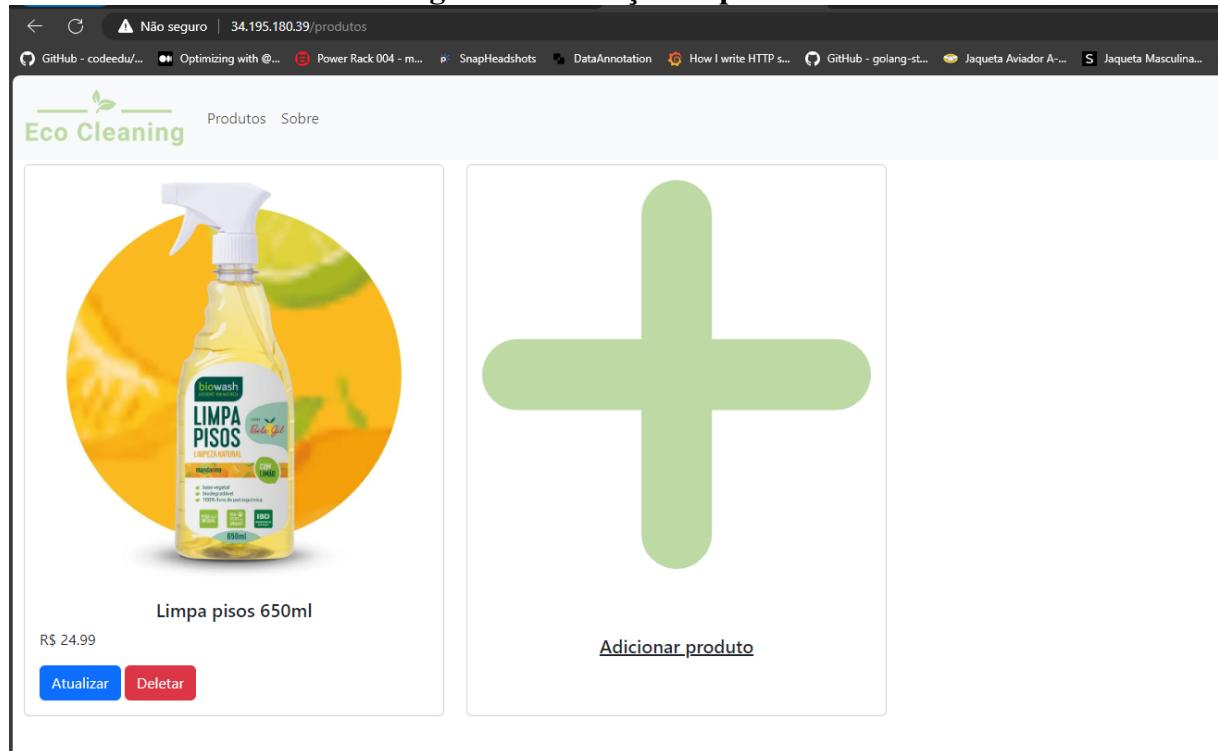


**Fonte: Aplicação Web**

#### **11.1.5 Deleção de produto**

O produto "Limpa vidros" foi deletado e apenas o "Limpa pisos" foi exibido.

**Figura 83 – Deleção de produto**



Fonte: Aplicação Web

## 11.2 Relatório de vulnerabilidades

Utilizar Java no servidor, assim como nas outras linguagens de programação, tem suas peculiaridades do ponto de vista de segurança e tem também suas vulnerabilidades. É de responsabilidade do desenvolvedor conhecer as vulnerabilidades do seu ecossistema e analisar sua aplicação para entender as vulnerabilidades existentes, seus riscos e formas de mitigação. Há diversas vulnerabilidades que podem acometer um backend Java, como por exemplo: Ataques de injeção de SQL: ocorrem quando as informações inseridas pelos usuários no sistema não são validadas e quando as instruções de banco de dados não são preparadas, deixando as informações inseridas no banco de dados do jeito que o usuário digitou. Isso pode dar acesso para os usuários controlarem indevidamente o banco de dados da aplicação, vazando dados ou excluindo tabelas. Cross-site scripting: ocorre quando dados não confiáveis são enviados para o navegador sem validação. Isso permite que scripts maliciosos sejam injetados em páginas carregadas por outros usuários. Roubo de sessão: ocorre quando hackers conseguem roubar os dados da sessão do usuários, ganhando poderes para impersonar o usuário. Logs e monitoramento insuficientes: ocorre quando a aplicação não tem logs o suficiente e causa dificuldades para a resolução de problemas. Vulnerabilidades em subida de arquivos: caso não sejam validados corretamente, arquivos enviados para o servidor executar código malicioso.

### ***11.2.1 Vulnerabilidades encontradas na aplicação***

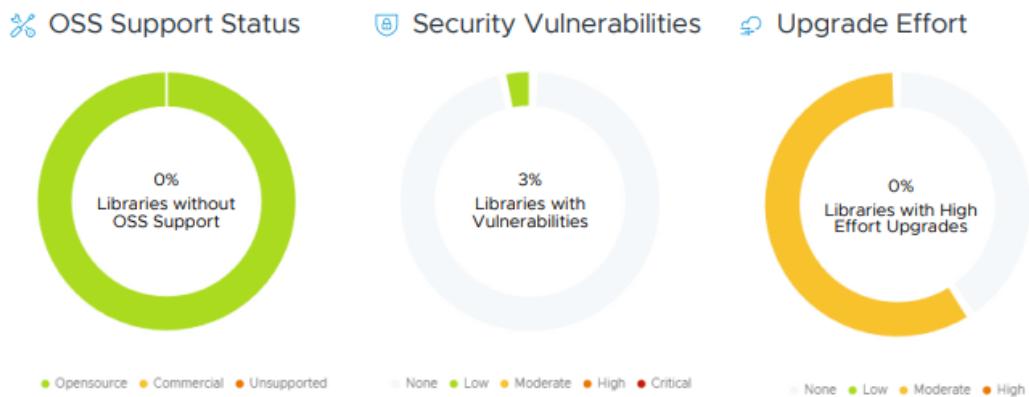
Foram utilizadas duas ferramentas para analisar as vulnerabilidades da aplicação: o Spring Health Assessment, que verifica as dependências do Spring da aplicação e gera um relatório de vulnerabilidades críticas, da dificuldade de corrigí-las e do tempo de suporte das dependências.

## Figura 84 – Spring Health Assessment

Created on Jun 30, 2024

32

Total Spring libraries used



### Findings

Your percentage of supported libraries will reduce from 100% to 40% over the next 4 months.

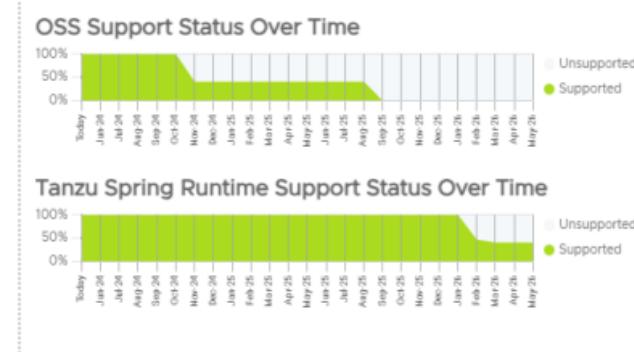
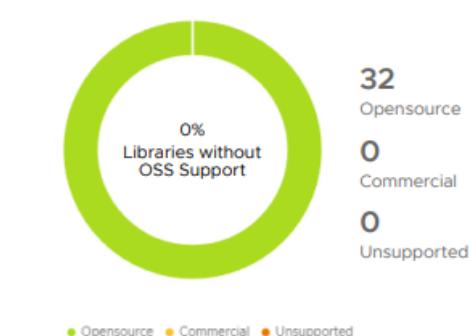
You have 1 libraries with security vulnerabilities.

### Recommendations

Purchase [Spring Runtime](#) to extend your support until Jun 30, 2025, for 32 libraries which are set to expire in 4 months.

Upgrade 1 libraries with identified vulnerabilities.

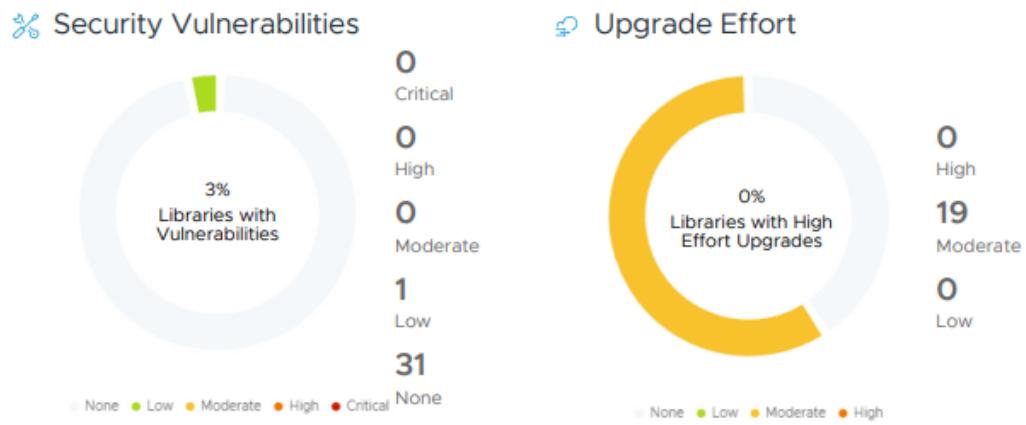
### OSS Support Status



Fonte: Spring Health Assessment

Empresa de manufatura com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km

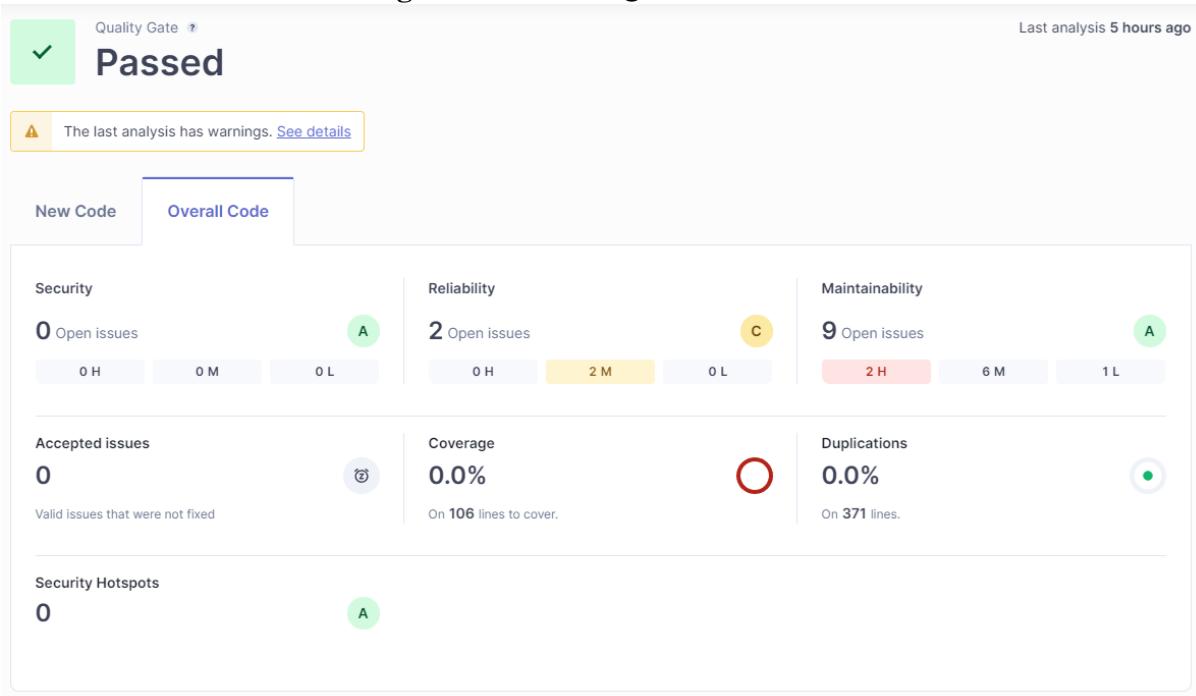
**Figura 85 – Spring Health Assessment**



**Fonte: Spring Health Assessment**

Também foi feita uma análise estática de código utilizando o SonarQube Community, que revelou 2 problemas de confiabilidade e 9 problemas de manutenibilidade, além de detectar a falta de testes unitários.

**Figura 86 – SonarQube - Overview**



**Fonte: SonarQube**

É interessante notar também que o SonarQube cria um ranking de vulnerabilidades por criticidades, sendo que foram encontradas 2 vulnerabilidades de criticidade alta, 7 sendo médias e 1 baixa.

**Figura 87 – SonarQube - Criticidades**



Fonte: SonarQube

Empresa de manufatura com escritórios no centro de uma região metropolitana, matriz em uma região industrial e filiais em 3 cidades distantes cerca de 200 km

---

## **REFERÊNCIAS**