



PUC Minas

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

Ana Maria Alves Onerio

Bárbara Bruna D'Áustole Gelape

Geocacio Viviano Nascimento de Souza

João Pedro Madeira Cristino

João Victor Dias Lopes

Lucas Vinicius Oliveira Mendes

PROJETO INFRAESTRUTURA DE REDES

Belo Horizonte

2024

PROJETO ONG DE DENÚNCIAS DE OCORRÊNCIAS AMBIENTAIS

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

Professor: Alexandre Teixeira

Belo Horizonte

2024

SUMÁRIO

1. TEMA.....	4
2. RESPONSABILIDADES	5
3. CRONOGRAMA DE ATIVIDADES.....	6
4. PLANEJAMENTO DOS RECURSOS DE REDE	7
4.1 CENÁRIO	7
4.2 DIVISÃO FÍSICA DA REDE.....	9
4.3 PLANILHA DE MATERIAIS	10
4.4 DIVISÃO LÓGICA DA REDE.....	11
4.5 PLANILHA LINKS.....	15
5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE	16
5.1 IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ	16
5.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP	16
5.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO ADUC	17
5.1.3 POLÍTICAS DE GRUPO APLICADAS.....	18
5.2 IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ.....	20
6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX	24
6.2 GERENCIAMENTO DO SERVIDOR DA NUVEM NO ZABBIX.....	32
6.3 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX ..	36
7. APLICAÇÃO BACK-END.....	39
7.1. TELAS DA APLICAÇÃO BACK-END.....	39
8. REFERÊNCIAS.....	41
ANEXO I.....	42

1. TEMA

O grupo optou pelo desenvolvimento de uma infraestrutura de rede de computadores para atender a uma ONG de ocorrências ambientais que atende o estado de Minas Gerais contendo aproximadamente 130 colaboradores.

Sobre a ONG ela é uma entidade dedicada à proteção e preservação do meio ambiente, com o objetivo de auxiliar os órgãos governamentais competentes em casos de emergências e incidentes ambientais. Sendo os seus pilares fundamentais descritos a seguir.

- **Missão Ambiental:** A principal missão da ONG é trabalhar para proteger e preservar o meio ambiente, buscando minimizar os danos causados por incidentes como poluição, desmatamento, derramamentos de produtos químicos, incêndios florestais, entre outros.
- **Parcerias e Colaborações:** Trabalha em colaboração com governos, outras ONGs, empresas e comunidades locais para enfrentar desafios ambientais de forma integrada e eficaz, buscando soluções sustentáveis e duradouras.
- **Capacitação e Engajamento Comunitário:** Além de responder a emergências, a ONG capacita comunidades locais para lidar com incidentes ambientais e promove o engajamento da sociedade civil na proteção do meio ambiente.
- **Transparência e Responsabilidade:** A organização opera de maneira transparente e responsável, prestando contas de suas ações e resultados à comunidade, aos doadores e às autoridades competentes.

Com base nessas premissas a estrutura organizacional que representa a ONG é composta pelos seguintes departamentos.

1. **Departamento Administrativo e Financeiro:** Responsável pela gestão financeira, contabilidade e recursos humanos da organização.
2. **Departamento de Desenvolvimento de Recursos:** Encarregado de gerenciar as atividades de captação de recursos para sustentar as operações da organização.
3. **Departamento Jurídico:** Encarregado de fornecer orientação legal e representar a organização em questões legais relacionadas ao meio ambiente.
4. **Departamento de Equipes de Campo e Especialistas Técnicos:** Incluindo profissionais especializados em biologia, geologia, engenharia ambiental, etc., responsáveis pela análise e parecer técnico das ocorrências ambientais.
5. **Departamento de Comunicação de Ocorrências Ambientais:** Encarregado de receber, comunicar e coordenar respostas a relatórios de ocorrências ambientais e encaminhá-las aos órgãos governamentais competentes na fiscalização ambiental.

Alinhada a essas informações e características operacionais da ONG, uma infraestrutura de rede de computadores que atenda às suas necessidades deve ser projetada de forma bem estruturada para garantir o seu funcionamento de maneira eficiente, segura e colaborativa, contribuindo assim para o sucesso de suas iniciativas de proteção e preservação do meio ambiente.

2. RESPONSABILIDADES

Nome	Papel	Responsabilidade
Ana Maria	Pesquisa e comunicação	<ul style="list-style-type: none"> • Participar das reuniões e informar aos integrantes do grupo os assuntos discutidos; • Pesquisar e elaborar a planilha de materiais e links.
Bárbara Bruna	Liderança	<ul style="list-style-type: none"> • Definição do tema do projeto; • Acompanhamento da sua evolução; • Coordenar, orientar e desenvolver o projeto com a equipe.
Geocacio Viviano	Supervisão	<ul style="list-style-type: none"> • Coordinar as reuniões semanais; • Distribuir as atividades; • Monitorar, verificar e corrigir as atividades executadas na etapa.
João Pedro	Edição	<ul style="list-style-type: none"> • Pesquisar, compilar, documentar e revisar as informações do projeto no relatório técnico.
João Victor	Programação	<ul style="list-style-type: none"> • Desenvolver o protótipo da infraestrutura de rede física e lógica (Cisco Packet Tracer).
Lucas Vinicius	Edição	<ul style="list-style-type: none"> • Pesquisar, compilar, documentar e revisar as informações do projeto no relatório técnico.

3. CRONOGRAMA DE ATIVIDADES

Semana	Dias de dedicação	Atividades
Semana 1 04/02/2024	5 dias	Orientações gerais sobre o projeto e formação de grupos
Semana 2 11/02/2024	5 dias	Definição dos integrantes do grupo e elaboração do tema para o projeto
Semana 3 18/02/2024	5 dias	Apresentação do tema escolhido e planejamento inicial da proposta para o projeto
Semana 4 25/02/2024	5 dias	Elaboração da documentação do projeto: descrição do tema e elaboração da planilha de recursos da rede
Semana 5 03/03/2024	5 dias	Elaboração do protótipo da rede lógica no software Cisco Packet Tracer
Semana 6 10/03/2024	5 dias	Testes e correções do protótipo da rede lógica no software Cisco Packet Tracer
Semana 6 10/03/2024	5 dias	Finalização e entrega da documentação do relatório de atividades da Etapa 1

4. PLANEJAMENTO DOS RECURSOS DE REDE

A infraestrutura de rede de computadores será composta pela matriz localizada em Belo Horizonte e que se conecta as outras 4 filiais, localizadas em Uberlândia, Juiz de Fora, Governador Valadares e Montes Claros.

Matriz (Belo Horizonte):

- Departamento Administrativo e Financeiro;
- Departamento de Desenvolvimento de Recursos;
- Departamento Jurídico;
- Departamento de Equipes de Campo e Especialistas Técnicos.

Escritórios Regionais:

Triângulo Mineiro e Alto Paranaíba (Uberlândia):

- Coordenador Regional.
- Equipe de Campo e Especialistas Técnicos.
- Departamento de Comunicação de Ocorrências Ambientais.
- Suporte Administrativo.

Zona da Mata (Juiz de Fora):

- Coordenador Regional.
- Equipe de Campo e Especialistas Técnicos.
- Departamento de Comunicação de Ocorrências Ambientais.
- Suporte Administrativo.

Vale do Rio Doce (Governador Valadares):

- Coordenador Regional.
- Equipe de Campo e Especialistas Técnicos.
- Departamento de Comunicação de Ocorrências Ambientais.
- Suporte Administrativo.

Norte e Noroeste de Minas (Montes Claros):

- Coordenador Regional.
- Equipe de Campo e Especialistas Técnicos.
- Departamento de Comunicação de Ocorrências Ambientais.
- Suporte Administrativo.

4.1 CENÁRIO

A seguir é apresentada uma estimativa de colaboradores para a ONG para cada localidade e por fim em sua totalidade.

Matriz (Belo Horizonte):

- Diretoria Executiva: 3 colaboradores
- Departamento Administrativo e Financeiro: 20 colaboradores
- Departamento de Desenvolvimento de Recursos: 10 colaboradores
- Departamento Jurídico: 12 colaboradores
- Departamento de Equipes de Campo e Especialistas Técnicos: 15 colaboradores

Escritórios Regionais:

Triângulo Mineiro e Alto Paranaíba (Uberlândia):

- Coordenador Regional: 1 colaborador
- Equipe de Campo e Especialistas Técnicos: 10 colaboradores
- Departamento de Comunicação de Ocorrências Ambientais: 5 colaboradores
- Suporte Administrativo: 4 colaboradores

Zona da Mata (Juiz de Fora):

- Coordenador Regional: 1 colaborador
- Equipe de Campo e Especialistas Técnicos: 10 colaboradores
- Departamento de Comunicação de Ocorrências Ambientais: 5 colaboradores
- Suporte Administrativo: 4 colaboradores

Vale do Rio Doce (Governador Valadares):

- Coordenador Regional: 1 colaborador
- Equipe de Campo e Especialistas Técnicos: 6 colaboradores
- Departamento de Comunicação de Ocorrências Ambientais: 4 colaboradores
- Suporte Administrativo: 4 colaboradores

Norte e Noroeste de Minas (Montes Claros):

- Coordenador Regional: 1 colaborador
- Equipe de Campo e Especialistas Técnicos: 6 colaboradores
- Departamento de Comunicação de Ocorrências Ambientais: 4 colaboradores
- Suporte Administrativo: 4 colaboradores

Total Geral:

- Matriz (Belo Horizonte): 60 colaboradores
- Escritório Regional 1: 20 colaboradores
- Escritório Regional 2: 20 colaboradores
- Escritório Regional 3: 15 colaboradores
- Escritório Regional 4: 15 colaboradores

4.2 DIVISÃO FÍSICA DA REDE

Propõe-se a topologia em estrela para atender às demandas de serviços de rede de computadores da ONG, conforme ilustrado na Figura 1.

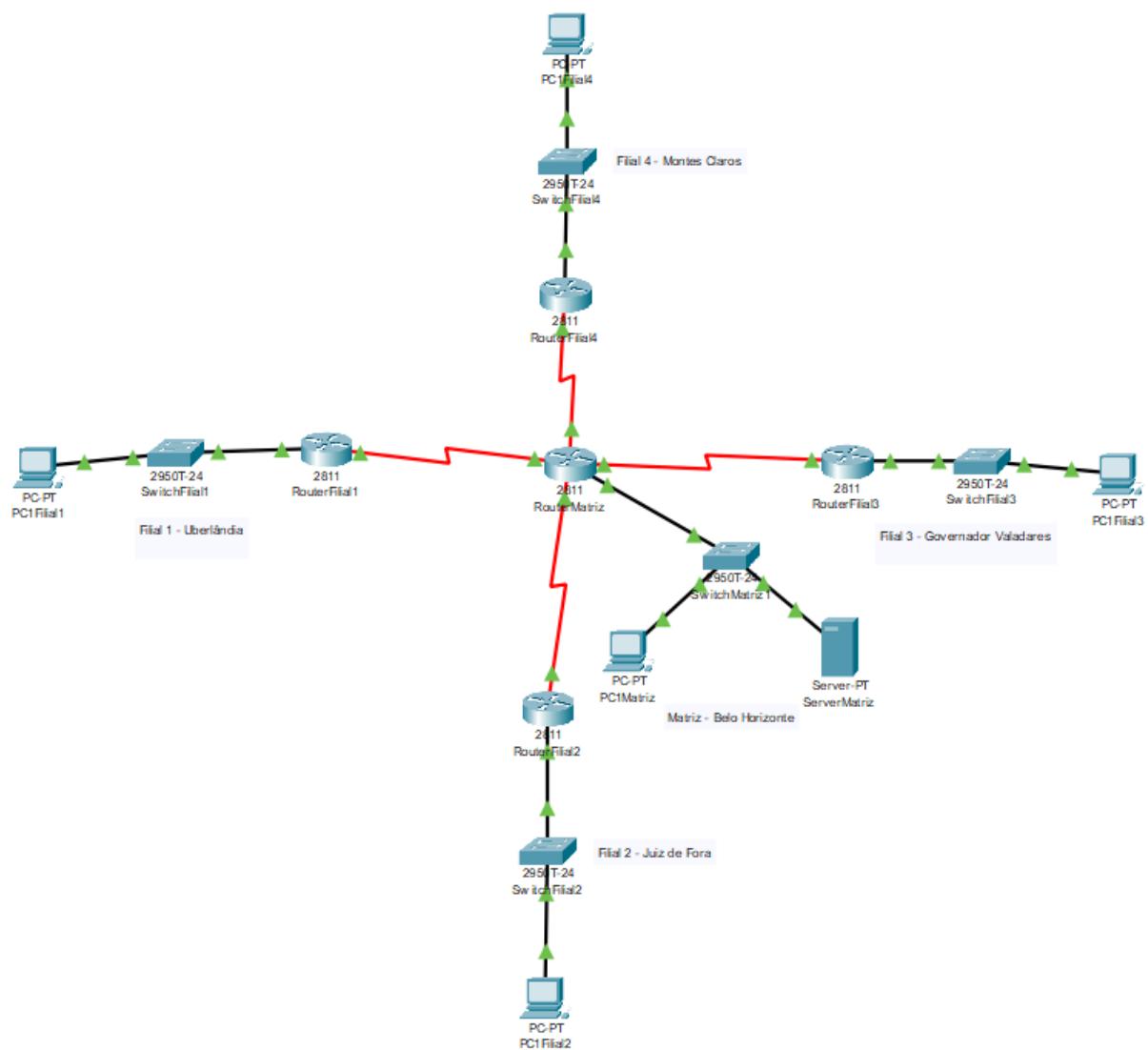


Figura 1 – Protótipo para divisão física da rede

Fonte: Elaborada pelos autores

4.3 PLANILHA DE MATERIAIS

Para atender às necessidades dos 130 colaboradores distribuídos entre a Matriz e suas quatro filiais (com 60 na Matriz, 20 na Filial 1, 20 na Filial 2, 15 na Filial 3 e 15 na Filial 4), foi elaborado um orçamento detalhado, especificando os materiais, quantidades e valores, conforme apresentado na Tabela 1 abaixo. Destaca-se que o custo total estimado para a implementação do projeto de infraestrutura de rede de computadores é de R\$ 1.014.666,82.

Item	Valor	Sede/Matriz		Filial 1		Filial 2		Filial 3		Filial 4	
		60		20		20		15		15	
		Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
Servidor Dell	R\$ 22.999,00	1	R\$ 22.999,00	0	R\$ -						
Estação Dell	R\$ 4.198,00	60	R\$ 251.880,00	20	R\$ 83.960,00	20	R\$ 83.960,00	15	R\$ 62.970,00	15	R\$ 62.970,00
Roteador Cisco	R\$ 14.328,94	1	R\$ 14.328,94	1	R\$ 14.328,94	1	R\$ 14.328,94	1	R\$ 14.328,94	1	R\$ 14.328,94
AP Wifi Cisco	R\$ 1.592,10	1	R\$ 1.592,10	1	R\$ 1.592,10	1	R\$ 1.592,10	1	R\$ 1.592,10	1	R\$ 1.592,10
Rack 44U Central Network	R\$ 2.156,98	1	R\$ 2.156,98	1	R\$ 2.156,98	1	R\$ 2.156,98	1	R\$ 2.156,98	1	R\$ 2.156,98
Serial Cisco	R\$ 789,28	4	R\$ 3.157,12	1	R\$ 789,28						
Switch Dell 24p	R\$ 15.276,67	4	R\$ 61.106,68	1	R\$ 15.276,67						
Cabo de rede CAT6 cx c/305m	R\$ 2.036,06	5	R\$ 10.180,30	1	R\$ 2.036,06						
Rj45 f CAT6	R\$ 52,77	64	R\$ 3.377,28	22	R\$ 1.160,94	22	R\$ 1.160,94	17	R\$ 897,09	17	R\$ 897,09
Patch Cord CAT6	R\$ 64,03	60	R\$ 3.841,80	20	R\$ 1.280,60	20	R\$ 1.280,60	15	R\$ 960,45	15	R\$ 960,45
Patch Panel CAT6	R\$ 882,55	4	R\$ 3.530,20	1	R\$ 882,55						
Organizador de Cabo Central Network	R\$ 20,76	4	R\$ 83,04	20	R\$ 415,20	20	R\$ 415,20	15	R\$ 311,40	15	R\$ 311,40
Impressora	R\$ 1.823,68	3	R\$ 5.471,04	1	R\$ 1.823,68						
Nobreak	R\$ 5.299,99	2	R\$ 10.599,98	1	R\$ 5.299,99						
Mesa + Cadeira	R\$ 997,90	60	R\$ 59.874,00	20	R\$ 19.958,00						
Total	R\$ 454.178,46	Total	R\$ 150.960,99	Total	R\$ 150.960,99	Total	R\$ 129.283,19	Total	R\$ 129.283,19	Total	R\$ 1.014.666,82
Total Geral											

Tabela 1 – Planilha de materiais
Fonte: Elaborada pelos autores

4.4 DIVISÃO LÓGICA DA REDE

Na Tabela 2 é apresentado os dispositivos da rede, seus nomes, endereçamentos, portas e roteamento.

Dispositivos	Nome	Portas / Endereçamento				
Servidor	ServidorMatriz	Device Name: ServerMatriz Device Model: Server-PT Port Link IP Address IPv6 Address FastEthernet0 Up 192.168.0.2/24 <not set> Gateway: 192.168.0.1 DNS Server: <not set> Line Number: <not set>				
Roteador	RoteadorMatriz	Device Name: RouterMatriz Custom Device Model: 2811 IOS15 Hostname: Router Port Link VLAN IP Address IPv6 Address FastEthernet0/0 Up -- 192.168.0.1/24 <not set> FastEthernet0/1 Down -- <not set> <not set> Serial0/0/0 Up -- 192.168.31.1/24 <not set> Serial0/0/1 Up -- 192.168.32.1/24 <not set> Serial0/1/0 Up -- 192.168.33.1/24 <not set> Serial0/1/1 Up -- 192.168.34.1/24 <not set> Vlan1 Down 1 <not set> <not set>				
Switch	SwitchMatriz1	Device Name: SwitchMatriz1 Device Model: 2950T-24 Hostname: Switch Port Link VLAN IP Address FastEthernet0/1 Up -- -- FastEthernet0/2 Up -- -- FastEthernet0/3 Up -- --				
Computador	PC1Matriz	Device Name: PC1Matriz Device Model: PC-PT Port Link IP Address IPv6 Address FastEthernet0 Up 192.168.0.11/24 <not set> Gateway: 192.168.0.1 DNS Server: <not set> Line Number: <not set>				
Roteador	RoteadorFilial1	Device Name: RouterFilial1 Custom Device Model: 2811 IOS15 Hostname: Router				

		<table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th><th>IPv6</th></tr> </thead> <tbody> <tr> <td>Address</td><td></td><td></td><td></td><td></td></tr> <tr> <td>FastEthernet0/0</td><td>Up</td><td>--</td><td>192.168.1.1/24</td><td><not set></td></tr> <tr> <td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td><td><not set></td></tr> <tr> <td>Serial0/0/0</td><td>Up</td><td>--</td><td>192.168.31.2/24</td><td><not set></td></tr> <tr> <td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td><td><not set></td></tr> <tr> <td>Vlan1</td><td>Down</td><td>1</td><td><not set></td><td><not set></td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	IPv6	Address					FastEthernet0/0	Up	--	192.168.1.1/24	<not set>	FastEthernet0/1	Down	--	<not set>	<not set>	Serial0/0/0	Up	--	192.168.31.2/24	<not set>	Serial0/0/1	Down	--	<not set>	<not set>	Vlan1	Down	1	<not set>	<not set>
Port	Link	VLAN	IP Address	IPv6																																	
Address																																					
FastEthernet0/0	Up	--	192.168.1.1/24	<not set>																																	
FastEthernet0/1	Down	--	<not set>	<not set>																																	
Serial0/0/0	Up	--	192.168.31.2/24	<not set>																																	
Serial0/0/1	Down	--	<not set>	<not set>																																	
Vlan1	Down	1	<not set>	<not set>																																	
Switch	SwitchFilial1	<p>Device Name: SwitchFilial1 Device Model: 2950T-24 Hostname: Switch</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th><th>IPv6</th></tr> </thead> <tbody> <tr> <td>FastEthernet0/1</td><td>Up</td><td>--</td><td>--</td><td></td></tr> <tr> <td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td><td></td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	IPv6	FastEthernet0/1	Up	--	--		FastEthernet0/2	Up	--	--																					
Port	Link	VLAN	IP Address	IPv6																																	
FastEthernet0/1	Up	--	--																																		
FastEthernet0/2	Up	--	--																																		
Computador	PC1Filial1	<p>Device Name: PC1Filial1 Device Model: PC-PT</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th><th>IPv6 Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>192.168.1.11/24</td><td><not set></td></tr> </tbody> </table> <p>Gateway: 192.168.1.1 DNS Server: <not set> Line Number: <not set></p>	Port	Link	IP Address	IPv6 Address	FastEthernet0	Up	192.168.1.11/24	<not set>																											
Port	Link	IP Address	IPv6 Address																																		
FastEthernet0	Up	192.168.1.11/24	<not set>																																		
Roteador	RoteadorFilial2	<p>Device Name: RouterFilial2 Custom Device Model: 2811 IOS15 Hostname: Router</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th><th>IPv6</th></tr> </thead> <tbody> <tr> <td>Address</td><td></td><td></td><td></td><td></td></tr> <tr> <td>FastEthernet0/0</td><td>Up</td><td>--</td><td>192.168.2.1/24</td><td><not set></td></tr> <tr> <td>FastEthernet0/1</td><td>Down</td><td>--</td><td><not set></td><td><not set></td></tr> <tr> <td>Serial0/0/0</td><td>Up</td><td>--</td><td>192.168.32.2/24</td><td><not set></td></tr> <tr> <td>Serial0/0/1</td><td>Down</td><td>--</td><td><not set></td><td><not set></td></tr> <tr> <td>Vlan1</td><td>Down</td><td>1</td><td><not set></td><td><not set></td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	IPv6	Address					FastEthernet0/0	Up	--	192.168.2.1/24	<not set>	FastEthernet0/1	Down	--	<not set>	<not set>	Serial0/0/0	Up	--	192.168.32.2/24	<not set>	Serial0/0/1	Down	--	<not set>	<not set>	Vlan1	Down	1	<not set>	<not set>
Port	Link	VLAN	IP Address	IPv6																																	
Address																																					
FastEthernet0/0	Up	--	192.168.2.1/24	<not set>																																	
FastEthernet0/1	Down	--	<not set>	<not set>																																	
Serial0/0/0	Up	--	192.168.32.2/24	<not set>																																	
Serial0/0/1	Down	--	<not set>	<not set>																																	
Vlan1	Down	1	<not set>	<not set>																																	
Switch	SwitchFilial2	<p>Device Name: SwitchFilial2 Device Model: 2950T-24 Hostname: Switch</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th><th>IPv6</th></tr> </thead> <tbody> <tr> <td>FastEthernet0/1</td><td>Up</td><td>--</td><td>--</td><td></td></tr> <tr> <td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td><td></td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	IPv6	FastEthernet0/1	Up	--	--		FastEthernet0/2	Up	--	--																					
Port	Link	VLAN	IP Address	IPv6																																	
FastEthernet0/1	Up	--	--																																		
FastEthernet0/2	Up	--	--																																		
Computador	PC1Filial2	<p>Device Name: PC1Filial2 Device Model: PC-PT</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th><th>IPv6 Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>192.168.2.11/24</td><td><not set></td></tr> </tbody> </table> <p>Gateway: 192.168.2.1</p>	Port	Link	IP Address	IPv6 Address	FastEthernet0	Up	192.168.2.11/24	<not set>																											
Port	Link	IP Address	IPv6 Address																																		
FastEthernet0	Up	192.168.2.11/24	<not set>																																		

		DNS Server: <not set> Line Number: <not set>																														
Roteador	RoteadorFilial3	<p>Device Name: RouterFilial3 Custom Device Model: 2811 IOS15 Hostname: Router</p> <table> <thead> <tr> <th>Port Address</th> <th>Link</th> <th>VLAN</th> <th>IP Address</th> <th>IPv6</th> </tr> </thead> <tbody> <tr> <td>FastEthernet0/0</td> <td>Up</td> <td>--</td> <td>192.168.3.1/24</td> <td><not set></td> </tr> <tr> <td>FastEthernet0/1</td> <td>Down</td> <td>--</td> <td><not set></td> <td><not set></td> </tr> <tr> <td>Serial0/0/0</td> <td>Up</td> <td>--</td> <td>192.168.33.2/24</td> <td><not set></td> </tr> <tr> <td>Serial0/0/1</td> <td>Down</td> <td>--</td> <td><not set></td> <td><not set></td> </tr> <tr> <td>Vlan1</td> <td>Down</td> <td>1</td> <td><not set></td> <td><not set></td> </tr> </tbody> </table>	Port Address	Link	VLAN	IP Address	IPv6	FastEthernet0/0	Up	--	192.168.3.1/24	<not set>	FastEthernet0/1	Down	--	<not set>	<not set>	Serial0/0/0	Up	--	192.168.33.2/24	<not set>	Serial0/0/1	Down	--	<not set>	<not set>	Vlan1	Down	1	<not set>	<not set>
Port Address	Link	VLAN	IP Address	IPv6																												
FastEthernet0/0	Up	--	192.168.3.1/24	<not set>																												
FastEthernet0/1	Down	--	<not set>	<not set>																												
Serial0/0/0	Up	--	192.168.33.2/24	<not set>																												
Serial0/0/1	Down	--	<not set>	<not set>																												
Vlan1	Down	1	<not set>	<not set>																												
Switch	SwitchFilial3	<p>Device Name: SwitchFilial3 Device Model: 2950T-24 Hostname: Switch</p> <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> </tbody> </table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Up	--	--	FastEthernet0/2	Up	--	--																		
Port	Link	VLAN	IP Address																													
FastEthernet0/1	Up	--	--																													
FastEthernet0/2	Up	--	--																													
Computador	PC1Filial3	<p>Device Name: PC1Filial3 Device Model: PC-PT</p> <table> <thead> <tr> <th>Port</th> <th>Link</th> <th>IP Address</th> <th>IPv6 Address</th> </tr> </thead> <tbody> <tr> <td>FastEthernet0</td> <td>Up</td> <td>192.168.3.11/24</td> <td><not set></td> </tr> </tbody> </table> <p>Gateway: 192.168.3.1 DNS Server: <not set> Line Number: <not set></p>	Port	Link	IP Address	IPv6 Address	FastEthernet0	Up	192.168.3.11/24	<not set>																						
Port	Link	IP Address	IPv6 Address																													
FastEthernet0	Up	192.168.3.11/24	<not set>																													
Roteador	RoteadorFilial4	<p>Device Name: RouterFilial4 Custom Device Model: 2811 IOS15 Hostname: Router</p> <table> <thead> <tr> <th>Port Address</th> <th>Link</th> <th>VLAN</th> <th>IP Address</th> <th>IPv6</th> </tr> </thead> <tbody> <tr> <td>FastEthernet0/0</td> <td>Up</td> <td>--</td> <td>192.168.4.1/24</td> <td><not set></td> </tr> <tr> <td>FastEthernet0/1</td> <td>Down</td> <td>--</td> <td><not set></td> <td><not set></td> </tr> <tr> <td>Serial0/0/0</td> <td>Up</td> <td>--</td> <td>192.168.34.2/24</td> <td><not set></td> </tr> <tr> <td>Serial0/0/1</td> <td>Down</td> <td>--</td> <td><not set></td> <td><not set></td> </tr> <tr> <td>Vlan1</td> <td>Down</td> <td>1</td> <td><not set></td> <td><not set></td> </tr> </tbody> </table>	Port Address	Link	VLAN	IP Address	IPv6	FastEthernet0/0	Up	--	192.168.4.1/24	<not set>	FastEthernet0/1	Down	--	<not set>	<not set>	Serial0/0/0	Up	--	192.168.34.2/24	<not set>	Serial0/0/1	Down	--	<not set>	<not set>	Vlan1	Down	1	<not set>	<not set>
Port Address	Link	VLAN	IP Address	IPv6																												
FastEthernet0/0	Up	--	192.168.4.1/24	<not set>																												
FastEthernet0/1	Down	--	<not set>	<not set>																												
Serial0/0/0	Up	--	192.168.34.2/24	<not set>																												
Serial0/0/1	Down	--	<not set>	<not set>																												
Vlan1	Down	1	<not set>	<not set>																												
Switch	SwitchFilial4	<p>Device Name: SwitchFilial4 Device Model: 2950T-24 Hostname: Switch</p> <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> </tbody> </table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Up	--	--	FastEthernet0/2	Up	--	--																		
Port	Link	VLAN	IP Address																													
FastEthernet0/1	Up	--	--																													
FastEthernet0/2	Up	--	--																													

Computador	PC1Filial4	<p>Device Name: PC1Filial4 Device Model: PC-PT</p> <table> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th><th>IPv6 Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>192.168.4.11/24</td><td><not set></td></tr> </tbody> </table> <p>Gateway: 192.168.4.1 DNS Server: <not set> Line Number: <not set></p>	Port	Link	IP Address	IPv6 Address	FastEthernet0	Up	192.168.4.11/24	<not set>
Port	Link	IP Address	IPv6 Address							
FastEthernet0	Up	192.168.4.11/24	<not set>							

Tabela 2 – Divisão lógica de rede

Fonte: Elaborada pelos autores

4.5 PLANILHA LINKS

O consumo de dados estimado para as aplicações e serviços necessários às atividades relacionadas à ONG está apresentado na Tabela 3, juntamente com a capacidade do link dedicado de Internet para suportá-los.

Cálculo de Links de dados e de Internet											
Necessidades Corporativas		Matriz = 60		Filial 1 = 20		Filial 2 = 20		Filial 3 = 15		Filial 4 = 15	
Aplicação	Requisitos (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)
Internet Banking	512	3	1536	1	512	1	512	1	512	1	512
Videoconferência	2000	60	120000	20	40000	20	40000	15	30000	15	30000
Suporte Remoto	1000	15	15000	15	15000	5	5000	10	10000	10	10000
Web	1000	60	60000	20	20000	5	5000	15	15000	15	15000
E-mail	512	60	30720	20	10240	5	2560	15	7680	15	7680
AWS	1000	27	27000	16	16000	11	11000	11	11000	11	11000
ERP	1000	33	33000	5	5000	5	5000	5	5000	5	5000
		Total App	287256	Total App	106752	Total App	69072	Total App	79192	Total App	79192
		Total Internet	239256	Total Internet	86752	Total Internet	59072	Total Internet	64192	Total Internet	64192
		Link Internet	Link Matriz <-> Filial 1		Link Matriz <-> Filial 2		Link Matriz <-> Filial 3		Link Matriz <-> Link Filial 4		
Redutor capacid.	1	513464		106752		69072		79192			79192

Tabela 3 – Divisão lógica de rede
Fonte: Elaborada pelos autores

5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE

5.1 IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ

A IMPLEMENTAÇÃO DO SERVIDOR LOCAL FOI EXECUTADA ATRAVÉS DA CRIAÇÃO DE UMA MÁQUINA VIRTUAL UTILIZANDO O SOFTWARE ORACLE VIRTUAL BOX. A CONFIGURAÇÃO DA MÁQUINA É APRESENTADA NA FIGURA 2.

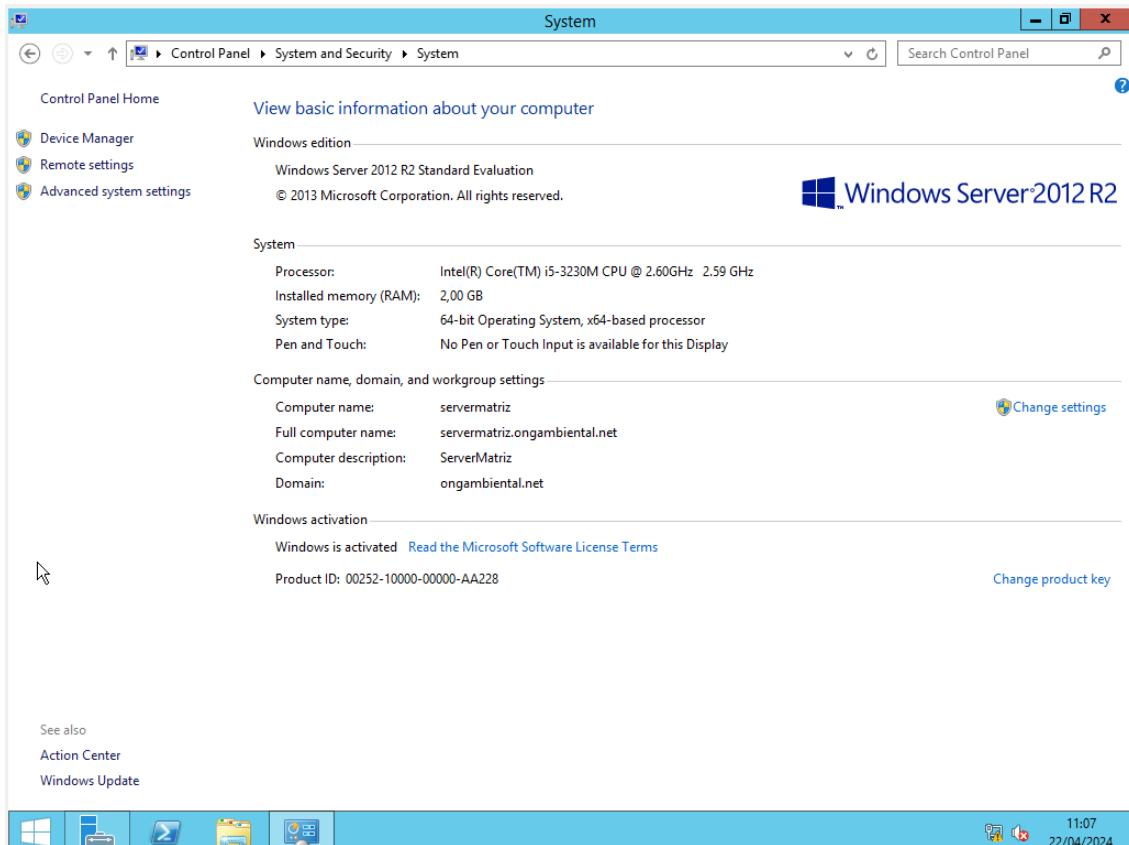


Figura 2 – Especificações servidor local

Fonte: Elaborada pelos autores

Pode-se destacar as seguintes especificações do servidor local da matriz:

- Sistema operacional: Windows Server 2012 R2 64bits;
- CPU: Intel Core i5-3230M @ 2.60GHz;
- Memória RAM: 2GB;
- Disco rígido: 15GB SSD;
- Nome do servidor: ServerMatriz;
- Domínio: ongambiental.net.

As credenciais de acesso são:

- Usuário: Administrador;
- Senha: puc@1958.

5.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP

Para atender a demanda de conexões no servidor, o protocolo DHCP foi configurado para prover mais de 60 endereços IP para os dispositivos ingressarem na rede local da matriz conforme necessário. A faixa de distribuição dos IPs é apresentada

na Figura 3.

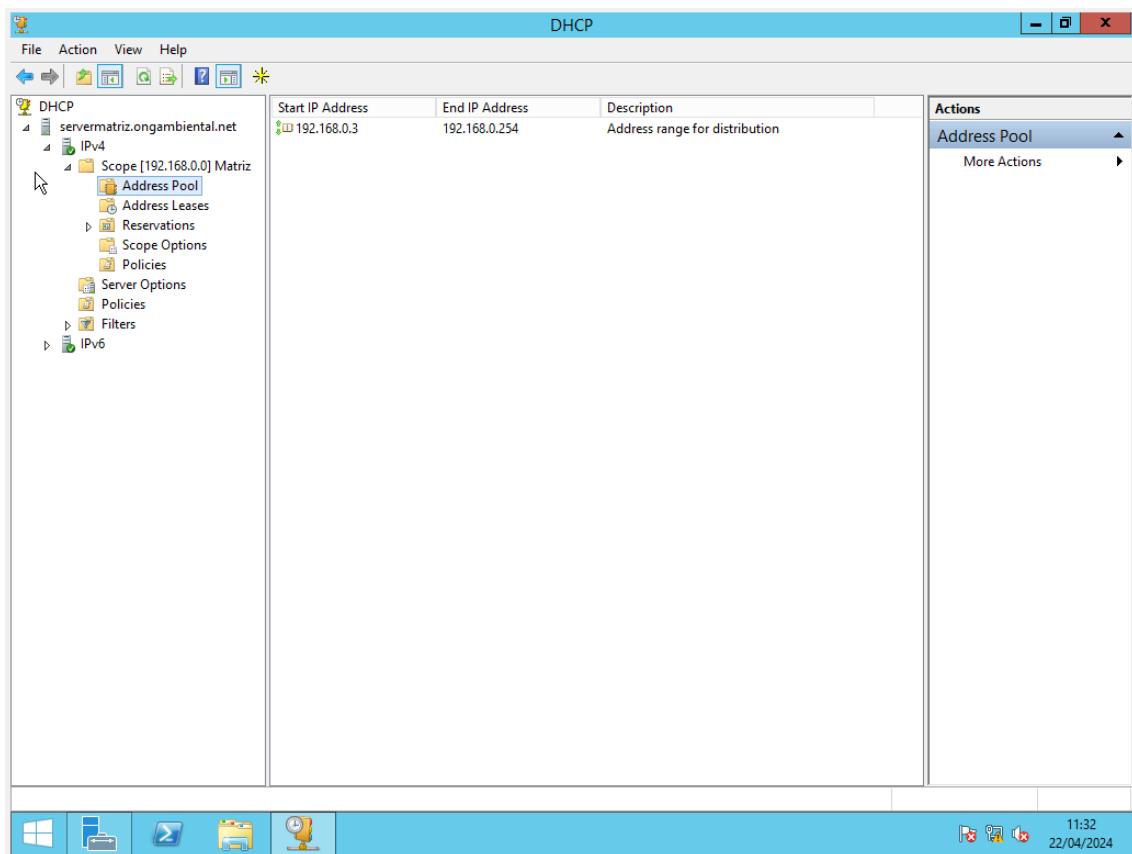


Figura 3 – Configuração do protocolo DHCP
Fonte: Elaborada pelos autores

5.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO ADUC

Foi instalado o Active Directory, configurado o domínio ongambiental.net e criado as estruturas organizacionais e inserido alguns usuários conforme a Figura 4.

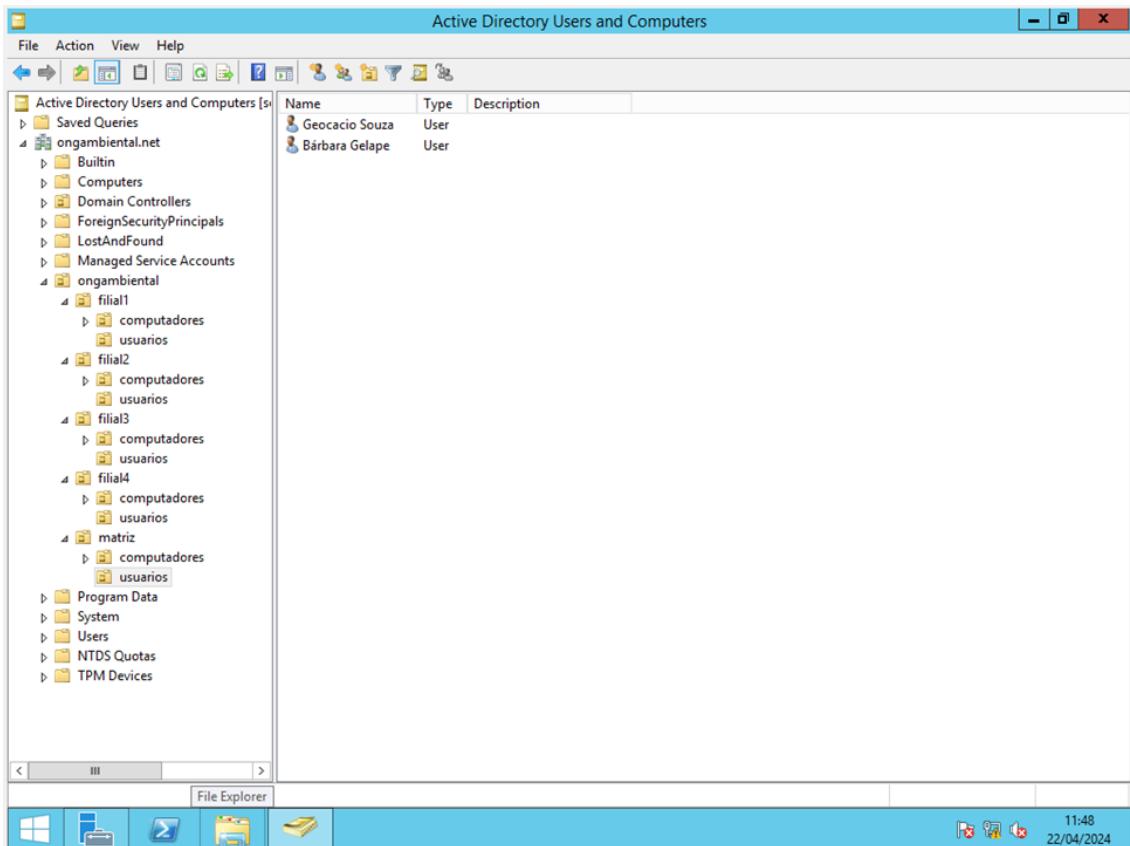


Figura 4 – Configuração do protocolo ADUC
Fonte: Elaborada pelos autores

5.1.3 POLÍTICAS DE GRUPO APLICADAS

Foram aplicadas as seguintes políticas de grupo:

- Restrição de acesso ao Painel de Controle e Configurações do PC;
- Direcionamento direto para a Área de Trabalho em vez do Menu Iniciar durante o login;
- Remoção do ícone de música do Menu Iniciar.

As políticas mencionadas estão detalhadas na Figura 5.

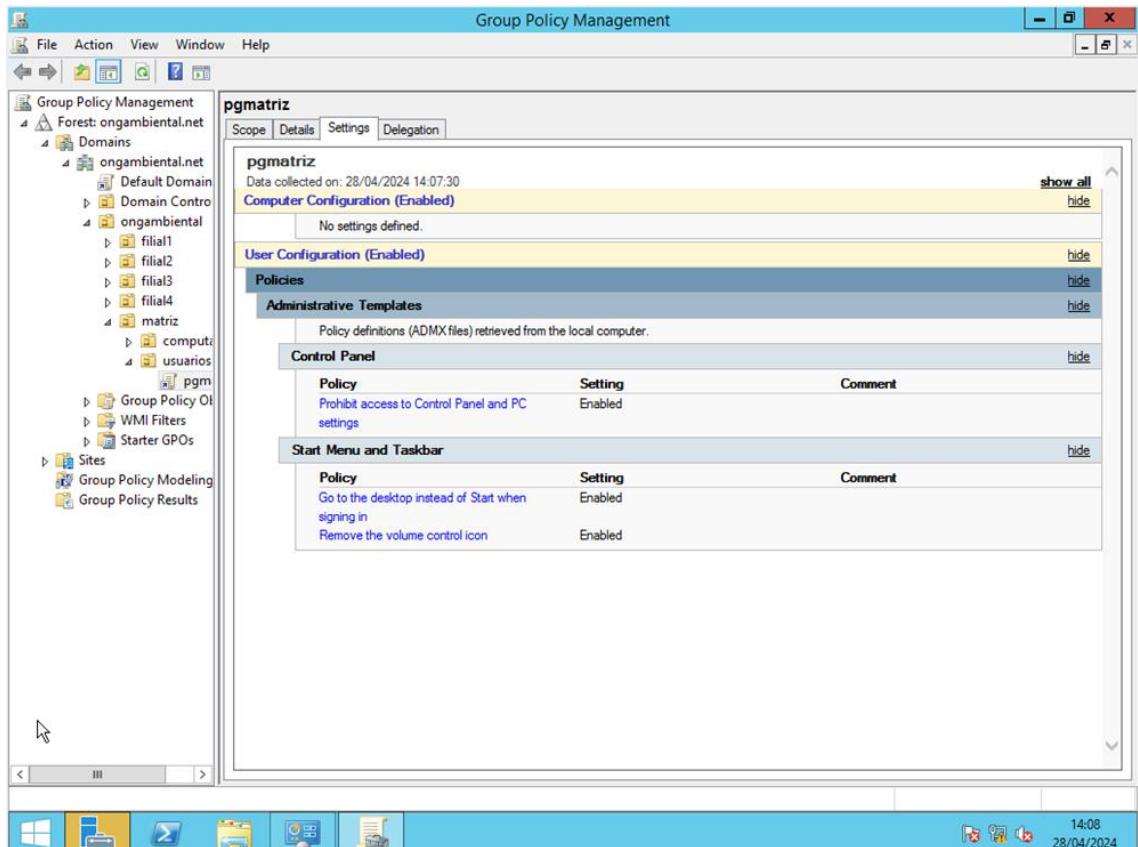


Figura 5 – Políticas de grupo
Fonte: Elaborada pelos autores

5.2 IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ

Na primeira etapa, foi iniciada uma rede de nuvem privada virtual (VPC) na AWS (Figura 6). Estabeleceu-se a VPC da ONG com duas sub-redes públicas e duas sub-redes privadas em duas zonas de disponibilidade distintas. Essa nova VPC permitirá a alocação do servidor dentro da infraestrutura da rede ONG-vpc.

The screenshot shows the AWS VPC console with the following details:

ID da VPC	Estado	Nomes de host DNS	Resolução de DNS
vpc-0a02bb617d8fb901	Available	Habilitado	Habilitado
Locação	Conjunto de opções de DHCP	Tabela de rota principal	Network ACL principal
Default	dopt-01dadf66e7093d22e	rtb-0919fd413be5caec6	acl-08dea349dbf6a816b
VPC padrão	CIDR IPv4	Grupo IPv6	CIDR IPv6 (Grupo de borda de rede)
Não	10.0.0.0/16	-	-
Métricas de uso do endereço de rede	Grupos de regras do Firewall de DNS do resolvedor do Route 53	ID do proprietário	-
Desabilitado	Falha ao carregar grupos de regras	269121367540	-

Below the table, there are tabs for 'Mapa de recursos', 'CIDRs', 'Logs de fluxos', 'Tags', and 'Integrações'. The 'Mapa de recursos' tab is selected.

Figura 6 – VPC Ong Ambiental
Fonte: Elaborada pelos autores

Na segunda etapa, um grupo de segurança foi desenvolvido para operar como um *firewall* em nossa rede. Estabeleceu-se duas regras de entrada: uma para permitir que qualquer endereço IPv4 acesse o servidor remotamente via RDP e outra para viabilizar o acesso de qualquer endereço IPv4 ao servidor por meio de um navegador web utilizando o protocolo HTTP. A Figura 7 ilustra o grupo de segurança criado e as duas regras de entrada.

The screenshot shows the AWS Network Firewall console with the following details:

Nome do grupo de segurança	ID do grupo de segurança	Descrição	ID da VPC
ongsec	sg-0f2f85896fce1193	web e terminal remoto	vpc-0a02bb617d8fb901
Proprietário	Número de regras de entrada	Número de regras de saída	-
269121367540	2 Entradas de permissão	1 Entrada de permissão	-

Below the table, there are tabs for 'Regras de entrada', 'Regras de saída', and 'Tags'. The 'Regras de entrada' tab is selected, showing a table with two entries:

Regras de entrada (2)	Pesquisar	Gerenciar tags	Editar regras de entrada
Regras de entrada (2)	Pesquisar	Gerenciar tags	Editar regras de entrada

Figura 7 – Grupo de segurança da VPC
Fonte: Elaborada pelos autores

Na terceira etapa, foi realizada a criação de uma instância na AWS para o servidor. Para isso, configura-se uma instância EC2 utilizando o sistema operacional Windows Server 2016 Base e selecionou-se o tipo t2.large, conforme

evidenciado nas Figuras 8 e 9. Esse tipo de instância oferece os recursos de hardware adequados para as necessidades do servidor. Em seguida, integramos a instância à VPC e ao grupo de segurança ongsec.

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar shows navigation options like 'Painel EC2', 'Visualização Global do EC2', 'Eventos', 'Console-to-Code', 'Instâncias' (selected), 'Tipos de instância', 'Modelos de execução', 'Solicitações spot', 'Savings Plans', 'Instâncias reservadas', 'Hosts dedicados', 'Reservas de capacidade', 'Imagens', 'AMIs', and 'Catálogo de AMIs'. The main content area displays 'Instâncias (1) Informações' with a table showing one instance: Name: ONGwebserver, ID da instância: i-0b2d0841775ba66ba, Estado da instância: Executando, Tipo de instância: t2.large, Verificação de status: 2/2 verificações aprovadas, Status do alarme: Exibir alarmes, and Zona de disponibilidade: us-east-1a. Below this is a modal window titled 'Selecionar uma instância' which also lists the same instance.

Figura 8 – Instância EC2 criada na VPC

Fonte: Elaborada pelos autores

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar shows the same navigation options as Figure 8. The main content area shows the 'Resumo da instância para i-0b2d0841775ba66ba (ONGwebserver)' with the following details: ID da instância: i-0b2d0841775ba66ba (ONGwebserver); Endereço IPv4 público: 35.175.203.141 [endereço aberto]; Endereço IPv6: -; Estado da instância: Executando; Tipo de nome do host: Nome do IP: ip-10-0-0-37.ec2.internal; Nome do DNS do recurso privado de resposta: -; Nome do DNS de IP privado (somente IPv4): ip-10-0-0-37.ec2.internal; Tipo de instância: t2.large; ID da VPC: vpc-0a02bb617d8fb9c01 (ONG-vpc); Função do IAM: -; ID da sub-rede: subnet-07284470878a6634b (ONG-subnet); Endereços IP privados: 10.0.0.37; DNS IPv4 público: ec2-35-175-203-141.compute-1.amazonaws.com [endereço aberto]; Endereços IP elásticos: -; Descoberta do AWS Compute Optimizer: Opte por participar do AWS Compute Optimizer para obter recomendações. [Saiba mais]; and Nome do Grupo do Auto Scaling: -.

Figura 9 – Informações da instância criada na VPC

Fonte: Elaborada pelos autores

Na quarta etapa, o servidor criado foi acessado via RDP (Figura 10) e procedeu-se à instalação do serviço de servidor web da Microsoft, o IIS (Figura 11). Após a conclusão da instalação do serviço, foi realizada o acesso à página web do servidor (Figura 12).

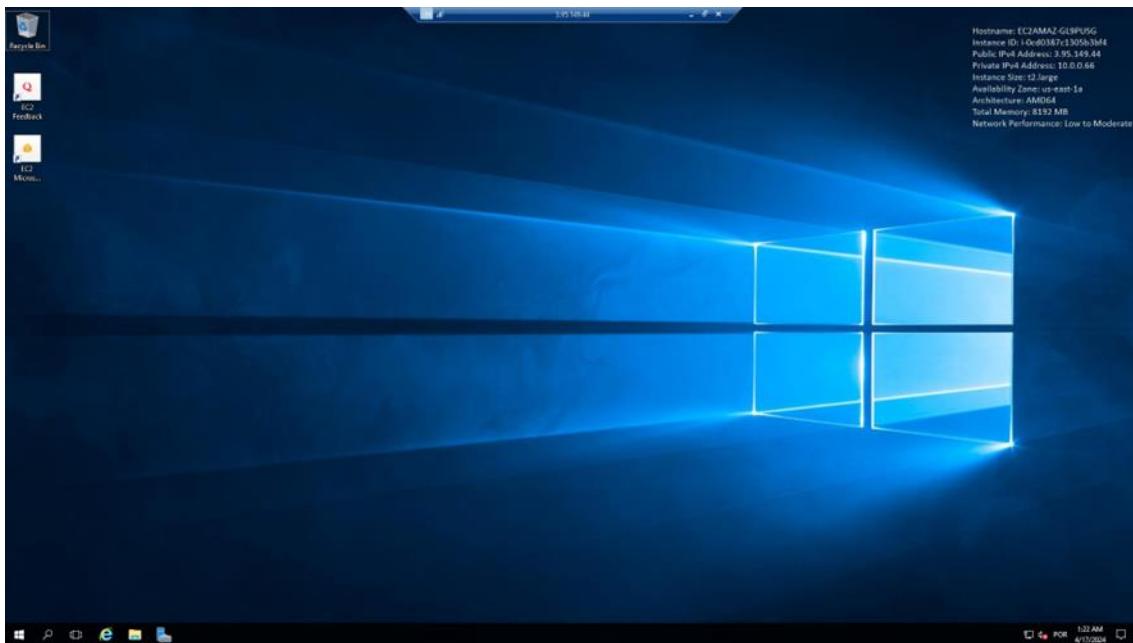


Figura 10 – Acesso via RDP ao servidor
Fonte: Elaborada pelos autores

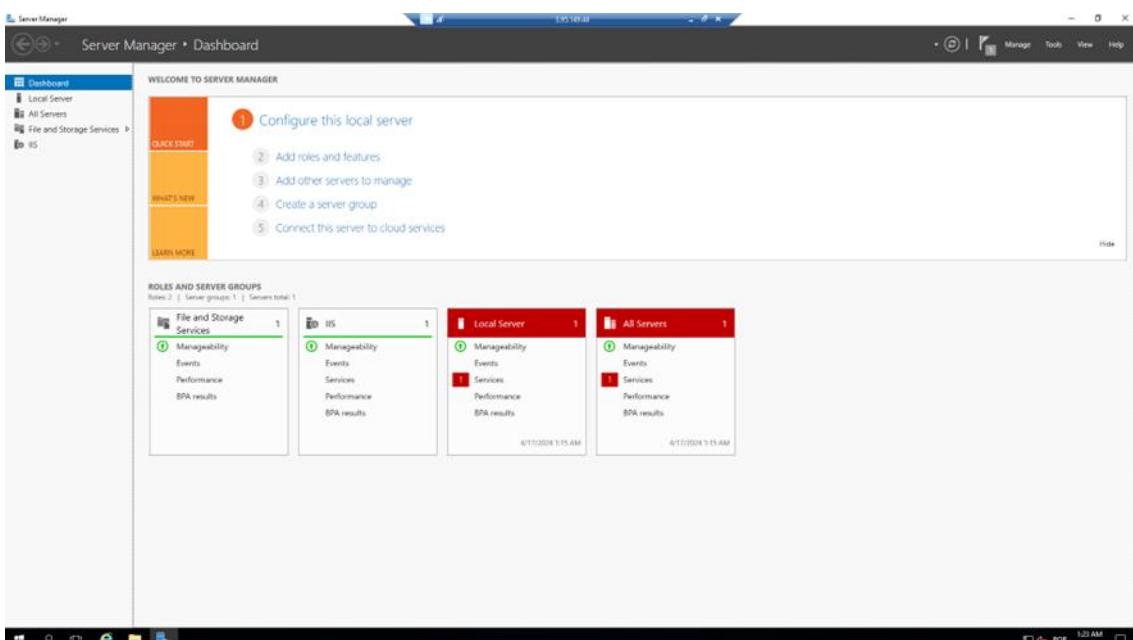


Figura 11 – Serviço IIS disponível no servidor
Fonte: Elaborada pelos autores



Figura 12 – Acesso a página web pelo navegador

Fonte: Elaborada pelos autores

6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX

6.1 GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX

Para estabelecer o monitoramento de parâmetros de rede do servidor local fez-se necessário baixar o arquivo de instalação do software Zabbix Appliance e importar essa appliance no Virtual Box, conforme pode ser visualizado na Figura 13.

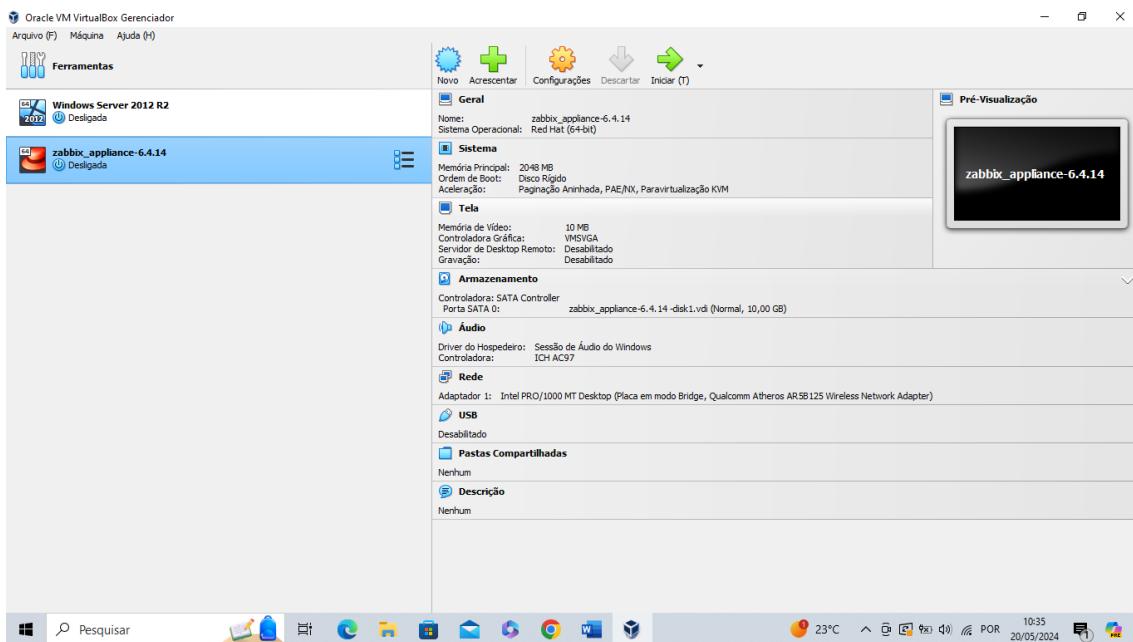


Figura 13 – Máquina virtual Zabbix Appliance

Fonte: Elaborada pelos autores

Finalizada a instalação do software é necessário configurar a placa de rede em modo Bridge (Figura 14) para em seguida inicializá-lo.

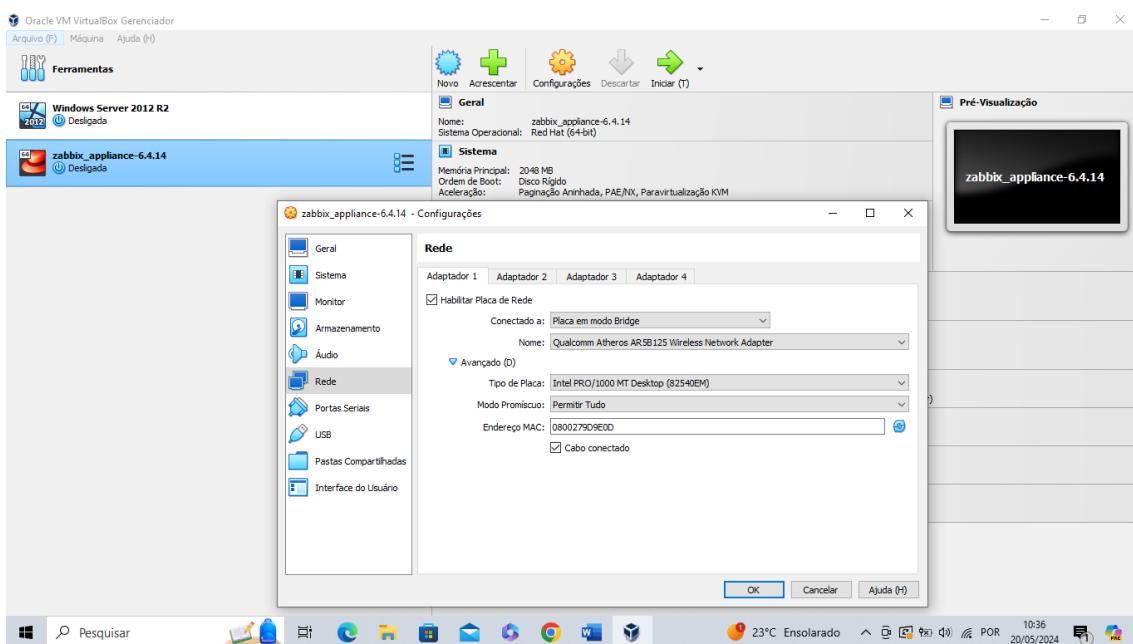
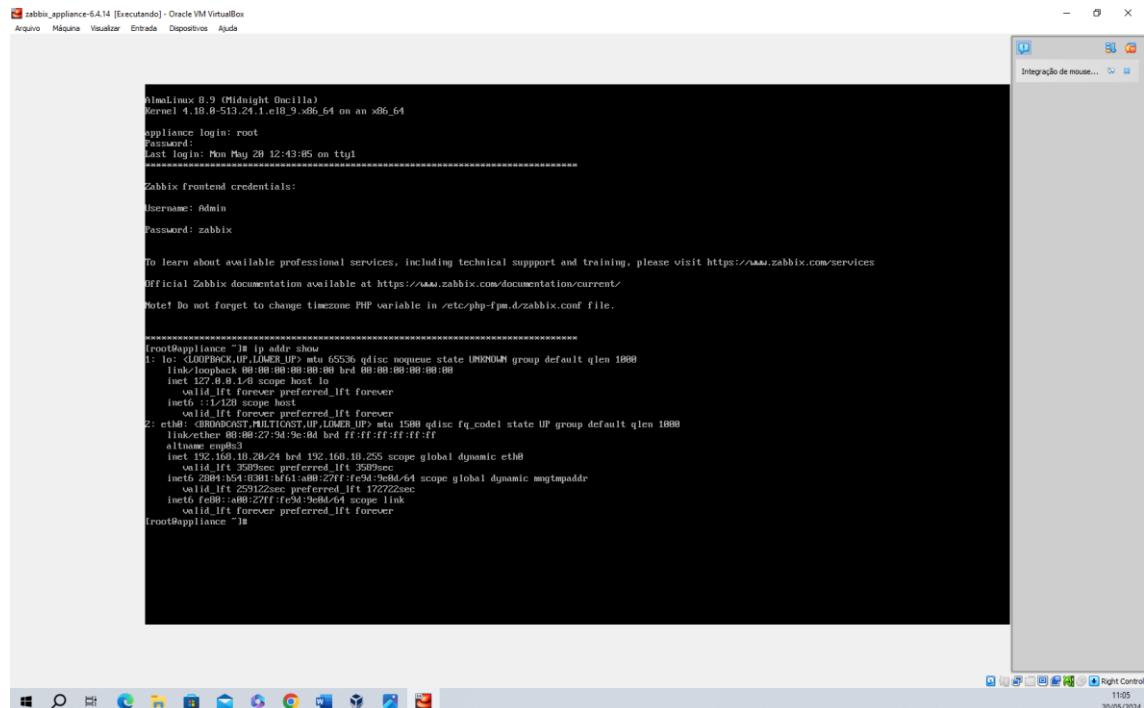


Figura 14 – Configuração placa de rede em modo Bridge no Zabbix
Fonte: Elaborada pelos autores

Após iniciar o Zabbix, deve-se inserir o usuário “root” e senha “zabbix” para ser possível gerar a interface gráfica no navegador a partir do endereço IP obtido pelo resultado do comando: *ip addr show*, na tela de comandos do software (Figura 15).



```
almalinux 8.9 (Midnight Oscilla)
Kernel 4.18.0-513.24.1.el8_9.x86_64 on an x86_64

appliance login: root
Password:
Last login: Mon May 28 12:43:05 on ttysl
=====
Zabbix frontend credentials:
Username: Admin
Password: zabbix

To learn about available professional services, including technical support and training, please visit https://www.zabbix.com/services
Official Zabbix documentation available at https://www.zabbix.com/documentation/current
Note! Do not forget to change timezone PHP variable in /etc/php-fpm.d/zabbix.conf file.

=====
[root@appliance ~]# ip addr show
1: lo: <LOOPBACK,NO-SILOUP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host lo
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:9d:9e:0d brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.10.255/24 brd 192.168.10.255 scope global dynamic eth0
        valid_lft 3599sec preferred_lft 3599sec
    inet6 2001:0db8:0:1000::f9d1:a00:27ff:fe9d:9e0d/64 scope global dynamic mngtmpaddr
        valid_lft 259122sec preferred_lft 172722sec
    inet6 fe80::f9d1:a00:27ff:fe9d:9e0d/64 brd fe80::ff:ffff:ffff:ffff scope link
        valid_lft forever preferred_lft forever
[root@appliance ~]#
```

Figura 15 – Endereço de IP para interface gráfica do Zabbix
Fonte: Elaborada pelos autores

Com isso, a interface gráfica é apresentada na Figura 16. Para acessar suas páginas e configurações, é necessário inserir o usuário “Admin” e a senha “zabbix”.

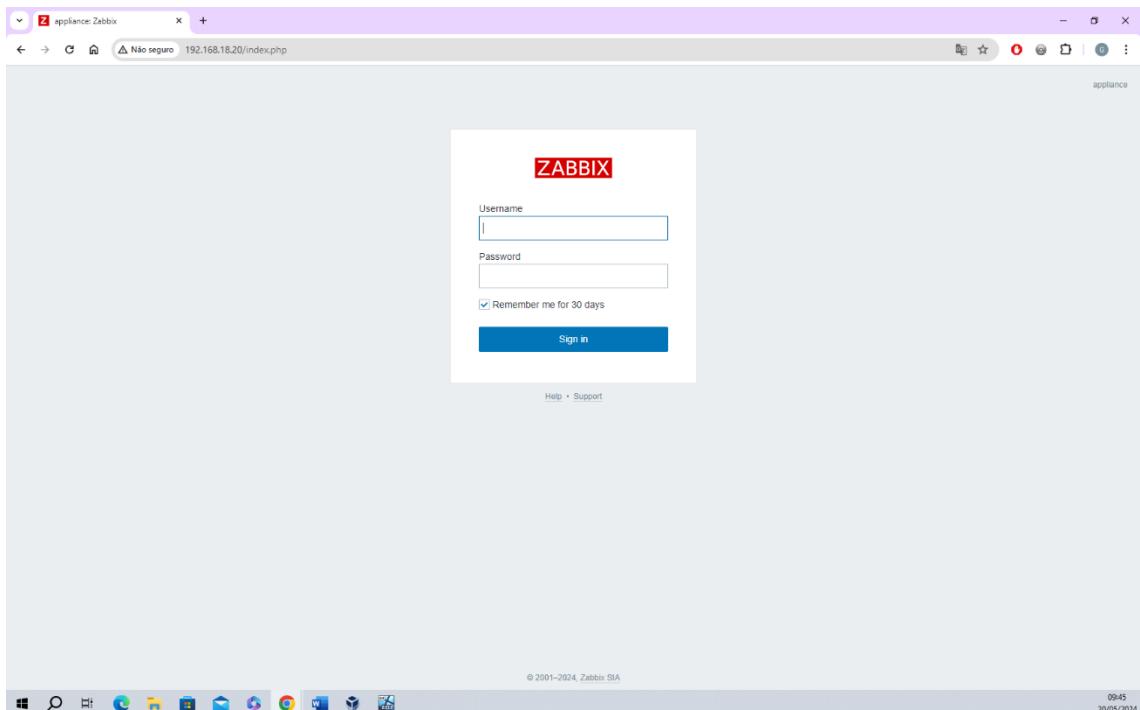


Figura 16 – Interface gráfica do Zabbix no navegador web
Fonte: Elaborada pelos autores

Em seguida, após inicializar a máquina virtual do servidor local e instalar o recurso SNMP (Figura 17), é preciso realizar a sua configuração (Figura 18). Para isso, é necessário adicionar a comunidade pública na aba segurança e selecionar o *checkbox* de aceitação de pacotes SNMP de qualquer *Host*. Posteriormente deve-se executar o comando de restart para aceitar as configurações do serviço.

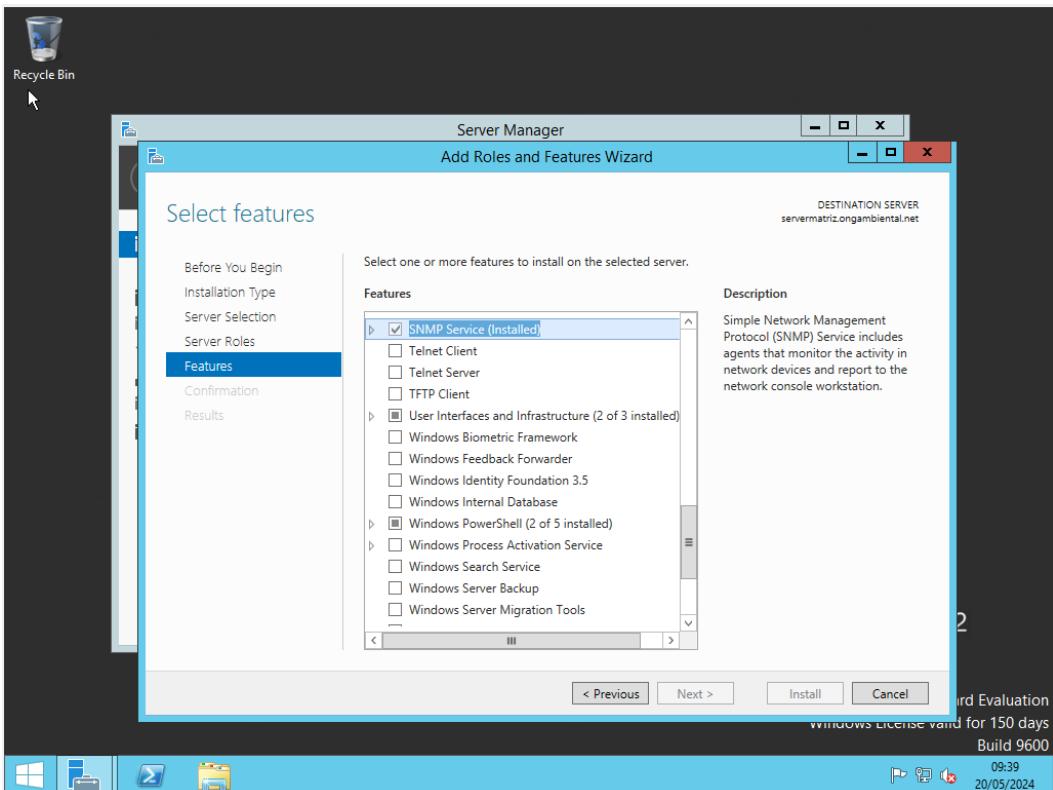


Figura 17 – Instalação do recurso SNMP no servidor local

Fonte: Elaborada pelos autores

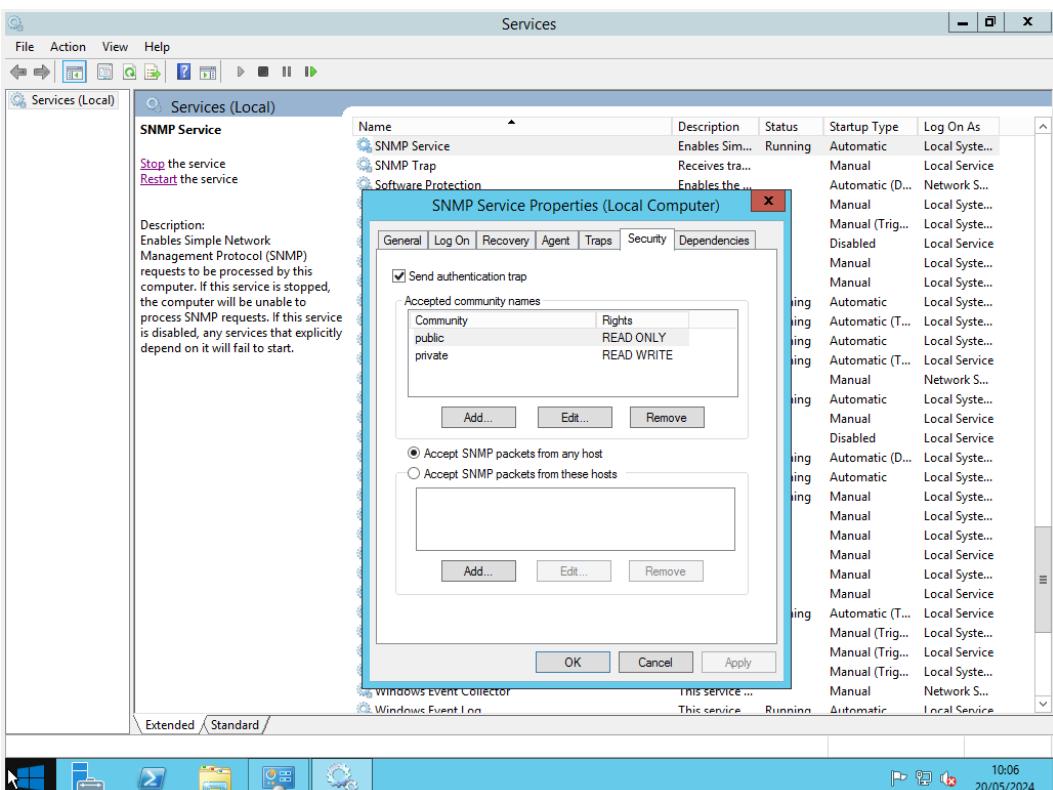


Figura 18 – Configuração do recurso SNMP no servidor local

Fonte: Elaborada pelos autores

No Zabbix foi criado o *Host* na seção “Data collection” em “Hosts”. A sua

configuração é apresentada na Figura 19.

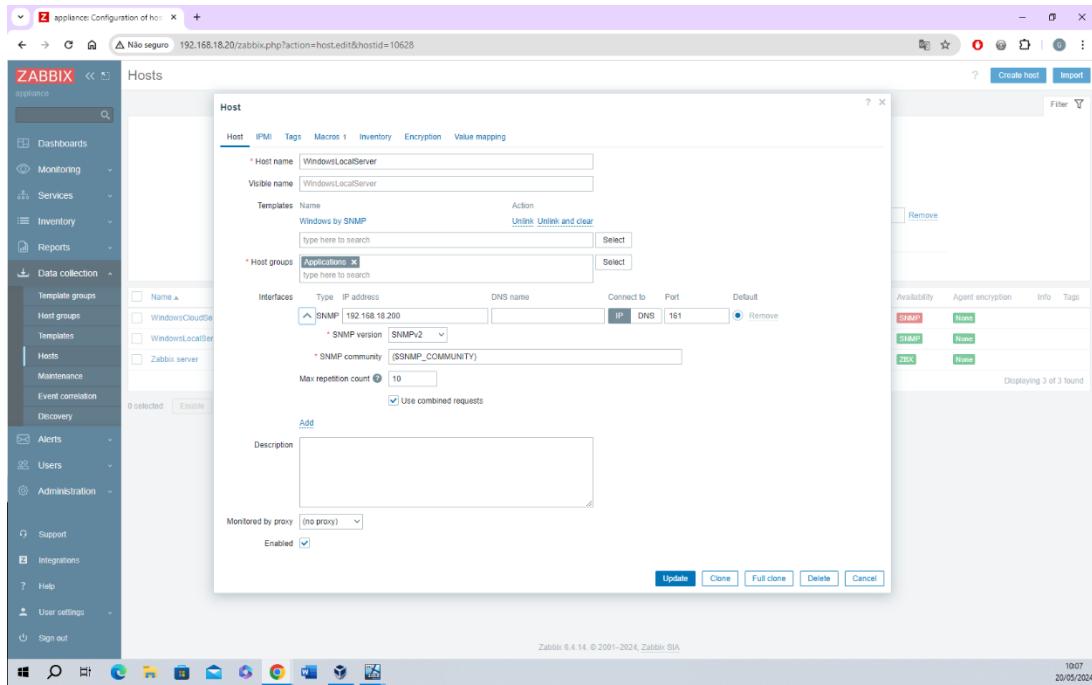


Figura 19 – Criação do Host do servidor local no Zabbix

Fonte: Elaborada pelos autores

Fez-se necessário também configurar a macro do protocolo SNMP para estabelecer a comunicação entre o Zabbix e o servidor local, conforme a Figura 20.

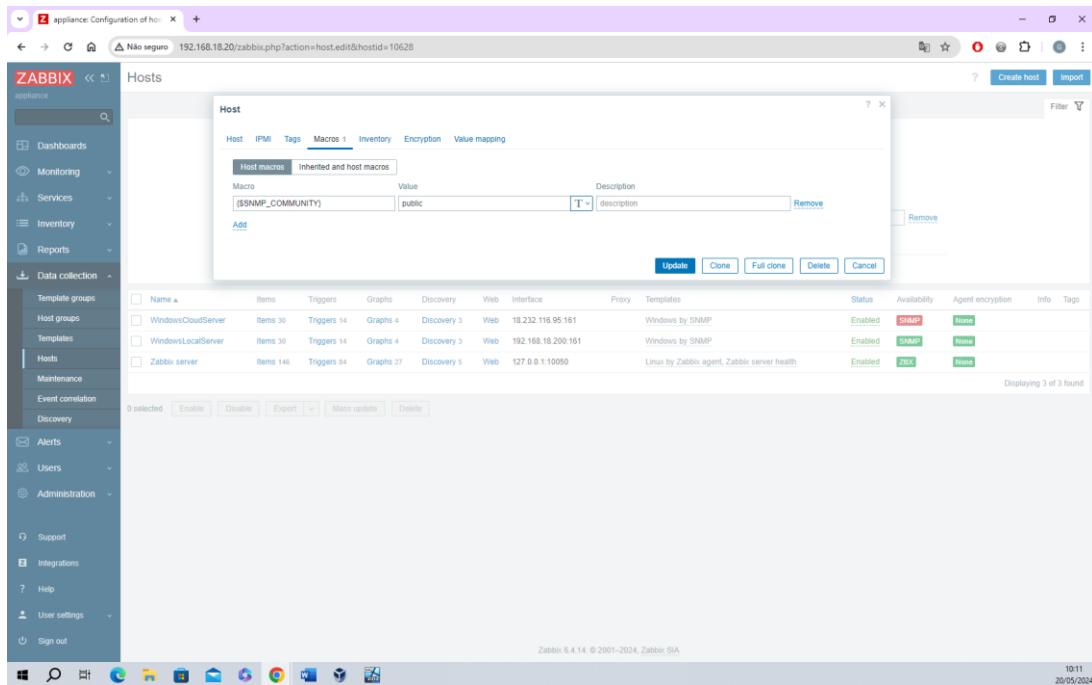


Figura 20 – Configuração da macro do servidor local no Zabbix

Fonte: Elaborada pelos autores

Após essas configurações iniciais para a comunicação entre o Zabbix e o servidor local, ocorreu o erro de *timeout* de resposta do servidor, assim impedindo o estabelecimento do canal de comunicação. Durante a análise do problema, foi identificado que o *firewall* do Windows no servidor local não estava liberando a porta 161. Para solucionar o problema na comunicação e troca de dados entre o Zabbix e o servidor local, foi realizada uma configuração adicional na regra de entrada do serviço SNMP no domínio privado do *firewall*, conforme a Figura 21.

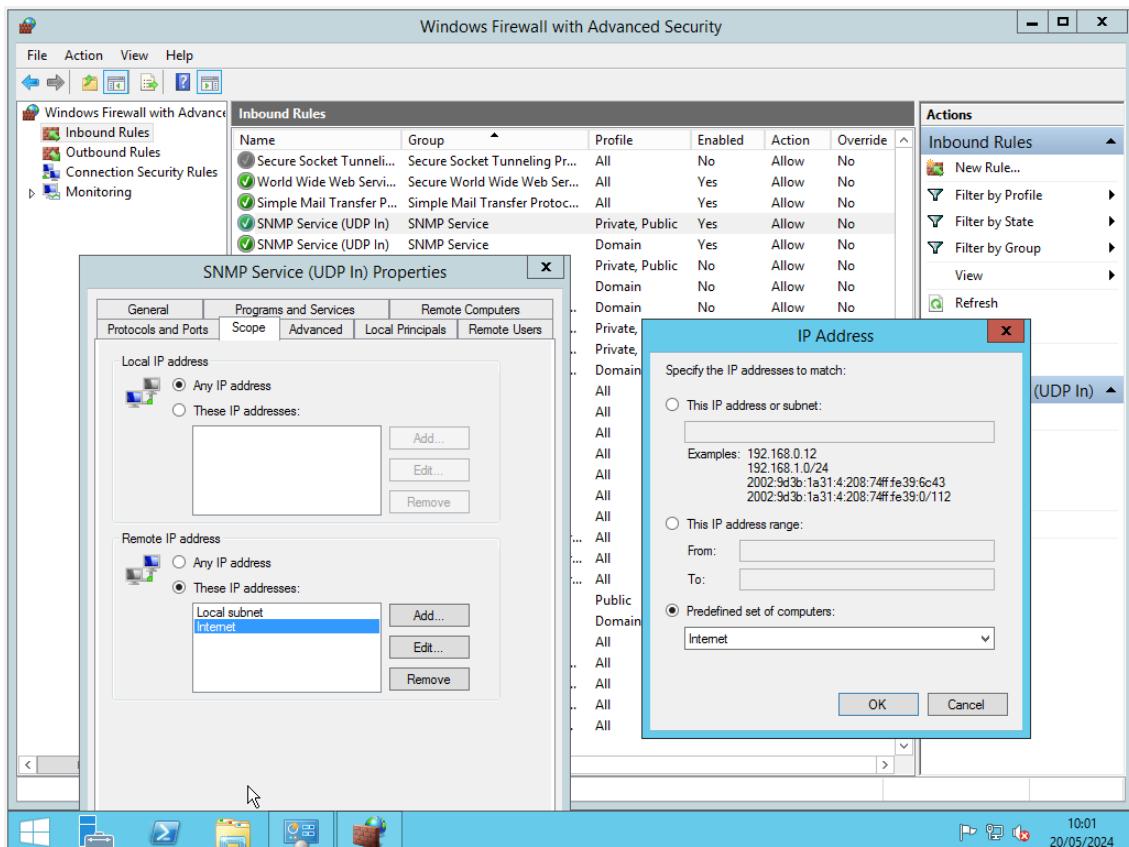


Figura 21 – Configuração do *firewall* do servidor local
Fonte: Elaborada pelos autores

Com isso, a comunicação via SNMP foi estabelecida e pode-se visualizar o Host “WindowsLocalServer” com “Status Ativo” e a comunicação via SNMP funcionando, conforme a Figura 22.

Figura 22 – Comunicação via SNMP funcionando
Fonte: Elaborada pelos autores

Prosseguiu-se então para a monitoração e geração de relatório específicos do servidor local no Zabbix, na seção “Monitoring” em “Hosts” (Figura 23).

Figura 23 – Monitoração do servidor local no Zabbix
Fonte: Elaborada pelos autores

Por fim, a Figura 24 apresenta a monitoração da interface de rede,

enquanto as Figura 25 e 26 a monitoração da performance do sistema.

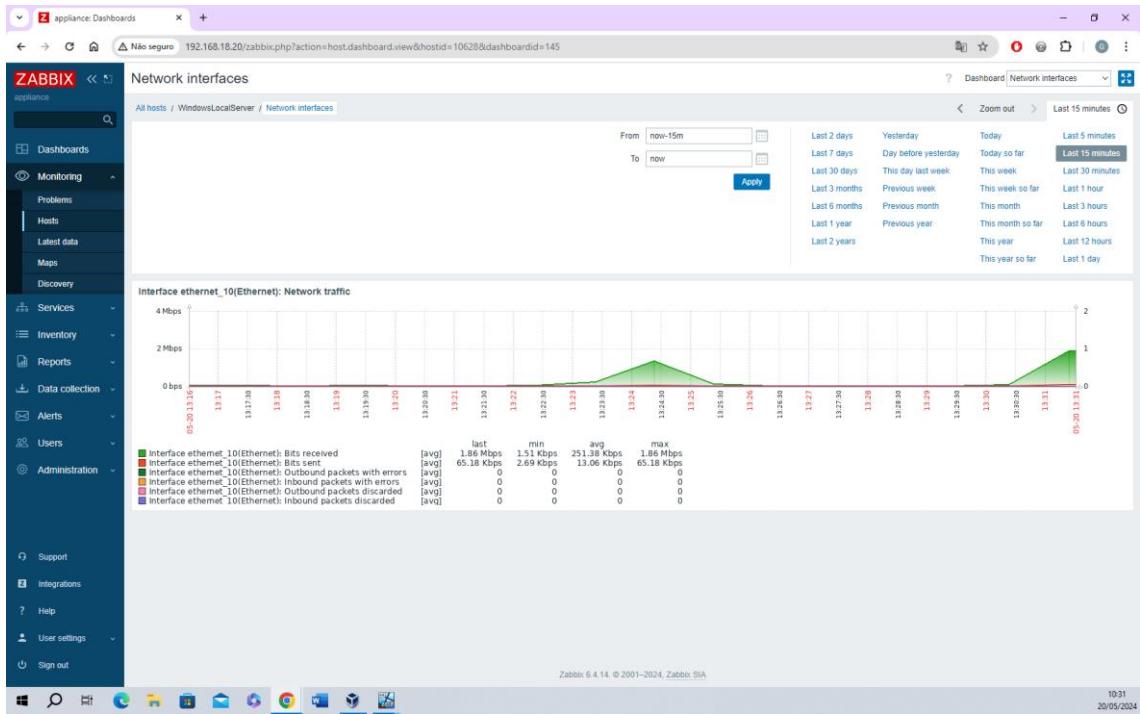


Figura 24 – Monitoração da interface de rede do servidor local no Zabbix
Fonte: Elaborada pelos autores

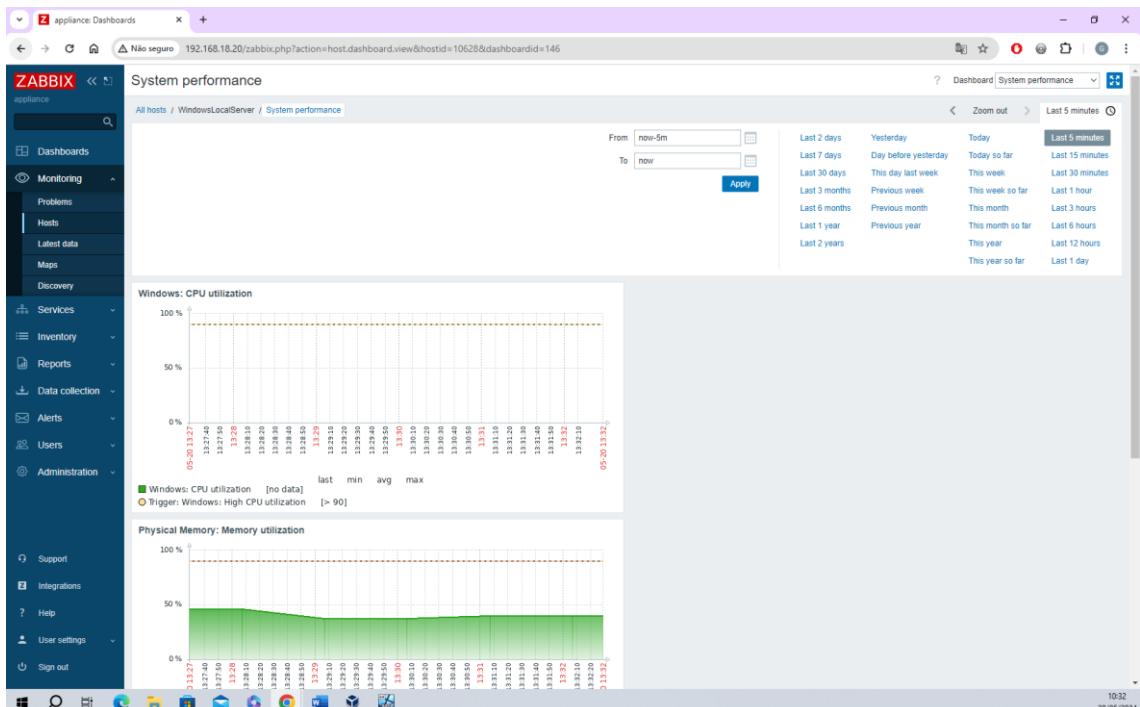


Figura 25 – Monitoração da performance do sistema do servidor local no Zabbix
Fonte: Elaborada pelos autores

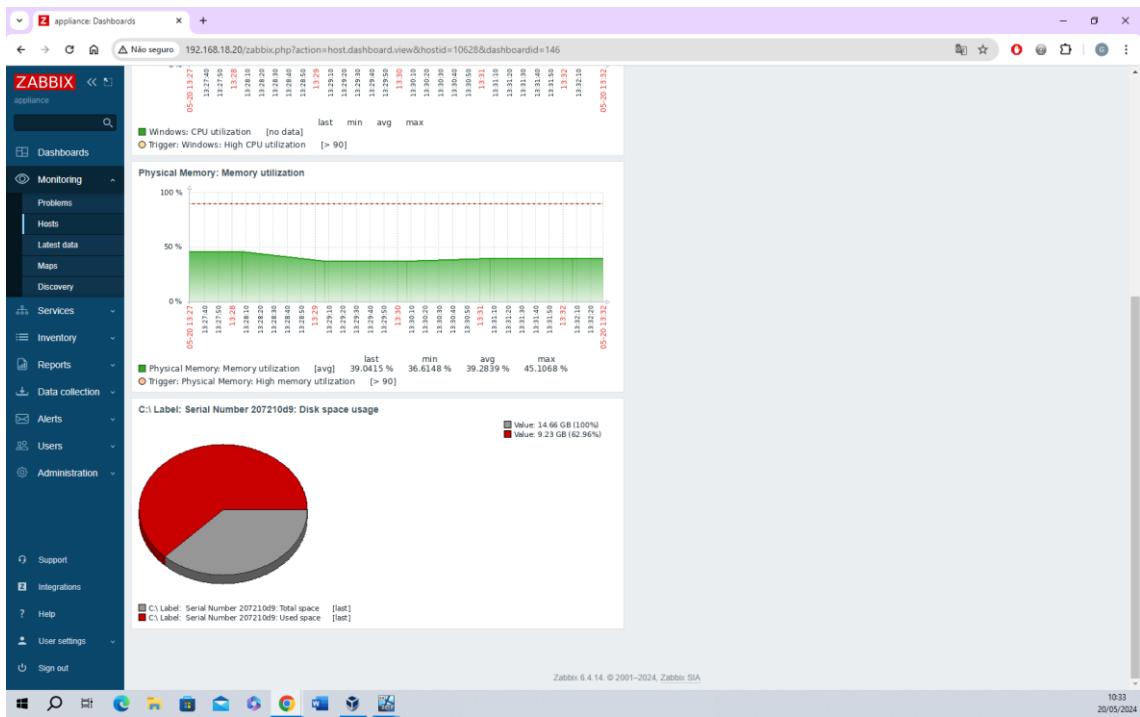


Figura 26 – Monitoração da performance do sistema do servidor local no Zabbix
Fonte: Elaborada pelos autores

6.2 GERENCIAMENTO DO SERVIDOR DA NUVEM NO ZABBIX

Após a inicialização de uma instância EC2 na VPC da AWS contendo o Windows Server 2016 Base, foi instalado o recurso SNMP na máquina e efetuado a configuração do serviço analogamente ao procedimento realizado no servidor local (Figura 27).

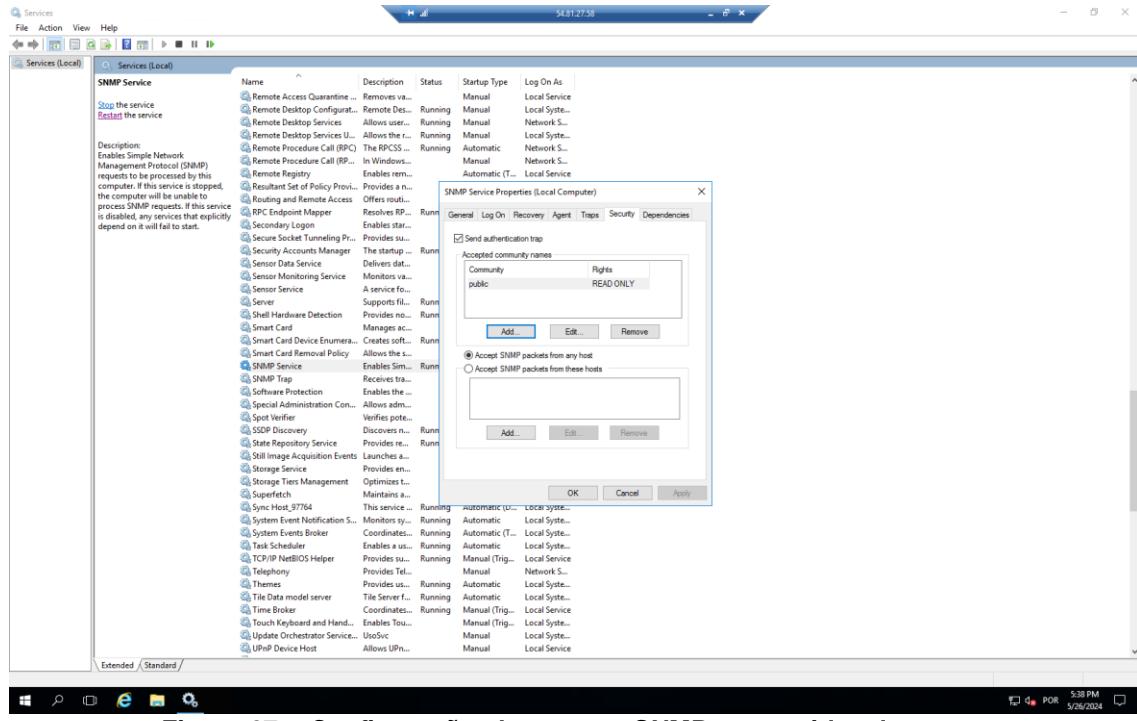
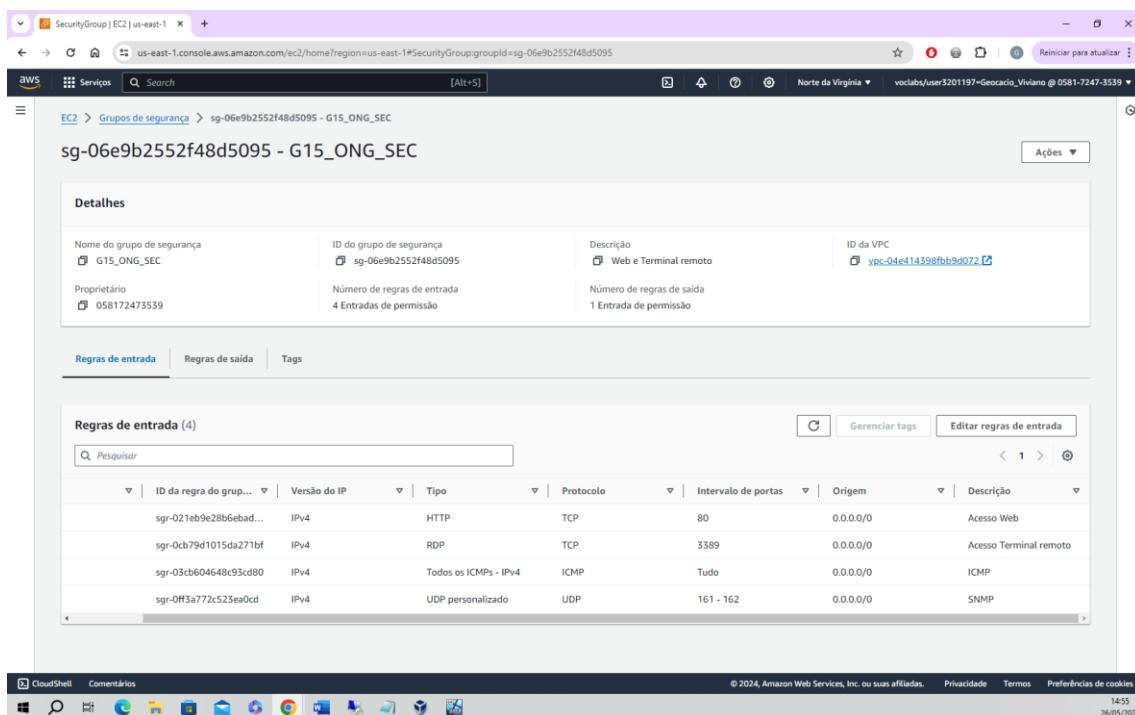


Figura 27 – Configuração do recurso SNMP no servidor da nuvem
Fonte: Elaborada pelos autores

A configuração do Zabbix para monitoração do servidor da nuvem é apresentada na Figura 28.

Figura 28 – Criação do Host do servidor da nuvem no Zabbix
Fonte: Elaborada pelos autores

Por fim, para estabelecer a comunicação via SNMP do servidor da nuvem foi necessário configurar o grupo de segurança da instância EC2 na AWS com a adição da regra de entrada ICMP, conforme apresentado na Figura 29.



The screenshot shows the AWS CloudFront interface for creating a security group rule. The URL is <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroup:groupId=sg-06e9b2552f48d5095>. The page displays the details of the security group 'sg-06e9b2552f48d5095 - G15_ONG_SEC' with the following information:

Nome do grupo de segurança G15_ONG_SEC	ID do grupo de segurança sg-06e9b2552f48d5095	Descrição Web e Terminal remoto	ID da VPC vpc-04e414398fb9d072
Proprietário 058172473539	Número de regras de entrada 4 Entradas de permissão	Número de regras de saída 1 Entrada de permissão	

Below this, there are tabs for 'Regras de entrada', 'Regras de saída', and 'Tags'. The 'Regras de entrada' tab is selected, showing a table with four rows of rules:

ID da regra do grupo	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
sgr-021eb9e28b6ebad...	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web
sgr-0cb79d1015da271bf	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso Terminal remoto
sgr-03cb604648c93cd80	IPv4	Todos os ICMPs - IPv4	ICMP	Tudo	0.0.0.0/0	ICMP
sgr-0ff3a772c523ea0cd	IPv4	UDP personalizado	UDP	161 - 162	0.0.0.0/0	SNMP

Figura 29 – Criação do Host do servidor da nuvem no Zabbix
Fonte: Elaborada pelos autores

A Figura 30 apresenta a monitoração da interface de rede e as Figura 31 e 32 a monitoração da performance do sistema.

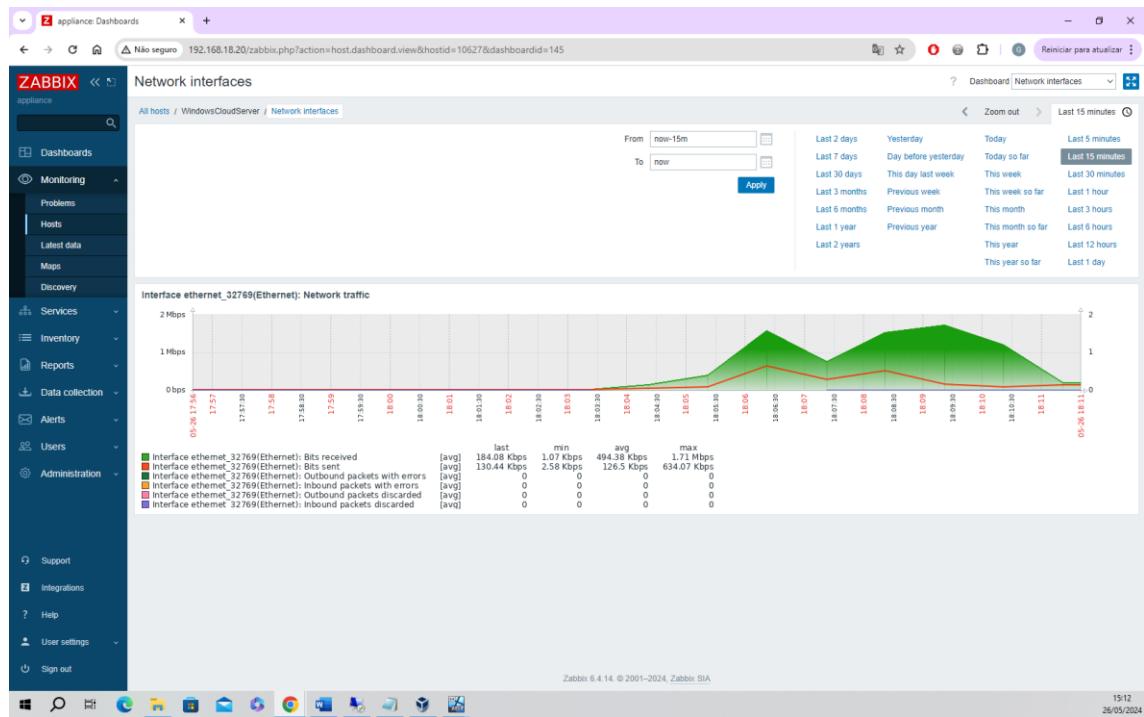


Figura 30 – Monitoração da interface de rede do servidor da nuvem no Zabbix
Fonte: Elaborada pelos autores

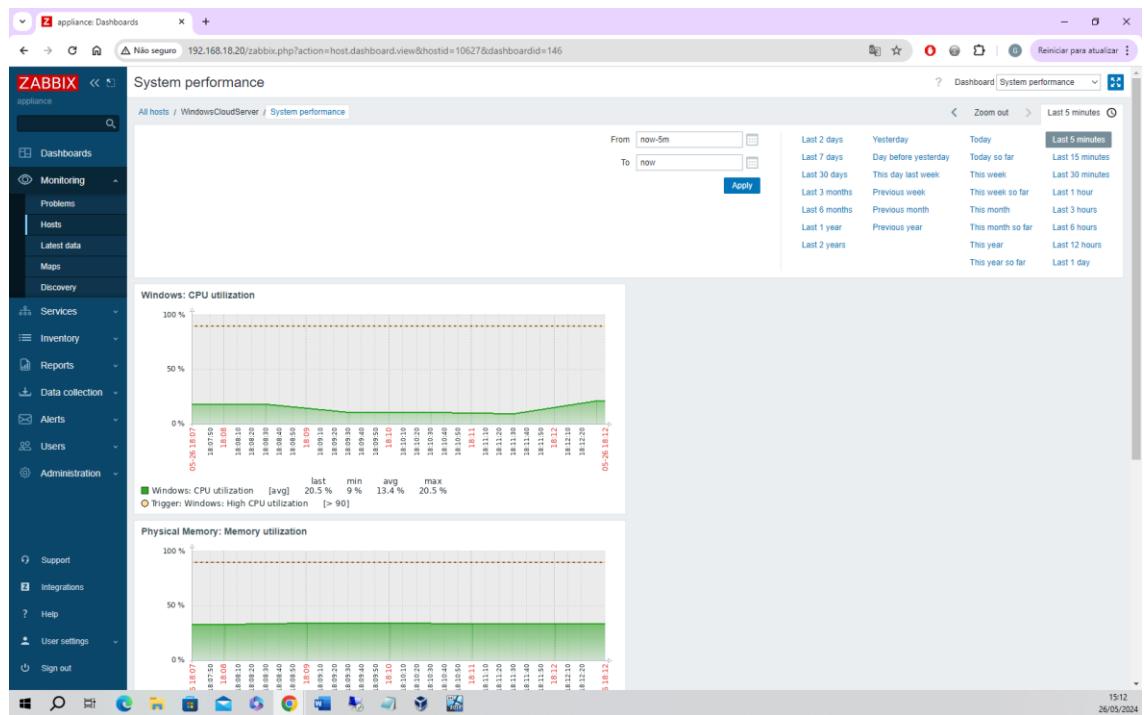


Figura 31 – Monitoração da performance do sistema do servidor da nuvem no Zabbix
Fonte: Elaborada pelos autores

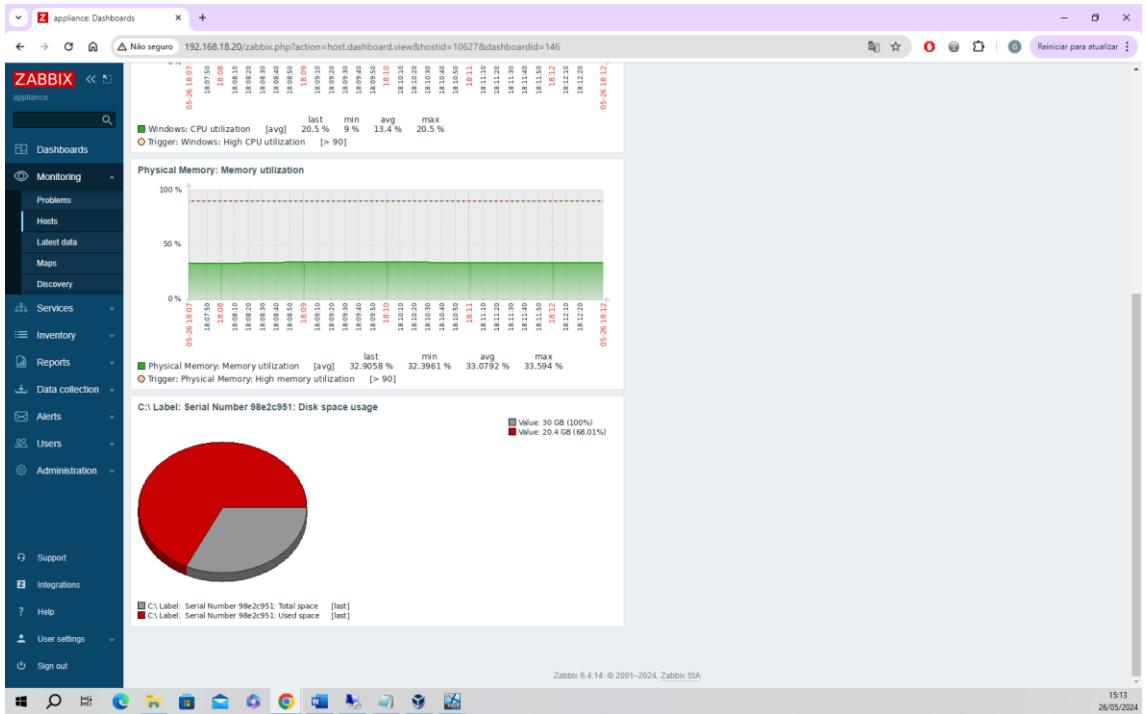


Figura 32 – Monitoração da performance do sistema do servidor da nuvem no Zabbix
Fonte: Elaborada pelos autores

6.3 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO

ZABBIX

Com as configurações adequadas realizadas tanto no servidor local quanto no servidor na nuvem, foi possível monitorá-los com sucesso no Zabbix, conforme apresentado na Figura 33.

The screenshot shows the Zabbix web interface with the URL 192.168.18.20/zabbix.php?action=host.list. The left sidebar navigation includes: Dashboards, Monitoring, Services, Inventory, Reports, Data collection (selected), Host groups, Templates, Hosts (selected), Maintenance, Event correlation, Discovery, Alerts, Users, Administration, Support, Integrations, Help, User settings, and Sign out. The main content area is titled 'Hosts' and contains search and filter fields for Host groups, Status, Monitored by (Any, Server, Proxy), Name, DNS, IP, Port, and Tags. Below these are buttons for 'Apply' and 'Reset'. A table lists three hosts:

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
WindowsCloudServer	Items 30	Triggers 14	Graphs 4	Discovery 3	Web	54.81.27.59:161	Windows by SNMP		Enabled	SNMP	None		
WindowsLocalServer	Items 30	Triggers 14	Graphs 4	Discovery 3	Web	192.168.18.200:161	Windows by SNMP		Enabled	SNMP	None		
Zabbix server	Items 146	Triggers 84	Graphs 27	Discovery 5	Web	127.0.0.1:1050	Linux by Zabbix agent, Zabbix server health		Enabled	ZBX	None		

At the bottom of the table are buttons for '0 selected', 'Enable', 'Disable', 'Export', 'Mass update', and 'Delete'. The footer of the page includes the text 'Zabbix 6.4.14. © 2001–2024, Zabbix SIA' and the date '15:46 26/05/2024'.

Figura 33 – Monitoração do servidor local e da nuvem no Zabbix

Fonte: Elaborada pelos autores

E por fim, a Figura 34 apresenta o mapa de rede, ilustrando a integração entre o Zabbix e os servidores.

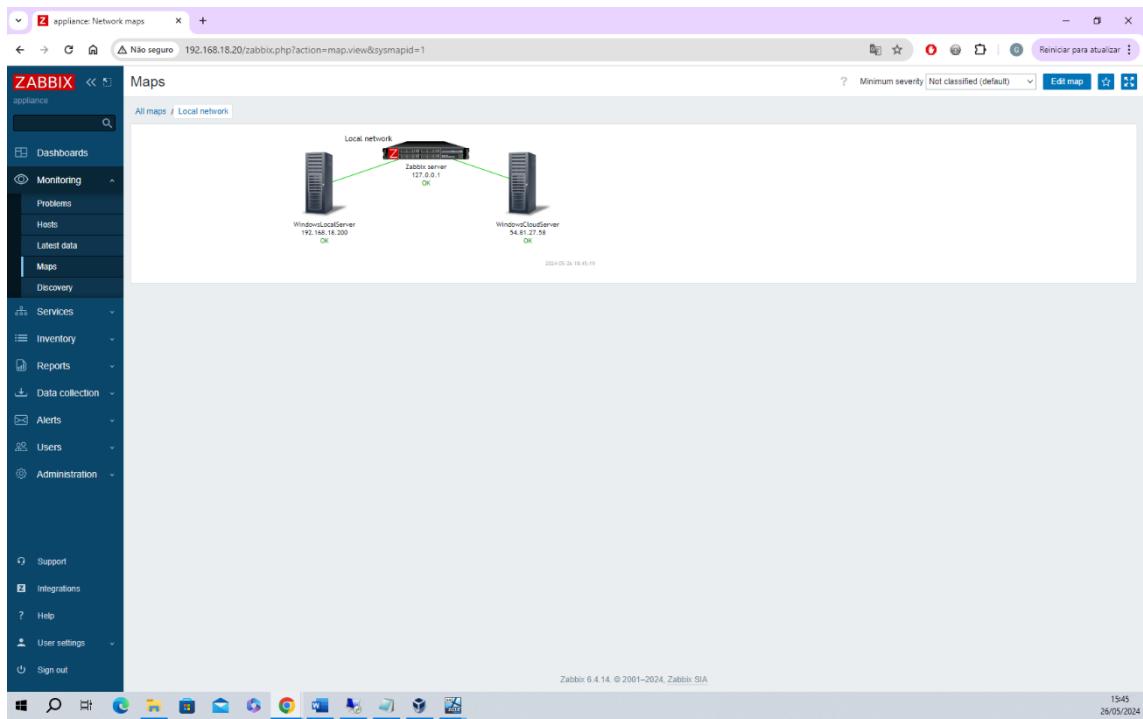


Figura 34 – Mapa de rede da infraestrutura monitorada pelo Zabbix
Fonte: Elaborada pelos autores

7. APLICAÇÃO BACK-END

O portal foi desenvolvido usando *JavaScript* como **Back-End** e é possível realizar as 4 operações básicas de banco de dados, tendo persistência entre as sessões. Porém, um banco de dados externo não foi integrado, tendo sido feito armazenamento local.

7.1. TELAS DA APLICAÇÃO BACK-END

É possível realizar as 4 operações básicas de banco de dados, sendo: *CREATE, READ, UPDATE e DELETE*. As operações são apresentadas a seguir.

Na Figura 35 é realizada o cadastro de ocorrência ambiental é realizada pelo usuário no formulário.

The screenshot shows a web-based form titled "Novo cadastro de ocorrência". The form has a light gray background with a white input area. It includes the following fields:

- Nome:** Fernando Mario
- Email:** nandomario32@sga.com.br
- Descrição da Ocorrência (Desmatamento, Poluição Hídrica, Carro Abandonado, Queimada, etc.):** Desmatamento
- Cidade:** Contagem
- Estado (UF):** Minas Gerais

At the bottom center of the form is a blue rectangular button labeled "Cadastrar".

Figura 35 – Novo cadastro de ocorrência (CREATE)
Fonte: Elaborada pelos autores

Após a criação da ocorrência as informações resumidas são incluídas em uma lista em que cada linha selecionada pode ser lida, atualizada e excluída conforme apresentado na Figura 36.

Nome	Email	Ocorrência	Cidade	Estado	Nova Ocorrência
João Pedro	joaopedro@hotmail.com	Queimada ilegal	São José da Lapa	Minas Gerais	Editar Excluir
Bárbara	barbara@hih.com.br	Descarte irregular lixo	Belo Horizonte	Minas Gerais	Editar Excluir
Francisco Junior	fran1234@outlook.com.br	Carro abandonado	Ibirité	Minas Gerais	Editar Excluir
Beatriz	bea12@hotmail.com	Desmatamento	Baldim	Minas Gerais	Editar Excluir
Fernando Mario	nandomario32@sga.com.br	Desmatamento	Contagem	Minas Gerais	Editar Excluir

Figura 36 – CRUD da aplicação Back-End para o Site da ONG

Fonte: Elaborada pelos autores

Por fim, na Figura 37 é apresentada a persistência dos dados no servidor local no formato de *DB JSON*.

```
admin > db.json > ...
admin > db.json > ...
1  {
2    "profile": [
3      {
4        "id": "cd96",
5        "nome": "João Pedro",
6        "email": "joaopedro@hotmail.com",
7        "ocorrencia": "Queimada ilegal",
8        "cidade": "São José da Lapa",
9        "uf": "Minas Gerais"
10       },
11      {
12        "id": "6334",
13        "nome": "Bárbara",
14        "email": "barbara@hih.com.br",
15        "ocorrencia": "Descarte irregular lixo",
16        "cidade": "Belo Horizonte",
17        "uf": "Minas Gerais"
18      },
19      {
20        "id": "cfa8",
21        "nome": "Francisco Junior",
22        "email": "fran1234@outlook.com.br",
23        "ocorrencia": "Carro abandonado",
24        "cidade": "Ibirité",
25        "uf": "Minas Gerais"
26      },
27      {
28        "id": "6885",
29        "nome": "Beatriz",
30        "email": "bea12@hotmail.com",
31        "ocorrencia": "Queimada ilegal",
32        "cidade": "Baldim",
33        "uf": "Minas Gerais"
34      }
35    ]
36  }
```

Figura 37 – Persistência dos dados no servidor local

Fonte: Elaborada pelos autores

8. REFERÊNCIAS

Tabela de Materiais:

Servidor Dell - Disponível em: [Link](#)

Estação Dell - Disponível em: [Link](#)

Roteador Cisco - Disponível em: [Link](#)

AP Cisco Wifi - Disponível em: [Link](#)

Rack 44 U Central Network - Disponível em: [Link](#)

Serial Cisco - Disponível em: [Link](#)

Switch Dell 24p - Disponível em: [Link](#)

Cabo de rede CAT6 cx c/305m - Disponível em: [Link](#)

RJ45 f CAT6 - Disponível em: [Link](#)

Patch Cord CAT 6 - Disponível em: [Link](#)

Patch Panel CAT 6 - Disponível em: [Link](#)

Organizador de Cabo Central Network - Disponível em: [Link](#)

Impressora - Disponível em: [Link](#)

Nobreak - Disponível em: [Link](#)

Mesa + Cadeira - Disponível em: [Link](#)

ANEXO I

A Cartilha da Política de Segurança da Informação da ONG, que aborda de forma concisa os tópicos da PSI, está ilustrada nas Figuras 38 e 39. Em seguida, a PSI é apresentada na íntegra.

CARTILHA DE SEGURANÇA DA INFORMAÇÃO

ONG AMBIENTAL 2024

OLÁ!

Esta cartilha foi elaborada para ajudá-lo a entender e seguir a Política de Segurança da Informação da ONG. Manter a segurança da informação é responsabilidade de todos. Leia atentamente e siga as diretrizes para proteger nossos dados e recursos.

1. INTRODUÇÃO

A Política de Segurança da Informação da ONG estabelece as diretrizes e responsabilidades para proteger os ativos de informação da organização contra ameaças internas e externas. Esta política abrange todas as áreas da organização e se aplica a todos os funcionários, voluntários, contratados e parceiros que tenham acesso a sistemas, dados e informações da ONG.

2. OBJETIVOS

- Proteger informações sensíveis: Assegurar que dados confidenciais estejam seguros contra acessos não autorizados.
- Cumprir com leis e regulamentos: Adotar práticas de segurança que atendam às exigências legais.
- Promover a conscientização: Informar e educar todos os usuários sobre a importância da segurança da informação.

3. RESPONSABILIDADES

- Todos os usuários: Devem seguir as diretrizes da política e relatar incidentes de segurança.
- Equipe de TI: Responsável pela implementação e manutenção das medidas de segurança.
- Gestores: Devem assegurar que suas equipes compreendam e sigam a política.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

- Confidencial: Dados altamente sensíveis, como informações pessoais e financeiras.
- Interna: Informações relacionadas às operações da ONG, acessíveis apenas a funcionários autorizados.
- Pública: Informações que podem ser divulgadas sem causar prejuízo à organização.

5. DISPOSIÇÕES GERAIS

- a. Uso da Internet
 - Utilize a internet apenas para fins profissionais.
 - Evite acessar sites não seguros ou de conteúdo inadequado.
- b. Uso do Email
 - Utilize o email corporativo apenas para comunicações relacionadas ao trabalho.
 - Não abra anexos ou links de remetentes desconhecidos.
 - c. Redes Sem Fio (WiFi)
 - Conecte-se apenas a redes WiFi seguras.
 - Utilize VPN para acessar recursos internos remotamente.
 - d. Uso de Recursos de TI
 - Use os equipamentos e softwares da ONG apenas para fins profissionais.
 - Não instale softwares não autorizados.
 - e. Uso de Mídias Sociais
 - Não compartilhe informações confidenciais ou sensíveis em mídias sociais.
 - Representar a ONG de maneira profissional e responsável.
 - f. Áudio, Vídeos e Fotos
 - Utilize mídias apenas para fins autorizados e relacionados ao trabalho
 - g. Limpeza e Organização do Ambiente de Trabalho
 - Mantenha a mesa de trabalho limpa e organizada.
 - Bloqueie a tela do computador sempre que se afastar da mesa e armazene documentos físicos de maneira segura.
 - Descarte documentos confidenciais, utilizando serviços de destruição apropriados.

ELABORADO PELO DEPARTAMENTO DE TI

Figura 38 – Frente da Cartilha

Fonte: Elaborada pelos autores

CARTILHA DE SEGURANÇA DA INFORMAÇÃO

ONG AMBIENTAL 2024

6. CONTROLE DE ACESSO



- Senhas Seguras: Use senhas fortes e únicas, alterando-as regularmente.
- Autenticação Multifator (MFA): Ative MFA para aumentar a segurança das contas.
- Privilégios de Acesso: Acesso aos sistemas e dados deve ser concedido com base na necessidade de conhecer.

7. PROTEÇÃO DE DADOS



- Criptografia: Utilize criptografia para proteger dados sensíveis durante armazenamento e transmissão.
- Backups: Realize backups regulares de dados críticos.



8. SEGURANÇA DA REDE

- Firewalls e Antivírus: Mantenha os sistemas protegidos com firewalls e software antivírus atualizados.
- Monitoramento de Rede: Monitore o tráfego de rede para identificar e responder a atividades suspeitas.

9. GESTÃO DE INCIDENTES

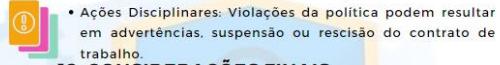


- Relato de Incidentes: Relate imediatamente quaisquer incidentes de segurança ou violações à equipe de TI.
- Resposta a Incidentes: Siga os procedimentos estabelecidos para responder rapidamente a incidentes.

10. REVISÃO E AUDITORIA

- Avaliações Periódicas: Realize auditorias regulares para garantir a conformidade com a política.
- Atualizações: Atualize a política conforme necessário para abordar novas ameaças e regulamentações.

11. PENALIDADES POR VIOLAÇÃO



12. CONSIDERAÇÕES FINAIS

- Ações Disciplinares: Violações da política podem resultar em advertências, suspensão ou rescisão do contrato de trabalho.

OBRIGADO PELA SUA COLABORAÇÃO!

ELABORADO PELO DEPARTAMENTO DE TI

Figura 39 – Verso da Cartilha

Fonte: Elaborada pelos autores

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução	3
2. Objetivos.....	3
2.1. Garantir a Confidencialidade.....	4
2.2. Assegurar a Integridade	4
2.3. Manter a Disponibilidade	4
2.4. Conformidade com Leis e Regulamentos	4
2.5. Proteção contra Ameaças.....	4
2.6. Gestão de Riscos.....	4
2.7. Educação e Conscientização	5
2.8. Proteção de Dados Pessoais.....	5
2.9. Melhoria Contínua.....	5
2.10. Sustentabilidade Operacional	5
3. Responsabilidades.....	5
3.1. Diretoria Executiva.....	5
3.2. Gerente de TI	6
3.3. Equipe de TI	6
3.4. Gestores de Departamento.....	6
3.5. Usuários (Funcionários, Voluntários e Prestadores de Serviços).....	7
3.6. Comitê de Segurança da Informação	7
3.7. Auditores Internos	7
3.8. Consultores Externos	7
4. Classificação da Informação	7
4.1. Confidencial.....	8
4.2. Interna.....	8
4.3. Pública.....	9
5. Disposições gerais	9
5.1. Internet.....	9
5.2. Recurso de correio eletrônico (e-mail)	9
5.3. Redes sem fio (Wi-Fi).....	9
5.4. Recursos de TI institucionais	10

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

5.5. Recursos de TI particulares	10
5.6. Mídias sociais.....	10
5.7. Uso de áudio, vídeos e fotos.....	10
6. Controle de Acesso.....	10
6.1. Princípio do Menor Privilégio	10
6.2. Autenticação.....	11
6.3. Autorização	11
6.4. Controle de Acesso Físico.....	11
6.5. Monitoramento e Auditoria.....	11
6.6. Gestão de Contas	11
6.7. Segregação de Funções.....	12
6.8. Acesso Remoto	12
7. Proteção de dados.....	12
7.1. Criptografia.....	12
7.2. <i>Backup</i> e Recuperação de Dados	12
7.3. Controle de Acesso.....	13
7.4. Descarte Seguro de Dados.....	13
7.5. Proteção Contra Malware e Ameaças Cibernéticas	13
7.6. Privacidade e Conformidade com a LGPD	13
7.7. Acordos de Confidencialidade.....	14
8. Segurança da informação.....	14
8.1. <i>Firewall</i>	14
8.2. Segurança de Perímetro.....	14
8.3. Criptografia de Dados	15
8.4. Controle de Acesso à Rede (NAC)	15
8.5. Atualizações e <i>Patches</i>	15
8.6. Proteção contra <i>Malware</i>	15
8.7. Segurança Física	15
9. Gestão de incidentes.....	16
9.1. Definição de Incidentes	16
9.2. Detecção e Notificação.....	16
9.3. Avaliação e Análise.....	16

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

9.4. Resposta e Mitigação.....	16
9.5. Comunicação e Notificação	17
9.6. Documentação e Relatório	17
9.7. Equipe de Resposta a Incidentes	17
Revisão e Melhoria Contínua	17
10. Revisão e auditoria.....	17
10.1. Auditorias Internas Regulares	18
10.2. Avaliação de Conformidade.....	18
10.3. Testes de Penetração e Vulnerabilidade.....	18
10.4. Revisão de Políticas e Procedimentos.....	18
10.5. Avaliação de Controles Técnicos	19
10.6. Avaliação de Conscientização e Treinamento	19
10.7. Análise de Incidentes Anteriores	19
10.8. Relatórios e Recomendações	19
10.9. Acompanhamento e Implementação de Recomendações	19
10.10. Melhoria Contínua do Processo de Auditoria.....	19
11. Penalidades de violação da política de segurança da informação	20
11.1. Ações Disciplinares:	20
11.2. Restrições de Acesso:.....	20
11.3. Responsabilidade Legal:.....	20
11.4. Educação e Conscientização Adicionais:	20
11.5. Perda de Privilégios:	21
11.6. Sanções Financeiras:	21
11.7. Revisão das Políticas e Procedimentos:	21
11.8. Comunicação Interna:	21
12. Considerações finais	21

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

1. Introdução

A segurança da informação é um componente crítico para a proteção dos ativos digitais e físicos de qualquer organização, incluindo as organizações não governamentais (ONGs), que frequentemente lidam com dados sensíveis de beneficiários, doadores e parceiros. No contexto atual, onde as ameaças cibernéticas estão em constante evolução, garantir a integridade, confidencialidade e disponibilidade das informações tornou-se indispensável.

Esta Política de Segurança da Informação foi desenvolvida para o Departamento de TI da ONG com o objetivo de estabelecer diretrizes claras e práticas que assegurem a proteção das informações e sistemas de informação da organização. Ao implementar esta política, busca-se não apenas cumprir com as exigências legais e regulamentares, mas também reforçar a confiança de todos os stakeholders que confiam na ONG para conduzir suas atividades de maneira segura e responsável.

A política está alinhada com a norma ABNT NBR ISO/IEC 27001, que estabelece requisitos para um sistema de gestão de segurança da informação (SGSI). Esta norma fornece uma abordagem sistemática para gerenciar informações sensíveis, garantindo sua segurança por meio da avaliação e tratamento de riscos, implementação de controles de segurança específicos e criação de uma estrutura organizacional robusta para a gestão de segurança da informação. A conformidade com a ABNT NBR ISO/IEC 27001 é uma evidência do compromisso da ONG com as melhores práticas de segurança da informação reconhecidas internacionalmente.

Reconhece-se que a segurança da informação é uma responsabilidade coletiva que requer a colaboração de todos os membros da ONG, desde a diretoria até os voluntários. Esta política detalha as responsabilidades de cada grupo dentro da organização, as medidas de segurança que devem ser adotadas, e os procedimentos para gerenciar incidentes de segurança. Além disso, enfatiza-se a importância de uma cultura de conscientização e de treinamento contínuo para todos os envolvidos.

Com esta política, a ONG reafirma seu compromisso em proteger as informações e em operar de maneira ética e segura, garantindo que suas atividades possam continuar a beneficiar aqueles a quem serve, sem comprometer a segurança e a privacidade dos dados.

2. Objetivos

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

A política de segurança da informação da ONG visa alcançar os seguintes objetivos fundamentais:

2.1. Garantir a Confidencialidade

- Proteger informações sensíveis contra acessos não autorizados.
- Assegurar que apenas pessoas autorizadas tenham acesso a dados confidenciais.

2.2. Assegurar a Integridade

- Manter a precisão e a completude das informações e dos sistemas de processamento de dados.
- Prevenir alterações não autorizadas nos dados, seja acidental ou intencionalmente.

2.3. Manter a Disponibilidade

- Garantir que as informações e os sistemas de informação estejam disponíveis para uso quando necessário.
- Minimizar o tempo de inatividade e assegurar a continuidade das operações.

2.4. Conformidade com Leis e Regulamentos

- Assegurar que todas as práticas de segurança da informação estejam em conformidade com as leis e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD).
- Atender aos requisitos de regulamentações específicas do setor e normas internacionais, como a ABNT NBR ISO/IEC 27001.

2.5. Proteção contra Ameaças

- Implementar medidas para identificar, prevenir e responder a ameaças cibernéticas.
- Proteger a organização contra-ataques cibernéticos, vazamentos de dados, malware e outras ameaças de segurança.

2.6. Gestão de Riscos

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Realizar avaliações contínuas de risco para identificar vulnerabilidades e implementar controles adequados.
- Desenvolver e manter um plano de resposta a incidentes para lidar com potenciais violações de segurança.

2.7. Educação e Conscientização

- Promover uma cultura de segurança da informação entre todos os membros da ONG.
- Oferecer treinamentos regulares e campanhas de conscientização para garantir que todos compreendam a importância da segurança da informação e saibam como proteger os dados.

2.8. Proteção de Dados Pessoais

- Assegurar que os dados pessoais dos beneficiários, doadores, voluntários e funcionários sejam tratados com respeito e protegidos contra usos indevidos.
- Implementar medidas para garantir a privacidade e a segurança dos dados pessoais conforme as melhores práticas e normas vigentes.

2.9. Melhoria Contínua

- Monitorar e revisar continuamente as práticas e políticas de segurança da informação para garantir sua eficácia.
- Implementar melhorias contínuas baseadas em novas ameaças, tecnologias emergentes e lições aprendidas de incidentes passados.

2.10. Sustentabilidade Operacional

- Assegurar que a segurança da informação suporte a missão e os objetivos estratégicos da ONG.
- Alinhar as práticas de segurança da informação com os valores e metas da organização para garantir a sustentabilidade a longo prazo.

3. Responsabilidades

Para garantir a eficácia da Política de Segurança da Informação, é essencial que todas as partes envolvidas entendam e cumpram suas responsabilidades. Abaixo estão definidas as responsabilidades de cada grupo dentro da organização:

3.1. Diretoria Executiva

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
Classificação: interna		Versão: 1.1
		Última revisão: 15/06/2024

- Aprovar e apoiar a implementação desta política.
- Alocar recursos necessários para a implementação e manutenção das medidas de segurança da informação.
- Promover uma cultura organizacional que valorize a segurança da informação.

3.2. Gerente de TI

- Desenvolver, implementar e manter a Política de Segurança da Informação.
- Realizar avaliações de risco periódicas e implementar controles adequados.
- Monitorar a conformidade com a política e relatar o status à diretoria.
- Coordenar a resposta a incidentes de segurança e a recuperação de desastres.
- Garantir que todos os sistemas de informação estejam devidamente protegidos contra ameaças.
- Supervisionar a aplicação de controles de acesso e garantir que as permissões estejam alinhadas com as funções e responsabilidades dos usuários.
- Realizar treinamentos de segurança da informação para todos os funcionários e voluntários.

3.3. Equipe de TI

- Implementar e manter os controles de segurança da informação conforme definido na política.
- Monitorar a rede e os sistemas de informação para detectar e responder a ameaças.
- Gerenciar a segurança física dos equipamentos de TI.
- Realizar backups regulares e garantir que os dados possam ser recuperados em caso de incidente.
- Assegurar que todos os dispositivos estejam atualizados com os patches de segurança mais recentes.
- Documentar e relatar incidentes de segurança ao Gerente de TI.

3.4. Gestores de Departamento

- Garantir que suas equipes compreendam e cumpram a Política de Segurança da Informação.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Colaborar com a equipe de TI para identificar e mitigar riscos específicos do departamento.
- Relatar quaisquer incidentes de segurança ou suspeitas de violações à equipe de TI imediatamente.

3.5. Usuários (Funcionários, Voluntários e Prestadores de Serviços)

- Cumprir todas as diretrizes e procedimentos de segurança da informação estabelecidos na política.
- Usar senhas fortes e mantê-las confidenciais.
- Relatar imediatamente quaisquer incidentes de segurança ou atividades suspeitas à equipe de TI.
- Participar dos treinamentos e programas de conscientização de segurança da informação.
- Manter a confidencialidade das informações acessadas durante suas atividades na ONG.
- Seguir as práticas recomendadas para o descarte seguro de informações sensíveis.

3.6. Comitê de Segurança da Informação

- Realizar revisões periódicas da Política de Segurança da Informação.
- Avaliar a eficácia dos controles de segurança e sugerir melhorias.
- Promover a conscientização sobre segurança da informação em toda a organização.
- Supervisionar a conformidade com as normas e regulamentações aplicáveis.

3.7. Auditores Internos

- Conduzir auditorias regulares para garantir a conformidade com a Política de Segurança da Informação.
- Identificar e reportar vulnerabilidades e não-conformidades.
- Recomendar melhorias baseadas nos achados das auditorias.

3.8. Consultores Externos

- Oferecer expertise em segurança da informação e apoiar na implementação de melhores práticas.
- Realizar avaliações independentes e testes de penetração para identificar vulnerabilidades.
- Fornecer treinamento especializado e capacitação para a equipe de TI.

4. Classificação da Informação

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

Para garantir a segurança e a adequada proteção das informações, todas as informações manejadas pela ONG serão classificadas em três categorias principais, baseadas em seu nível de sensibilidade e necessidade de proteção:

4.1. Confidencial

Informações que, se divulgadas sem autorização, podem causar dano significativo à ONG, seus beneficiários, doadores, parceiros ou funcionários. O acesso a estas informações é estritamente limitado a indivíduos autorizados.

Exemplos:

- Dados pessoais de beneficiários (ex.: informações de saúde, dados financeiros).
- Dados pessoais de funcionários e voluntários (ex.: CPF, endereços, dados bancários).
- Documentos estratégicos da ONG (ex.: planos de negócios, estratégias de captação de recursos).
- Informações financeiras e contábeis confidenciais.
- Contratos e acordos com parceiros e fornecedores.
- Informações sobre doadores e suas doações.

Medidas de Proteção:

- Criptografia em repouso e em trânsito.
- Controle de acesso rigoroso, baseado na necessidade de conhecimento.
- Backup seguro e armazenamento em locais seguros.
- Descarte seguro, como Trituração de documentos físicos e exclusão segura de arquivos digitais.

4.2. Interna

Informações destinadas ao uso interno da ONG, que não são publicamente disponíveis, mas cuja divulgação não autorizada teria impacto moderado. Disponível para todos os funcionários e voluntários, mas não deve ser compartilhada fora da organização sem autorização.

Exemplos:

- Políticas e procedimentos internos.
- Relatórios de reuniões internas.
- Comunicação interna (ex.: e-mails, memorandos).
- Dados operacionais não sensíveis.

Medidas de Proteção:

- Controle de acesso moderado.
- Senhas e autenticação para acesso a sistemas internos.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Backup regular e medidas de segurança básicas.

4.3. Pública

Informações que podem ser divulgadas sem restrições e cuja divulgação não causa danos à ONG, seus beneficiários, doadores, parceiros ou funcionários. Estas informações estão disponíveis para o público em geral.

Exemplos:

- Informações publicadas no site da ONG (ex.: missão, visão, valores, relatórios anuais).
- Comunicados de imprensa.
- Material de divulgação e campanhas publicitárias.
- Dados estatísticos e de impacto já divulgados.

Medidas de Proteção:

- Revisão e autorização antes da divulgação para garantir precisão.
- Monitoramento contínuo para evitar desinformação ou uso indevido.

5. Disposições gerais

5.1. Internet

- O uso da internet deve ser estritamente para fins comerciais relacionados às atividades da organização.
- Evitar o acesso a sites não seguros ou conteúdo inadequado que possa comprometer a segurança da informação.

5.2. Recurso de correio eletrônico (e-mail)

- O e-mail da organização deve ser usado apenas para fins comerciais legítimos.
- Evitar o envio ou recebimento de e-mails não relacionados ao trabalho ou de conteúdo inadequado.

5.3. Redes sem fio (Wi-Fi)

- A ONG, quando possível, oferecem à comunidade administrativa, nos ambientes autorizados e limitados ao perímetro físico da instituição, uma rede sem fio (Wi-Fi) própria para finalidades administrativas.
- Somente os colaboradores expressamente autorizados podem ter acesso à rede sem fio (Wi-Fi) da instituição e devem comprometer-se a fazer uso seguro desse recurso.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024 Versão: 1.1 Última revisão: 15/06/2024
	Classificação: interna	

- Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização do gestor imediato.

5.4. Recursos de TI institucionais

- Os recursos de TI institucionais devem ser usados apenas por funcionários autorizados para fins comerciais.

5.5. Recursos de TI particulares

- O uso de recursos de TI particulares na rede da organização deve ser autorizado e estar em conformidade com esta política.

5.6. Mídias sociais

- O uso de mídias sociais deve estar em conformidade com as diretrizes estabelecidas pela organização.

5.7. Uso de áudio, vídeos e fotos

- O uso de áudio, vídeos e fotos deve ser estritamente para fins comerciais relacionados às atividades da organização.

5.8. Limpeza e Organização do Ambiente de Trabalho

- Mantenha a mesa de trabalho limpa e organizada.
- Bloqueie a tela do computador sempre que se afastar da mesa e armazene documentos físicos de maneira segura.
- Descarte documentos confidenciais, utilizando serviços de destruição apropriados.

6. Controle de Acesso

O controle de acesso é um componente fundamental da Política de Segurança da Informação da ONG, garantindo que apenas indivíduos autorizados possam acessar informações e sistemas de acordo com suas responsabilidades e necessidades. A seguir estão detalhados os mecanismos e práticas de controle de acesso que serão implementados:

6.1. Princípio do Menor Privilégio

Todos os usuários receberão o nível mínimo de acesso necessário para realizar suas funções. Este princípio minimiza a exposição de informações sensíveis e reduz o risco de acesso não autorizado.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

6.2. Autenticação

Senhas Fortes: Todos os usuários devem utilizar senhas complexas que atendam aos seguintes critérios:

- Mínimo de 8 caracteres.
- Incluindo letras maiúsculas e minúsculas, números e caracteres especiais.
- Autenticação Multifator (MFA): Implementar MFA para acessos críticos, garantindo uma camada adicional de segurança além das senhas.
- Política de Troca de Senhas: As senhas devem ser trocadas regularmente, pelo menos a cada 90 dias, e nunca reutilizadas.

6.3. Autorização

- Perfis de Acesso: Os perfis de acesso são baseados em funções, garantindo que os usuários tenham acesso apenas aos recursos necessários para suas funções específicas.
- Revisão de Acessos: Realizar revisões periódicas dos acessos concedidos para assegurar que apenas as pessoas apropriadas mantenham seus privilégios.

6.4. Controle de Acesso Físico

- Áreas Restritas: As áreas com sistemas de informação sensíveis devem ser fisicamente protegidas, acessíveis apenas a pessoal autorizado.
- Cartões de Acesso e Biometria: Utilizar cartões de acesso ou sistemas biométricos para controlar a entrada em áreas restritas.

6.5. Monitoramento e Auditoria

- Logs de Acesso: Manter logs detalhados de todas as tentativas de acesso aos sistemas e informações sensíveis, incluindo sucesso e falha.
- Monitoramento Contínuo: Implementar ferramentas de monitoramento contínuo para detectar e alertar sobre atividades suspeitas ou anômalas.
- Auditorias Periódicas: Realizar auditorias periódicas para revisar os logs de acesso e garantir a conformidade com a política de controle de acesso.

6.6. Gestão de Contas

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Criação e Desativação de Contas: Contas de usuário devem ser criadas, modificadas e desativadas conforme a entrada, movimentação e saída de funcionários e voluntários, assegurando que os acessos sejam apropriados ao status do usuário.
- Acesso Temporário: Acessos temporários devem ser concedidos somente quando necessário e devem ter uma validade predeterminada.

6.7. Segregação de Funções

- Divisão de Responsabilidades: Assegurar que nenhuma pessoa tenha controle total sobre todas as fases de uma transação ou processo sensível, minimizando riscos de fraude e erros.

6.8. Acesso Remoto

- VPN Segura: O acesso remoto aos sistemas da ONG é realizado exclusivamente através de uma rede privada virtual (VPN) segura e autenticada.
- Políticas de BYOD (*Bring Your Own Device*): Estabelecer políticas claras para o uso de dispositivos pessoais, incluindo requisitos de segurança e conformidade com as normas da ONG.

7. Proteção de dados

A proteção de dados é um aspecto crítico da segurança da informação, especialmente para uma ONG que lida com dados sensíveis de beneficiários, doadores, parceiros e funcionários. A seguir estão detalhadas as medidas que nossa ONG implementará para garantir a proteção adequada dos dados:

7.1. Criptografia

- Dados em Repouso: Todos os dados sensíveis devem ser criptografados quando armazenados em servidores, dispositivos de armazenamento e backups.
- Dados em Trânsito: A criptografia deve ser usada para proteger dados durante a transmissão, usando protocolos seguros como SSL/TLS.
- Chaves Criptográficas: As chaves criptográficas devem ser gerenciadas de forma segura, com acesso restrito e práticas de rotação regular.

7.2. Backup e Recuperação de Dados

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- *Backups Regulares:* Realizar *backups* regulares dos dados importantes, garantindo que cópias de segurança sejam armazenadas em locais seguros.
- *Armazenamento de Backups:* Backups devem ser armazenados em locais separados fisicamente e logicamente do local original dos dados.
- *Teste de Recuperação:* Realizar testes periódicos de recuperação de dados para garantir que os *backups* possam ser restaurados com sucesso em caso de necessidade.

7.3. Controle de Acesso

- *Autenticação e Autorização:* Implementar controles rigorosos de autenticação e autorização para garantir que apenas usuários autorizados possam acessar dados sensíveis.
- *Segregação de Funções:* Garantir que funções e responsabilidades sejam segregadas para prevenir acesso não autorizado e fraudes.
- *Monitoramento de Acesso:* Manter registros detalhados de acessos a dados sensíveis e revisar regularmente esses registros para detectar atividades suspeitas.

7.4. Descarte Seguro de Dados

- *Dados Digitais:* Implementar procedimentos seguros para a exclusão de dados digitais, como o uso de software de exclusão segura que impede a recuperação de dados.
- *Documentos Físicos:* Utilizar métodos seguros para o descarte de documentos físicos, como trituração, para garantir que informações confidenciais não possam ser recuperadas.

7.5. Proteção Contra Malware e Ameaças Cibernéticas

- *Antivírus e Antimalware:* Utilizar software antivírus e *antimalware* atualizado em todos os dispositivos e servidores.
- *Firewalls:* Implementar *firewalls* para proteger a rede contra acessos não autorizados e ataques externos.
- *Atualizações e Patches:* Manter todos os sistemas e aplicativos atualizados com os *patches* de segurança mais recentes.

7.6. Privacidade e Conformidade com a LGPD

- *Política de Privacidade:* Estabelecer e comunicar uma política de privacidade que descreva como os dados pessoais são coletados, usados, armazenados e protegidos.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Consentimento Informado: Obter consentimento explícito dos indivíduos antes de coletar e processar seus dados pessoais, conforme exigido pela Lei Geral de Proteção de Dados (LGPD).
- Direitos dos Titulares: Assegurar que os titulares dos dados possam exercer seus direitos, como acesso, correção, exclusão e portabilidade de seus dados pessoais.
- Relatórios e Auditorias: Realizar auditorias regulares para garantir a conformidade com a LGPD e outras regulamentações de privacidade.

7.7. Acordos de Confidencialidade

- Funcionários e Voluntários: Exigir que todos os funcionários e voluntários assinem acordos de confidencialidade para proteger informações sensíveis.
- Terceiros e Parceiros: Estabelecer contratos de confidencialidade com terceiros e parceiros que possam ter acesso a dados sensíveis, garantindo o cumprimento das normas de proteção de dados da ONG.

8. Segurança da informação

A segurança de rede é essencial para proteger as informações e garantir a integridade e disponibilidade dos sistemas de informação da ONG. As medidas de segurança de rede descritas abaixo visam prevenir acessos não autorizados, ataques cibernéticos e outras ameaças, assegurando a operação contínua e segura da organização.

8.1. Firewall

- Implementação de *Firewall*: Utilizar *firewalls* para controlar o tráfego de rede entre a rede interna da ONG e redes externas, como a internet. Os firewalls devem ser configurados para bloquear acessos não autorizados e permitir apenas tráfego legítimo.
- Regras de *Firewall*: Estabelecer e revisar regularmente regras de *firewall* para garantir que apenas o tráfego necessário seja permitido.

8.2. Segurança de Perímetro

- IDS/IPS: Implementar sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar e analisar o tráfego de rede em busca de atividades suspeitas e ataques em potencial.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Segmentação de Rede: Segmentar a rede interna em diferentes zonas de segurança, isolando sistemas críticos e dados sensíveis para limitar o impacto de um possível incidente.

8.3. Criptografia de Dados

- VPN: Utilizar redes privadas virtuais (VPNs) para proteger dados em trânsito entre dispositivos remotos e a rede da ONG. As VPNs devem usar protocolos de criptografia robustos para garantir a confidencialidade e integridade dos dados.
- Wi-Fi Seguro: Configurar redes Wi-Fi internas com criptografia WPA3 e senhas fortes. Redes Wi-Fi para convidados devem ser separadas da rede principal da ONG.

8.4. Controle de Acesso à Rede (NAC)

- Autenticação: Implementar mecanismos de autenticação forte para acessar a rede, como autenticação multifator (MFA).
- Acesso Baseado em Funções: Utilizar controles de acesso baseados em funções (RBAC) para garantir que os usuários tenham acesso apenas aos recursos necessários para suas funções específicas.

8.5. Atualizações e *Patches*

- Gerenciamento de *Patches*: Manter todos os dispositivos de rede, sistemas operacionais e aplicativos atualizados com os *patches* de segurança mais recentes.
- Automatização: Automatizar o processo de atualização de software sempre que possível para garantir que as correções sejam aplicadas prontamente.

8.6. Proteção contra *Malware*

- Antivírus e *Antimalware*: Implementar software antivírus e *antimalware* em todos os dispositivos conectados à rede e garantir que sejam atualizados regularmente.
- Filtragem de Conteúdo: Utilizar filtragem de conteúdo para bloquear sites maliciosos e impedir *downloads* de arquivos perigosos.

8.7. Segurança Física

- Proteção de Equipamentos de Rede: Garantir que os equipamentos de rede (como roteadores, switches e servidores) estejam localizados em áreas seguras e com acesso restrito.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Monitoramento Físico: Utilizar câmeras de vigilância e controles de acesso físico para proteger os locais onde estão os equipamentos de rede.

9. Gestão de incidentes

A gestão de incidentes é uma parte fundamental da Política de Segurança da Informação da ONG, visando identificar, responder e mitigar incidentes de segurança de forma eficaz para minimizar o impacto nos nossos sistemas e dados. A seguir estão detalhados os procedimentos e responsabilidades relacionados à gestão de incidentes:

9.1. Definição de Incidentes

- Classificação de Incidentes: Identificar e documentar incidentes, incluindo acesso não autorizado, *malware*, *phishing*, violação de dados e interrupções de serviço.

9.2. Detecção e Notificação

- Mecanismos de Detecção: Implementar sistemas de detecção de intrusões, monitoramento de rede e outras ferramentas para identificar incidentes de segurança o mais rápido possível.
- Procedimentos de Notificação: Estabelecer canais de comunicação claros e procedimentos para relatar incidentes à equipe de segurança da informação e à diretoria.

9.3. Avaliação e Análise

- Investigação Preliminar: Realizar uma análise inicial para determinar a natureza e a extensão do incidente.
- Coleta de Evidências: Coletar e preservar evidências relacionadas ao incidente, incluindo logs de sistema, registros de acesso e capturas de tela.

9.4. Resposta e Mitigação

- Contenção: Agir rapidamente para conter o incidente e evitar que se espalhe para outros sistemas ou áreas da organização.
- Erradicação: Identificar e remover completamente o malware, as vulnerabilidades ou as ameaças que causaram o incidente.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Recuperação: Restaurar os sistemas afetados para um estado operacional normal, incluindo a recuperação de dados se necessário.

9.5. Comunicação e Notificação

- Comunicação Interna: Manter a equipe informada sobre o status do incidente e as medidas tomadas para responder e mitigar o impacto.
- Notificação Externa: Se necessário e conforme exigido por regulamentos, notificar autoridades regulatórias, parceiros ou clientes afetados pelo incidente.

9.6. Documentação e Relatório

- Registro de Incidentes: Documentar detalhadamente todos os aspectos do incidente, incluindo a cronologia dos eventos, as ações tomadas e as lições aprendidas.
- Análise Pós-Incidente: Realizar uma análise pós-incidente para identificar falhas no processo e áreas de melhoria.

9.7. Equipe de Resposta a Incidentes

- Designação de Papéis: Designar funções e responsabilidades específicas para os membros da equipe de resposta a incidentes, incluindo líderes de equipe, investigadores, analistas e comunicadores.
- Treinamento Especializado: Garantir que a equipe de resposta a incidentes receba treinamento especializado e tenha acesso às ferramentas e recursos necessários para realizar suas funções com eficácia.

9.8. Revisão e Melhoria Contínua

- Avaliação Pós-Incidente: Realizar revisões pós-incidente para avaliar a eficácia da resposta e identificar oportunidades de melhoria.
- Atualização de Procedimentos: Atualizar os procedimentos de gestão de incidentes com base nas lições aprendidas e nos resultados das análises pós-incidente.

10. Revisão e auditoria

A revisão e auditoria em segurança da informação são processos cruciais para garantir a eficácia das políticas, procedimentos e controles de segurança implementados pela ONG. Essas atividades permitem identificar possíveis

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

vulnerabilidades, avaliar o cumprimento de normas e regulamentos, e fornecer recomendações para melhorias. Abaixo estão detalhadas as práticas de revisão e auditoria que serão adotadas:

10.1. Auditorias Internas Regulares

- Escopo Abrangente: Realizar auditorias internas abrangentes para avaliar todos os aspectos da segurança da informação, incluindo políticas, procedimentos, controles técnicos e práticas de conformidade.
- Plano de Auditoria: Desenvolver um plano de auditoria anual que estabeleça os objetivos, escopo, métodos e cronograma das auditorias internas.

10.2. Avaliação de Conformidade

- Normas e Regulamentos: Verificar o cumprimento das normas e regulamentos relevantes, como a Lei Geral de Proteção de Dados (LGPD), ISO/IEC 27001 e outras diretrizes específicas do setor.
- Políticas Internas: Comparar as práticas e procedimentos internos com as políticas de segurança da informação da organização para garantir alinhamento e conformidade.

10.3. Testes de Penetração e Vulnerabilidade

- Simulação de Ataques: Realizar testes de penetração e avaliações de vulnerabilidade para identificar possíveis pontos fracos na infraestrutura de TI e nos sistemas da organização.
- Remediação de Vulnerabilidades: Tomar medidas corretivas imediatas para mitigar quaisquer vulnerabilidades identificadas durante os testes de penetração.

10.4. Revisão de Políticas e Procedimentos

- Atualização Contínua: Revisar regularmente as políticas e procedimentos de segurança da informação para garantir que estejam alinhados com as melhores práticas do setor e as mudanças nas necessidades e requisitos da organização.
- Participação Multidisciplinar: Envolvimento de diversas partes interessadas na revisão e atualização das políticas, incluindo a equipe de TI, a liderança executiva e os representantes de departamentos-chave.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

10.5. Avaliação de Controles Técnicos

- Eficácia dos Controles: Avaliar a eficácia dos controles técnicos implementados para proteger os sistemas e dados da organização, como firewalls, sistemas de detecção de intrusões e antivírus.
- Configurações Seguras: Verificar se os dispositivos e sistemas estão configurados de acordo com as melhores práticas de segurança e as políticas da organização.

10.6. Avaliação de Conscientização e Treinamento

- Participação e Conscientização: Avaliar o nível de participação e conscientização dos funcionários e voluntários em relação às práticas de segurança da informação.
- Eficácia do Treinamento: Avaliar a eficácia dos programas de treinamento e conscientização em segurança da informação, medindo o impacto nas práticas de segurança dos participantes.

10.7. Análise de Incidentes Anteriores

- Lições Aprendidas: Analisar incidentes de segurança anteriores para identificar falhas nos controles de segurança e implementar medidas corretivas para evitar recorrências.
- Melhoria Contínua: Utilizar as lições aprendidas com incidentes anteriores para melhorar continuamente as práticas de segurança da informação da organização.

10.8. Relatórios e Recomendações

- Relatórios Abrangentes: Elaborar relatórios detalhados que destaque as descobertas das revisões e auditorias, incluindo recomendações claras para melhorias.
- Comunicação Efetiva: Comunicar os resultados das revisões e auditorias de forma clara e objetiva à liderança executiva e às partes interessadas relevantes.

10.9. Acompanhamento e Implementação de Recomendações

- Planos de Ação: Desenvolver planos de ação claros para implementar as recomendações identificadas durante as revisões e auditorias.
- Acompanhamento Regular: Acompanhar regularmente o progresso na implementação das recomendações e tomar medidas corretivas conforme necessário.

10.10. Melhoria Contínua do Processo de Auditoria

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Classificação: interna	Versão: 1.1
		Última revisão: 15/06/2024

- Feedback e Avaliação: Solicitar feedback das partes interessadas e participantes sobre o processo de auditoria para identificar áreas de melhoria.
- Atualização de Metodologias: Atualizar continuamente as metodologias de auditoria com base nas melhores práticas e nas mudanças no ambiente de segurança da informação.

11. Penalidades de violação da política de segurança da informação

As penalidades para violação da política de segurança podem variar dependendo da gravidade da violação, das políticas internas da organização e das leis e regulamentos aplicáveis. Abaixo estão algumas das possíveis penalidades que podem ser aplicadas:

11.1. Ações Disciplinares:

- Advertência verbal ou escrita: Para violações menores ou de baixo impacto, uma advertência pode ser emitida para o funcionário infrator.
- Suspensão temporária: Em casos mais graves, pode ser aplicada uma suspensão temporária do trabalho como consequência da violação da política.
- Demissão: Se a violação for significativa ou repetida, pode resultar em demissão do funcionário, especialmente se houver negligência grave ou intenção de causar danos.

11.2. Restrições de Acesso:

- Revogação de privilégios de acesso: O acesso aos sistemas e dados da organização pode ser temporariamente ou permanentemente revogado como medida disciplinar.
- Restrição de funções: O funcionário infrator pode ter suas responsabilidades reduzidas ou limitadas como resultado da violação da política.

11.3. Responsabilidade Legal:

- Ações legais: Em casos extremos, a violação da política de segurança pode levar a ações legais contra o funcionário infrator, especialmente se a violação resultar em danos significativos à organização ou a terceiros.

11.4. Educação e Conscientização Adicionais:

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
Classificação: interna		Versão: 1.1
		Última revisão: 15/06/2024

- Treinamento adicional: Como parte da medida disciplinar, o funcionário infrator pode ser obrigado a participar de treinamentos adicionais sobre segurança da informação para aumentar a conscientização e prevenir violações futuras.

11.5. Perda de Privilégios:

- Perda de benefícios ou privilégios: Dependendo da gravidade da violação, o funcionário infrator pode perder certos benefícios ou privilégios dentro da organização, como bonificações ou oportunidades de promoção.

11.6. Sanções Financeiras:

- Multas internas: Em algumas organizações, pode haver a imposição de multas financeiras como consequência da violação da política de segurança da informação.
- Responsabilidade por danos: O funcionário infrator pode ser responsabilizado por quaisquer danos financeiros resultantes da violação, incluindo custos de remediação e perda de receita.

11.7. Revisão das Políticas e Procedimentos:

- Atualização das políticas: A violação da política pode levar à revisão e atualização das políticas e procedimentos de segurança da informação para prevenir violações futuras e fortalecer os controles de segurança.

11.8. Comunicação Interna:

- Divulgação da violação: Dependendo da gravidade da violação, pode ser necessário comunicar a violação da política de segurança aos funcionários da organização para destacar a importância da conformidade.

12. Considerações finais

A segurança da informação é uma responsabilidade compartilhada por todos os membros da ONG. Ao seguir esta política e colaborar ativamente na proteção dos ativos de informação da organização, podemos garantir a confidencialidade, integridade e disponibilidade dos dados, além de promover uma cultura de segurança da informação em toda a organização.

Ademais, esta política será revisada regularmente para garantir sua eficácia contínua e para incorporar quaisquer mudanças nas leis, regulamentos ou nas necessidades da organização.

 ONG AMBIENTAL	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
		Versão: 1.1
	Classificação: interna	Última revisão: 15/06/2024

Data de Entrada em Vigor: 03/06/2024

Data de Revisão: 15/06/2024

Por fim, esta política de segurança da informação é parte integrante das práticas de governança da ONG e deve ser respeitada por todos os colaboradores, independentemente do cargo ou função que ocupam. O cumprimento destas diretrizes é essencial para manter a confiança dos beneficiários, doadores e parceiros, além de garantir a continuidade e a integridade das operações da organização.