



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA
Bacharelado em Sistemas de Informação

Andressa Cordeiro Kahn
Carolina Meneses de Carvalho Moura
Gabriella Victória da Silveira Pecsén
Luiz Carlos Ferreira
Rafael Machado Bueno
Davisson José de Souza Gomes

PROJETO INFRAESTRUTURA DE REDES

Belo Horizonte
2023

PROJETO MANUFATURA

Trabalho apresentado como requisito parcial à aprovação na disciplina Projeto: Infraestrutura de Redes de Computadores.

Professor: Alexandre Teixeira

Belo Horizonte

2023

SUMÁRIO

1. TEMA	4
2. RESPONSABILIDADES	5
3. CRONOGRAMA DE ATIVIDADES	7
4. PLANEJAMENTO DOS RECURSOS DE REDE	8
5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE	16
6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX	24
7. REFERÊNCIAS	30
8. ANEXO I - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)	36

1. TEMA

O grupo optou pela escolha de uma empresa de manufatura com um quadro de funcionários de aproximadamente 1000 colaboradores e especializada em bens de consumo de linha branca como batedeiras, liquidificadores, cafeteiras e assadeiras.

De acordo com as classificações do IBGE, uma empresa com esse tamanho é considerada de grande porte, o que implica em responsabilidades e desafios distintos em comparação com empresas de menor porte para a distribuição e definição de sua estrutura de rede.

A estrutura de uma empresa de manufatura de grande porte é altamente complexa e precisa estar organizada. Para operar de maneira eficiente, ela geralmente é composta por diferentes departamentos e setores interconectados. A seguir, temos alguns dos principais aspectos dessa estrutura:

1. **Departamento de Produção:** A produção de eletrodomésticos de linha branca envolve várias etapas, desde o design e desenvolvimento de produtos até a fabricação em si.
2. **Pesquisa e Desenvolvimento:** Para se manter competitiva no mercado, a empresa investe em pesquisa e desenvolvimento para criar produtos inovadores e eficientes em termos energéticos.
3. **Logística e Cadeia de Suprimentos:** O gerenciamento eficaz da cadeia de suprimentos é essencial para garantir que os componentes e materiais necessários estejam disponíveis quando necessário e que os produtos acabados sejam entregues aos clientes.
4. **Controle de Qualidade:** Dada a natureza crítica dos produtos eletrodomésticos em termos de segurança e desempenho, a empresa necessita ter um rigoroso controle de qualidade em cada etapa de fabricação.
5. **Recursos Humanos:** Com 1000 funcionários, a gestão de recursos humanos é um departamento vital, encarregado de contratação, treinamento, avaliação de desempenho e desenvolvimento profissional dos colaboradores.
6. **Vendas e Marketing:** Para atingir um público amplo e diversificado, a empresa precisa investir em estratégias de vendas e marketing para promover seus produtos e expandir sua base de clientes.

7. Finanças e Administração: O departamento financeiro cuida das finanças da empresa, incluindo orçamento, contabilidade e relatórios financeiros.

Uma empresa de manufatura de grande porte como a nossa é caracterizada por uma abordagem orientada para a automação de seus processos e a tecnologia aplicada em pesquisa, visando aumentar a eficiência e a produtividade a cada ano.

A seguir, destacam-se várias razões pelas quais uma infraestrutura de rede eficiente é crucial para o sucesso desse tipo de empresa:

- Comunicação Interna e Cooperação;
- Segurança de Dados;
- Expansão e Escalabilidade;
- Acesso Remoto;
- Competitividade;
- Automação e Controle de Processos;
- Gestão de Cadeia de Suprimentos;
- Gestão de Manutenção.

Definitivamente uma estrutura de rede bem-sucedida é um componente crítico para garantir a eficiência operacional, a qualidade do produto e a competitividade de uma empresa de grande porte de manufatura, como a especializada em eletrodomésticos de linha branca. Ela permite uma integração eficaz de todos os aspectos da operação, desde o chão de fábrica até a gestão de recursos, promovendo a excelência nos negócios.

2. RESPONSABILIDADES

Nome	Papel	Responsabilidade
Andressa	Prazo e controle de qualidade;	- Realizar a contextualização das demandas do projeto, compreendendo as necessidades e objetivos;

Nome	Papel	Responsabilidade
		<ul style="list-style-type: none"> - Acompanhar o andamento das atividades, verificando o progresso em relação ao cronograma e identificando eventuais desvios.
Carolina	Redatora/editora	<ul style="list-style-type: none"> - Coordenar a elaboração do cronograma do projeto, definindo etapas e prazos para as atividades; - Coletar, organizar e documentar dados relevantes para o projeto, garantindo a disponibilidade de informações para subsidiar as atividades.
Davisson	Comunicador	<ul style="list-style-type: none"> - Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados; - Coordenar a planilha de Recursos e Redes.
Gabriella	Programadora	<ul style="list-style-type: none"> - Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados; - Coordenar o Protótipo da rede no Simulador da Cisco Packet Tracer.

Nome	Papel	Responsabilidade
Luiz Carlos	Líder do projeto	<ul style="list-style-type: none"> - Coordenar as reuniões semanais de acompanhamento do projeto; - Realizar a distribuição de tarefas entre os membros da equipe.
Rafael	Pesquisador	<ul style="list-style-type: none"> - Realizar levantamento de requisitos; - Definir objetivos e metas alinhados com as demandas de rede.

3. CRONOGRAMA DE ATIVIDADES

Semana	Dias de dedicação	Atividades
Semana 1 16/08/2023	Cinco dias	<ul style="list-style-type: none"> - Formação dos grupos e definição do tema junto ao professor; - Início dos estudos dos microfundamentos para a etapa.
Semana 2 30/08/2023	Cinco dias	<ul style="list-style-type: none"> - Definição do tema e planejamento inicial da proposta; - Curso do Cisco Packet Tracer;
Semana 3 06/09/2023	Cinco dias	<ul style="list-style-type: none"> - Planilha de Recursos de Rede; - Protótipo da rede no Simulador da Cisco Packet Tracer.
Semana 4 13/09/2023	Cinco dias	<ul style="list-style-type: none"> - Dúvidas finais com o professor; - Revisão e entrega da Entrega 1 (Primeira Etapa).

4. PLANEJAMENTO DOS RECURSOS DE REDE

Cenário: a rede será composta da matriz da empresa em Betim (MG) que se liga com seus 2 escritórios em Belo Horizonte (MG). Além disso, a empresa também contará com 3 filiais, localizadas em São Paulo (SP), Curitiba (PR) e Rio de Janeiro (RJ). Segue algumas características de cada local da rede:

- Matriz (Betim, MG)
 - Departamento de Produção
 - Departamento de Logística e Distribuição
 - Departamento de Qualidade e Segurança
 - Produção

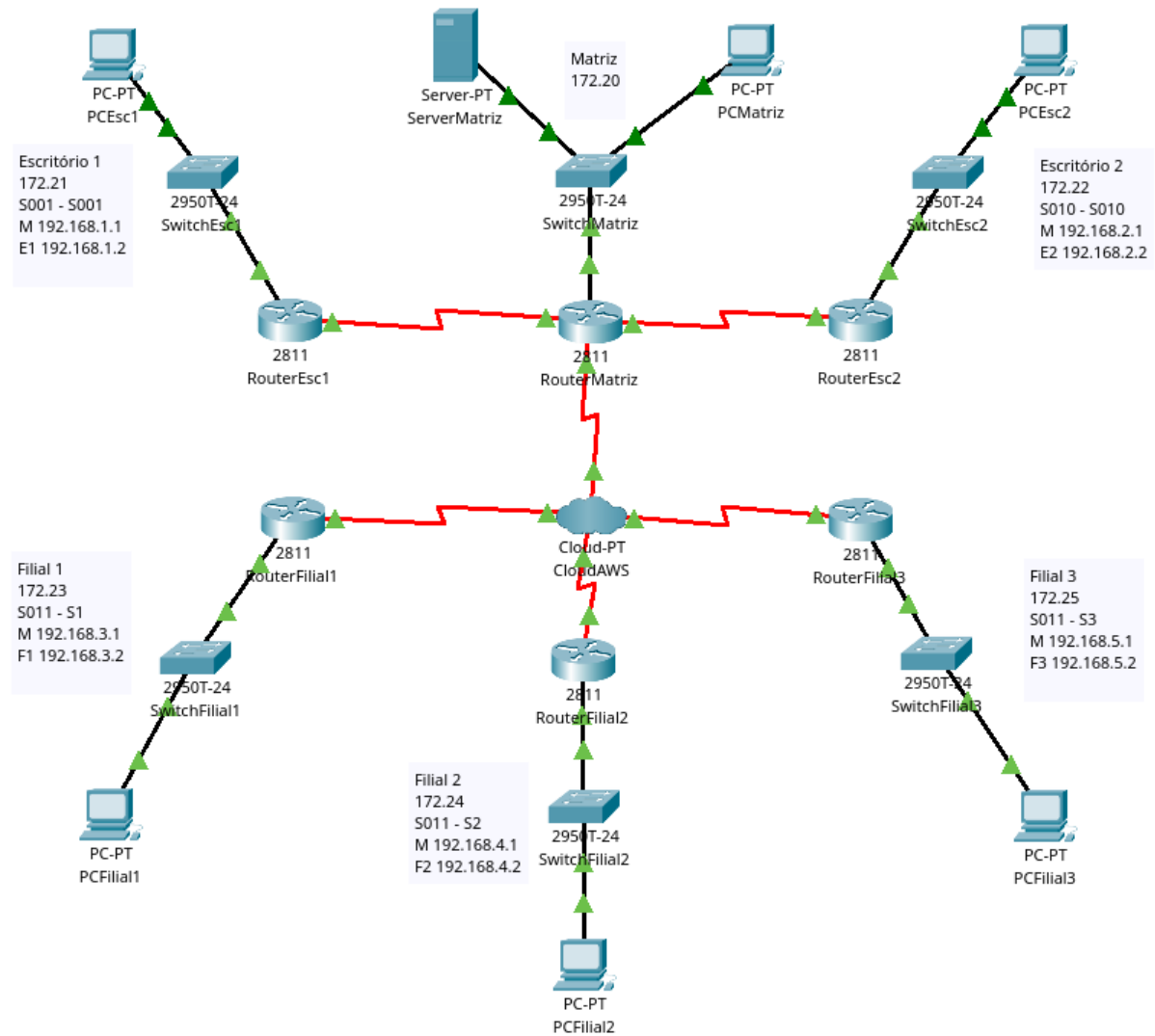
- Escritório 1: Planejamento e estratégia (Belo Horizonte, MG)
 - Diretoria Executiva
 - Departamento de Pesquisa e Desenvolvimento (P&D)
 - Departamento de TI

- Escritório 2: Escritório de Desenvolvimento de Mercado (Belo Horizonte, MG)
 - Departamento de Marketing e Vendas
 - Departamento de Recursos Humanos
 - Departamento Financeiro e Contábil

- Filiais (Cada uma das filiais possua os departamentos abaixo)
 - Departamento de Operações Regionais
 - Departamento de Vendas Regionais
 - Departamento de Logística Regional
 - Departamento de Gerenciamento de Filiais
 - Departamento de Suporte Técnico Regional

4.1 DIVISÃO FÍSICA DA REDE

Com base em todo esse cenário, a divisão física da rede ficou representada conforme a imagem abaixo. A topologia escolhida foi a hierárquica.



Fonte: Cisco Packet Tracer

4.2 PLANILHA DE MATERIAIS

A tabela a seguir reflete a lista de materiais que serão empregados no projeto bem como seus valores correspondentes. A final é demonstrado o valor orçado que será necessário para a Matriz (R\$ 1.285.56,21), Escritório 1 (R\$ 231.422,90), Escritório 2 (R\$ 407.666,30), Filial 1 (R\$ 761.51,60), Filial 2 (R\$ 581.903,90) e Filial 3 (R\$ 581.903,90). O total geral estimado para este projeto é de R\$3.268.073,91.

		Matriz		Escritório 1		Escritório 2		Filial 1		Filial 2		Filial 3	
		350		50		100		200		150		150	
Item	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
Nutanix HPC		0	R\$ 0,00	0	R\$ 0,00	0	R\$ 0,00	1	R\$ 0,00	1	R\$ 0,00	1	R\$ 0,00
Estação Dell	R\$ 1.199,00	350	R\$ 419.650,00	50	R\$ 59.950,00	100	R\$ 119.900,00	200	R\$ 239.800,00	150	R\$ 179.850,00	150	R\$ 179.850,00
Roteador CISCO	R\$ 2.031,92	1	R\$ 2.031,92	1	R\$ 2.031,92	1	R\$ 2.031,92	1	R\$ 2.031,92	1	R\$ 2.031,92	1	R\$ 2.031,92
Serial CISCO	R\$ 215,00	2	R\$ 430,00	1	R\$ 215,00	1	R\$ 215,00	1	R\$ 215,00	1	R\$ 215,00	1	R\$ 215,00
Switch Dell 24p	R\$ 16.788,00	16	R\$ 268.608,00	4	R\$ 67.152,00	6	R\$ 100.728,00	10	R\$ 167.880,00	8	R\$ 134.304,00	8	R\$ 134.304,00
Cabo UTP CAT6 cx	R\$ 4.254,00	46	R\$ 195.684,00	7	R\$ 29.778,00	14	R\$ 59.556,00	27	R\$ 114.858,00	20	R\$ 85.080,00	20	R\$ 85.080,00
RJ45 f Cat6	R\$ 217,89	352	R\$ 76.697,28	52	R\$ 11.330,28	102	R\$ 22.224,78	202	R\$ 44.013,78	152	R\$ 33.119,28	152	R\$ 33.119,28
Patch Cord CAT 6	R\$ 46,50	704	R\$ 32.736,00	104	R\$ 4.836,00	204	R\$ 9.486,00	404	R\$ 18.786,00	304	R\$ 14.136,00	304	R\$ 14.136,00
Patch Panel CAT 6	R\$ 886,95	16	R\$ 14.191,20	4	R\$ 3.547,80	6	R\$ 5.321,70	10	R\$ 8.869,50	8	R\$ 7.095,60	8	R\$ 7.095,60
Rack 44 U	R\$ 3.604,41	2	R\$ 7.208,82	1	R\$ 3.604,41	1	R\$ 3.604,41	1	R\$ 3.604,41	1	R\$ 3.604,41	1	R\$ 3.604,41
Cx + placa	R\$ 40,00	352	R\$ 14.080,00	52	R\$ 2.080,00	102	R\$ 4.080,00	202	R\$ 8.080,00	152	R\$ 6.080,00	152	R\$ 6.080,00
AP Rukus WiFi 6	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00
Organizador de Cabo	R\$ 338,00	16	R\$ 5.408,00	4	R\$ 1.352,00	6	R\$ 2.028,00	10	R\$ 3.380,00	8	R\$ 2.704,00	8	R\$ 2.704,00
Impressora	R\$ 1.124,10	10	R\$ 11.241,00	5	R\$ 5.620,50	5	R\$ 5.620,50	10	R\$ 11.241,00	7	R\$ 7.868,70	7	R\$ 7.868,70
Nobreak	R\$ 479,99	1	R\$ 479,99	1	R\$ 479,99	1	R\$ 479,99	1	R\$ 479,99	1	R\$ 479,99	1	R\$ 479,99
Mesa + Cadeira	R\$ 658,90	350	R\$ 230.615,00	50	R\$ 32.945,00	100	R\$ 65.890,00	200	R\$ 131.780,00	150	R\$ 98.835,00	150	R\$ 98.835,00
Total			R\$ 1.285.561,21	Total	R\$ 231.422,90	Total	R\$ 407.666,30	Total	R\$ 761.519,60	Total	R\$ 581.903,90	Total	R\$ 581.903,90
Total Geral												R\$ 3.268.073,91	

Tabela de Materiais

4.3 DIVISÃO LÓGICA DA REDE

A tabela abaixo contém os dispositivos da rede, seus nomes, endereçamento, portas e roteamento.

Dispositivos	Nome	Portas / Endereçamento																																																				
Nuvem	CloudAWS	<div>Device Name: CloudAWS</div> <div>Device Model: Cloud-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>DLCI/Phone Number</th></tr></thead><tbody><tr><td>Serial0</td><td>Up</td><td>103, 104, 105</td></tr><tr><td>Serial1</td><td>Up</td><td>201</td></tr><tr><td>Serial2</td><td>Up</td><td>301</td></tr><tr><td>Serial3</td><td>Up</td><td>401</td></tr><tr><td>Modem4</td><td>Down</td><td><not set></td></tr><tr><td>Modem5</td><td>Down</td><td><not set></td></tr><tr><td>Ethernet6</td><td>Down</td><td>--</td></tr><tr><td>Coaxial7</td><td>Down</td><td>--</td></tr></tbody></table>	Port	Link	DLCI/Phone Number	Serial0	Up	103, 104, 105	Serial1	Up	201	Serial2	Up	301	Serial3	Up	401	Modem4	Down	<not set>	Modem5	Down	<not set>	Ethernet6	Down	--	Coaxial7	Down	--																									
Port	Link	DLCI/Phone Number																																																				
Serial0	Up	103, 104, 105																																																				
Serial1	Up	201																																																				
Serial2	Up	301																																																				
Serial3	Up	401																																																				
Modem4	Down	<not set>																																																				
Modem5	Down	<not set>																																																				
Ethernet6	Down	--																																																				
Coaxial7	Down	--																																																				
Roteador	RouterMatriz	<div>Device Name: RouterMatriz</div> <div>Custom Device Model: 2811 IOS15</div> <div>Hostname: RouterMatriz</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.20.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Up</td><td>--</td><td>192.168.1.1/24</td></tr><tr><td>Serial0/1/0</td><td>Up</td><td>--</td><td>192.168.2.1/24</td></tr><tr><td>Serial0/1/1</td><td>Up</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/1.3</td><td>Up</td><td>--</td><td>192.168.3.1/24</td></tr><tr><td>Serial0/1/1.4</td><td>Up</td><td>--</td><td>192.168.4.1/24</td></tr><tr><td>Serial0/1/1.5</td><td>Up</td><td>--</td><td>192.168.5.1/24</td></tr><tr><td>Serial0/2/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/2/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.20.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Up	--	192.168.1.1/24	Serial0/1/0	Up	--	192.168.2.1/24	Serial0/1/1	Up	--	<not set>	Serial0/1/1.3	Up	--	192.168.3.1/24	Serial0/1/1.4	Up	--	192.168.4.1/24	Serial0/1/1.5	Up	--	192.168.5.1/24	Serial0/2/0	Down	--	<not set>	Serial0/2/1	Down	--	<not set>	Vlan1	Down	1	<not set>
Port	Link	VLAN	IP Address																																																			
FastEthernet0/0	Up	--	172.20.0.1/16																																																			
FastEthernet0/1	Down	--	<not set>																																																			
Serial0/0/0	Down	--	<not set>																																																			
Serial0/0/1	Up	--	192.168.1.1/24																																																			
Serial0/1/0	Up	--	192.168.2.1/24																																																			
Serial0/1/1	Up	--	<not set>																																																			
Serial0/1/1.3	Up	--	192.168.3.1/24																																																			
Serial0/1/1.4	Up	--	192.168.4.1/24																																																			
Serial0/1/1.5	Up	--	192.168.5.1/24																																																			
Serial0/2/0	Down	--	<not set>																																																			
Serial0/2/1	Down	--	<not set>																																																			
Vlan1	Down	1	<not set>																																																			
Roteador	RouterEsc1	<div>Device Name: RouterEsc1</div> <div>Custom Device Model: 2811 IOS15</div> <div>Hostname: Router</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.21.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Up</td><td>--</td><td>192.168.1.2/24</td></tr><tr><td>Serial0/1/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.21.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Up	--	192.168.1.2/24	Serial0/1/0	Down	--	<not set>	Serial0/1/1	Down	--	<not set>	Vlan1	Down	1	<not set>																				
Port	Link	VLAN	IP Address																																																			
FastEthernet0/0	Up	--	172.21.0.1/16																																																			
FastEthernet0/1	Down	--	<not set>																																																			
Serial0/0/0	Down	--	<not set>																																																			
Serial0/0/1	Up	--	192.168.1.2/24																																																			
Serial0/1/0	Down	--	<not set>																																																			
Serial0/1/1	Down	--	<not set>																																																			
Vlan1	Down	1	<not set>																																																			
Roteador	RouterEsc2	<div>Device Name: RouterEsc2</div> <div>Custom Device Model: 2811 IOS15</div> <div>Hostname: Router</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.22.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/0</td><td>Up</td><td>--</td><td>192.168.2.2/24</td></tr><tr><td>Serial0/1/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.22.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Down	--	<not set>	Serial0/1/0	Up	--	192.168.2.2/24	Serial0/1/1	Down	--	<not set>	Vlan1	Down	1	<not set>																				
Port	Link	VLAN	IP Address																																																			
FastEthernet0/0	Up	--	172.22.0.1/16																																																			
FastEthernet0/1	Down	--	<not set>																																																			
Serial0/0/0	Down	--	<not set>																																																			
Serial0/0/1	Down	--	<not set>																																																			
Serial0/1/0	Up	--	192.168.2.2/24																																																			
Serial0/1/1	Down	--	<not set>																																																			
Vlan1	Down	1	<not set>																																																			

Roteador	RouterFilial1	<div>Device Name: RouterFilial1 Custom Device Model: 2811 IOS15 Hostname: RouterFilial1</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.23.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/1</td><td>Up</td><td>--</td><td>192.168.3.2/24</td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.23.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Down	--	<not set>	Serial0/1/0	Down	--	<not set>	Serial0/1/1	Up	--	192.168.3.2/24	Vlan1	Down	1	<not set>								
Port	Link	VLAN	IP Address																																							
FastEthernet0/0	Up	--	172.23.0.1/16																																							
FastEthernet0/1	Down	--	<not set>																																							
Serial0/0/0	Down	--	<not set>																																							
Serial0/0/1	Down	--	<not set>																																							
Serial0/1/0	Down	--	<not set>																																							
Serial0/1/1	Up	--	192.168.3.2/24																																							
Vlan1	Down	1	<not set>																																							
Roteador	RouterFilial2	<div>Device Name: RouterFilial2 Custom Device Model: 2811 IOS15 Hostname: RouterFilial2</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.24.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/1</td><td>Up</td><td>--</td><td>192.168.4.2/24</td></tr><tr><td>Serial0/2/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/2/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.24.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Down	--	<not set>	Serial0/1/0	Down	--	<not set>	Serial0/1/1	Up	--	192.168.4.2/24	Serial0/2/0	Down	--	<not set>	Serial0/2/1	Down	--	<not set>	Vlan1	Down	1	<not set>
Port	Link	VLAN	IP Address																																							
FastEthernet0/0	Up	--	172.24.0.1/16																																							
FastEthernet0/1	Down	--	<not set>																																							
Serial0/0/0	Down	--	<not set>																																							
Serial0/0/1	Down	--	<not set>																																							
Serial0/1/0	Down	--	<not set>																																							
Serial0/1/1	Up	--	192.168.4.2/24																																							
Serial0/2/0	Down	--	<not set>																																							
Serial0/2/1	Down	--	<not set>																																							
Vlan1	Down	1	<not set>																																							
Roteador	RouterFilial3	<div>Device Name: RouterFilial3 Custom Device Model: 2811 IOS15 Hostname: RouterFilial3</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/0</td><td>Up</td><td>--</td><td>172.25.0.1/16</td></tr><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/1/1</td><td>Up</td><td>--</td><td>192.168.5.2/24</td></tr><tr><td>Serial0/2/0</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Serial0/2/1</td><td>Down</td><td>--</td><td><not set></td></tr><tr><td>Vlan1</td><td>Down</td><td>1</td><td><not set></td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/0	Up	--	172.25.0.1/16	FastEthernet0/1	Down	--	<not set>	Serial0/0/0	Down	--	<not set>	Serial0/0/1	Down	--	<not set>	Serial0/1/0	Down	--	<not set>	Serial0/1/1	Up	--	192.168.5.2/24	Serial0/2/0	Down	--	<not set>	Serial0/2/1	Down	--	<not set>	Vlan1	Down	1	<not set>
Port	Link	VLAN	IP Address																																							
FastEthernet0/0	Up	--	172.25.0.1/16																																							
FastEthernet0/1	Down	--	<not set>																																							
Serial0/0/0	Down	--	<not set>																																							
Serial0/0/1	Down	--	<not set>																																							
Serial0/1/0	Down	--	<not set>																																							
Serial0/1/1	Up	--	192.168.5.2/24																																							
Serial0/2/0	Down	--	<not set>																																							
Serial0/2/1	Down	--	<not set>																																							
Vlan1	Down	1	<not set>																																							
Switch	SwitchMatriz	<div>Device Name: SwitchMatriz Device Model: 2950T-24 Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Up	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--																								
Port	Link	VLAN	IP Address																																							
FastEthernet0/1	Up	--	--																																							
FastEthernet0/2	Up	--	--																																							
FastEthernet0/3	Up	--	--																																							
Switch	SwitchEsc1	<div>Device Name: SwitchEsc1 Device Model: 2950T-24 Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--																								
Port	Link	VLAN	IP Address																																							
FastEthernet0/1	Down	--	--																																							
FastEthernet0/2	Up	--	--																																							
FastEthernet0/3	Up	--	--																																							
Switch	SwitchEsc2	<div>Device Name: SwitchEsc2 Device Model: 2950T-24 Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--																								
Port	Link	VLAN	IP Address																																							
FastEthernet0/1	Down	--	--																																							
FastEthernet0/2	Up	--	--																																							
FastEthernet0/3	Up	--	--																																							

Switch	SwitchFilial1	<div>Device Name: SwitchFilial1</div> <div>Device Model: 2950T-24</div> <div>Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Switch	SwitchFilial2	<div>Device Name: SwitchFilial2</div> <div>Device Model: 2950T-24</div> <div>Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Switch	SwitchFilial3	<div>Device Name: SwitchFilial3</div> <div>Device Model: 2950T-24</div> <div>Hostname: Switch</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Servidor	ServerMatriz	<div>Device Name: ServerMatriz</div> <div>Device Model: Server-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>172.20.0.2/16</td></tr></tbody></table> <div>Gateway: 172.20.0.1</div> <div>DNS Server: 172.20.0.2</div> <div>Line Number: <not set></div>	Port	Link	IP Address	FastEthernet0	Up	172.20.0.2/16										
Port	Link	IP Address																
FastEthernet0	Up	172.20.0.2/16																
Computador	PC1Matriz	<div>Device Name: PCMatriz</div> <div>Device Model: PC-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>172.20.2.11/16</td></tr><tr><td>Bluetooth</td><td>Down</td><td><not set></td></tr></tbody></table> <div>Gateway: 172.20.0.1</div> <div>DNS Server: 172.20.0.2</div> <div>Line Number: <not set></div>	Port	Link	IP Address	FastEthernet0	Up	172.20.2.11/16	Bluetooth	Down	<not set>							
Port	Link	IP Address																
FastEthernet0	Up	172.20.2.11/16																
Bluetooth	Down	<not set>																
Computador	PC2Matriz	IPv4 Address: 172.20.2.12/16 (Notação CIDR)																
Computador	PC1Esc1	<div>Device Name: PCEsc1</div> <div>Device Model: PC-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>172.21.0.11/16</td></tr><tr><td>Bluetooth</td><td>Down</td><td><not set></td></tr></tbody></table> <div>Gateway: 172.21.0.1</div> <div>DNS Server: 172.21.0.2</div> <div>Line Number: <not set></div>	Port	Link	IP Address	FastEthernet0	Up	172.21.0.11/16	Bluetooth	Down	<not set>							
Port	Link	IP Address																
FastEthernet0	Up	172.21.0.11/16																
Bluetooth	Down	<not set>																
Computador	PC2Esc1	IPv4 Address: 172.21.0.12/16 (Notação CIDR)																
Computador	PC1Esc2	<div>Device Name: PCEsc2</div> <div>Device Model: PC-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>172.22.0.11/16</td></tr><tr><td>Bluetooth</td><td>Down</td><td><not set></td></tr></tbody></table> <div>Gateway: 172.22.0.1</div> <div>DNS Server: 172.22.0.2</div> <div>Line Number: <not set></div>	Port	Link	IP Address	FastEthernet0	Up	172.22.0.11/16	Bluetooth	Down	<not set>							
Port	Link	IP Address																
FastEthernet0	Up	172.22.0.11/16																
Bluetooth	Down	<not set>																

Computador	PC2Esc2	IPv4 Address: 172.22.0.12/16 (Notação CIDR)									
Computador	PC1Filial1	Device Name: PCFilial1 Device Model: PC-PT <table> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> <tr> <td>FastEthernet0</td><td>Up</td><td>172.23.0.11/16</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td><not set></td></tr> </table> Gateway: 172.23.0.1 DNS Server: 172.23.0.2 Line Number: <not set>	Port	Link	IP Address	FastEthernet0	Up	172.23.0.11/16	Bluetooth	Down	<not set>
Port	Link	IP Address									
FastEthernet0	Up	172.23.0.11/16									
Bluetooth	Down	<not set>									
Computador	PC2Filial1	IPv4 Address: 172.23.0.12/16 (Notação CIDR)									
Computador	PC1Filial2	Device Name: PCFilial2 Device Model: PC-PT <table> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> <tr> <td>FastEthernet0</td><td>Up</td><td>172.24.0.11/16</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td><not set></td></tr> </table> Gateway: 172.24.0.1 DNS Server: 172.24.0.2 Line Number: <not set>	Port	Link	IP Address	FastEthernet0	Up	172.24.0.11/16	Bluetooth	Down	<not set>
Port	Link	IP Address									
FastEthernet0	Up	172.24.0.11/16									
Bluetooth	Down	<not set>									
Computador	PC2Filial2	IPv4 Address: 172.24.0.12/16 (Notação CIDR)									
Computador	PC1Filial3	Device Name: PCFilial3 Device Model: PC-PT <table> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> <tr> <td>FastEthernet0</td><td>Up</td><td>172.25.0.11/16</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td><not set></td></tr> </table> Gateway: 172.25.0.1 DNS Server: 172.25.0.2 Line Number: <not set>	Port	Link	IP Address	FastEthernet0	Up	172.25.0.11/16	Bluetooth	Down	<not set>
Port	Link	IP Address									
FastEthernet0	Up	172.25.0.11/16									
Bluetooth	Down	<not set>									
Computador	PC2Filial3	IPv4 Address: 172.25.0.12/16 (Notação CIDR)									

4.4 PLANILHA LINKS

A tabela abaixo contém informações correspondentes a divisão de colaboradores por cada localidade dentro da estrutura da empresa e da utilização da estrutura de rede quanto a aplicações e serviços. A matriz conta com um número abrangente de 350 colaboradores por ser a sede de produção, o escritório 1 conta com 50 colaboradores que atuam como diretoria e estratégia de negócio, escritório 2 conta com 100 colaboradores atuando em vendas e RH e as filias compartilham estruturas locais centralizadas variando entre 150 e 200 colaboradores.

APPs	LB (kbps)	Matriz		Escritório 1		Escritório 2		Filial 1		Filial 2		Filial 3	
		350		50		100		200		150		150	
		Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB
Web	100	350	35000	50	5000	100	10000	200	20000	150	15000	150	15000
E-mail	50	350	17500	50	2500	100	5000	200	10000	150	7500	150	7500
Bankline	100	20	2000	50	5000	100	10000	25	2500	15	1500	15	1500
Suporte	80	3	240	1	80	2	160	2	160	2	160	2	160
Videoconferência	500	20	10000	50	25000	100	50000	25	12500	15	7500	15	7500
ERP	50	20	1000	50	2500	100	5000	25	1250	15	750	15	750
AWS	100	350	35000	50	5000	100	10000	200	20000	150	15000	150	15000
CRM	50	23	1150	20	1000	100	5000	25	1250	15	750	15	750
Sistema Operativo	90	350	31500	0	0	0	0	150	13500	110	9900	110	9900
Sistema de Gestão de Operações	60	20	1200	20	1200	40	2400	25	1500	15	900	15	900
Sistema para Gestão de Vendas	50	0	0	10	500	45	2250	0	0	0	0	0	0
Recrutamento e Seleção e Admissão	40	0	0	10	400	15	600	0	0	0	0	0	0
Total		134590		48180		100410		82660		58960		58960	
M		E1		E2		F1		F2		F3			

Tabela de Cabeamento

5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE

5.1 IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ

Foi implementado servidor local através do Oracle VM VirtualBox contendo os seguintes recursos:

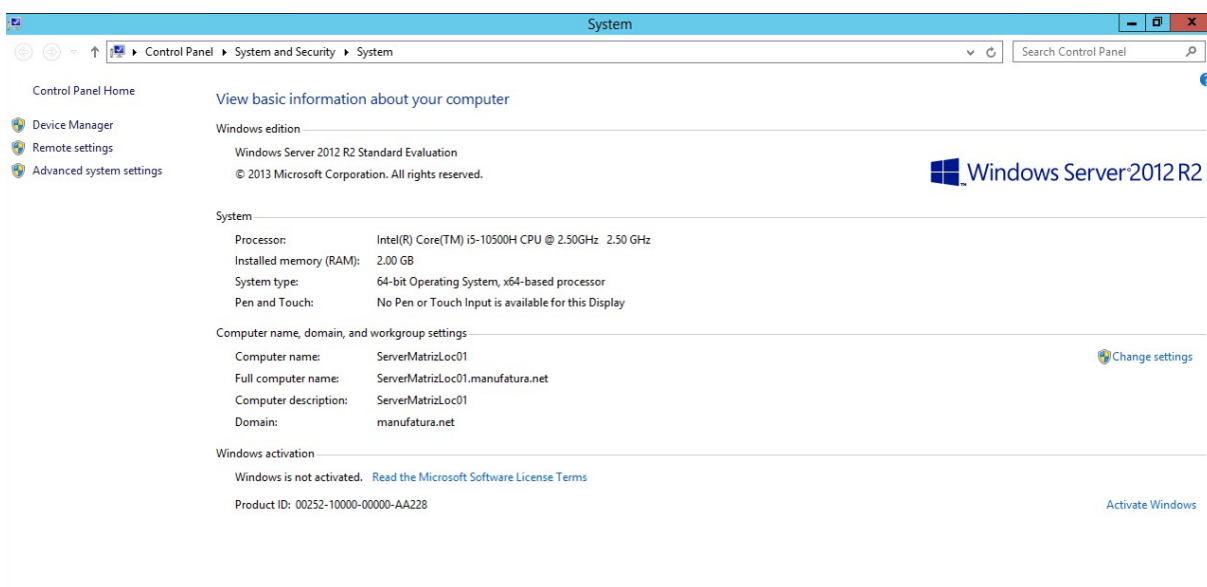
Sistema Operacional: Windows Server 2012 R2 64 bits

CPU: Intel Core I5 - 10500 h 2.50GHz 5.50GHz

Memória RAM: 2GB

Nome do servidor: ServerMatrizLoc01

Domínio: manufatura.net



Especificações do servidor local (Windows 2012). Fonte: autoria própria

Credenciais de acesso:

Usuário: Administrador

Senha: puc@1958

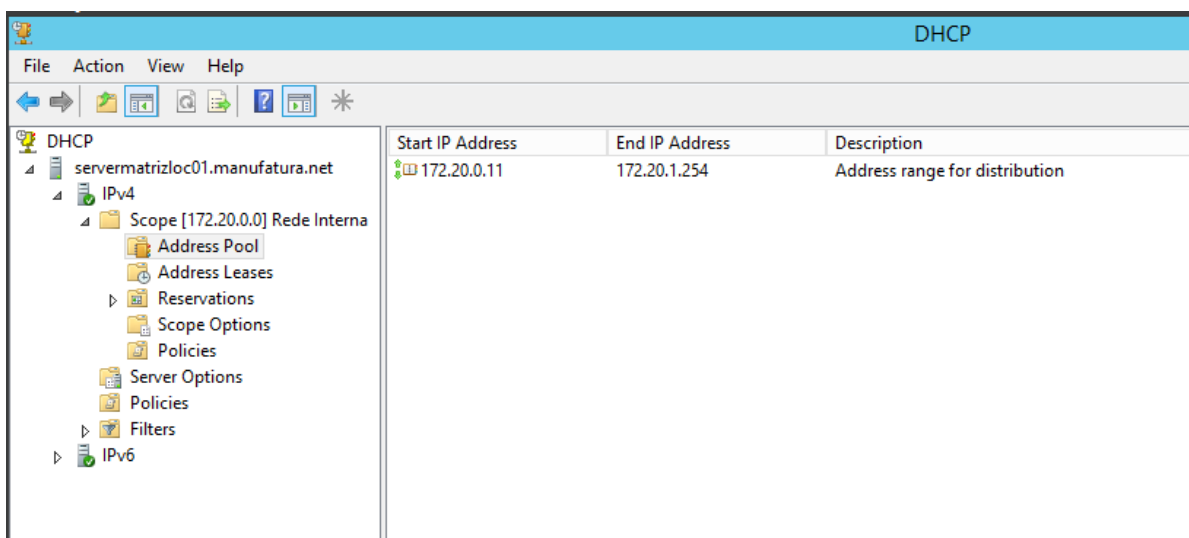
5.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP

Foi instalado e configurado o protocolo DHCP para distribuição de IP's dentro da faixa abaixo:

Faixa inicial: 172.20.0.11

Faixa final: 172.20.1.254

Desta forma poderá atender aos 350 computadores da Matriz e caso seja necessário acrescentar computadores a rede local, já será possível disponibilizar IP's para estes novos computadores.



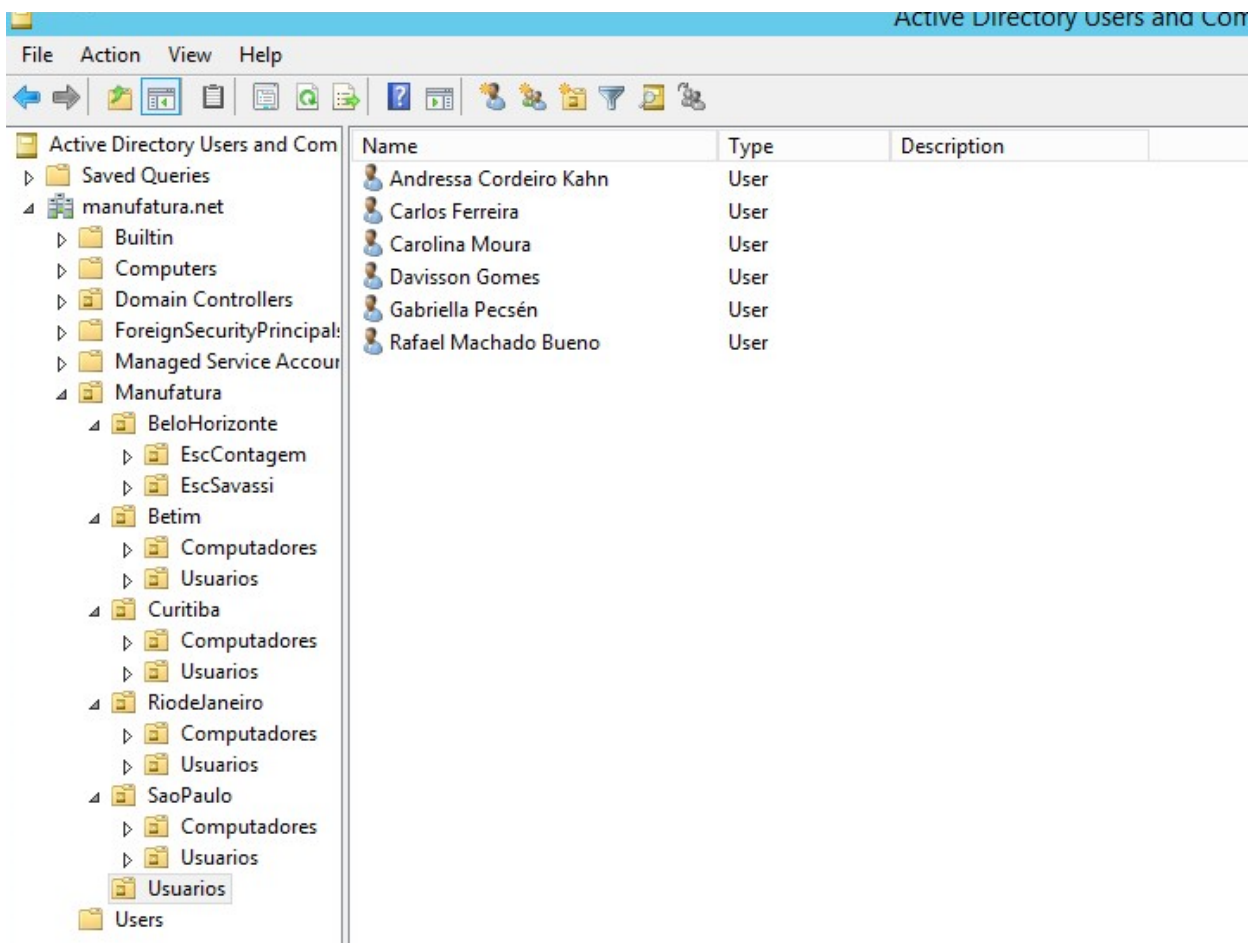
Protocolo DHCP Instalado. Fonte: autoria própria

5.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP

Foi ativado o recurso do Active Directory e configurado para o domínio manufatura.net onde foram criadas as seguintes estruturas organizacionais:

- Belo Horizonte (MG), contemplando os dois escritórios localizados em Belo Horizonte;
- Betim (MG);
- Curitiba (PR);
- Rio de Janeiro (RJ);
- São Paulo (SP).

Também foram criados usuários dentro do domínio:

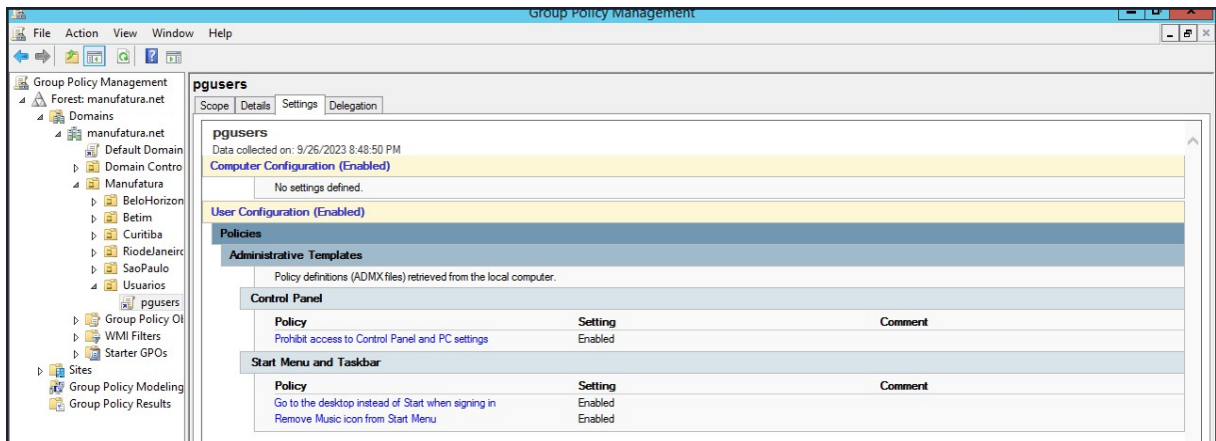


Usuários ativos. Fonte: autoria própria

5.1.3 POLÍTICAS DE GRUPO APLICADAS

Foram aplicadas as políticas abaixo:

- Proibir acesso ao Painel de Controle e Configurações do PC;
- Ir para o Desktop ao invés do Iniciar ao realizar login;
- Remover ícone de música do menu Iniciar.

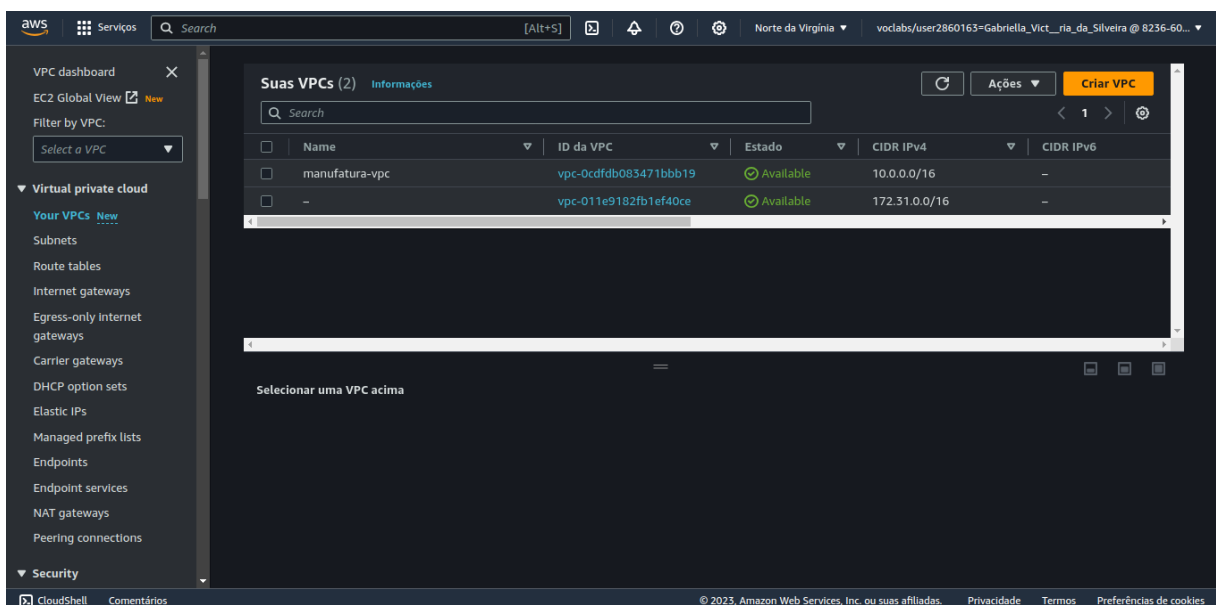


Políticas Aplicadas. Fonte: autoria própria

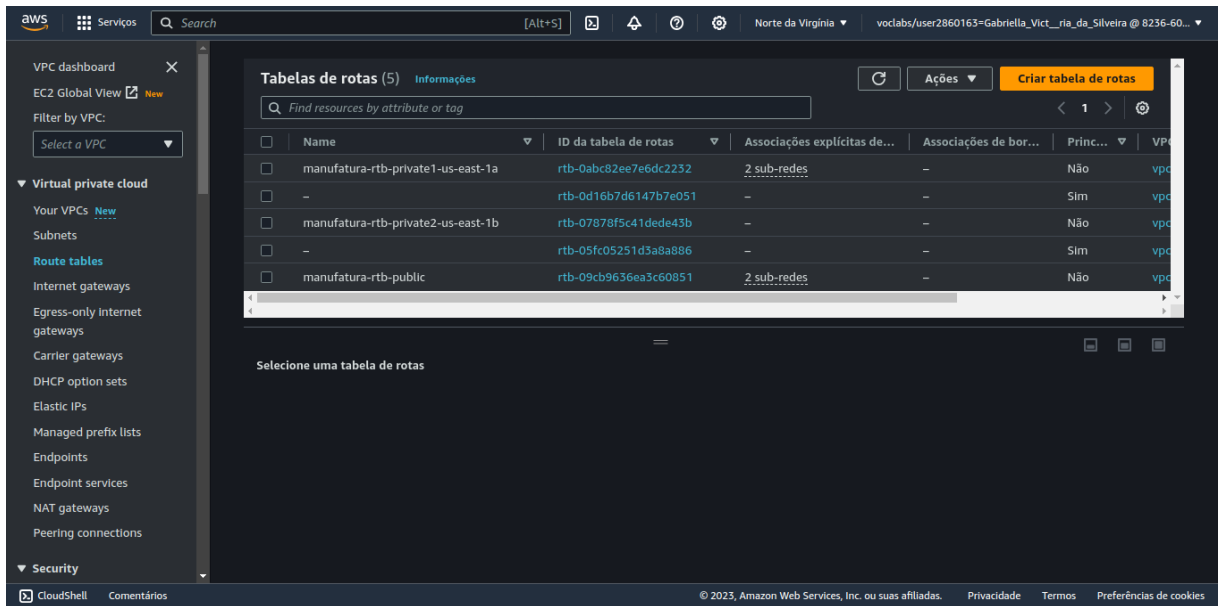
5.2 IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ

Com o objetivo de criarmos um servidor para a matriz na AWS, prestadora de serviços em nuvem, foi preciso executar os seguintes passos mostrados abaixo:

A 1ª etapa foi a criação de uma rede virtual (VPC) para a configuração dos recursos da rede. Para isso, criamos a *manufatura-vpc* com 2 subredes públicas e 2 subredes privadas em 2 zonas de disponibilidade distintas. A criação da VPC permitirá a alocação do servidor dentro da rede *manufatura-vpc* criada.

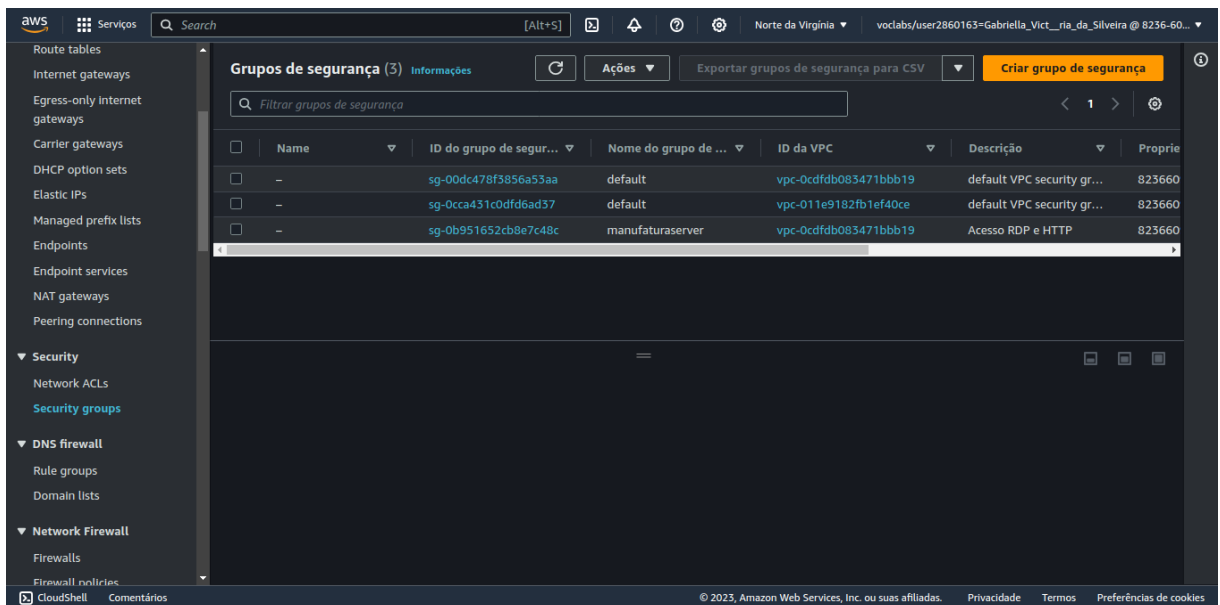


VPCs na AWS. Fonte: AWS

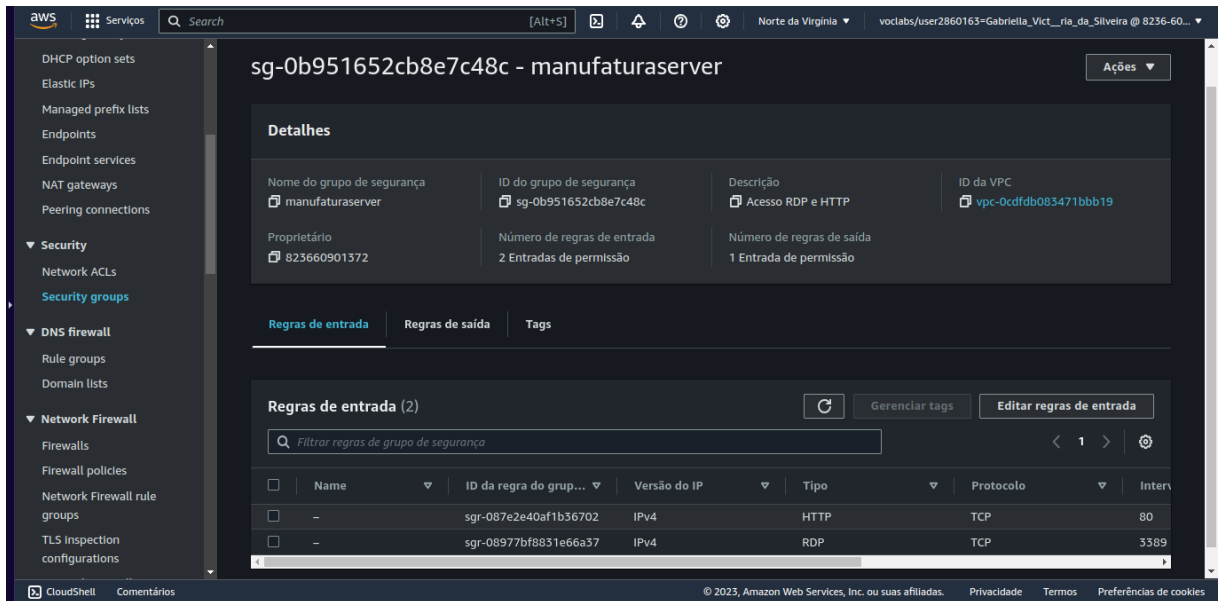


Subredes na AWS. Fonte: AWS

A 2ª etapa consistiu na criação de um grupo de segurança para atuar como um firewall de nossa rede. Criamos 2 regras de entrada: uma para permitir que qualquer endereço IPV4 pudesse acessar o servidor remotamente via RDP; outra para permitir que qualquer endereço IPV4 pudesse acessar o endereço IP de nosso servidor a partir de um navegador web com o protocolo HTTP. A imagem abaixo mostra o grupo de segurança criado e as 2 regras de entrada.

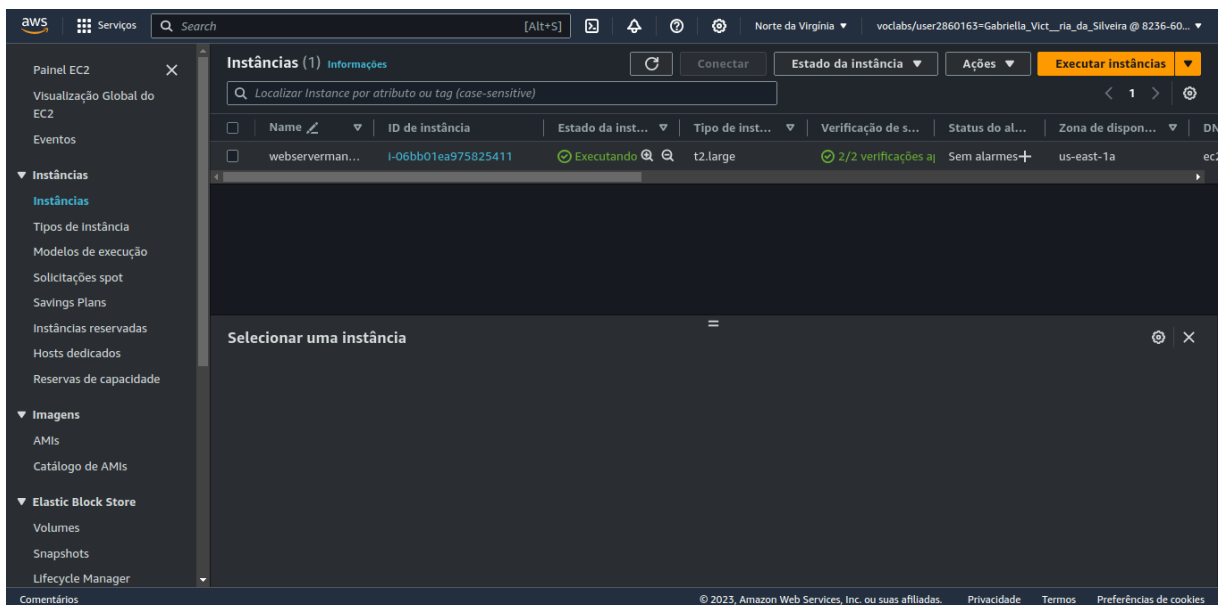


Grupos de Segurança. Fonte: AWS



Regras de Entrada do Grupo de Segurança. Fonte: AWS

A 3ª etapa foi criar uma instância na AWS para o nosso servidor. Para isso, criamos uma instância EC2 com o sistema operacional do Windows Server 2016 Base e no tipo t2.large. Esse tipo de instância possui recursos de hardware suficientes para o nosso servidor. Colocamos a instância dentro da VPC e do grupo de segurança *manufaturaserver*.



Instância do Servidor Web.

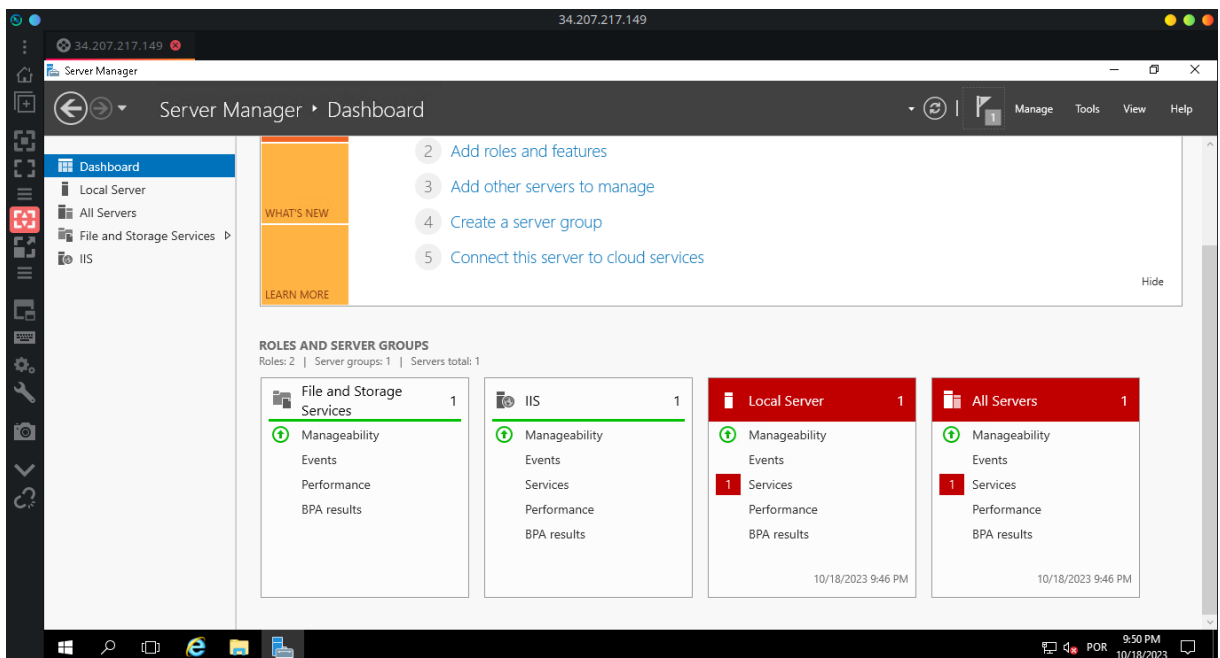
Fonte: AWS

A 4ª etapa foi para acessarmos o servidor criado via RDP e instalar o serviço de servidor web da Microsoft, o IIS. Realizamos a instalação do serviço e seguimos com a tentativa de acesso à página web de nosso servidor. As imagens abaixo mostram todo esse processo. Algumas imagens mostram IPs públicos diferentes em relação

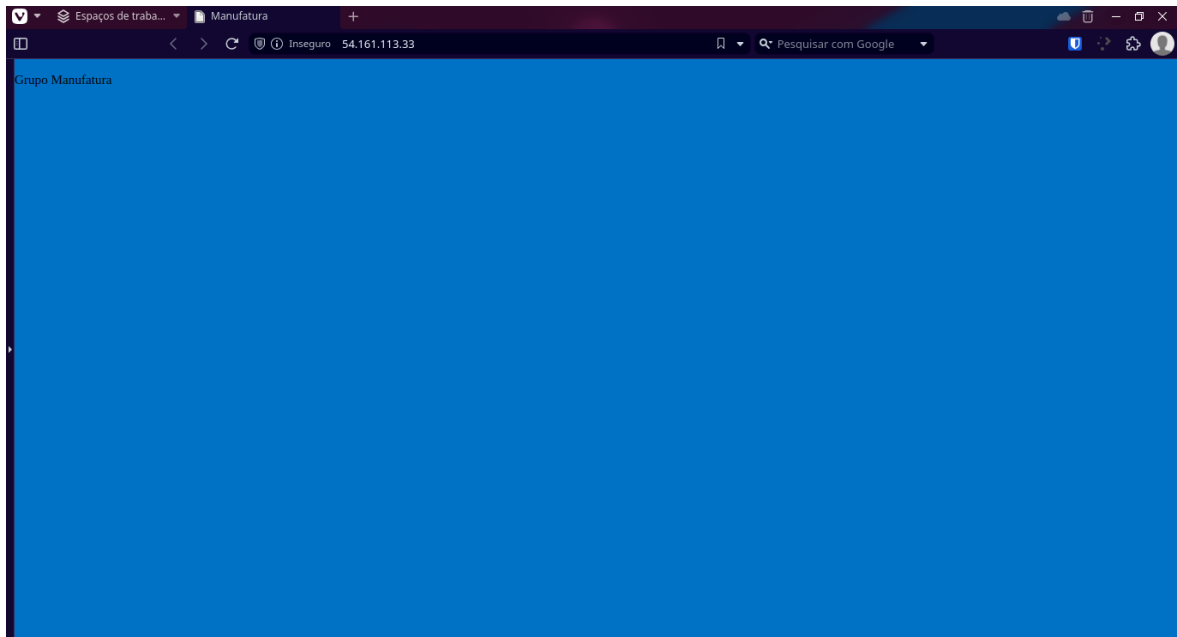
ao servidor. Isso ocorreu, pois a AWS altera o IP público do servidor após algum tempo.



Acesso via RDP ao servidor.
Fonte: autoria própria



Serviço IIS disponível no servidor.
Fonte: Autoria própria.



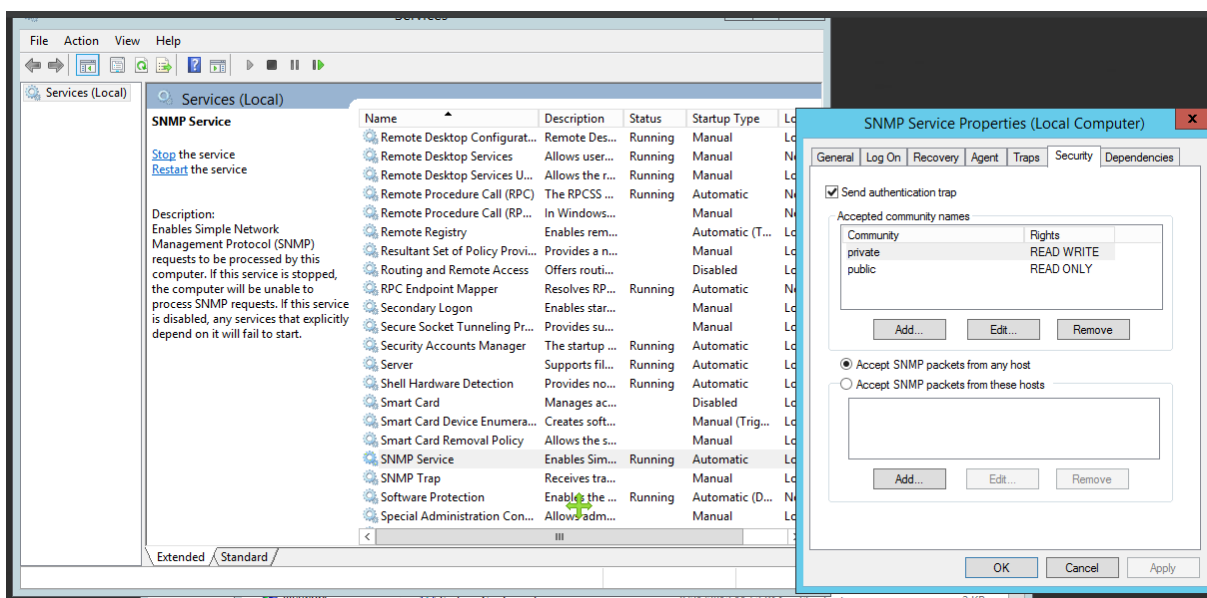
Acesso a página do servidor web pelo navegador.
Fonte: autoria própria

6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX

6.1 GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX

Para sermos capazes de realizar o monitoramento do servidor físico na rede, foi necessário realizar a integração desse servidor no zabbix, uma ferramenta de monitoramento de infraestrutura de TI. Para isso, o protocolo SNMP foi utilizado, pois ele permite o gerenciamento de dispositivos em uma rede por meio do seu IP.

Conforme a imagem mostrada abaixo, o serviço do protocolo SNMP foi configurado no servidor local em relação às suas community com duas strings: private (para acesso de leitura e escrita) e public (para acesso somente de leitura). Essas strings funcionam como chaves de acesso para a integração do servidor com o software Zabbix.

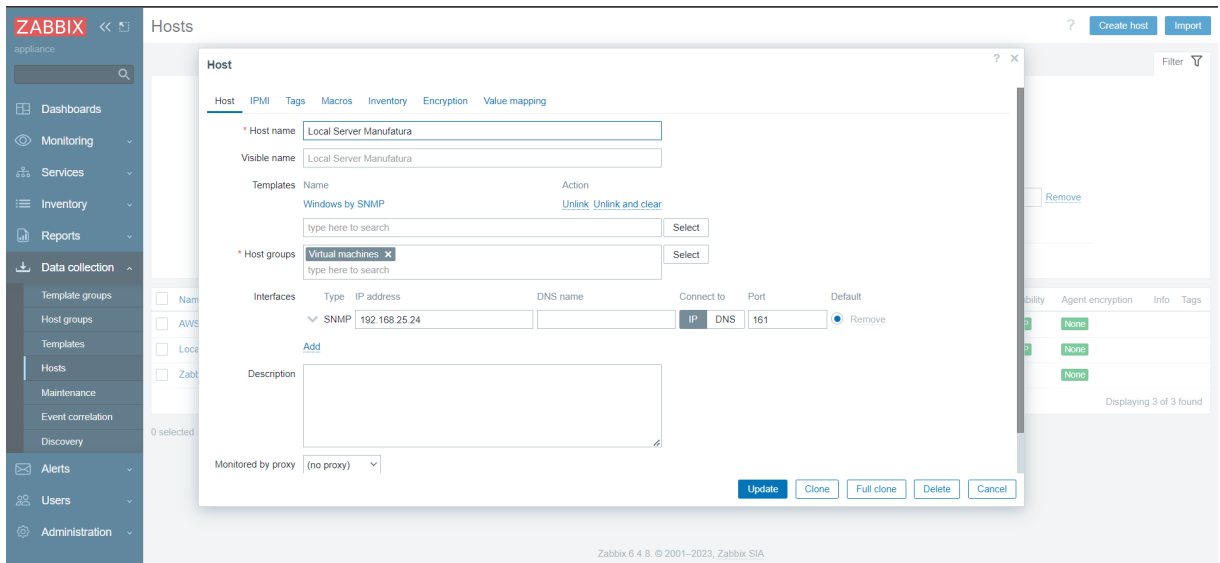


Serviço de SNMP no servidor local.

Fonte: autoria própria

Com a configuração das communities no servidor local, iniciamos o processo de configuração do host no zabbix. Para isso foi necessário o preenchimento de algumas informações na plataforma de monitoramento como o nome do host, o protocolo utilizado, seu IP, a porta, seu template e seu host group. Essas informações foram necessárias para o Zabbix ser capaz de encontrar e requisitar informações do host que desejávamos monitorar.

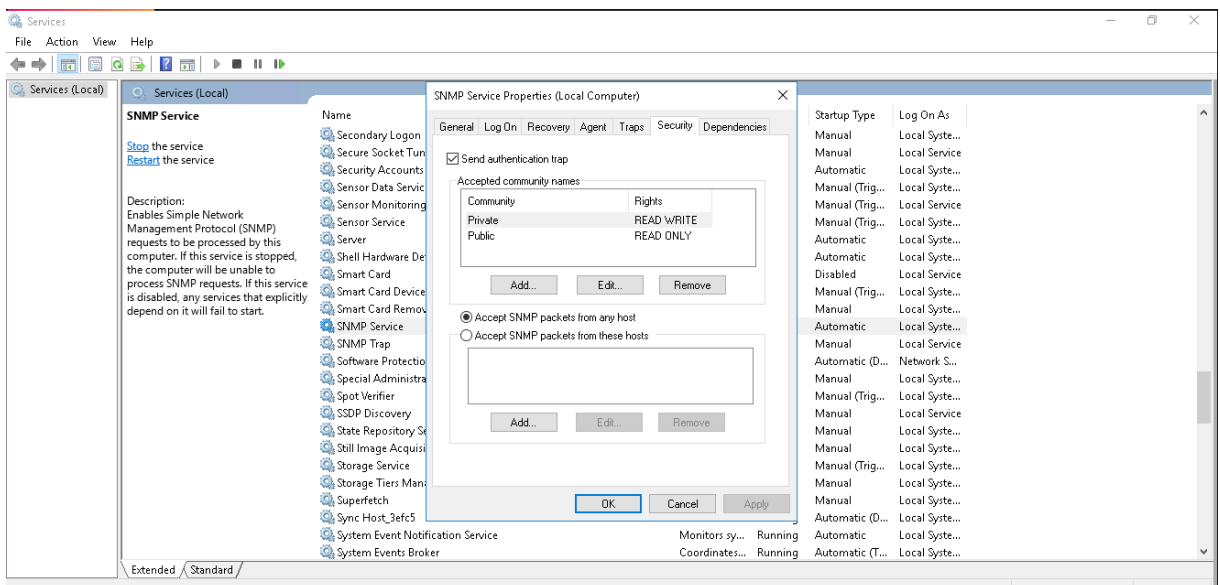
As regras de firewall no servidor local foram observadas para que o acesso do zabbix na porta 161 não fosse bloqueado. Entretanto, não encontramos qualquer impedimento nesse processo.



Adição do servidor local na plataforma Zabbix.
Fonte: autoria própria

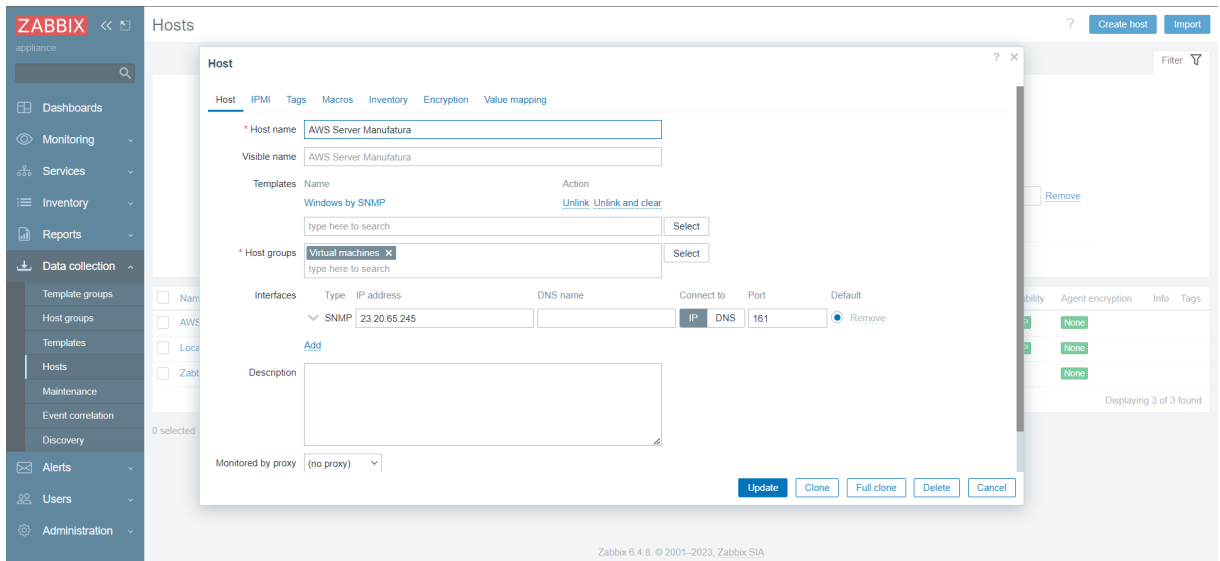
6.2 GERENCIAMENTO DO SERVIDOR DA NUVEM NO ZABBIX

A configuração do SNMP no servidor localizado em nuvem seguiu os mesmos passos do servidor local com a execução do serviço SNMP e a configuração das communities *private* e *public*.



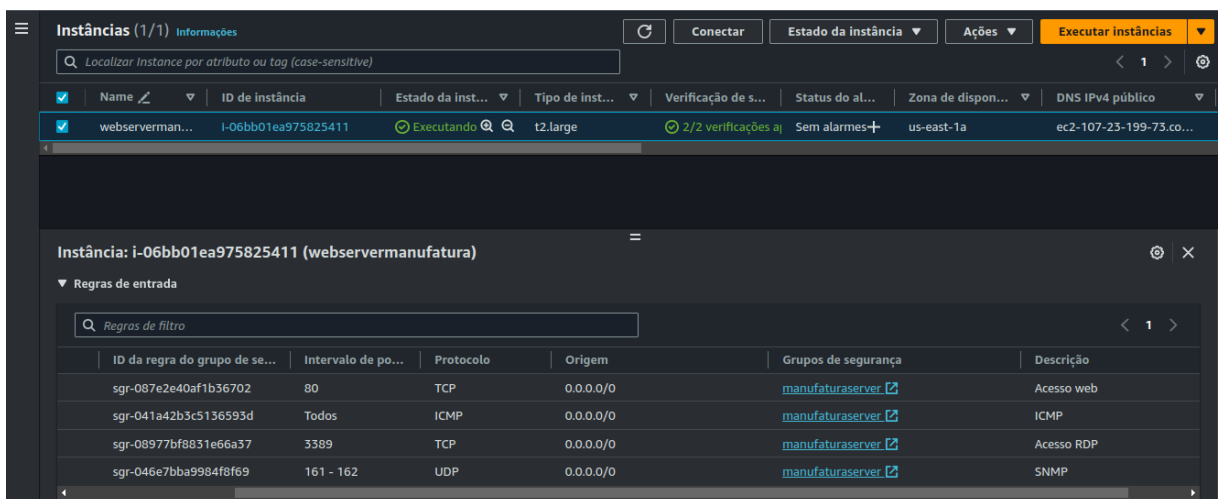
Serviço de SNMP no servidor da nuvem.
Fonte: autoria própria

A configuração do servidor localizado em nuvem no zabbix seguiu os mesmos critérios em relação ao preenchimento das suas informações na plataforma, conforme imagem abaixo.

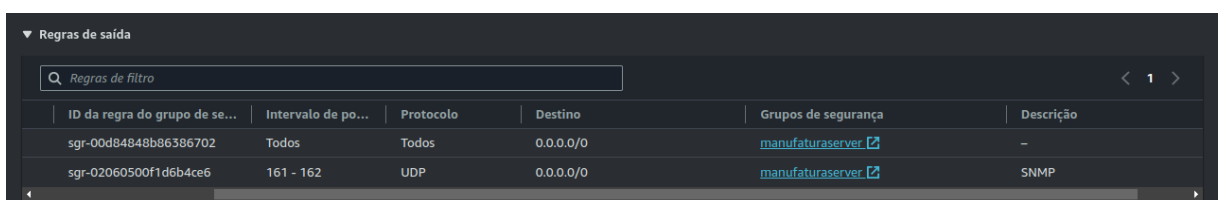


Adição de servidor da nuvem no Zabbix.
Fonte: autoria própria

A diferença consistiu na necessidade da liberação de portas no grupo de segurança criado na AWS, pois sem essa liberação não seria possível o Zabbix realizar a comunicação com o servidor na nuvem. As portas relacionadas aos protocolos SNMP e ICMP foram liberadas.



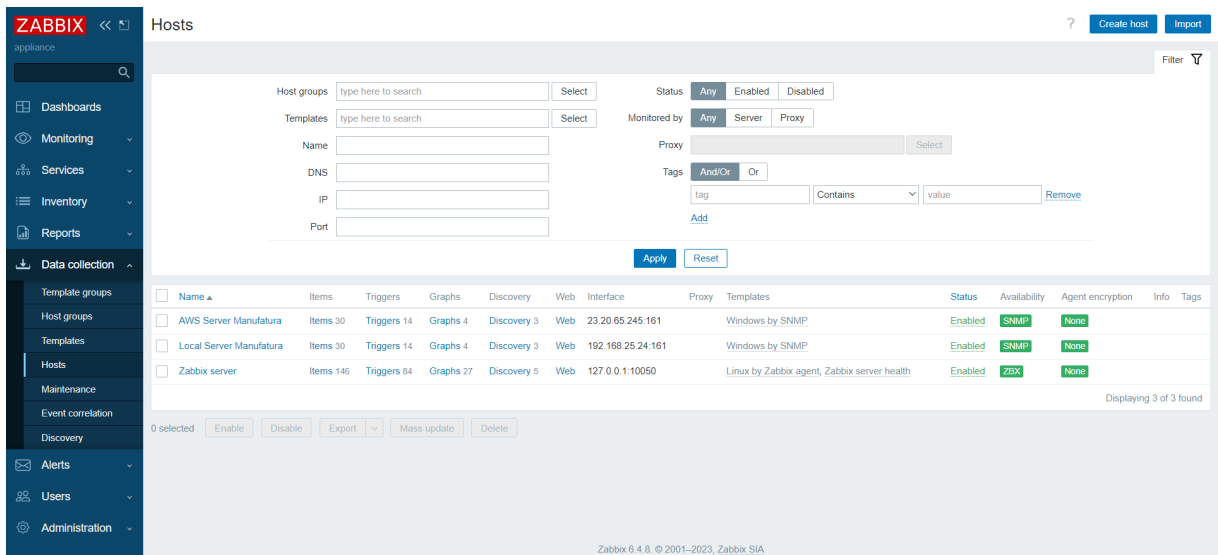
Regras de entrada no grupo de segurança da nuvem.
Fonte: Autoria própria



Regras de saída no grupo de segurança da nuvem.
Fonte: autoria própria

6.3 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX

Com a configuração realizada no servidor local e no servidor da nuvem, o Zabbix já conseguia monitorar os servidores. Verificamos na ferramenta que ambas as comunicações com os hosts estavam sendo executadas sem qualquer falha, conforme imagens abaixo.

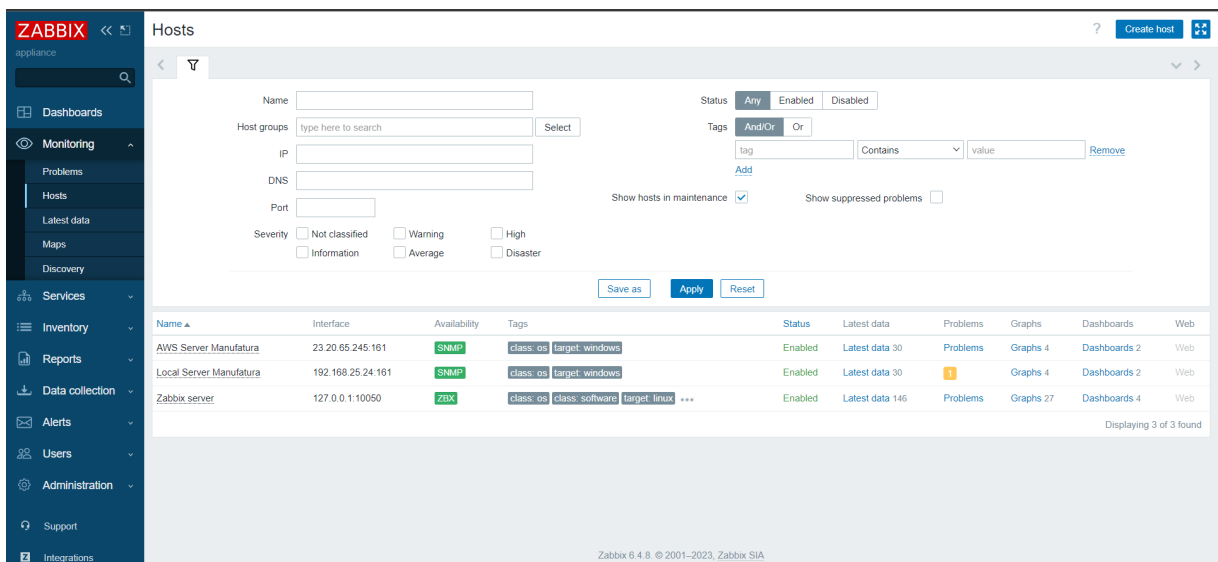


The screenshot shows the Zabbix web interface for the 'Hosts' section. The left sidebar contains navigation links: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Template groups, Host groups, Templates, Hosts, Maintenance, Event correlation, Discovery, Alerts, Users, and Administration. The main content area displays a table of hosts with columns for Name, Items, Triggers, Graphs, Discovery, Web, Interface, Proxy, Templates, Status, Availability, Agent encryption, Info, and Tags. Three hosts are listed:

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
AWS Server Manufatura	Items 30	Triggers 14	Graphs 4	Discovery 3	Web	23.20.65.245:161		Windows by SNMP	Enabled	SNMP	None		
Local Server Manufatura	Items 30	Triggers 14	Graphs 4	Discovery 3	Web	192.168.25.24:161		Windows by SNMP	Enabled	SNMP	None		
Zabbix server	Items 146	Triggers 84	Graphs 27	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None		

At the bottom of the table, it says 'Displaying 3 of 3 found'. Below the table are buttons for '0 selected', 'Enable', 'Disable', 'Export', 'Mass update', and 'Delete'.

Visualização dos hosts adicionados para coleta de dados no Zabbix.
Fonte: Autoria própria



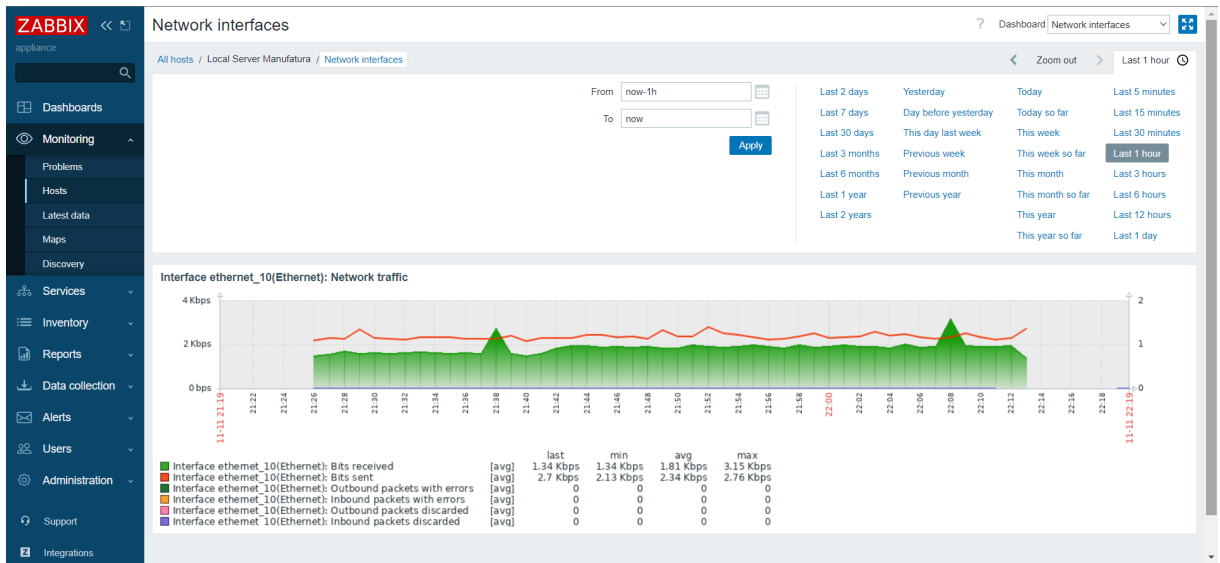
This screenshot shows the Zabbix web interface for the 'Hosts' section, displaying detailed monitoring information for the hosts. The left sidebar is the same as the previous screenshot. The main content area displays a table of hosts with columns for Name, Interface, Availability, Tags, Status, Latest data, Problems, Graphs, Dashboards, and Web. Three hosts are listed:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
AWS Server Manufatura	23.20.65.245:161	SNMP	class: os target: windows	Enabled	Latest data 30	Problems	Graphs 4	Dashboards 2	Web
Local Server Manufatura	192.168.25.24:161	SNMP	class: os target: windows	Enabled	Latest data 30	1	Graphs 4	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Enabled	Latest data 146	Problems	Graphs 27	Dashboards 4	Web

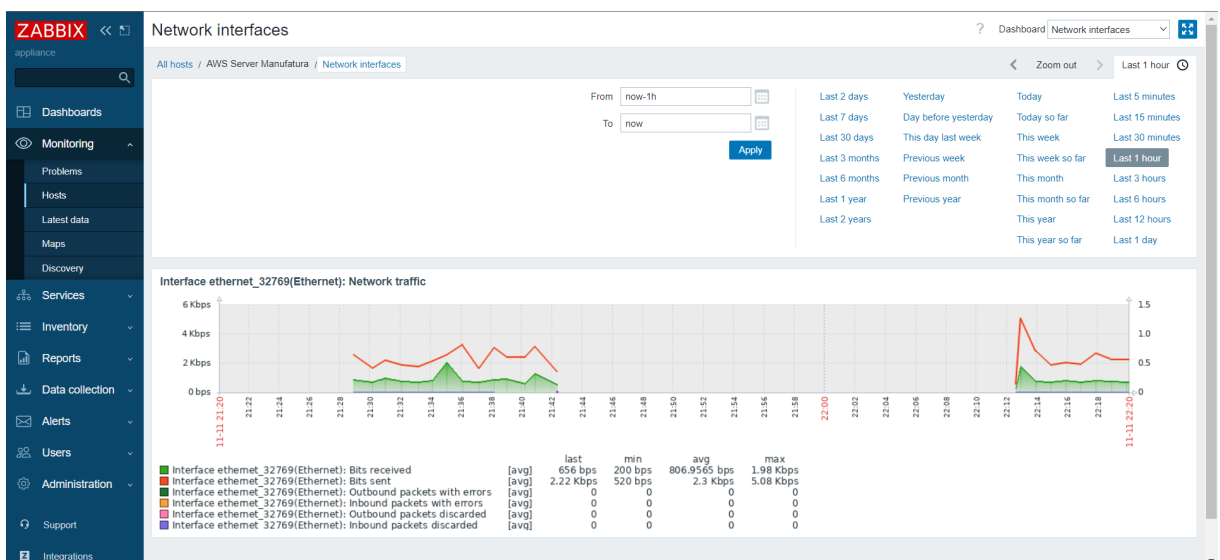
At the bottom of the table, it says 'Displaying 3 of 3 found'. Below the table are buttons for 'Save as', 'Apply', and 'Reset'.

Visualização dos hosts adicionados para monitoramento no Zabbix.
Fonte: Autoria própria

As telas abaixo mostram o resultado do monitoramento de ambos os hosts: servidor local e servidor da nuvem. Os gráficos mostram a quantidade de tráfego de rede advinda dos servidores na última hora.

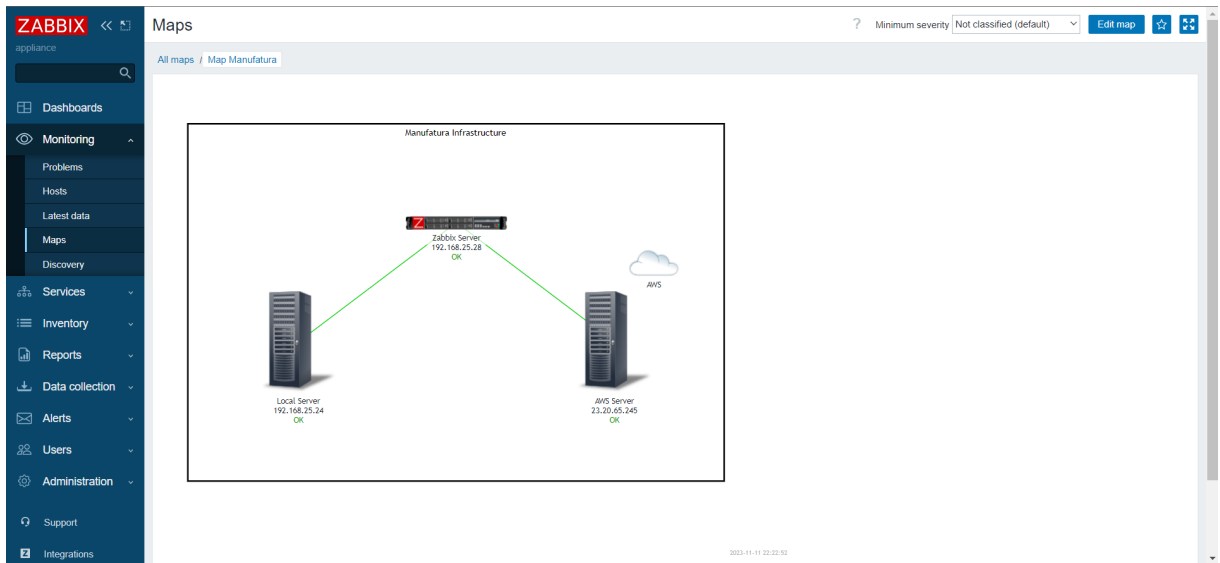


Monitoramento do tráfego de rede do servidor local no zabbix.
Fonte: Autoria própria



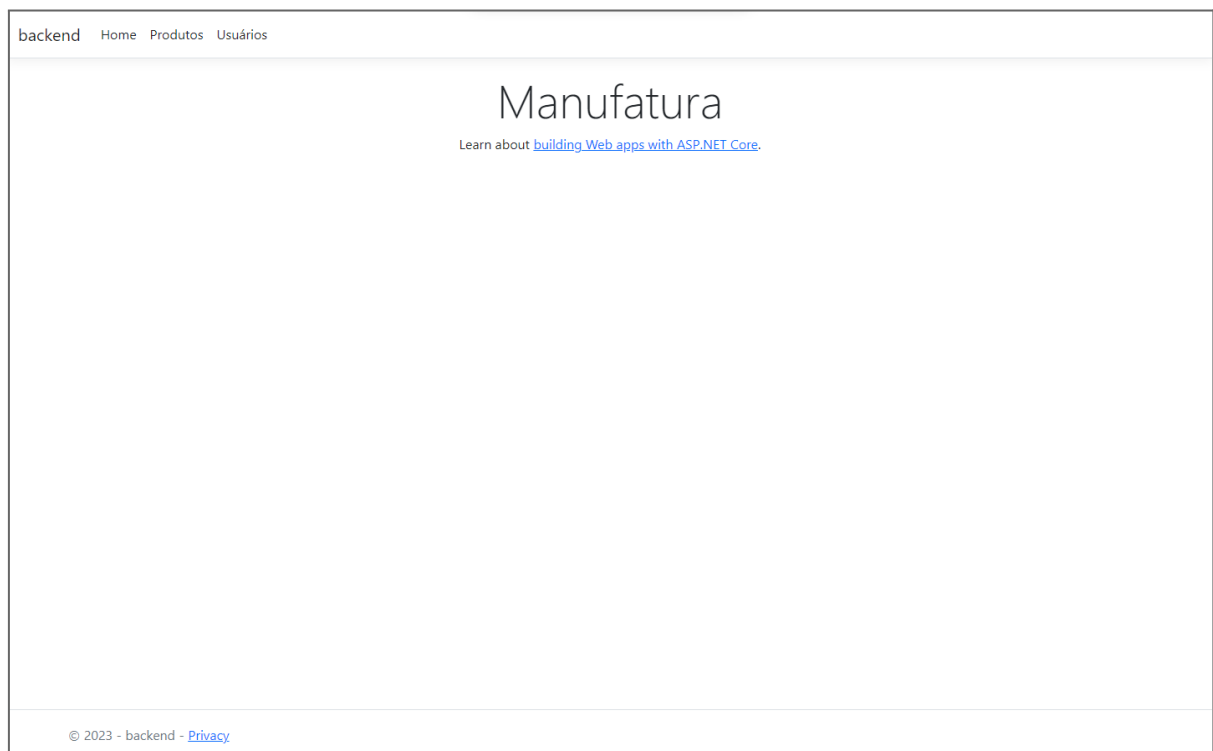
Monitoramento do tráfego de rede do servidor localizado em nuvem no Zabbix.
Fonte: Autoria própria

A plataforma Zabbix também torna possível a visualização de um mapa de nossa infraestrutura de rede que está sendo monitorada. A imagem abaixo mostra o servidor do Zabbix e sua integração com o servidor local e o servidor da nuvem.



Mapa de rede da infraestrutura que está sendo monitorada no Zabbix.
Fonte: Autoria própria

7. APLICAÇÃO BACK-END



backend Home Produtos Usuários

Lista de produtos

Adicionar novo produto

Nome	Cor	Preço	Quantidade em estoque	
Geladeira	Branca	1000,00	10	<div>EditarVisualizarApagar</div>

© 2023 - backend - [Privacy](#)

Página 02 - Lista de Produtos

backend Home Produtos Usuários

Adicionar novo produto

Produto

Nome

Cor

Preço

Quantidade em estoque

Voltar

Adicionar

© 2023 - backend - [Privacy](#)

Página 03 - Adicionar novo produto (Create)

[backend](#) [Home](#) [Produtos](#) [Usuários](#)

Dados do produto

Produto

Nome	Geladeira
Cor	Branca
Preço	1000,00
Quantidade em estoque	10

[Voltar](#) [Editar](#)

© 2023 - backend - [Privacy](#)

Página 04 - Dados do produto (Read)

[backend](#) [Home](#) [Produtos](#) [Usuários](#)

Editar dados do produto

Produto

Nome

Cor

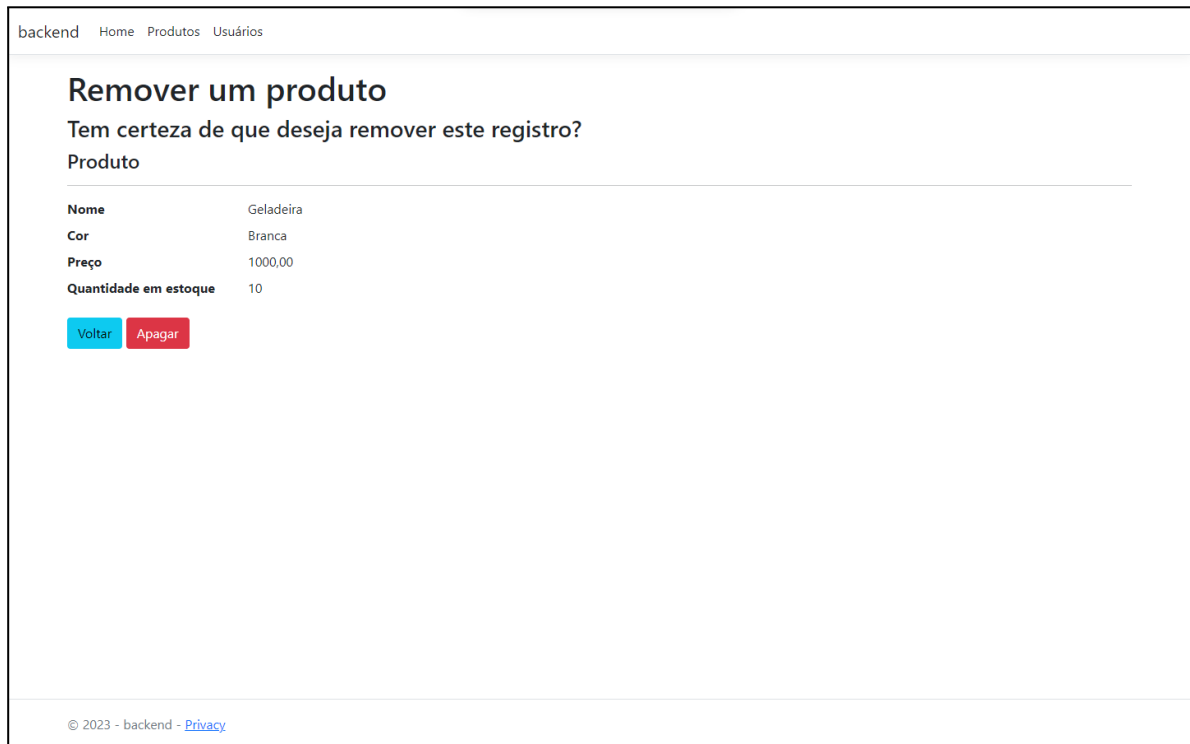
Preço

Quantidade em estoque

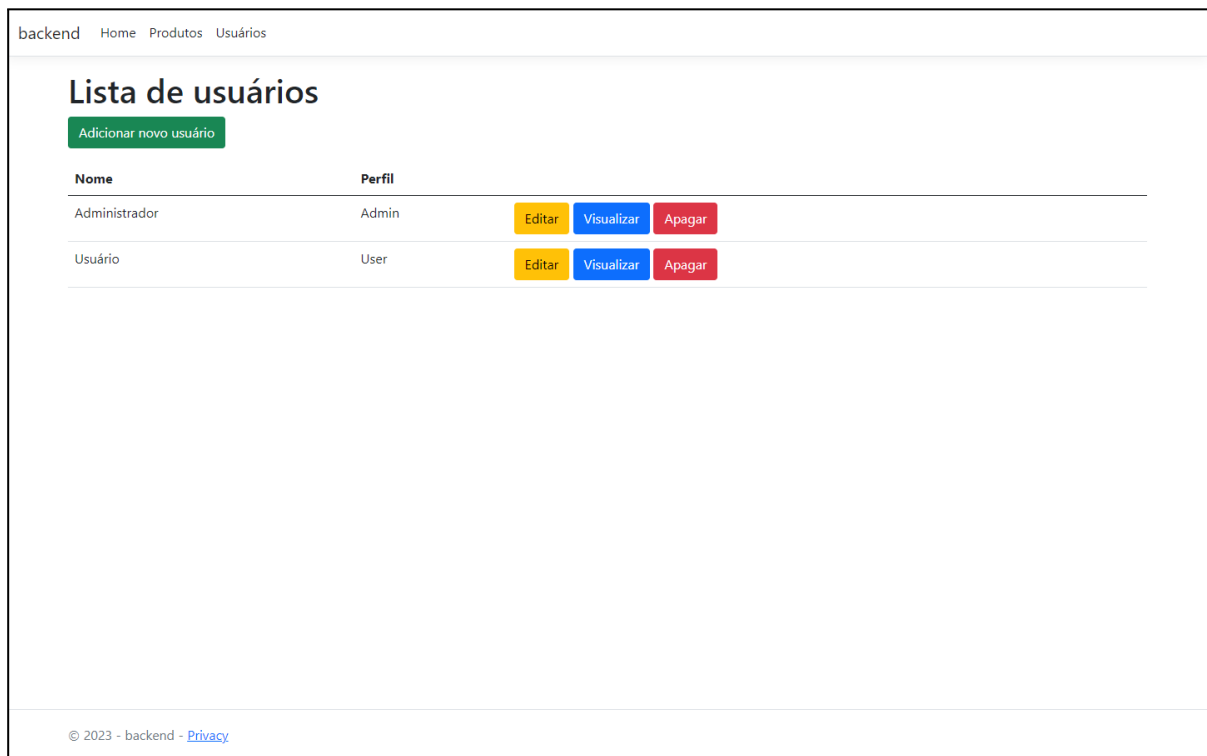
[Voltar](#) [Salvar](#)

© 2023 - backend - [Privacy](#)

Página 05 - Editar dados do produto (Update)



Página 06 - Remover um produto (Delete)



Página 07 - Lista de usuários (Users)

backend Home Produtos Usuários

Adicionar novo usuário

Usuário

Nome

Senha

Perfil

User

Voltar

Adicionar

© 2023 - backend - [Privacy](#)

Página 08 - Adicionar novo usuário (Create)

backend Home Produtos Usuários

Dados do usuário

Usuário

Nome	Usuário
Perfil	User

Voltar

Editar

© 2023 - backend - [Privacy](#)

Página 09 - Dados do usuário (Read)

backend Home Produtos Usuários

Editar dados do usuário

Usuário

Nome

Usuário

Senha

Perfil

User

Voltar

Salvar

© 2023 - backend - [Privacy](#)

Página 10 - Editar dados do usuário (Update)

backend Home Produtos Usuários

Remover um usuário

Tem certeza de que deseja remover este registro?

Usuário

Nome

Usuário

Perfil

User

Voltar

Apagar

© 2023 - backend - [Privacy](#)

Página 11 - Remover um usuário (Delete)

8. REFERÊNCIAS

PORTAL DA INDÚSTRIA. **Qual a definição de micro e pequena empresa?** Disponível em: <https://www.portaldaindustria.com.br/industria-de-a-z/micro-e-pequena-empresa/>
Acesso em: 20 agosto 2023.

OITCHAU. **Setores de uma empresa: Quais os principais? O que fazem?** Disponível em: <https://www.oitchau.com.br/blog/setores-de-uma-empresa-e-o-que-eles-fazem/>
Acesso em: 21 agosto 2023.

GERASOMA. **Conhecendo os 7 Elementos da sua empresa (parte 1)** Disponível em: <https://gerasoma.com.br/conhecendo-os-7-elementos-da-sua-empresa-parte-1/>
Acesso em: 21 agosto 2023.

Rockcontent. **Descubra os 9 melhores softwares de vendas para você implementar na sua empresa.** Disponível em: <https://rockcontent.com/br/blog/softwares-de-vendas/>
Acesso em: 21 agosto 2023.

Method. **Top 10 best manufacturing software for 2023.** Disponível em: <https://www.method.me/blog/software-for-manufacturing/>
Acesso em: 22 agosto 2023.

Tabela de Materiais - Página 10:

Estação Dell - Disponível em: [Link](#)
Roteador CISCO - Disponível em: [Link](#)
Serial CISCO - Disponível em: [Link](#)
Switch Dell 24p - Disponível em: [Link](#)
Cabo UTP CAT6 cx - Disponível em: [Link](#)
RJ45 f Cat6 - Disponível em: [Link](#)
Patch Cord CAT 6 - Disponível em: [Link](#)
Patch Panel CAT 6 - Disponível em: [Link](#)
Rack 44 U - Disponível em: [Link](#)
Cx + placa - Disponível em: [Link](#)
AP Rukus WiFi 6 - Disponível em: [Link](#)
Organizador de Cabo - Disponível em: [Link](#)
Impressora - Disponível em: [Link](#)
Nobreak - Disponível em: [Link](#)
Mesa + Cadeira - Disponível em: [Link](#)

Anexo I

Política de Segurança da Informação

Novembro de 2023

Tipo de Documento: Política	
Data de Aprovação: 20/11/2023	Revisão: Anual
Data de Efetivação: 20/11/2023	Código do Documento: PSIV001

SUMÁRIO

1. INTRODUÇÃO	1
1.1 PROPÓSITO	1
1.2 ESCOPO	2
1.3 PAPÉIS E RESPONSABILIDADES	2
2. GESTÃO DE RISCO DA INFORMAÇÃO	2
3. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES	3
4. GERENCIAMENTO DOS ATIVOS DE TI	3
5. SEGURANÇA DE PESSOAL	4
6. GERENCIAMENTO DE INCIDENTES CIBERNÉTICOS	4
7. SEGURANÇA FÍSICA E DO AMBIENTE	4
8. CONTROLE DE ACESSO E GESTÃO DE CONTAS	4
9. SEGURANÇA DE SISTEMAS	4
10. GERENCIAMENTO DE VULNERABILIDADES	4
11. CONFORMIDADE	4

1. INTRODUÇÃO

1.1 PROPÓSITO

Esta política abrange todo o conjunto de diretrizes que estabelece os parâmetros técnicos e as configurações de segurança exigidas para que os usuários e os administradores de Tecnologia da Informação (TI) implementem no ambiente. Seu objetivo é assegurar a integridade, a disponibilidade e a confidencialidade do ambiente de dados na Organização. Funciona como um documento central que requer familiaridade por parte de todos os colaboradores e contratados, definindo ações e restrições obrigatórias para todos os usuários. Além disso, oferece aos gestores de TI políticas e orientações relacionadas ao uso adequado de tecnologias, e-mails, conexões à internet e outros recursos futuros de tecnologia e processamento de informações.

Os critérios e limitações descritos nesta política abrangem infraestruturas de rede, bancos de dados, mídias externas, criptografia, relatórios impressos, filmes, apresentações, modelos, redes sem fio, comunicações, bem como todos os métodos de transmissão de conhecimento e ideias, em todos os tipos de hardware, software e sistemas de transmissão de dados. Esta política deve ser seguida por todos os colaboradores permanentes ou temporários da organização, em todas as suas localidades.

1.2 ESCOPO

Este documento de política estipula os requisitos de segurança comuns para todos os membros e sistemas da organização envolvidos na criação, manutenção, armazenamento, acesso, processamento ou transmissão de informações. Ele também se estende aos recursos de informação pertencentes a outras entidades, como os contratados da organização, nos casos em que a organização tem a obrigação legal ou contratual de proteger esses recursos enquanto estão sob sua responsabilidade. Se houver conflito, prevalecerão as medidas mais restritivas. Esta política engloba o sistema de rede da organização, que inclui diversos dispositivos de hardware, software, equipamentos de comunicação e outros dispositivos projetados para facilitar a criação, recebimento, armazenamento, processamento e transmissão de informações. Isso abarca os dispositivos conectados aos domínios ou VLANs da organização, tanto por meio de conexões físicas quanto sem fio, e abrange todos os equipamentos individuais utilizados nos escritórios ou em locais remotos pela organização.

1.3 PAPÉIS E RESPONSABILIDADES

Liderança Executiva e Gestão de SI

A alta administração é encarregada de criar uma cultura de segurança. Isso envolve fornecer recursos financeiros, estabelecer metas claras e promover a importância da segurança da informação em todos os níveis da organização. A gestão de SI, por sua vez, é responsável por implementar e manter medidas de segurança, monitorar sistemas continuamente e responder a incidentes de segurança.

Equipe de Segurança da Informação

A equipe de segurança da informação tem um papel crucial. Ela desenvolve e supervisiona a aplicação das políticas de segurança. Além disso, atua como ponto focal para questões e decisões relacionadas à segurança da informação, assegurando a conformidade e a atualização contínua das medidas de proteção.

Colaboradores

Todos os colaboradores têm um papel a desempenhar. Eles devem seguir as políticas e procedimentos de segurança estabelecidos, participar de treinamentos regulares e reportar quaisquer incidentes de segurança que observarem. O RH garante que os novos colaboradores recebam o treinamento necessário durante a integração e promovam campanhas de conscientização para toda a empresa.

2. GESTÃO DE RISCO DA INFORMAÇÃO

- a. Todo sistema ou processo que suporta operações empresariais precisa ser cuidadosamente gerenciado em relação aos riscos de informação e passar por avaliações de risco de informação, pelo menos uma vez ao ano, como parte do ciclo de vida seguro do desenvolvimento do sistema.
- b. Avaliações de risco de segurança da informação são exigidas para novos projetos, implementações de tecnologias novas, mudanças significativas no ambiente de operação, ou diante da descoberta de uma vulnerabilidade importante.
- c. As entidades têm a responsabilidade de escolher a abordagem de avaliação de risco que melhor se adapte às suas necessidades, considerando também as leis, regulamentações e políticas aplicáveis.
- d. É imprescindível documentar os resultados das avaliações de risco, assim como as decisões tomadas com base nesses resultados.

3. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

- a. Toda informação criada, adquirida ou utilizada para apoiar atividades empresariais deve ser exclusivamente empregada para seus propósitos comerciais previstos.
- b. Todos os ativos de informação devem ter um responsável pela informação estabelecida dentro das áreas de negócio.
- c. A informação deve ser adequadamente gerenciada desde sua criação, através do uso autorizado, até sua disposição adequada.
- d. Toda informação deve ser classificada continuamente com base em suas características de confidencialidade, integridade e disponibilidade.
- e. Um ativo de informação deve ser classificado com base no nível mais elevado exigido por seus elementos de dados individuais.
- f. Se a entidade não puder determinar a classificação de confidencialidade da informação ou se a informação for de identificação pessoal (IIP), a informação deve ter uma classificação de confidencialidade elevada e, portanto, estará sujeita a controles rigorosos de confidencialidade.
- g. Todas as reproduções de informação na íntegra devem ter a mesma classificação de confidencialidade que o original. Reproduções parciais precisam ser avaliadas para determinar se uma nova classificação é justificada.
- h. Cada classificação possui um conjunto aprovado de controles básicos projetados para proteger essas classificações, e esses controles devem ser seguidos.
- i. A entidade deve comunicar os requisitos para o manuseio seguro da informação à sua força de trabalho.
- j. Deve ser mantido um inventário escrito ou eletrônico de todos os ativos de informação.
- k. O conteúdo disponibilizado ao público em geral deve ser revisado de acordo com um processo que será definido e aprovado pela entidade. O processo deve incluir a revisão e aprovação das atualizações do conteúdo disponibilizado publicamente e deve considerar o tipo e classificação das informações postadas.
- l. IIP não deve ser disponibilizado sem salvaguardas apropriadas aprovadas pela entidade.
- m. Para que informações não públicas sejam divulgadas fora da entidade ou compartilhadas entre outras entidades, um processo de segurança deve ser estabelecido.

4. GERENCIAMENTO DOS ATIVOS DE TI

- a. Todos os ativos de hardware e software de TI devem ser atribuídos a uma unidade de negócios designada ou indivíduo específico.
- b. As entidades devem manter um inventário dos ativos de hardware e software, incluindo todos os componentes do sistema (por exemplo, endereço de rede, nome da máquina, versão do software) em um nível de detalhe considerado necessário para rastreamento e relatórios. Este inventário deve ser automatizado quando tecnicamente viável.
- c. Processos, incluindo varreduras regulares, devem ser implementados para identificar hardware e/ou software não autorizados e notificar o pessoal apropriado quando descobertos.

5. SEGURANÇA DE PESSOAL

- a. Todos os funcionários devem passar por treinamento geral de conscientização em segurança, incluindo reconhecimento e relato de ameaças internas, dentro de 40 dias após a contratação. Treinamentos adicionais sobre procedimentos de segurança específicos, se necessários, devem ser concluídos antes que o acesso seja concedido a informações sensíveis da entidade que não estão cobertas no treinamento geral de segurança. Todo treinamento de segurança deve ser reforçado pelo menos anualmente e deve ser rastreado pela entidade.
- b. A entidade deve exigir que sua força de trabalho siga a Política de Uso Aceitável de Recursos de Tecnologia da Informação, e um processo auditável deve estar em vigor para os usuários reconhecerem que concordam em seguir os requisitos da política.
- c. Todas as posições de trabalho devem ser avaliadas pela entidade para determinar se exigem acesso a informações sensíveis e/ou ativos de tecnologia de informação sensíveis.
- d. As entidades são responsáveis por garantir que todo o patrimônio emitido seja devolvido antes da separação de um funcionário e que as contas sejam desativadas e o acesso removido imediatamente após a separação.

6. GERENCIAMENTO DE INCIDENTES CIBERNÉTICOS

A Política de Gerenciamento de Incidentes Cibernéticos na organização é um guia detalhado que estabelece regras específicas e passos a serem seguidos para garantir a segurança da informação em todos os níveis da organização.

1. Responsabilidades e Regras para Usuários e Administradores de TI:

- a) Todos os colaboradores e contratados devem estar plenamente familiarizados com as regras estabelecidas nesta política.
- b) Administradores de TI têm a responsabilidade de implementar e monitorar as configurações de segurança exigidas.
- c) Colaboradores devem participar de treinamentos anuais de conscientização em segurança cibernética, garantindo que estejam atualizados sobre as últimas ameaças.
- d) Administradores de TI são responsáveis por realizar auditorias regulares nos acessos do usuário para identificar atividades suspeitas.

2. Ações e Restrições Obrigatórias:

- a) Definição clara de ações imediatas em caso de incidentes cibernéticos.
- b) Restrições explícitas sobre práticas não autorizadas que possam comprometer a segurança.
- c) Em caso de perda de dispositivos móveis contendo informações corporativas, os usuários devem relatar imediatamente à equipe de segurança e seguir os procedimentos de bloqueio remoto.

3. Cobertura Abrangente:

- a) Infraestruturas de rede, bancos de dados, mídias externas, criptografia, relatórios impressos, filmes, apresentações, modelos, redes sem fio e comunicações estão incluídos.
- b) Todos os métodos de transmissão de conhecimento e ideias, em hardware, software e sistemas de transmissão de dados, são abrangidos.
- c) Todas as transmissões de dados confidenciais através de meios eletrônicos devem ser criptografadas, incluindo comunicações por e-mail e transferências de arquivos.

4. Aplicação Universal:

- a) A política se aplica a todos os colaboradores, independentemente da posição ou tipo de emprego, permanentes ou temporários, e em todas as localidades da organização.
- b) Durante o processo de integração, novos colaboradores devem passar por uma sessão de treinamento específica sobre a Política de Gerenciamento de Incidentes Cibernéticos antes de obterem acesso aos sistemas.

5. Proteção de Recursos de Informação de Terceiros:

- a) Quando a organização tem a obrigação legal ou contratual, esta política se estende à proteção de recursos de informação pertencentes a outras entidades, como contratados.
- b) Contratados externos devem aderir às mesmas práticas de segurança cibernética que os funcionários internos durante o período em que colaboram com a organização.

6. Sistema de Rede:

- a) Todos os dispositivos de hardware, software e equipamentos de comunicação no sistema de rede da [Nome da Empresa] são cobertos.
- b) Inclui dispositivos conectados aos domínios ou VLANs da empresa, tanto por meio de conexões físicas quanto sem fio.
- c) Dispositivos conectados à rede devem ser configurados para monitorar automaticamente atividades incomuns e gerar alertas à equipe de segurança.

Procedimentos para Lidar com Incidentes Cibernéticos:

Identificação:

- a) Detectar e relatar qualquer atividade suspeita imediatamente;
- b) Utilizar softwares de detecção de ameaças para identificar padrões de atividade suspeita nos logs do sistema.

Análise e Avaliação:

- a) Avaliar a gravidade do incidente e seu impacto nos dados e operações;
- b) Classificar a gravidade do incidente com base em uma matriz de risco que leve em consideração o potencial impacto nos dados e operações.

Contenção e Mitigação:

- a) Isolar o incidente para evitar danos adicionais e implementar medidas para minimizar os impactos.

Erradicação:

- a) Eliminar completamente a ameaça e restaurar os sistemas afetados.

Recuperação:

- a) Restaurar completamente os sistemas e dados afetados para o estado normal de operação.

Análise Pós-Incidente:

- a) Realizar uma análise detalhada do incidente para aprender com a experiência e melhorar a postura de segurança.

7. SEGURANÇA FÍSICA E DO AMBIENTE

A Política de Segurança Física e Ambiental foi desenvolvida com diretrizes específicas e regras detalhadas para garantir a proteção integral dos ativos e informações da organização.

1. Segurança do Ambiente Físico:

- a) Controle de Acesso: O acesso físico a instalações críticas é restrito com base na necessidade de conhecimento. Utilizar cartões de acesso e sistemas biométricos para autenticação.
- b) Monitoramento 24/7: Câmeras de vigilância são instaladas para monitoramento contínuo de áreas sensíveis, com gravação de dados por no mínimo 30 dias.

2. Proteção de Mídias e Documentos Físicos:

- a) Armazenamento Seguro: Documentos físicos contendo informações sensíveis são armazenados em salas cofre com acesso restrito, equipadas com sistemas de extinção de incêndio.
- b) Criptografia de Mídias Externas: Todas as mídias externas que armazenam dados sensíveis são criptografadas antes de serem removidas das instalações.

3. Infraestruturas de Rede e Dispositivos:

- a) Segurança em Redes Sem Fio: Redes sem fio são protegidas com WPA3 e autenticação de dois fatores para dispositivos conectados.
- b) Auditorias Regulares: Realizar auditorias mensais nos dispositivos conectados à rede para identificar e corrigir possíveis vulnerabilidades.

4. Ambientes Remotos:

- a) Requisitos para Equipamentos Pessoais: Colaboradores remotos são obrigados a utilizar apenas dispositivos aprovados pela organização, com software antivírus e firewalls atualizados.

- b) VPN Obrigatória: Toda conexão remota à rede da organização deve ser feita por meio de uma VPN segura.

5. Responsabilidades e Regras para Colaboradores:

- a) Treinamento Anual: Todos os colaboradores participam de treinamentos anuais que abordam procedimentos de segurança física e ambiental, incluindo simulações de evacuação.
- b) Relato Imediato de Incidentes: Incidentes ou comportamentos suspeitos devem ser relatados imediatamente ao departamento de segurança, incentivando uma cultura de vigilância.

6. Proteção de Recursos de Informação de Terceiros:

- a) Avaliação Contínua: Recursos de informação de terceiros sob nossa responsabilidade são submetidos a avaliações regulares para garantir a conformidade com os padrões de segurança.

7. Procedimentos em Caso de Incidentes:

7.1. Evacuação Segura

- a) Em caso de ameaça iminente, todos os colaboradores devem seguir rotas de evacuação pré-determinadas para garantir a segurança física.

7.2. Resposta a Desastres Naturais:

- a) Em caso de desastres naturais, como terremotos ou incêndios, colaboradores devem seguir protocolos específicos para minimizar riscos e proteger a integridade física.

8. CONTROLE DE ACESSO E GESTÃO DE CONTAS

Esta política oferece diretrizes específicas para o controle de acesso e gestão de contas no ambiente de Tecnologia da Informação (TI) da organização, com o objetivo claro de preservar a integridade, disponibilidade e confidencialidade dos dados.

1. Objetivo e Alcance:

- a) Objetivo Principal: Garantir a integridade, disponibilidade e confidencialidade dos dados, com foco explícito na proteção dos sistemas de TI contra acessos não autorizados.
- b) Abrangência: Aplica-se a todos os colaboradores permanentes e temporários da organização em todas as localidades, enfatizando a responsabilidade individual na manutenção da segurança da informação.

2. Critérios e Limitações:

a) Infraestrutura de Rede: Inclui configurações detalhadas para dispositivos de rede, como firewalls e roteadores, com exemplos práticos de como configurar permissões de acesso e bloquear tráfego não autorizado.

b) Bancos de Dados: Estabelece diretrizes específicas para controle de acesso a bancos de dados, com exemplos de permissões de usuário e restrições de consulta para garantir a segurança dos dados sensíveis.

a) Mídias Externas: Define restrições claras sobre o uso de dispositivos de armazenamento externo, como pen drives, com exemplos de políticas para evitar a transferência não autorizada de dados confidenciais.

3. Criptografia: Detalha a implementação de criptografia, com exemplos de algoritmos e chaves, ilustrando como proteger comunicações e armazenamento de dados sensíveis.

4. Relatórios Impressos, Filmes e Apresentações: Fornece diretrizes específicas para a criação e distribuição segura de relatórios impressos e multimídia, com exemplos de práticas recomendadas.

5. Redes Sem Fio: Estipula parâmetros de segurança para redes Wi-Fi, com exemplos de configurações de autenticação e criptografia para proteger contra acessos não autorizados.

6. Comunicações: Oferece diretrizes específicas sobre o uso seguro de e-mails, mensagens instantâneas e outras formas de comunicação, com exemplos de como identificar e evitar ameaças cibernéticas.

7. Hardware, Software e Sistemas de Transmissão de Dados: Estabelece restrições detalhadas e práticas de segurança específicas, com exemplos de configurações para proteger contra vulnerabilidades e ataques.

8. Responsabilidades:

a) Colaboradores e Contratados: Esclarece a responsabilidade de todos em seguir as normas, com exemplos de como relatar atividades suspeitas e proteger suas credenciais de acesso.

b) Gestores de TI: Detalha o papel dos gestores na implementação e monitoramento das políticas, com exemplos de auditorias regulares e treinamentos de conscientização.

9. Recursos de Informação de Terceiros:

a) Explica como esta política se aplica aos recursos de informação de terceiros, com exemplos de contratos e acordos para garantir a proteção desses recursos.

10. Conflitos e Medidas Restritivas:

a) Oferece exemplos de situações de conflito e destaca como as medidas mais restritivas são aplicadas para assegurar a proteção máxima dos dados.

11. Sistema de Rede Organizacional:

a) Detalha todos os dispositivos de hardware, software e equipamentos de comunicação, com exemplos de como configurar firewalls e sistemas de detecção de intrusões para proteger contra ameaças.

b) Inclui exemplos específicos de dispositivos conectados fisicamente e sem fio, abrangendo escritórios e locais remotos da organização.

Esta política, quando seguida rigorosamente, é essencial para manter a segurança da informação. Revisões periódicas são recomendadas para garantir a eficácia contínua, e o não cumprimento das diretrizes pode resultar em medidas disciplinares, incluindo a revogação de privilégios de acesso.

9. SEGURANÇA DE SISTEMAS

Esta política oferece um conjunto de diretrizes e práticas específicas destinadas a proteger os sistemas de informação da organização assegurando a robustez e a confiabilidade dos sistemas utilizados, garantindo a proteção adequada contra ameaças internas e externas.

1. Controle de Acesso:

a) Todos os usuários terão acesso apenas às informações e recursos necessários para desempenhar suas funções.

b) O controle de acesso será baseado no princípio do menor privilégio, limitando o acesso conforme a necessidade.

2. Monitoramento e Auditoria:

a) Implementação de sistemas de monitoramento contínuo para identificar atividades suspeitas, como acessos não autorizados.

b) Auditorias regulares serão conduzidas para avaliar a eficácia dos controles de segurança, garantindo a conformidade e a detecção precoce de possíveis ameaças.

3. Proteção contra Malware:

a) Utilização de software antivírus atualizado em todos os sistemas para prevenir e detectar a presença de malware.

b) Restrição de instalação de software não autorizado para mitigar potenciais vetores de infecção.

10. GERENCIAMENTO DE VULNERABILIDADES

O gerenciamento de vulnerabilidades é um componente crítico dentro da Política de Segurança da Informação (PSI) que visa identificar, avaliar e mitigar as vulnerabilidades nos sistemas e na infraestrutura de uma organização.

1. Análise de Vulnerabilidades:

a) Realização de análises regulares de vulnerabilidades em sistemas e aplicativos.

b) Priorização e correção de vulnerabilidades identificadas de acordo com o risco associado.

2. Patch Management:

a) Implementação de um processo de gerenciamento de patches para garantir que todos os sistemas estejam atualizados.

b) Realização de testes antes da aplicação de patches críticos.

3. Resposta a Incidentes:

a) Estabelecimento de um plano de resposta a incidentes para lidar com possíveis explorações de vulnerabilidades.

b) Treinamento periódico da equipe para responder eficazmente a incidentes de segurança.

11. CONFORMIDADE

Essa política desempenha um papel crucial na proteção da organização, garantindo que ela opere dentro dos limites legais e éticos, e estabelecendo práticas sólidas para a segurança da informação.

1. Leis e Regulamentações:

- a) Cumprimento de todas as leis e regulamentações relacionadas à segurança da informação.
- b) Atualização contínua para garantir a conformidade com novas legislações.

2. Padrões Internos:

- a) Estabelecimento e revisão regular de padrões internos de segurança da informação.
- b) Comunicação clara e treinamento sobre os padrões internos para todos os colaboradores.

3. Avaliação de Conformidade:

- a) Realização de avaliações periódicas para garantir a conformidade com políticas e padrões estabelecidos.
- b) Correção imediata de quaisquer desvios identificados durante as avaliações.

12. CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à governança para sua avaliação e decisão.

Esta Política de Segurança da Informação (PSI) será revisada anualmente ou conforme necessário para garantir sua eficácia contínua.