



**PUC Minas**

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS**

**INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA**

**Bacharelado em Sistemas de Informação**

**PROJETO INFRAESTRUTURA DE REDES**

Amanda Costa Dutra

Allan Diego Pereira do Nascimento

Fernanda Fonseca Ribeiro Bertoldo

Gabriel Novais Maia

Higor Henrique Batista Souza

Lara Alves de Freitas

Renato Cifuentes Dias de Araújo Neto

Belo Horizonte

2024

## **PROJETO ONG RECICLAR**

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	7
4. PLANEJAMENTO DOS RECURSOS DE REDE	8
5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE	16
6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX	24
7. REFERÊNCIAS	30
8. ANEXO I - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)	310
9. ANEXO II - CARTILHA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	36

## **1. TEMA**

O grupo optou por escolher o Instituto Reciclar (<https://reciclar.org.br/>), Organização Não Governamental cujo foco é a formação profissional e inclusão social de jovens em situação de vulnerabilidade. A atuação da organização reflete uma escolha estratégica alinhada com sua missão de promover o desenvolvimento sustentável e a transformação social. Ao trabalhar nesse sentido, o instituto reconhece os desafios e responsabilidades específicos associados à sua missão e à sua escala de atuação.

O Instituto Reciclar necessita de uma estrutura organizacional complexa, exigindo uma abordagem organizada e interconectada para atingir seus objetivos. Dentre os principais aspectos dessa estrutura estão:

- 1. Programa Educacional:** O programa educacional envolve diversas etapas, desde o desenvolvimento curricular até a implementação das atividades educativas.
- 2. Pesquisa e Desenvolvimento Educacional:** Pesquisa e desenvolvimento de metodologias inovadoras de ensino e aprendizagem.
- 3. Logística e Gestão de Parcerias:** Gerenciamento eficiente das parcerias e recursos necessários para implementar programas educacionais e conectar os jovens ao mercado de trabalho é essencial para o sucesso da organização.
- 4. Avaliação de Impacto:** Realização de uma avaliação de impacto para garantir a eficácia de seus programas na transformação da vida dos jovens.
- 5. Gestão de Recursos Humanos:** Com uma equipe dedicada e voluntários engajados, a gestão de recursos humanos é vital para recrutar, capacitar e manter os colaboradores comprometidos com a missão da organização.
- 6. Comunicação e Mobilização de Recursos:** Investimento em estratégias de comunicação e mobilização de recursos para ampliar seu alcance e garantir o apoio necessário para suas operações.
- 7. Administração e Finanças:** O departamento administrativo e financeiro do Instituto Reciclar cuida das operações financeiras da organização, garantindo transparência e eficiência na gestão dos recursos.

Uma ONG como o Instituto Reciclar é caracterizada por uma abordagem orientada para a automação de seus processos e a tecnologia aplicada em pesquisa, visando aumentar a eficiência e a produtividade a cada ano.

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

- Comunicação Interna e Cooperação;
- Segurança de Dados;
- Expansão e Escalabilidade;
- Conexões com parceiros e colaboradores;
- Acesso a recursos educacionais;
- Compartilhamento de melhores práticas;
- Gerenciamento de programas e alunos;
- Acesso a parcerias e oportunidades;

Certamente, uma estrutura de rede é fundamental para garantir o sucesso nas operações organizacionais bem como garantir a eficiência operacional, a qualidade dos serviços e a competitividade da ONG Reciclar. Isso permitirá uma integração eficaz de todas as atividades, desde a capacitação dos jovens até a gestão de recursos, impulsionando o impacto positivo em nossa comunidade.

## 2. RESPONSABILIDADES

	<b>Atividade</b>	<b>Participantes</b>	<b>Tempo Dedicado (h)</b>
01	Definição do tema do projeto	Amanda, Allan, Fernanda, Gabriel, Higor, Lara, Renato	1
02	Elaboração de texto com justificativa e contextualização	Allan, Gabriel, Higor, Lara, Renato	2
03	Planejamento da estrutura organizacional	Gabriel, Lara, Renato	1,5
04	Criação de planilha com lista de materiais de infraestrutura	Gabriel, Lara, Renato	3
05	Definição dos serviços necessários	Allan, Higor	2
06	Planilha Recurso de Rede	Amanda, Lara, Renato	2
07	Divisão Lógica da Rede	Allan, Fernanda	4
08	Projeto Packet Tracer	Gabriel, Higor, Allan	2

	Revisão do documento para primeira entrega	Lara,Renato e Amanda	1
--	--------------------------------------------	----------------------	---

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

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

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

### 3. CRONOGRAMA DE ATIVIDADES

<b>Semana</b>	<b>Dias de dedicação</b>	<b>Atividades</b>
Semana 1 06/02/24 17/03/24	10 dias úteis	<ul style="list-style-type: none"> <li>- Formação dos grupos e definição do tema junto ao professor;</li> <li>- Início dos estudos dos microfundamentos para a etapa.</li> </ul>
Semana 2 18/03/24 14/04/24	12 dias úteis	<ul style="list-style-type: none"> <li>- Definição do tema e planejamento inicial da proposta;</li> <li>- Curso do Cisco Packet Tracer;</li> <li>- Documento contendo endereços dos servidores hospedados em nuvem com seus respectivos nomes, IPs, usuários e acessos.</li> <li>- Arquivo PDF contendo Prints dos servidores instalados localmente demonstrando os serviços instalados por meio e suas respectivas configurações.</li> <li>- Link de vídeo em plataforma online (não listado) demonstrando acesso e testes dos serviços instalados</li> </ul>
Semana 3 15/04/24 05/05/24	10 dias úteis	<ul style="list-style-type: none"> <li>- Planilha de Recursos de Rede;</li> <li>- Protótipo da rede no Simulador da Cisco Packet Tracer.</li> <li>- Mapa de Monitoramento dos Servidores no Zabbix</li> </ul>

Semana 4 06/05/24 01/06/24	4 dias úteis	<ul style="list-style-type: none"> <li>- Documento da Política de Segurança da Informação</li> <li>- Cartilha de boas práticas de acesso seguro</li> <li>- Link da aplicação back-end implantada em servidor na nuvem</li> <li>-</li> </ul>
Semana 5 02/06/24 22/06/24	20 dias úteis	<ul style="list-style-type: none"> <li>- Documento nas regras da PUC demonstrando cada uma das etapas elaboradas com sua respectiva conclusão</li> <li>- Slide para apresentação do projeto</li> <li>- Apresentação final do projeto pelo grupo em seminários</li> </ul>

## **4. PLANEJAMENTO DOS RECURSOS DE REDE**

A rede será proposta com a sede da empresa localizada na capital Belo Horizonte (MG), composta por dois escritórios. Adicionalmente, a organização contará com três filiais, cada uma situada na região metropolitana sendo elas em Contagem, Betim e Nova Lima, também no estado de Minas Gerais, sendo que cada filial possuirá um escritório próprio. Abaixo, estão descritas algumas características de cada ponto da rede:

- Matriz em Belo Horizonte (MG):

Aplicação de Cursos: A matriz será responsável pela condução direta dos cursos, oferecendo formações em tecnologia e outros temas relevantes.

Programa de Mentoría: Coordenação centralizada para fornecer suporte e orientação aos beneficiários em todas as unidades.

Gerenciamento das Filiais: Supervisão e coordenação das atividades das filiais, assegurando a consistência e o alinhamento com os objetivos da ONG.

-Escritório 1:

- Coordenação dos demais escritórios;
- Diretoria executiva;
- Recursos Humanos;
- Setor de Garantia de Qualidade;
- Setor de Administração das Filiais;

-Escritório 2:

- Time de Tecnologia;
- Equipe de Marketing e Estratégia;
- Financeiro e Contábil;
- Setor de Inovação e Desenvolvimento;
- Setor de Assistência Técnica;

- Filiais (Contagem, Betim e Nova Lima): cada uma delas realizará as seguintes atividades:
  - Desenvolvimento de atividades: Estimula a criatividade e a resolução de problemas, focando na aplicação prática dos conhecimentos adquiridos.
  - Orientação Vocacional: Apoio na escolha de carreiras alinhadas com os objetivos individuais, promovendo o autoconhecimento.
  - Mentoría: Conexão de profissionais experientes aos jovens atendidos pela filial, apoiando o desenvolvimento de habilidades relevantes para a entrada no mercado de trabalho.
  - Implementação de cursos técnicos: Abrange áreas como TI e administração.
- Escritório das Filiais (Ambos realizam as mesmas Tarefas):
  - Gerenciamento de todas as atividades realizadas na ONG;
  - SAC (Serviço de Atendimento ao Cliente);
  - Garantir uma troca regular de informações e alinhamento estratégico entre as filiais e a sede central;
  - Setor de Garantia de Qualidade;
  - Setor de Assistência Técnica;
- Laboratórios: Ambos os laboratórios serão espaços dedicados ao ensino prático dos cursos técnicos, equipados com vários computadores, proporcionando um

ambiente propício para o desenvolvimento de habilidades práticas e aplicação de conhecimentos adquiridos.

- Sala de vídeo:

Este espaço será destinado à gravação de aulas, workshops e conteúdos educacionais. Equipada com recursos audiovisuais avançados, a sala de vídeo possibilitará a criação de material didático de alta qualidade

## 4.1 ESTRUTURA FÍSICA DA ORGANIZAÇÃO

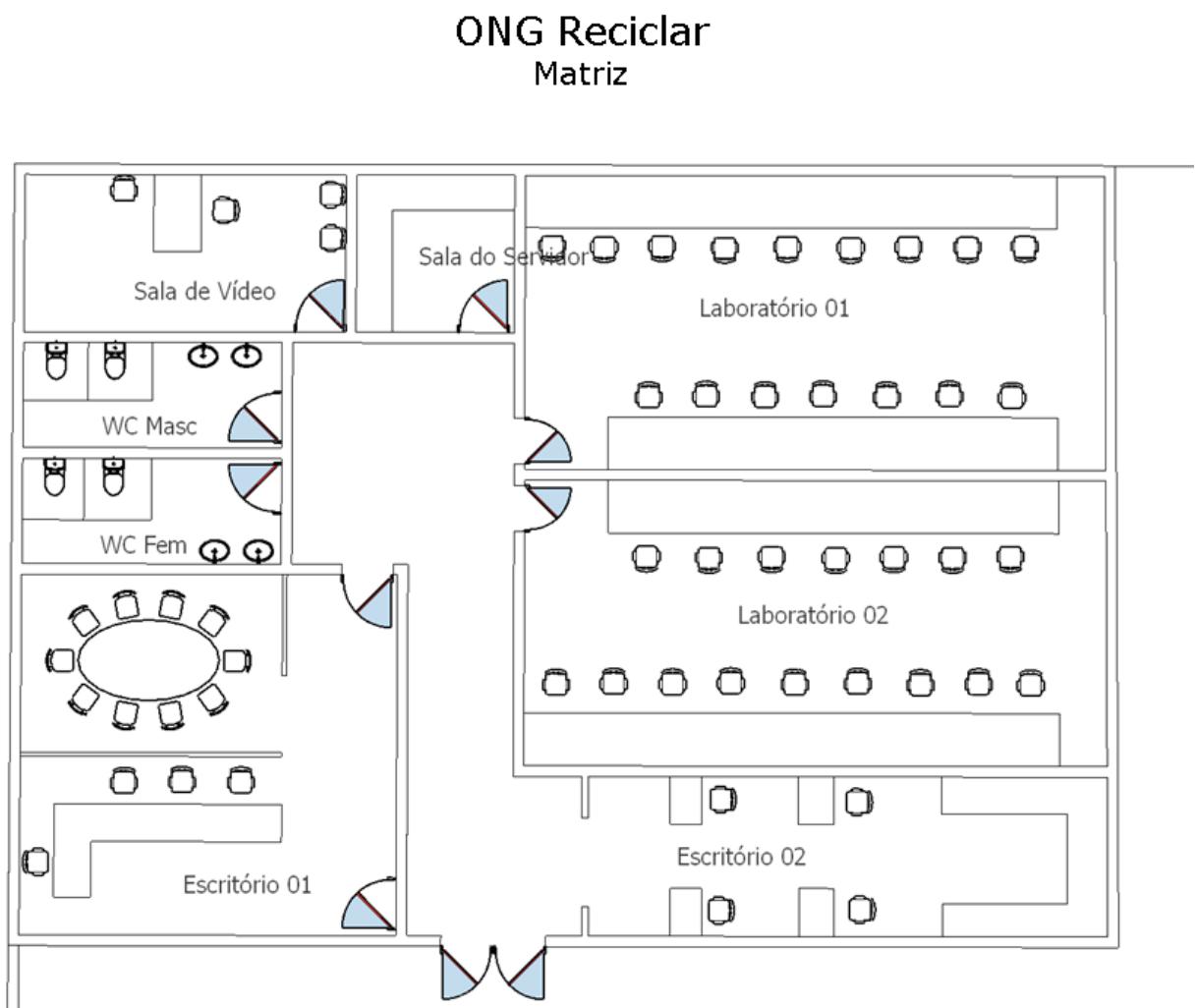


Figura 01 – Planta Baixa - Sede da ONG

**ONG Reciclar**  
Filiais

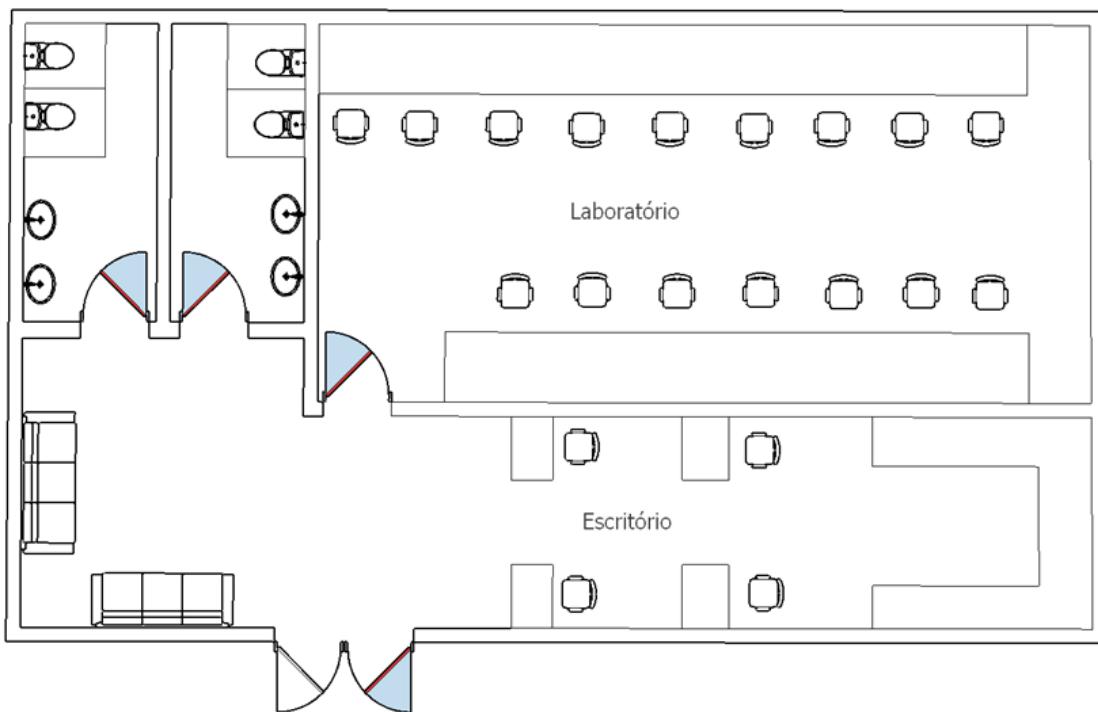


Figura 02 – Planta Baixa - Filial

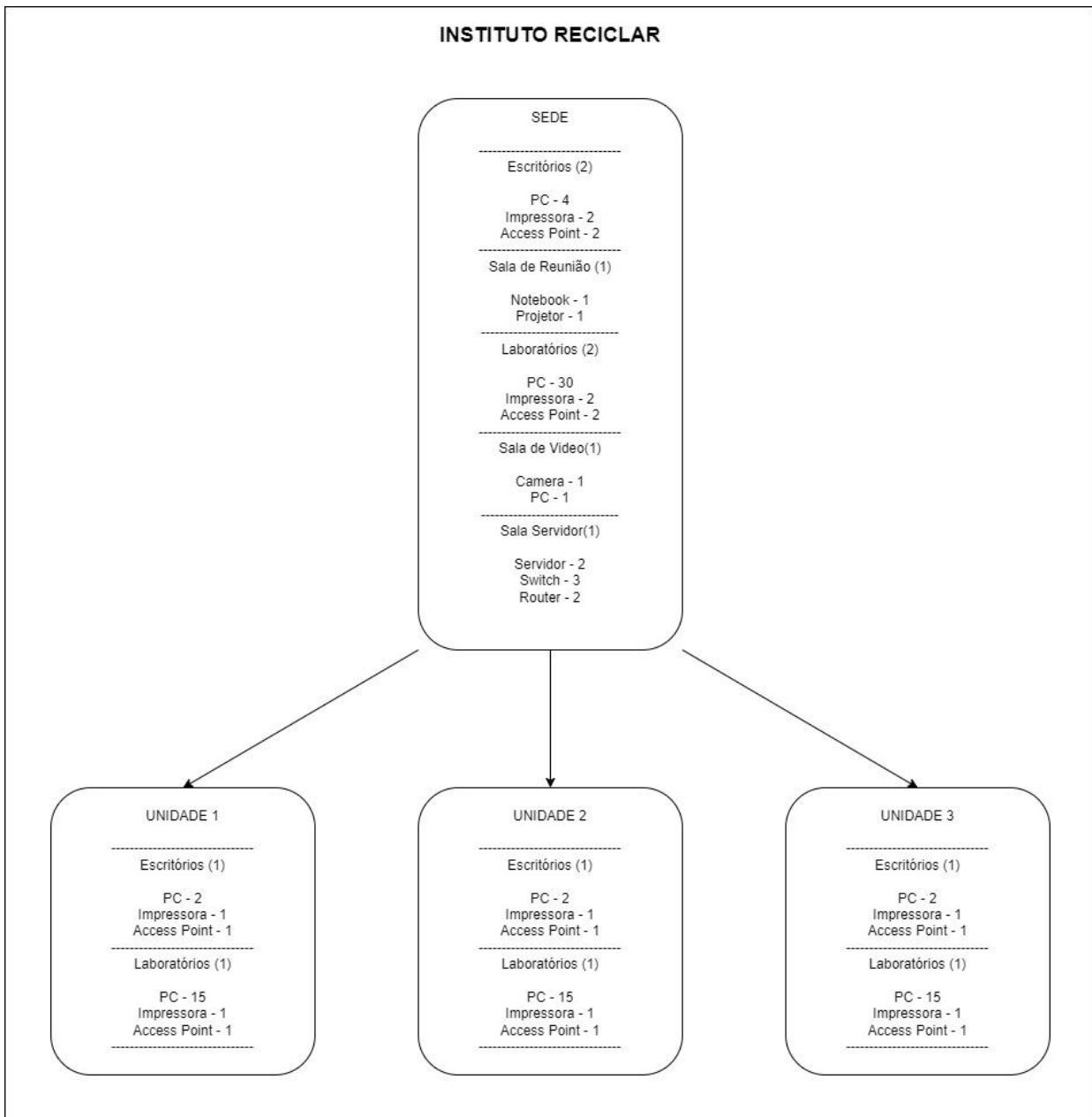


Figura 03 – Estrutura da Rede

## 4.2 DIVISÃO FÍSICA DA REDE

Com base em todo esse cenário, a divisão física da rede ficou representada conforme a imagem abaixo. A topologia escolhida foi a hierárquica. Inicialmente foi elaborado um diagrama da rede usando a plataforma Visio (figura 1) para definição da estrutura física e lógica da rede.

**ONG RECICLAR**  
**Projeto de Rede**  
**Topologia Lógica**

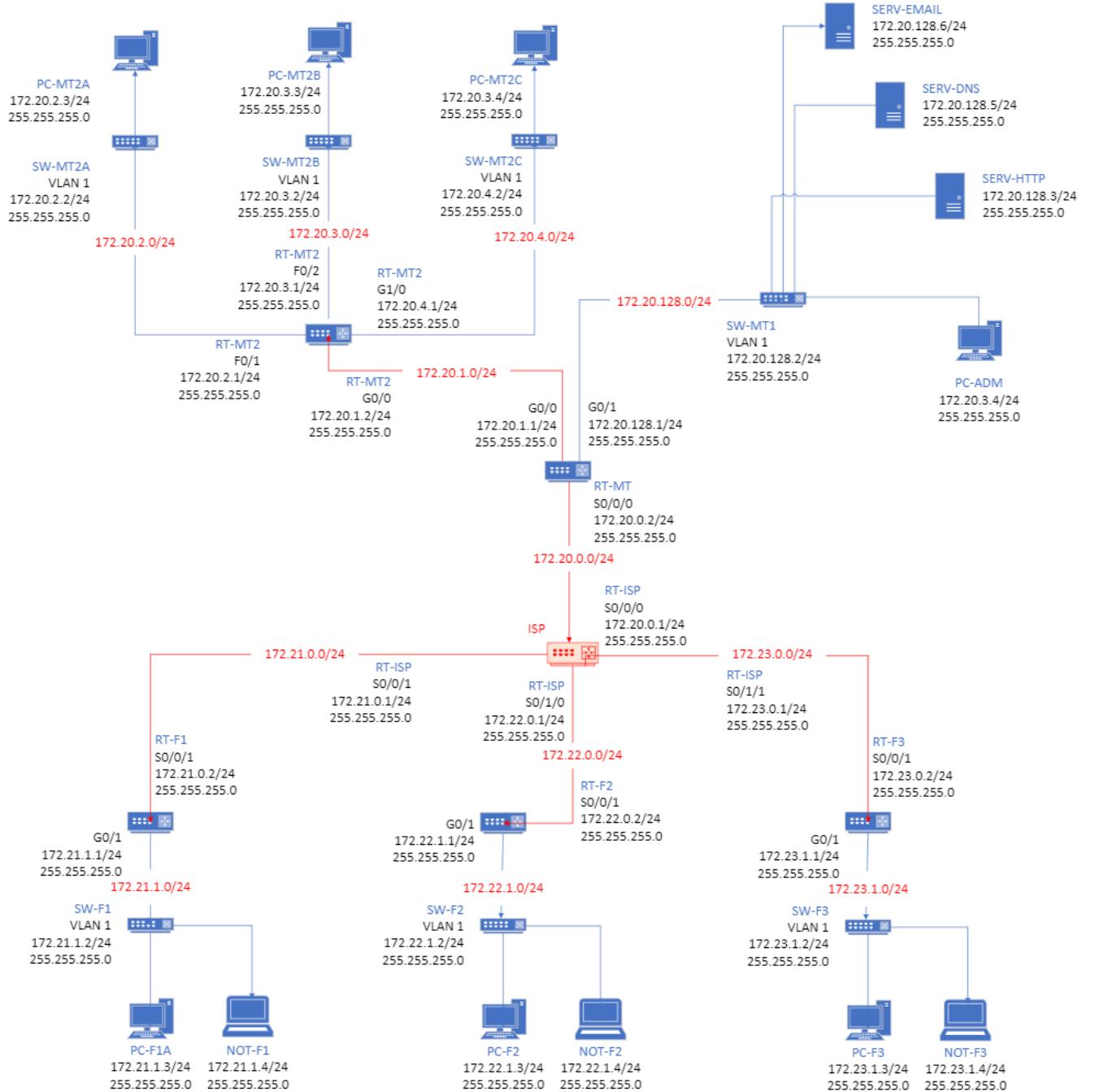
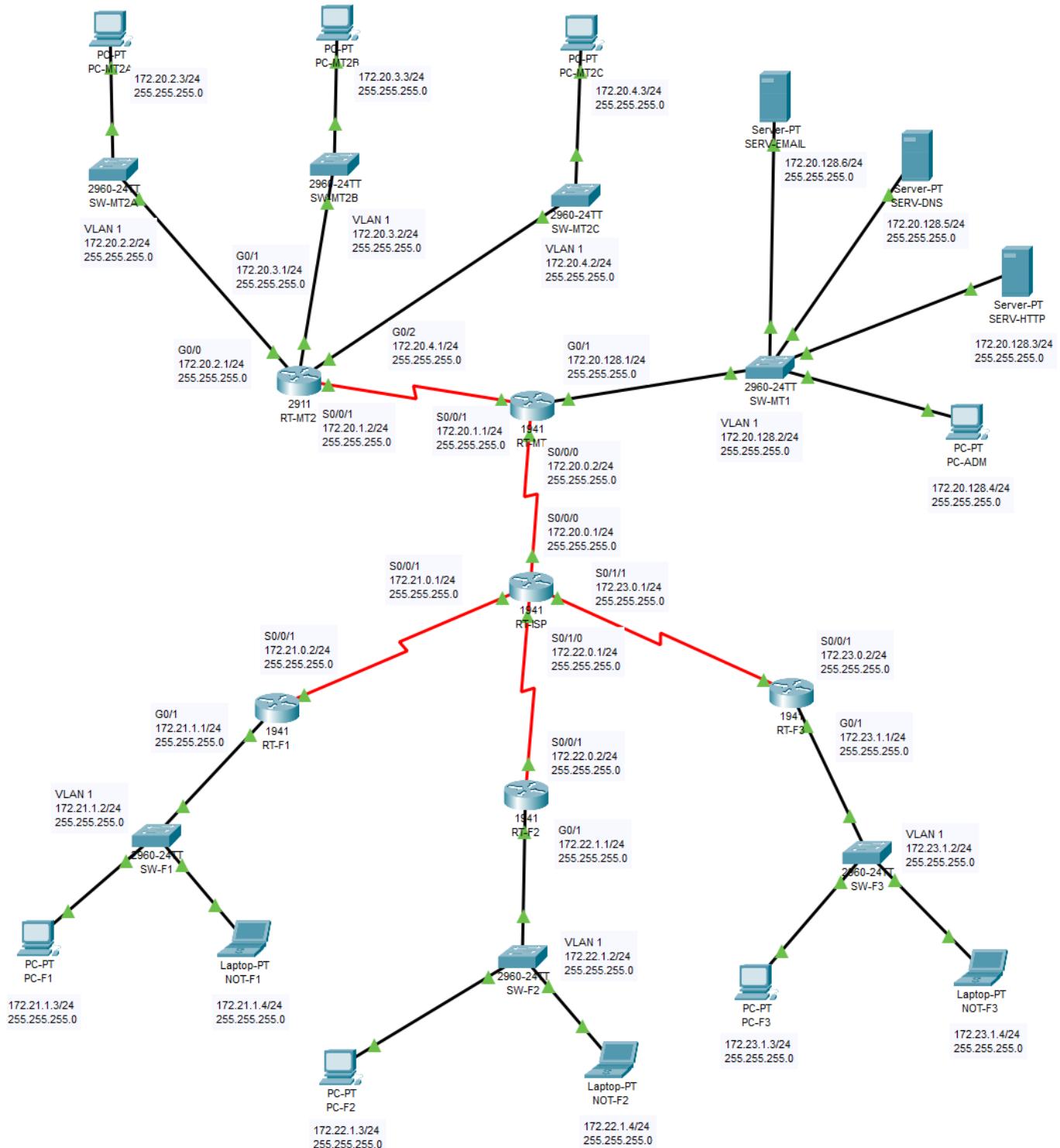


Figura 04 – Diagrama de Rede



Fonte: Cisco Packet Tracer

### 4.3 PLANILHA DE MATERIAIS

A tabela a seguir reflete a lista de materiais que serão utilizados no projeto bem como seus valores correspondentes. O valor orçado necessário será para a Matriz (R\$ 277.494,03), para as unidades 1,2 e 3 o valor necessário será (R\$ 103.906,80). O total estimado para este projeto é de R\$589.214,43.

Item	Valor	Matriz		Unidade 1		Unidade 2		Unidade 3	
		35		17		17		17	
		Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
OptiPlex Micro	R\$ 2.399,00	35	R\$ 83.965,00	17	R\$ 40.783,00	17	R\$ 40.783,00	17	R\$ 40.783,00
Impressora	R\$ 765,00	4	R\$ 3.060,00	2	R\$ 1.530,00	2	R\$ 1.530,00	2	R\$ 1.530,00
AP IntelBras	R\$ 463,00	4	R\$ 1.852,00	2	R\$ 926,00	2	R\$ 926,00	2	R\$ 926,00
Câmera	R\$ 190,00	1	R\$ 190,00	0	R\$ -	0	R\$ -	0	R\$ -
Rj45 Furukawa Cat6	R\$ 230,00	20	R\$ 4.600,00	12	R\$ 2.760,00	12	R\$ 2.760,00	12	R\$ 2.760,00
Switch TL-SG2428P / pelo menos 2 por lab	R\$ 2.249,90	3	R\$ 6.749,70	2	R\$ 4.499,80	2	R\$ 4.499,80	2	R\$ 4.499,80
NoBreak 1500VA	R\$ 1.010,83	1	R\$ 1.010,83	0	R\$ -	0	R\$ -	0	R\$ -
Cabo Rede Furukawa Cat6 Gigalan 305 m	R\$ 1.792,00	8	R\$ 2.792,00	4	R\$ 1.396,00	4	R\$ 1.396,00	4	R\$ 1.396,00
Patch Cord Cat6 GigaLan Azul 5 Metros c/24	R\$ 1.404,00	47	R\$ 65.988,00	21	R\$ 29.484,00	21	R\$ 29.484,00	21	R\$ 29.484,00
Patch Panel 24 Cat 6 Furukawa	R\$ 750,00	3	R\$ 2.250,00	2	R\$ 1.500,00	2	R\$ 1.500,00	2	R\$ 1.500,00
Cabo Serial Cisco	R\$ 50,00	1	R\$ 50,00	0	R\$ -	0	R\$ -	0	R\$ -
Organizador de cabos 1,5m	R\$ 20,00	49	R\$ 980,00	24	R\$ 480,00	24	R\$ 480,00	24	R\$ 480,00
Roteador Cisco Business 220 24p	R\$ 2.100,00	2	R\$ 4.200,00	1	R\$ 2.100,00	1	R\$ 2.100,00	1	R\$ 2.100,00
Rack de Piso 44U	R\$ 2.270,50	1	R\$ 2.270,50	0	R\$ -	0	R\$ -	0	R\$ -
Servidor Rack PowerEdge R7625	R\$ 60.000,00	1	R\$ 60.000,00	0	R\$ -	0	R\$ -	0	R\$ -
Mesa + Cadeira	R\$ 700,00	35	R\$ 24.500,00	17	R\$ 11.900,00	17	R\$ 11.900,00	17	R\$ 11.900,00
Teclado e mouse	R\$ 118,00	35	R\$ 4.130,00	17	R\$ 2.006,00	17	R\$ 2.006,00	17	R\$ 2.006,00
Headset Multi Pro	R\$ 38,00	35	R\$ 1.330,00	17	R\$ 646,00	17	R\$ 646,00	17	R\$ 646,00
Servidor Cloud AWS	R\$ -								
		Total	R\$ 277.494,03	Total	R\$ 103.906,80	Total	R\$ 103.906,80	Total	R\$ 103.906,80
		Total Geral							

Tabela de Materiais

#### 4.4 DIVISÃO LÓGICA DA REDE

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

Addressing Table						
Local	Device	Name	Interface	IP Address	Subnet Mask	Default Gateway
INTERNET	Router	RT-ISP	S0/0/0	172.20.0.1	255.255.0.0	N/A
			S0/0/1	172.21.0.1	255.255.0.0	N/A
			S0/1/0	172.22.0.1	255.255.0.0	N/A
			S0/1/1	172.23.0.1	255.255.0.0	N/A
MATRIZ	Router	RT-MT	S0/0/0	172.20.0.2	255.255.0.0	N/A
			G0/0	172.20.1.1	255.255.255.0	N/A
			G0/1	172.20.128.1	255.255.255.0	N/A
		RT-MT2	G0/0	172.20.1.2	255.255.255.0	N/A
			G1/0	172.20.4.1	255.255.255.0	N/A
	Switch	SW-MT1	F0/2	172.20.3.1	255.255.255.0	N/A
			F0/1	172.20.2.1	255.255.255.0	N/A
		SW-MT2A	VLAN 1	172.20.128.2	255.255.255.0	172.20.128.1
			VLAN 1	172.20.2.2	255.255.255.0	172.20.2.1
	Computador	SW-MT2B	VLAN 1	172.20.3.2	255.255.255.0	172.20.3.1
			VLAN 1	172.20.4.2	255.255.255.0	172.20.4.1
		PC-ADM	F0/1	172.20.128.4	255.255.255.0	172.20.128.1
			F0/1	172.20.2.3	255.255.255.0	172.20.2.1
	Servidor	PC-MT2A	F0/1	172.20.3.3	255.255.255.0	172.20.3.1
			F0/1	172.20.3.4	255.255.255.0	172.20.3.1
		SERV-EMAIL	F0/1	172.20.128.6	255.255.255.0	172.20.128.1
	Computador	SERV-DNS	F0/1	172.20.128.5	255.255.255.0	172.20.128.1
		SERV-HTTP	F0/1	172.20.128.3	255.255.255.0	172.20.128.1
FILIAL 1	Router	RT-F1	S0/1/0	172.21.0.2	255.255.0.0	N/A
			G0/0	172.21.1.1	255.255.255.0	N/A
	Switch	SW-F1	VLAN 1	172.21.1.2	255.255.255.0	172.21.1.1
	Computador	PC-F1A	F0/1	172.21.1.3	255.255.255.0	172.21.1.1
FILIAL 2	Notebook	NOT-F1	F0/1	172.21.1.4	255.255.255.0	172.21.1.1
			F0/1	172.21.1.4	255.255.255.0	172.21.1.1
	Router	RT-F2	S0/1/0	172.22.0.2	255.255.0.0	N/A
			G0/0	172.22.1.1	255.255.255.0	N/A
	Switch	SW-F2	VLAN 1	172.22.1.2	255.255.255.0	172.22.1.1
FILIAL 3	Computador	PC-F2	F0/1	172.22.1.3	255.255.255.0	172.22.1.1
			F0/1	172.22.1.4	255.255.255.0	172.22.1.1
	Notebook	NOT-F2	F0/1	172.22.1.4	255.255.255.0	172.22.1.1
			F0/1	172.22.1.4	255.255.255.0	172.22.1.1
	Router	RT-F3	S0/1/0	172.23.0.2	255.255.0.0	N/A
			G0/0	172.23.1.1	255.255.255.0	N/A
	Switch	SW-F3	VLAN 1	172.23.1.2	255.255.255.0	172.23.1.1
	Computador	PC-F3	F0/1	172.23.1.3	255.255.255.0	172.23.1.1
	Notebook	NOT-F3	F0/1	172.23.1.4	255.255.255.0	172.23.1.1

#### 4.5 PLANILHA LINKS

A tabela abaixo contém informações correspondentes à demanda dos serviços de rede e estrutura de cada local da organização. A matriz está dividida em dois escritórios para atividades de diretoria, estratégia de negócio e suporte, além de dois laboratórios para treinamento. Cada filial está equipada com escritório para atividades administrativas e um laboratório com capacidade para 16 alunos. Cada filial terá uma conexão VPN com a sede para acesso aos serviços necessários, conforme tabela.

	Matriz		Filial 1		Filial 2		Filial 3		
	60		20		20		20		
APPs	LB (kbps)	Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB
Web	200	50	10000	20	4000	20	4000	20	4000
Email	100	50	5000	20	2000	20	2000	20	2000
Bankline	100	5	500	3	300	3	300	3	300
Suporte	100	5	500	3	300	3	300	3	300
Videoconferência	1000	50	50000	20	20000	20	20000	20	20000
AWS	200	8	1600	3	600	3	600	3	600
CRM	100	5	500	3	300	3	300	3	300
Sistema de Arquivos	50	50	2500	20	1000	20	1000	20	1000
<b>TOTAL APP</b>		<b>70600</b>		<b>28500</b>		<b>28500</b>		<b>28500</b>	
<b>TOTAL INTERNET</b>		<b>67100</b>		<b>28500</b>		<b>28500</b>		<b>28500</b>	
<b>TOTAL LINK DE DADOS</b>		<b>152600</b>		<b>28500</b>		<b>28500</b>		<b>28500</b>	
		M		F1		F2		F3	

Tabela de Link de Dados

## 5. IMPLEMENTAÇÃO DOS RECURSOS DA REDE

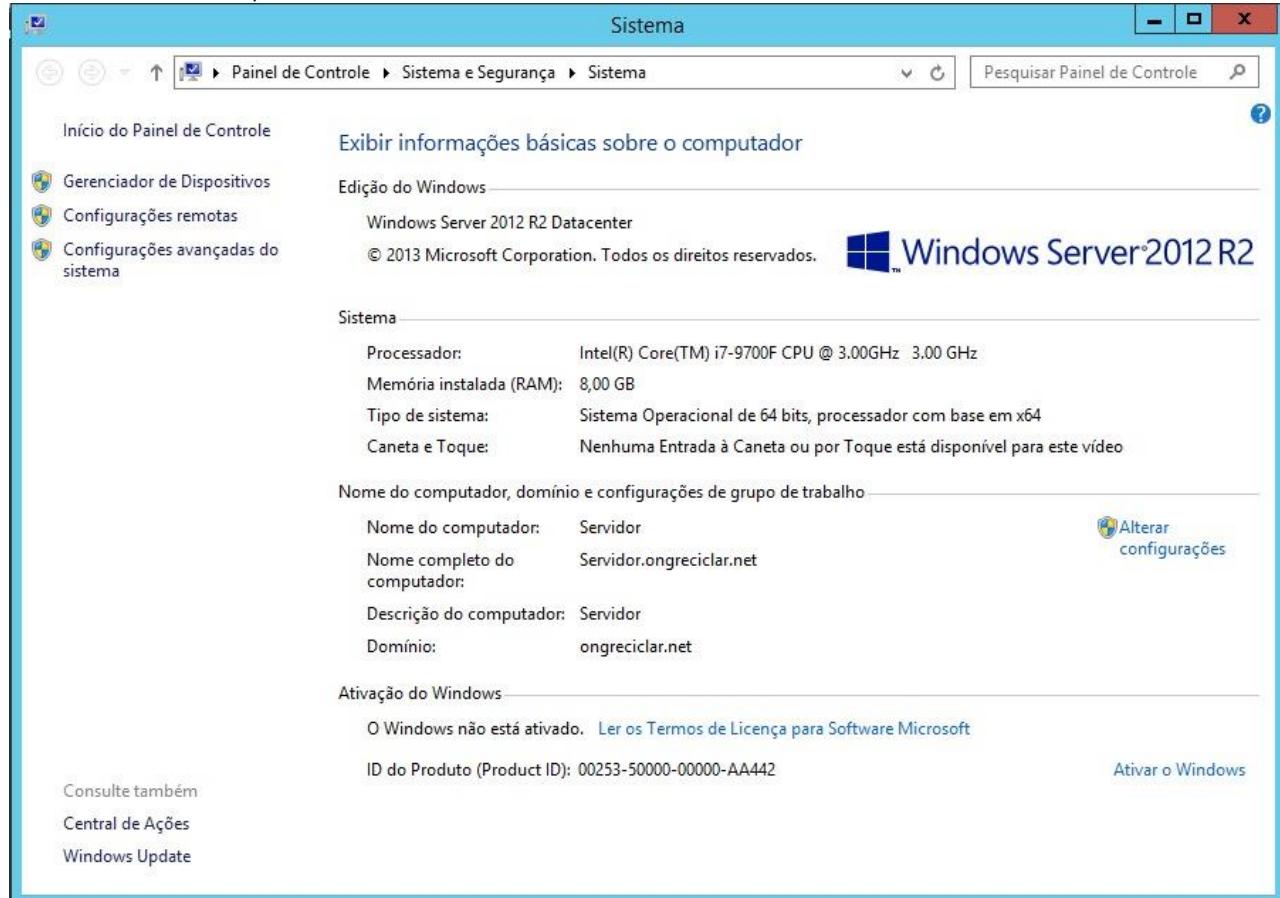
### 5.1 IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ

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

Sistema Operacional: Windows Server 2012 R2 64 bits

CPU: Intel Core I7 - 9700F @ 3.00GHz 3.00GHz

Memória RAM: 8,00 GB



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

Nome do servidor: Servidor \*

Domínio: ongreciclar.net

\*Colocamos o nome “Servidor” por  
haver apenas um servidor virtual, pois  
com ele executamos os 3 servidores  
que utilizamos.

**Credenciais de acesso:**

**Usuário:** Administrador

**Senha:** 0NGReciclar

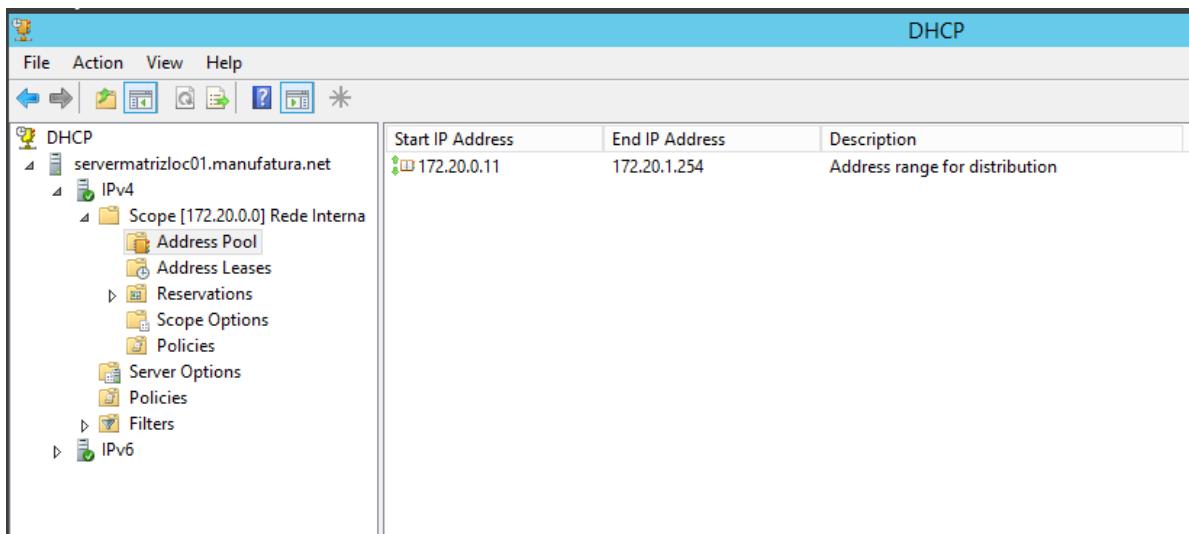
### **5.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP**

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

**Faixa inicial:** 172.20.0.11

**Faixa final:** 172.20.1.254

Desta forma poderá atender aos 35 computadores da Matriz e caso seja necessário acrescentar computadores a rede local, já será possível disponibilizar IP's para estes novos computadores.



Protocolo DHCP Instalado. Fonte: autoria própria

### **5.1.2 INSTALAÇÃO E CONFIGURAÇÃO DO DHCP**

Foi ativado o recurso do Active Directory e configurado para o domínio ongreciclar.net onde foram criadas as seguintes estruturas organizacionais contemplando os quatro escritórios localizados:

- Belo Horizonte (MG);
- Betim (MG);
- Contagem (MG);
- Nova Lima (MG);

Também foram criados usuários dentro do domínio:

Nome	Tipo	Descrição
Fernanda FFRB. Fonseca Ribeiro Bertoldo	Usuário	
Gabriel GNM. Novais Maia	Usuário	

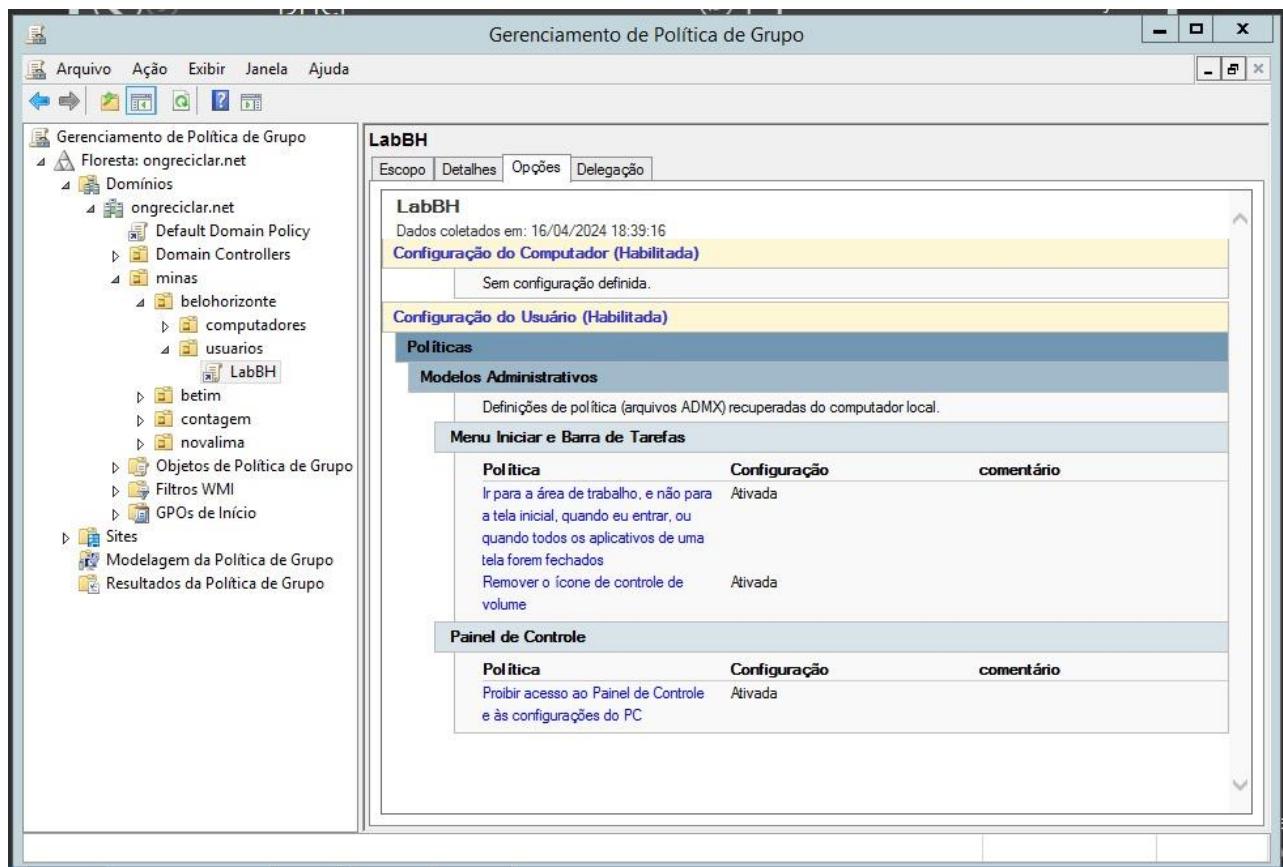
Usuários ativos na localidade belohorizonte. Fonte: autoria própria

\*Os demais usuários estão em pastas em suas devidas localidades.

### 5.1.3 POLÍTICAS DE GRUPO APLICADAS

Foram aplicadas as políticas abaixo:

- Ir para a área de trabalho, e não para a tela inicial, quando eu entrar ou quando todos os aplicativos de uma tela forem fechados.
- Remover o ícone de controle de volume.
- Proibir acesso ao Painel de Controle e às configurações do PC



Políticas Aplicadas. Fonte: autoria própria

## 5.2 IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ

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

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

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with various navigation options under 'Nuvem privada virtual' and 'Segurança'. The main area displays a table titled 'Suas VPCs (2) Informações' with the following data:

Name	ID da VPC	Estado	CIDR IPv4	CIDR IPv6	Conjunto de opções ...	Tabela de rota principal
vpc-0e24b1d4c1441d2c74	vpc-0e24b1d4c1441d2c74	Available	172.31.0.0/16	-	dopt-0c6fca69a860c4b94	rtb-070d84585ba9cae6
ongReciclar-vpc	vpc-0d181c90a9cc4514a	Available	10.0.0.0/16	-	dopt-0c6fca69a860c4b94	rtb-0c0204880506d5b9a

At the bottom of the page, there are links for CloudShell, Comentários, and footer information: © 2024, Amazon Web Services, Inc. ou suas afiliadas. | Privacidade | Termos | Preferências de cookies.

VPCs na AWS. Fonte:AWS

**Tabelas de rotas (5) informações**

Name	ID da tabela de rotas	Associações explícitas...	Associações de ...	Principal	VPC	ID do proprietário
ongReciclar-rtb-private1-us-east-1a	rtb-05238207b6098c18b	2 sub-redes	–	Não	vpc-0d181c90a9cc4514a   ongR...	164743580150
ongReciclar-rtb-public	rtb-0369cf5f994ea4084c	2 sub-redes	–	Não	vpc-0d181c90a9cc4514a   ongR...	164743580150
–	rtb-070e84585ba9ce6e	–	–	Sim	vpc-0e24b14c1441d2c74	164743580150
ongReciclar-rtb-private2-us-east-1b	rtb-01ea038bf6fa27af2	–	–	Não	vpc-0d181c90a9cc4514a   ongR...	164743580150
–	rtb-0c0204880506d5b9a	–	–	Sim	vpc-0d181c90a9cc4514a   ongR...	164743580150

Subredes na AWS. Fonte:AWS

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

**Grupos de segurança (3) Informações**

Name	ID do grupo de segurança	Nome do grupo de segurança	ID da VPC	Descrição	Proprietário
–	sg-0070e2078a61b46de	default	vpc-0d181c90a9cc4514a	default VPC security group	164743580150
–	sg-0a8e2c722799137fc	default	vpc-0e24b14c1441d2c74	default VPC security group	164743580150
–	sg-0740eb6ee6bdab5f7	ongReciclarsec	vpc-0d181c90a9cc4514a	Web e Terminal remoto	164743580150

Grupos de Segurança. Fonte: AWS

**Detalhes**

Nome do grupo de segurança	ID do grupo de segurança	Descrição	ID da VPC
ongReciclarsec	sg-0740db6ee6bdbab5f7	Web e Terminal remoto	vpc-0d181c90a9cc4514a

**Regras de entrada (2)**

Name	ID da regra do grupo...	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
-	sgr-057158574d107d...	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso Terminal
-	sgr-041a357fc301b3abc	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web

Regras de Entrada do Grupo de Segurança. Fonte: AWS

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

**Instâncias (1) Informações**

Name	ID da instância	Estado da inst...	Tipo de inst...	Verificação de stat...	Status do alarm...	Zona de dispon...	DNS IPv4 público	Endereço IP...	IP elástico
ongReciclarWe...	i-0d5a5ab3880686791	Executando	t2.large	2/2 verificações aj...	Exibir alarmes	us-east-1a	ec2-54-83-65-36.comp...	54.83.65.36	-

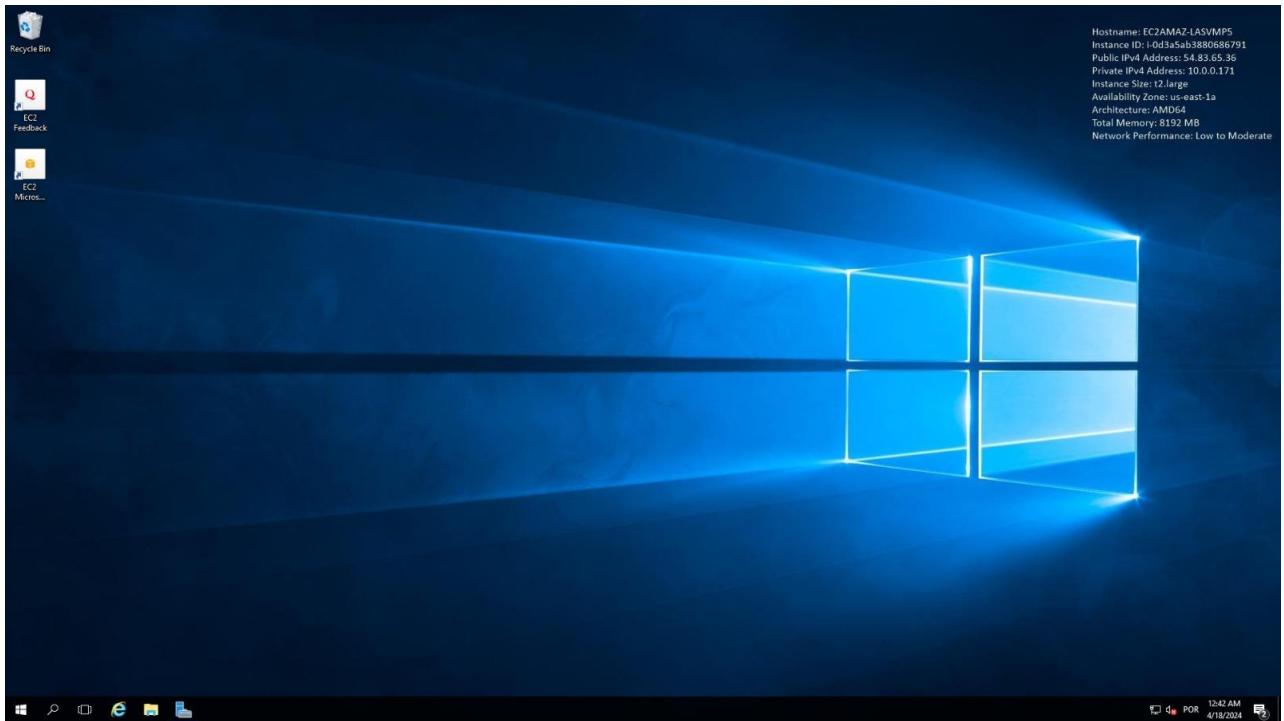
**Selecionar uma instância**

Instância do Servidor Web.  
Fonte: AWS

A 4<sup>a</sup> etapa foi para acessarmos o servidor criado via RDP e instalar o serviço de servidor web da Microsoft, o IIS. Realizamos a instalação do serviço e seguimos com a tentativa de acesso à página web de nosso servidor. As imagens abaixo mostram

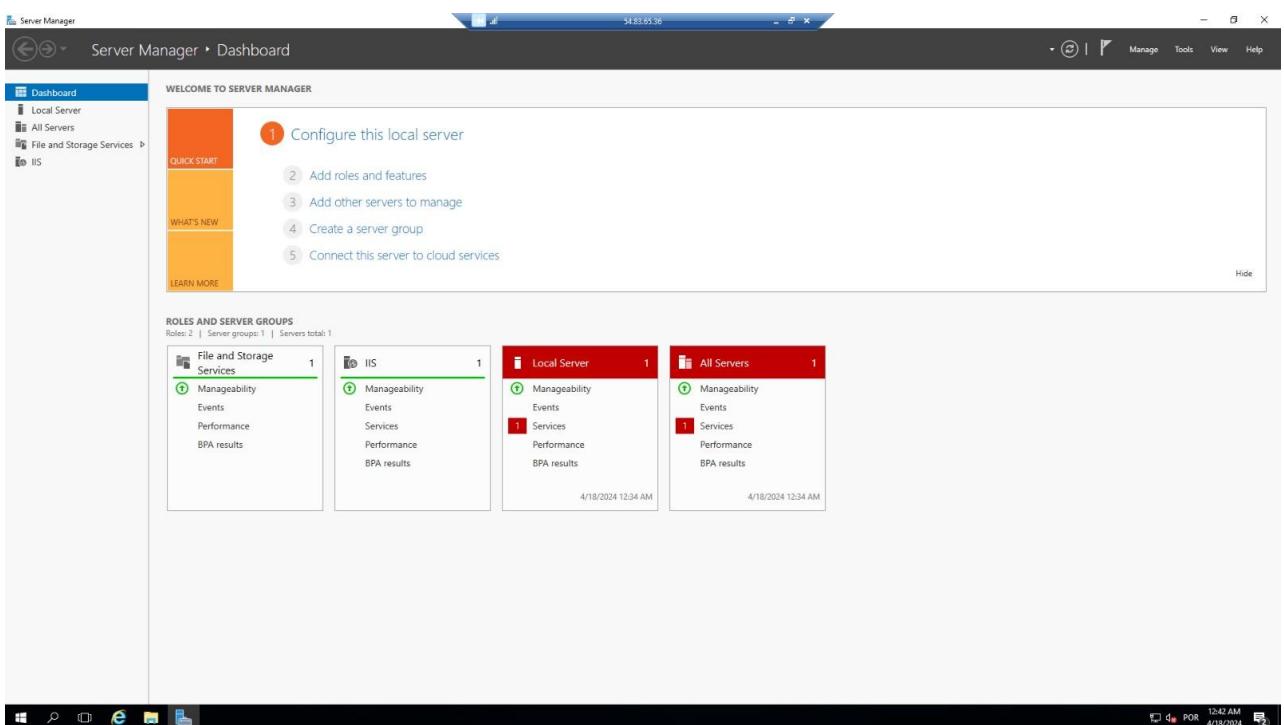
todo esse processo. Algumas imagens mostram IPs públicos diferentes em relação

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

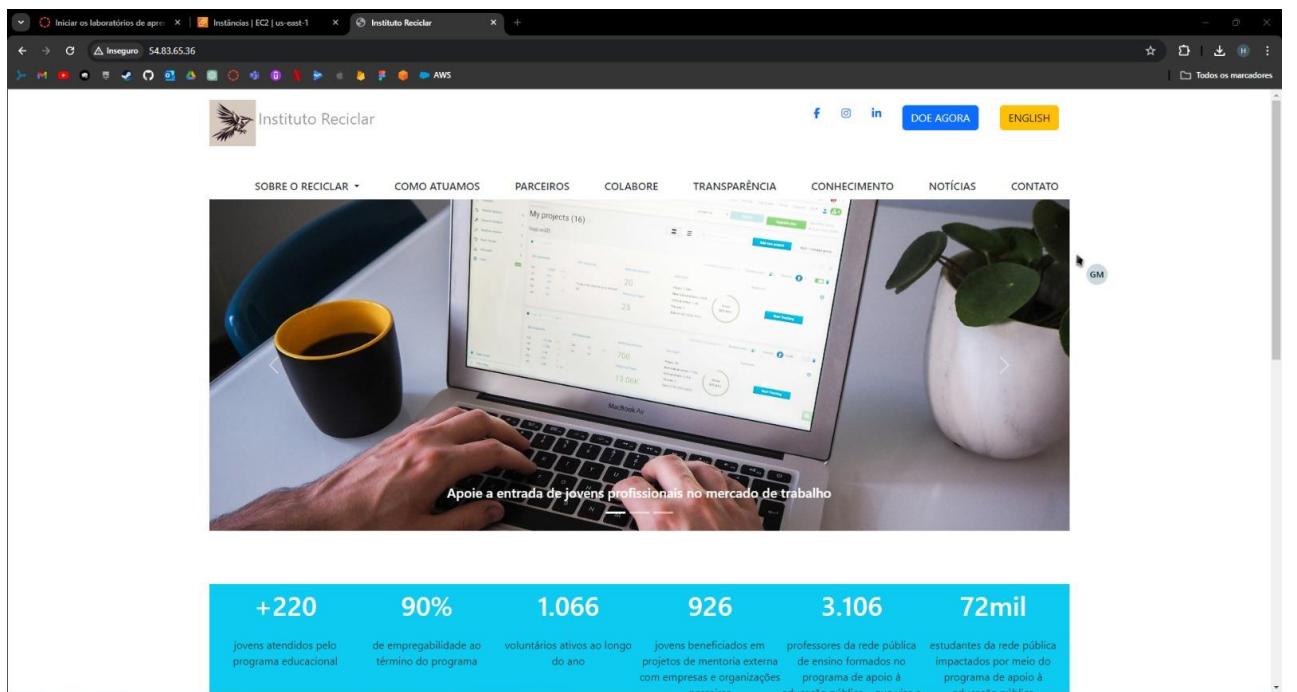


Acesso via RDP ao servidor.

Fonte: autoria própria



Serviço IIS disponível no servidor. Fonte: Autoria própria.



**+220**

jovens atendidos pelo  
programa educacional

**90%**

de empregabilidade ao  
término do programa

**1.066**

voluntários ativos ao longo  
do ano

**926**

jovens beneficiados em  
projetos de mentoria externa  
com empresas e organizações

**3.106**

professores da rede pública  
de ensino formados no  
programa de apoio à

**72mil**

estudantes da rede pública  
impactados por meio do  
programa de apoio à

Acesso a página do servidor web pelo navegador.

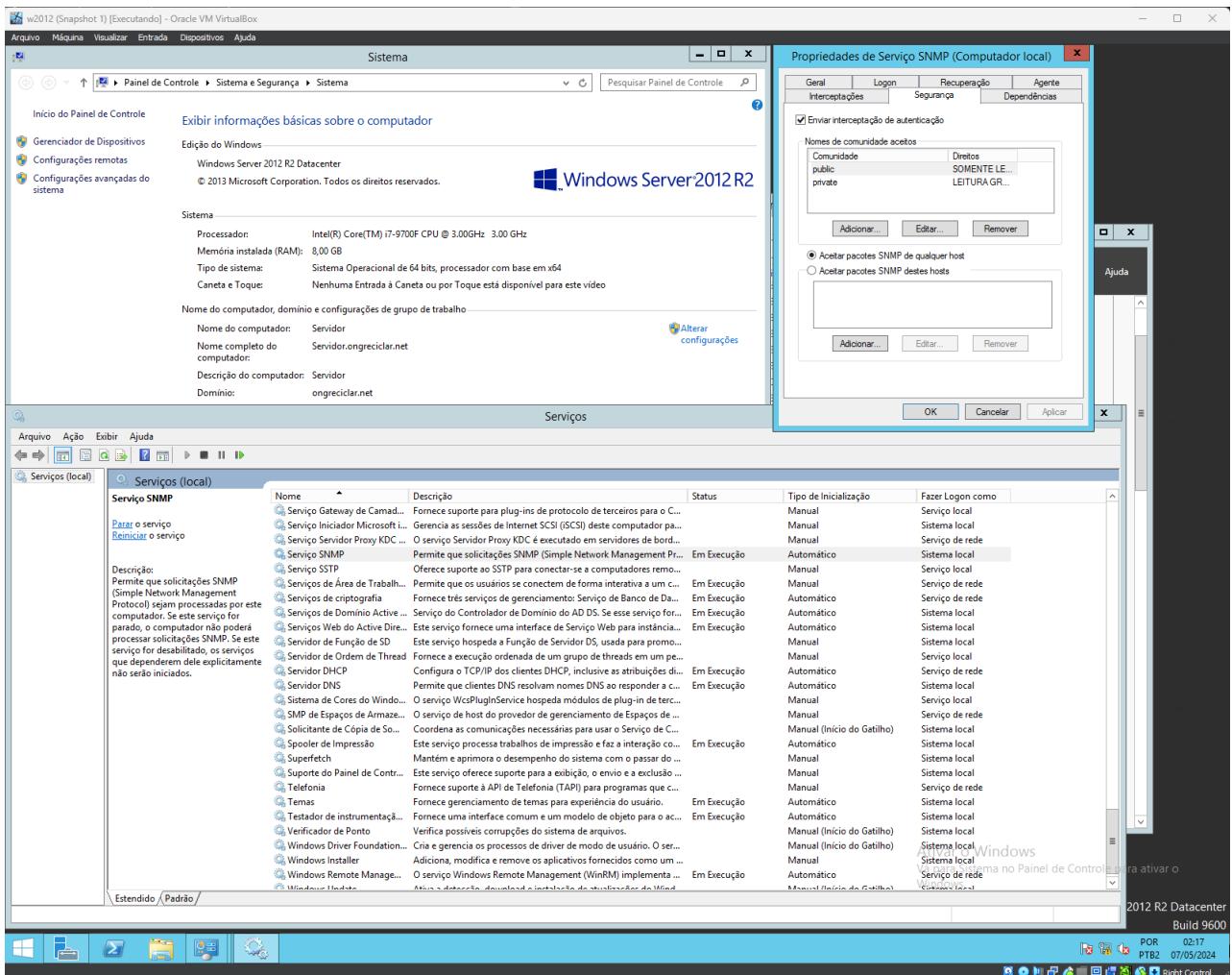
Fonte: autoria própria

## 6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX

### 6.1 GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX

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

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



Serviço de SNMP no servidor local.

Fonte: autoria própria

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

que desejávamos monitorar.

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

Host

Host IPMI Tags Macros Inventory Encryption Value mapping

\* Host name Servidor Local

Visible name Servidor Local

Templates Name Action  
Windows by SNMP Unlink Unlink and clear

type here to search Select

\* Host groups Virtual machines X Select

type here to search

Interfaces Type IP address DNS name Connect to Port Default

SNMP 192.168.1.2 IP DNS 161 Remove

Add

Description

Monitored by proxy (no proxy) ▾

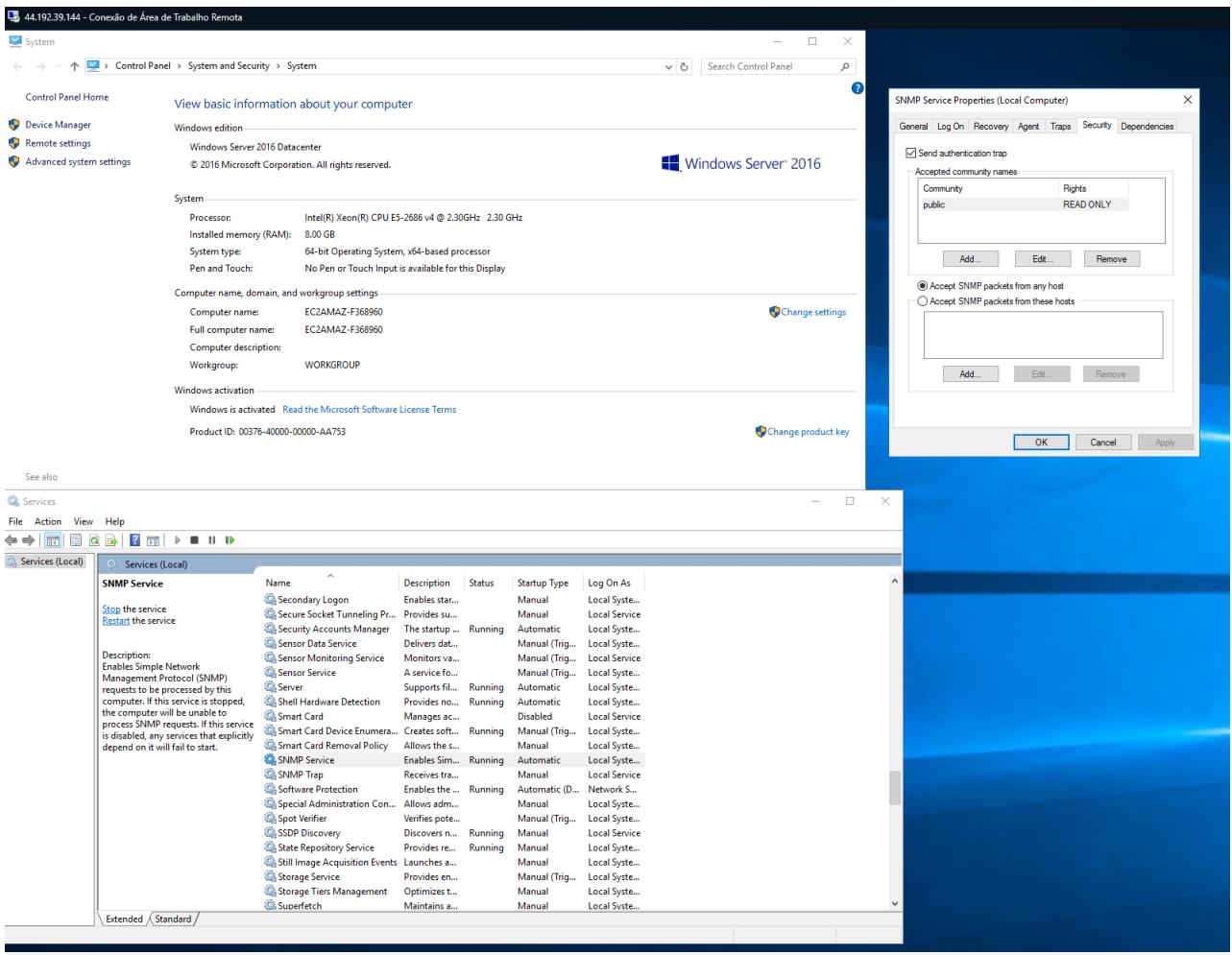
Enabled

Update Clone Full clone Delete Cancel

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

## 6.2 GERENCIAMENTO DO SERVIDOR DA NUVEM NO ZABBIX

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



### Serviço de SNMP no servidor da nuvem.

Fonte: autoria própria

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

**Host**

- Host**
- IPMI**
- Tags**
- Macros**
- Inventory**
- Encryption**
- Value mapping**

* Host name	Servidor Cloud					
Visible name	Servidor Cloud					
Templates	Name	Action				
Windows by SNMP		Unlink Unlink and clear				
type here to search		Select				
* Host groups	Virtual machines <input checked="" type="checkbox"/>	Select				
type here to search						
Interfaces	Type	IP address	DNS name	Connect to	Port	Default
▼ SNMP		44.192.39.144		IP	DNS	161
<a href="#">Add</a>						
Description						
Monitored by proxy	(no proxy)					
Enabled	<input checked="" type="checkbox"/>					
<a href="#">Update</a> <a href="#">Clone</a> <a href="#">Full clone</a> <a href="#">Delete</a> <a href="#">Cancel</a>						

Adição de servidor da nuvem no Zabbix.

Fonte: autoria própria

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

**Instâncias (1/1) Informações**

ID da instância	Nome	Estado da inst...	Tipo de inst...	Verificação de star...	Status do alarme	Zona de dispon...	DNS IPv4 público	Endereço IP p...	IP elástico	IPs IPv6	Monitoram...	Nome do grupo de segurança
i-0c85c28b4b51deebe	OngReciclarW...	Executando	t2 large	2/2 verificações a...	Exibir alarmes	us-east-1a	ec2-44-192-39-144.co...	44.192.39.144	-	-	-	disabled

**i-0c85c28b4b51deebe (OngReciclarWebServer)**

Detalhes	Status e alarmes	Monitoramento	Segurança	Redes	Armazenamento	Tags																																				
Função IAM	-	-	ID do proprietário: 107161436643	Date de lançamento: Fri May 14 2024 19:40:05 GMT-0300 (Horário Padrão de Brasília)	-	-																																				
Grupos de segurança	sg-0f948ffaa05275e6 (ongReciclarsec)	-	-	-	-	-																																				
Regras de entrada	<table border="1"> <thead> <tr> <th>Regras de filtro</th> </tr> </thead> <tbody> <tr> <td>Nome</td> <td>ID da regra do grupo de se...</td> <td>Intervalo de po...</td> <td>Protocolo</td> <td>Origem</td> <td>Grupos de segurança</td> <td>Descrição</td> </tr> <tr> <td>-</td> <td>sgr-08895352adc17a70</td> <td>80</td> <td>TCP</td> <td>0.0.0.0/0</td> <td>ongReciclarsec</td> <td>Acesso Web</td> </tr> <tr> <td>-</td> <td>egr-08915c2c7c9f6d6</td> <td>3389</td> <td>TCP</td> <td>0.0.0.0/0</td> <td>ongReciclarsec</td> <td>Acesso Terminal Remoto</td> </tr> <tr> <td>-</td> <td>sgr-082458514e47d745ab</td> <td>161 - 162</td> <td>UDP</td> <td>0.0.0.0/0</td> <td>ongReciclarsec</td> <td>Protocolo UDP para Zabbix</td> </tr> <tr> <td>-</td> <td>sgr-043f07472cb8d42</td> <td>Todos</td> <td>ICMP</td> <td>0.0.0.0/0</td> <td>ongReciclarsec</td> <td>ICMP para Zabbix</td> </tr> </tbody> </table>						Regras de filtro	Nome	ID da regra do grupo de se...	Intervalo de po...	Protocolo	Origem	Grupos de segurança	Descrição	-	sgr-08895352adc17a70	80	TCP	0.0.0.0/0	ongReciclarsec	Acesso Web	-	egr-08915c2c7c9f6d6	3389	TCP	0.0.0.0/0	ongReciclarsec	Acesso Terminal Remoto	-	sgr-082458514e47d745ab	161 - 162	UDP	0.0.0.0/0	ongReciclarsec	Protocolo UDP para Zabbix	-	sgr-043f07472cb8d42	Todos	ICMP	0.0.0.0/0	ongReciclarsec	ICMP para Zabbix
Regras de filtro																																										
Nome	ID da regra do grupo de se...	Intervalo de po...	Protocolo	Origem	Grupos de segurança	Descrição																																				
-	sgr-08895352adc17a70	80	TCP	0.0.0.0/0	ongReciclarsec	Acesso Web																																				
-	egr-08915c2c7c9f6d6	3389	TCP	0.0.0.0/0	ongReciclarsec	Acesso Terminal Remoto																																				
-	sgr-082458514e47d745ab	161 - 162	UDP	0.0.0.0/0	ongReciclarsec	Protocolo UDP para Zabbix																																				
-	sgr-043f07472cb8d42	Todos	ICMP	0.0.0.0/0	ongReciclarsec	ICMP para Zabbix																																				

**Regras de saída**

Regras de filtro						
Nome	ID da regra do grupo de se...	Intervalo de po...	Protocolo	Destino	Grupos de segurança	Descrição
-	sgr-0e75e052b237a9db6	Todos	Todos	0.0.0.0/0	ongReciclarsec	-

Regras de entrada no grupo de segurança da nuvem.

Fonte: Autoria própria

Regras de saída no grupo de segurança da nuvem.

Fonte: autoria própria

## 6.3 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX

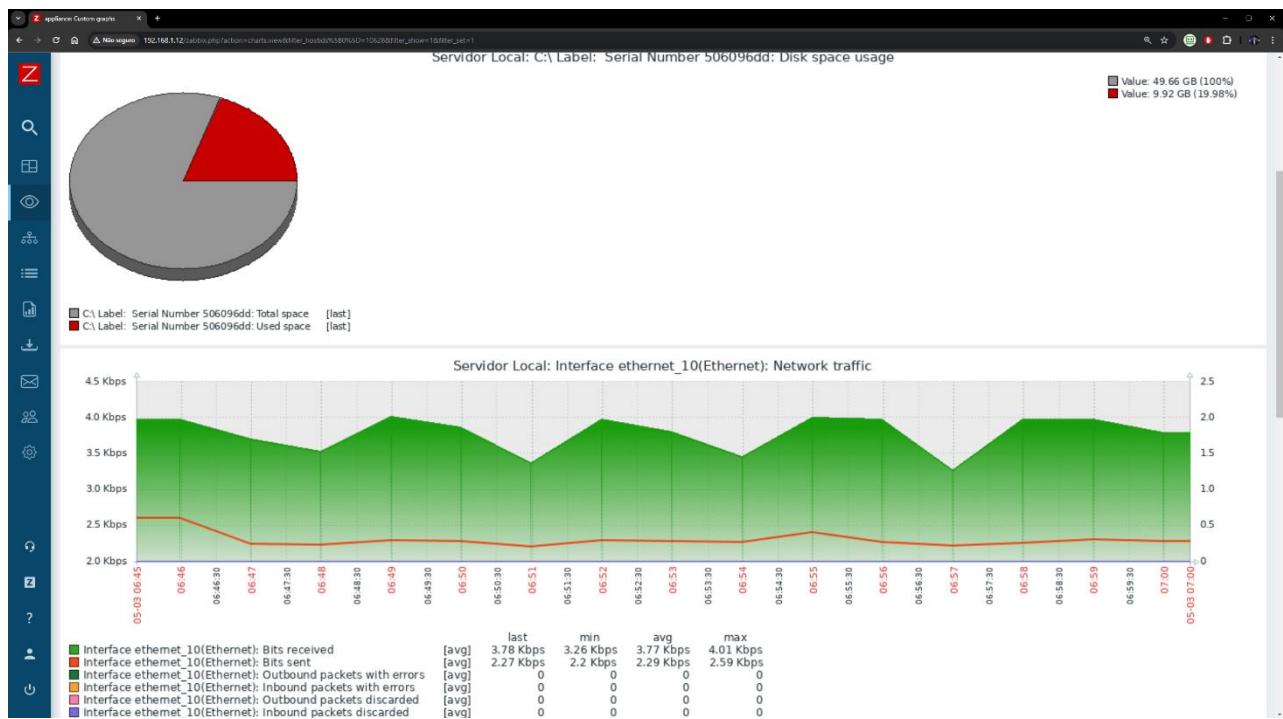
Com a configuração realizada no servidor local e no servidor da nuvem, o Zabbix já conseguia monitorar os servidores. Verificamos na ferramenta que ambas as comunicações com os hosts estavam sendo executadas sem qualquer falha, conforme imagens abaixo.

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Servidor Cloud	44.192.39.144:161	SNMP	class: os   target: windows	Enabled	Latest data 30	1	Graphs 4	Dashboards 2	Web
Servidor Local	192.168.1.2:161	SNMP	class: os   target: windows	Enabled	Latest data 30	Problems	Graphs 4	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os   class: software   target: linux	Enabled	Latest data 146	Problems	Graphs 27	Dashboards 4	Web

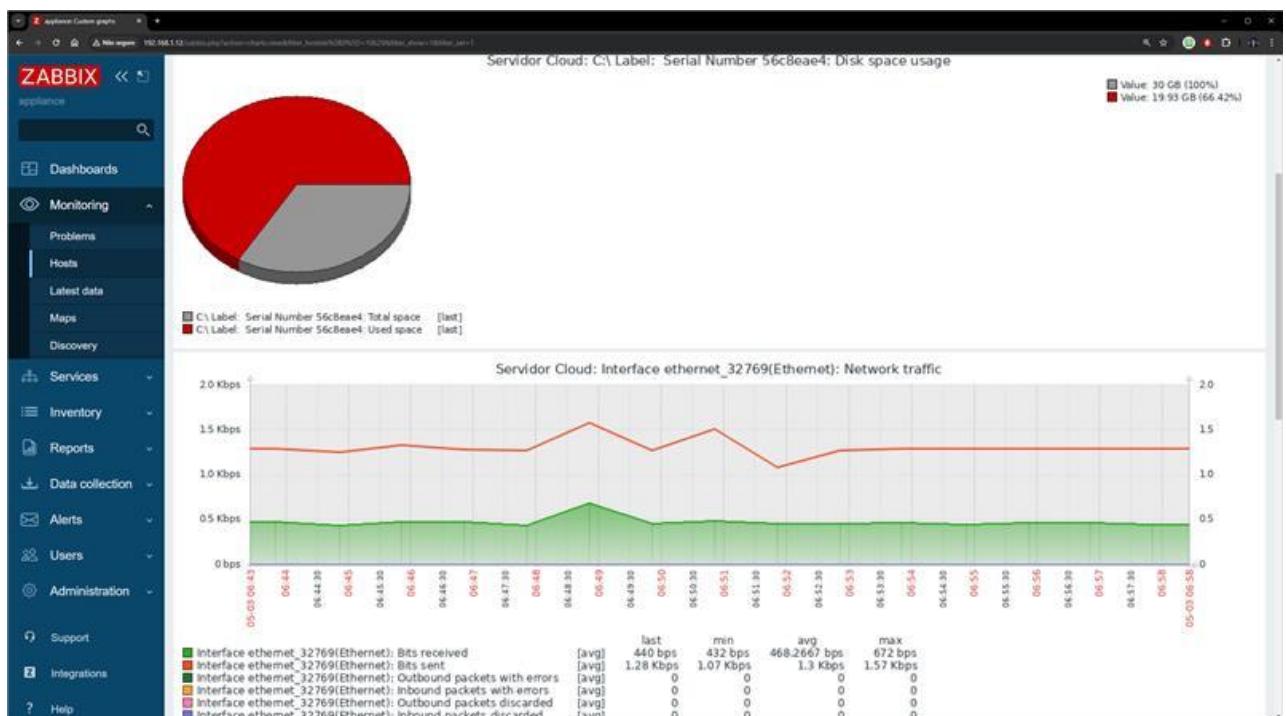
Visualização dos hosts adicionados para coleta de dados no Zabbix.

Fonte: Autoria própria

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



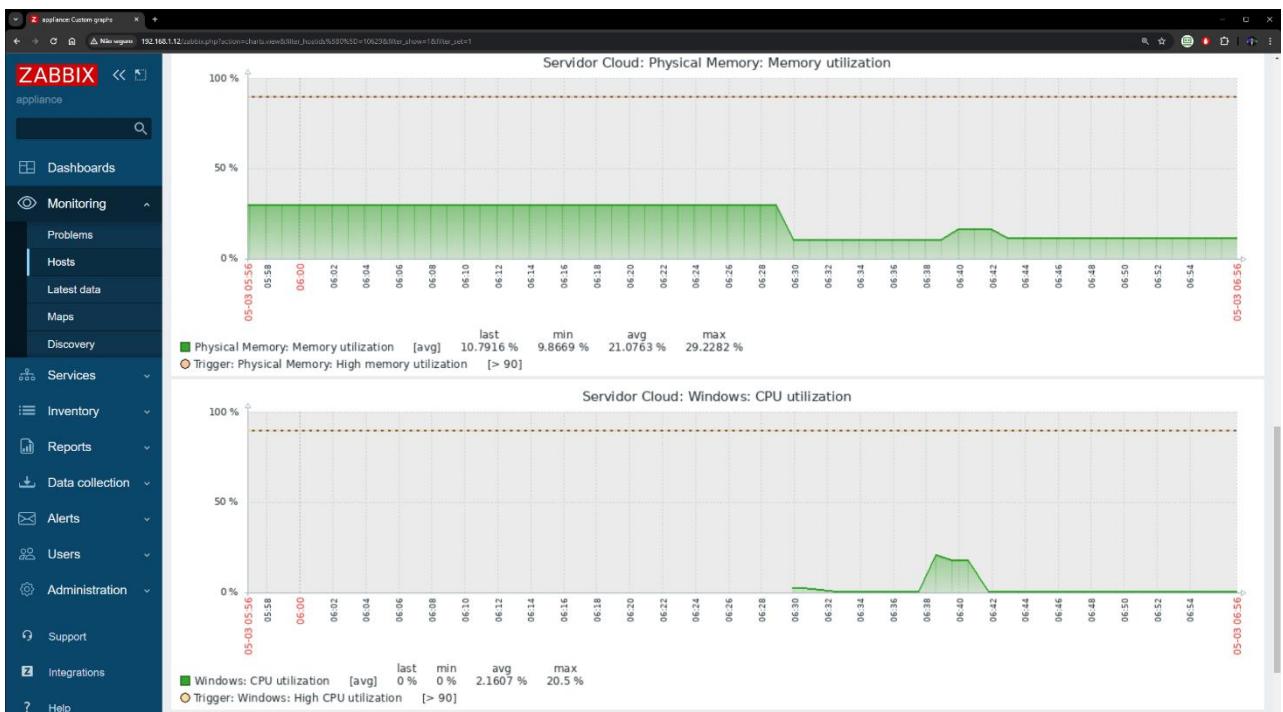
Monitoramento de disco e tráfego de rede do servidor local no zabbix.  
Fonte: Autoria própria



Monitoramento de disco e tráfego de rede do Servidor localizado em nuvem no Zabbix.  
Fonte: Autoria própria



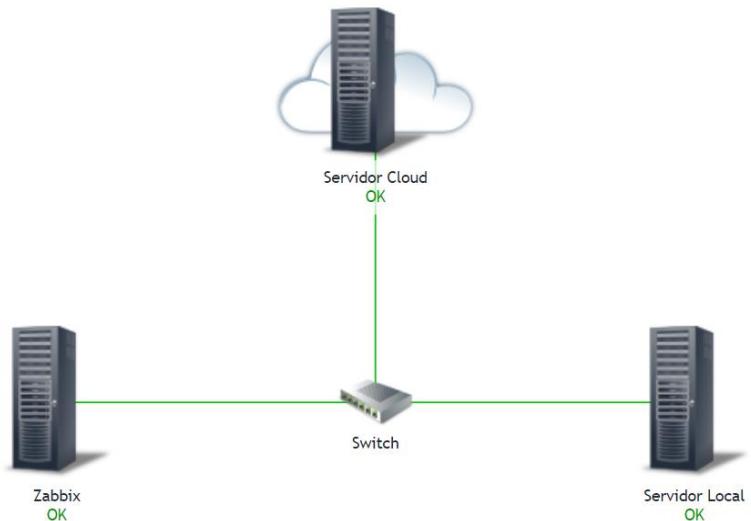
Monitoramento do Uso de Memória e Cpu Servidor Local no Zabbix.  
Fonte: Autoria própria



Monitoramento do Uso de Memória e Cpu Servidor Cloud  
Fonte: Autoria própria

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

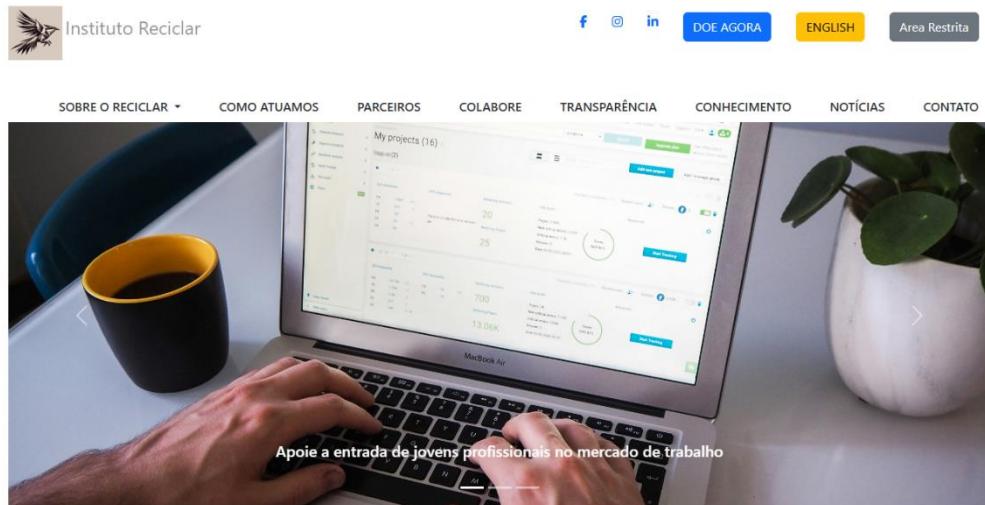
OngReciclar



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

## 7. APLICAÇÃO BACK-END

Nessa etapa, foi criada uma política de segurança e essa política de segurança, ela está disponível no apêndice. Foi também criado uma aplicação Back End, cujas telas se encontram nas seguintes figuras.



The screenshot shows the homepage of the Instituto Reciclar website. At the top, there is a navigation bar with links for 'SOBRE O RECICLAR', 'COMO ATUAMOS', 'PARCEIROS', 'COLABORE', 'TRANSPARÊNCIA', 'CONHECIMENTO', 'NOTÍCIAS', and 'CONTATO'. There are also social media icons for Facebook, Instagram, and LinkedIn, a 'DOE AGORA' button, an 'ENGLISH' link, and a 'Área Restrita' link. Below the navigation bar, there is a large image of a person's hands typing on a laptop keyboard. The laptop screen displays a project management application titled 'My projects (16)' with various project details like names, descriptions, and progress bars. To the left of the laptop is a black mug with a yellow interior, and to the right is a white vase with green plants. A banner at the bottom of the image reads 'Apoie a entrada de jovens profissionais no mercado de trabalho'.

+220	90%	1.066	926	3.106	72mil
jovens atendidos pelo programa educacional	de empregabilidade ao término do programa	voluntários ativos ao longo do ano	jovens beneficiados em projetos de mentoria externa com empresas e organizações parceiras	professores da rede pública de ensino formados no programa de apoio à educação pública – que visa a capacitação dos profissionais de educação	estudantes da rede pública impactados por meio do programa de apoio à educação pública

Página Principal – Home  
Nessa tela se encontra a página central inicial de quando acessamos a aplicação.



Instituto Reciclar

[Home](#)

### Relação de Alunos

[Aluno](#) [Buscar](#)

[+](#)  
Adicionar Aluno

Matrícula	Nome	Data Nasc.	Telefone	Email		
Gabriel.270935	Gabriel Novais Maia	01/02/1999	31912345678	@gmail.com		
Luana.412766	Luana Piovanni	31/05/2004	31998651214	luana@gmail.com		



**CONTATO**  
Av. Presidente Altino, 973  
Jaguaré – São Paulo, SP  
Telefone: (11) 3768-3607  
E-mail: [reciclar@reciclar.org.br](mailto:reciclar@reciclar.org.br)

**Horário de Atendimento**  
Segunda a Sexta: 8h00 – 18h00

**NEWSLETTER**  
Fique por dentro! Cadastre seu e-mail no campo abaixo para receber notícias e informações sobre a gente!

**SIGA A GENTE**  
[f](#) [@](#) [in](#)

**SELOS E PREMIAÇÕES**

**Página 02 - Lista de Alunos**  
Podemos notar nesta tela a lista de alunos, onde se encontra no bottom "Área Restrita" e podemos ver a relação de usuários (Alunos)



Instituto Reciclar

[Home](#)

**Relação de Alunos**

[Aluno](#) [Buscar](#)

[+](#)  
Adicionar Aluno

Matrícula	Nome	
Gabriel.270935	Gabriel Novais Maia	

[Adicionar Aluno](#)

[Email](#)

@gmail.com

Nome

CPF  Data de Nascimento

Telefone  Email

Endereço

[Fechar](#) [Salvar](#)

[SIGA A GENTE](#)  
[f](#) [@](#) [in](#)

[SELOS E PREMIAÇÕES](#)

Instituto Reciclar

**Página 03 - Adicionar novo Aluno (Create)**  
Nesta tela é opção de adicionar novo usuário(Aluno)

**Relação de Alunos**

Matrícula	Nome
Gabriel.270935	Gabriel Novais Maia
Luana.412766	Luana Piovanni

**Adicionar Aluno**

Nome: Luana Piovanni

CPF: 58965415263 Data de Nascimento: 31/05/2004

Telefone: 31998651214 Email: luana@gmail.com

Endereço: Rua da Luz

**Fechar** **Salvar**

Horário de Atendimento: Segunda a Sexta: 8h00 - 18h00

**Página 04 - Dados do Aluno (Read)**  
Nesta tela visualizamos os dados de usuários que cadastramos

**Relação de Alunos**

Matrícula	Nome
Gabriel.270935	Gabriel Novais Maia
Luana.412766	Luana Piovanni

**Editar Aluno**

Nome: Luana Piovanni

CPF: 58965415263 Data de Nascimento: 31/05/2004

Telefone: 31998651214 Email: luana@gmail.com

Endereço: Rua da Luz

**Fechar** **Salvar**

Horário de Atendimento: Segunda a Sexta: 8h00 - 18h00

**Página 05 - Editar dados do Aluno (Update)**  
Nesta tela podemos editar os dados dos alunos como nome, CPF, data de nascimento, telefone, email e endereço.

**Relação de Alunos**

Matrícula	Nome	Data Nasc.	Telefone	Email
Gabriel.270935	Gabriel Novais Maia	01/02/1999	31912345678	@gmail.com
Luana.412766	Luana Piovanni Gomes	31/05/2004	31998651214	luana@gmail.com.br

**CONTATO**  
Av. Presidente Altino, 973  
Jaguaré – São Paulo, SP  
Telefone: (11) 3768-3607  
E-mail: reciclar@reciclar.org.br

**NEWSLETTER**  
Fique por dentro! Cadastre seu e-mail no campo abaixo para receber notícias e informações sobre a gente!

**SIGA A GENTE**  
[f](#) [g](#) [in](#)

**SELOS E PREMIAÇÕES**

**Instituto Reciclar**

### Página 06 - Remover um Aluno (Delete)

Notamos nessa tela que podemos apagar e remover um aluno que já cadastramos.

**Relação de Alunos**

Matrícula	Nome	Data Nasc.	Telefone	Email
Gabriel.270935	Gabriel Novais Maia	01/02/1999	31912345678	@gmail.com
Luana.412766	Luana Piovanni Gomes	31/05/2004	31998651214	luana@gmail.com.br

**CONTATO**  
Av. Presidente Altino, 973  
Jaguaré – São Paulo, SP  
Telefone: (11) 3768-3607  
E-mail: reciclar@reciclar.org.br

**NEWSLETTER**  
Fique por dentro! Cadastre seu e-mail no campo abaixo para receber notícias e informações sobre a gente!

**SIGA A GENTE**  
[f](#) [g](#) [in](#)

**SELOS E PREMIAÇÕES**

**Instituto Reciclar**

### Página 07 - Lista de usuários/ alunos (Users)

Aqui podemos ver a lista de usuários com os respectivos dados dos cadastrados.

## **8. REFERÊNCIAS**

Site Instituto Reciclar. Disponível em:<https://reciclar.org.br/>

Acesso em: 16 Junho 2023

### **Tabela de Materiais:**

OptiPlex Micro - Disponível em: Link

Impressora Disponível em: [Link](#) —

Ap Intel Brás Disponível em: [Link](#)

Câmera Disponível em: [Link](#)

No Break Disponível em: [Link](#)

Cabo Rede Furukawa Disponível em: [Link](#)

Rack de Piso 44U Disponível em: [Link](#)

Teclado e Mouse Disponível em: [Link](#)

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

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

## Anexo I - Política de Segurança ONG Reciclar

Versão	Data	Alteração
Versão 1.0	02/06/2024	Lançamento da Primeira versão

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### 1. INTRODUÇÃO

3

### 2. OBJETIVOS

3

### 3. ABRANGÊNCIA

4

### 4. DIRETRIZES GERAIS

4

#### 4.1 Interpretação

4

#### 4.2 Propriedade

5

#### 4.3 Classificação da Informação

6

#### 4.4 Controle de Acesso

7

#### 4.5 Internet

8

#### 4.6 Correio Eletrônico

9

#### 4.7 REDE SEM FIO (WI-FI)

9

#### 4.8 Recursos de TIC

Institucionais.....

.....10

#### 4.9 Recursos de TIC Particulares

12

#### 4.10 Armazenamento de Informações

13	
4.11	<b>Repositórios Digitais</b>
14	
4.12	<b>Áudio, Vídeos e Fotos</b>
15	
4.13	<b>Uso de Imagem, Som da Voz e Nome</b>
16	
4.14	<b>Aplicativos de Comunicação</b>
16	
4.15	<b>Monitoramento</b>
16	
4.16	<b>Combate à Intimidação Sistemática (BULLYING)</b>
17	
4.17	<b>Segurança da Informação</b>
17	
5.	<b>PAPÉIS E RESPONSABILIDADES</b>
18	
TODOS.....	
18	
Gestores e Coordenadores	
19	
Colaboradores	19
6.	<b>DISPOSIÇÕES FINAIS</b>
21	
7.	<b>DOCUMENTOS DE REFERÊNCIA</b>
22	

## **1. INTRODUÇÃO**

O Instituto Reciclar, conforme previsto em seu Estatuto, é uma organização sem fins lucrativos dedicada à promoção da inclusão produtiva de jovens em situação de vulnerabilidade social. Com mais de 25 anos de experiência, sua missão é proporcionar qualificação profissional, estabelecer conexões com o mercado de trabalho e compartilhar seu conhecimento especializado. Para atingir esses objetivos, o Instituto adota metodologias inovadoras e práticas educativas que visam à formação integral dos jovens, oferecendo-lhes as ferramentas necessárias para um futuro promissor.

No entanto, o cenário atual, caracterizado por rápidas mudanças e avanços tecnológicos, apresenta novos desafios que demandam maior atenção e cuidados específicos. A mobilidade e a ausência de fronteiras físicas, características da sociedade moderna, exigem estratégias robustas para garantir a segurança e a proteção dos jovens atendidos e de toda a equipe do Instituto.

Nesse contexto, a segurança da informação se torna uma atividade fundamental para proteger todos os ativos tangíveis e intangíveis do Instituto Reciclar, como imagem, reputação, conhecimento, patrimônio e a própria informação. Portanto, é essencial que todos os membros da organização, desde a administração até os instrutores e beneficiários, pratiquem e promovam as boas práticas de segurança digital.

Em resposta a essas novas necessidades, o Instituto Reciclar está implementando um Sistema de Gestão de Segurança da Informação (SGSI), que tem como diretriz principal a Política de Segurança da Informação (PSI). Esse sistema é crucial para atender às especificidades do segmento social e educacional em que o Instituto atua, garantindo a proteção dos ativos durante o processo de formação e inclusão produtiva dos jovens. Para que os objetivos do Instituto Reciclar sejam plenamente alcançados, é imprescindível que essas novas regras sejam observadas por todos os envolvidos.

## 2. OBJETIVOS

- Estabelecer **diretrizes estratégicas e princípios para a proteção dos ativos tangíveis e intangíveis**: Isso inclui a proteção da imagem, reputação, marca, propriedade intelectual, bancos de dados, conhecimento e recursos de tecnologia da informação e comunicação (TIC) do Instituto, além das informações dos jovens atendidos.
  - Guiar a **tomada de decisões e a execução das atividades profissionais e educacionais**: Todas as ações dos colaboradores do Instituto, em ambientes presenciais ou digitais, devem estar alinhadas às normas institucionais e à legislação nacional vigente.
  - Definir **princípios para o desenvolvimento de atividades educacionais seguras**: Assegurar que as atividades não causem danos à reputação do Instituto e seus beneficiários.
- 
- Construir **uma cultura de uso seguro das informações**: Formar indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital, promovendo a conscientização sobre a importância da segurança da informação.
  - Preservar a **confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e recursos de TIC**: Garantir que as informações e recursos tecnológicos do Instituto estejam sempre protegidos e acessíveis de maneira segura e legal.
  - Orientar a **definição de normas e procedimentos específicos de segurança da informação**: Implementar controles e processos que assegurem o cumprimento das políticas de segurança, criando um ambiente confiável para o desenvolvimento das atividades do Instituto.

### **3. ABRANGÊNCIA**

Esta Política de Segurança da Informação (PSI) é um regulamento interno, com valor jurídico e aplicabilidade imediata e irrestrita a todo o público atendido e colaboradores do Instituto Reciclar. Aplica-se aos ambientes educacional, administrativo e operacional, abrangendo todos aqueles que tenham acesso e/ou utilizem as informações, recursos de tecnologia da informação e comunicação (TIC) e/ou demais ativos tangíveis ou intangíveis do Instituto.

### **4. DIRETRIZES GERAIS**

#### **4.1 Interpretação**

##### **4.1.1**

Para os fins desta Política de Segurança da Informação (PSI), são adotadas as siglas, os termos e definições constantes no Apêndice A.

##### **4.1.2**

Esta PSI deve ser interpretada de forma restritiva. Casos excepcionais ou não tratados por ela só podem ser realizados após prévia e expressa autorização do Instituto Reciclar.

###### **4.1.2.1**

Qualquer exceção ou permissão diferenciada será concedida de forma pontual, aplicável apenas ao solicitante, dentro dos limites e motivos que a fundamentaram. A aprovação dessas exceções será por mera liberalidade do Instituto Reciclar e terá duração limitada, podendo ser revogada a qualquer momento, sem necessidade de aviso prévio.

#### **4.2 Propriedade**

##### **4.2.1**

As informações geradas, acessadas, recebidas, manuseadas ou armazenadas, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis do Instituto Reciclar, são de propriedade e de direito de uso exclusivos da organização.

##### **4.2.2**

Os recursos de TIC fornecidos pelo Instituto Reciclar para o desenvolvimento de atividades educacionais, administrativas e operacionais são de propriedade da instituição ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito. Portanto, devem ser utilizados exclusivamente para o cumprimento das finalidades a que se destinam.

#### **4.2.3**

Todos os ativos tangíveis e intangíveis do Instituto Reciclar só podem ser utilizados para o cumprimento das atividades profissionais e educacionais, limitados à função do público atendido ou colaborador.

#### **4.2.4**

A utilização das marcas, identidade visual e demais sinais distintivos do Instituto Reciclar, atuais e futuros, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais e educacionais, mediante prévia e expressa autorização.

#### **4.2.5**

Todo o público atendido e colaboradores podem fazer menção à marca em conteúdos e materiais para citação do local onde trabalham, ministram aulas ou estudam. No entanto, a marca não pode, em hipótese alguma, ser utilizada para criação de perfis em mídias sociais em nome da instituição ou para se fazer passar por ela.

### **4.3 Classificação da informação**

#### **4.3.1**

Para garantir a adequada proteção das informações, é responsabilidade do colaborador classificá-las no momento em que forem geradas, assegurando a devida confidencialidade, especialmente em relação a conteúdos e dados pessoais. Desse modo a informação pode ser classificada da seguinte forma:

##### **4.3.1.1 Informação pública**

Informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à instituição e aos jovens atendidos.

##### **4.3.1.2 Informação interna**

Informação que pode ser divulgada para o público atendido e colaboradores da instituição, enquanto estiverem desempenhando atividades educacionais e profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

##### **4.3.1.3 Informação confidencial**

Informação exclusiva para quem se destina, que requer tratamento especial. Contém dados pessoais e/ou sigilosos que, se divulgados, podem afetar a reputação e a imagem da instituição ou causar impactos graves sob os aspectos financeiro, legal e normativo.

#### **4.3.2 Rotulagem da Informação**

Informações não públicas devem ser rotuladas no momento em que forem geradas, armazenadas ou disponibilizadas.

#### **4.3.2.1**

Para informações geradas e/ou armazenadas em mídias removíveis ou papel, utilize carimbo, etiqueta ou texto padronizado para identificar o nível de classificação da informação: interna ou confidencial.

#### **4.3.2.2**

Para informações geradas ou mantidas em ambientes lógicos, utilize documentação específica para definir o nível de classificação da informação, tais como documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados, Plano Diretor de Segurança e Políticas de Uso.

#### **4.3.3**

Todo o público atendido e colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusearem ou com que vierem a tomar contato.

##### **4.3.3.1**

Em caso de dúvida, a informação deve ser tratada como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à instituição, incluindo a internet e mídias sociais, sem prévia e expressa autorização do Instituto Reciclar.

#### **4.3.4**

Todo colaborador deve respeitar o sigilo profissional e contratual. Portanto, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, jovens atendidos, fornecedores, prestadores de serviços ou demais detalhes institucionais críticos.

#### **4.3.5**

O público atendido deve respeitar o sigilo das informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros jovens e colaboradores da instituição.

#### **4.3.6**

Toda informação envolvendo dados pessoais do público atendido, especialmente o prontuário escolar, e de colaboradores deve ser tratada como sigilosa, utilizada com cautela e apenas por pessoas autorizadas.

#### **4.3.7**

A Gestão de Tecnologia da Informação (GTI) é responsável por homologar os mecanismos de criptografia, cifragem ou codificação para o armazenamento e a transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade.

### **4.4 Controle de acesso**

#### **4.4.1**

Para cada jovem atendido e colaborador é fornecida uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC do Instituto Reciclar.

##### **4.4.1.1**

A identidade digital é monitorada e controlada pelo Instituto Reciclar.

##### **4.4.1.2**

O público atendido e o colaborador são responsáveis pelo uso e sigilo de sua identidade digital. Não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

#### **4.4.2**

Quando a identidade for disponibilizada e fornecida pelo Instituto, todos os colaboradores, prestadores de serviços e visitantes, enquanto presentes nas dependências físicas da instituição, devem estar devidamente identificados, portando o crachá individual de forma visível.

##### **4.4.2.1**

O crachá de identificação é de uso individual, não sendo autorizado o compartilhamento com outro colaborador ou terceiro, tampouco seu uso fora das dependências do Instituto Reciclar.

#### **4.4.3**

Para garantir a segurança física, o Instituto Reciclar deve estabelecer áreas fisicamente seguras para proteger os espaços que criam, desenvolvem, processam ou armazenam informações críticas e que contenham ativos críticos para a instituição, tais como datacenters, salas de telecomunicações e salas de documentação crítica.

#### **4.4.4**

Os ativos críticos para a instituição devem estar protegidos contra falta de energia elétrica e outras interrupções causadas por falhas, além de serem submetidos a correta manutenção para assegurar sua contínua integridade e disponibilidade.

### **4.5 Internet**

#### **4.5.1**

Os recursos de conectividade são fornecidos para atender aos propósitos administrativos e educacionais do Instituto Reciclar, considerando que o acesso à internet é um direito essencial para o exercício da cidadania no Brasil. No entanto, é imprescindível que o público atendido e colaboradores utilizem a internet em estrita observância das leis em

vigor. Qualquer uso inadequado ou ilícito da internet será de responsabilidade individual do usuário, que responderá por eventuais infrações ou danos causados.

#### 4.5.2

O acesso à internet é concedido ao público atendido e colaboradores através de uma identidade digital, composta por login e senha, que é pessoal e intransferível. Cada usuário é o único responsável pelas atividades realizadas com sua identidade digital. Isso inclui a obrigação de manter a confidencialidade de suas credenciais de acesso e a responsabilidade por qualquer ação ou dano decorrente do uso indevido ou não autorizado. É fundamental que cada usuário esteja ciente de sua responsabilidade em relação à segurança e ao uso ético da internet, contribuindo para um ambiente seguro e produtivo dentro da instituição.

#### 4.5.3

Adicionalmente, o Instituto Reciclar pode implementar políticas de uso aceitável e monitoramento para assegurar que o acesso à internet seja utilizado de maneira apropriada e em conformidade com as normas institucionais. Medidas de segurança, como filtros de conteúdo e controle de acesso, podem ser aplicadas para proteger os recursos tecnológicos e a integridade das informações.

#### 4.5.4

Qualquer violação das políticas de uso da internet pode resultar em sanções disciplinares, que variam desde advertências até a suspensão do acesso à internet e outros recursos institucionais. Em casos graves, as consequências podem incluir medidas legais, conforme as leis aplicáveis.

#### 4.5.5

O Instituto Reciclar se compromete a fornecer orientação e capacitação contínua sobre o uso seguro e responsável da internet, visando a conscientização de todo o público e colaboradores sobre a importância da segurança digital e do cumprimento das normas legais e institucionais.

### 4.6 Correio eletrônico

#### 4.6.1

A utilização do correio eletrônico corporativo ou educacional deve estar restrita à execução das atividades profissionais e educacionais, respeitando as normas de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

#### 4.6.2

O correio eletrônico corporativo ou educacional pode ser acessado em dispositivos móveis particulares. No entanto, é importante ressaltar que o acesso às mensagens e informações institucionais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador. Tal acesso pode ocorrer por ato de liberalidade e/ou conveniência, sem a necessidade de expressa e prévia requisição da instituição.

#### 4.6.3

A utilização de correio eletrônico particular ou público é permitida apenas para a transmissão ou recebimento de conteúdo ou informações particulares. É fundamental que o uso de e-mails particulares não prejudique as atividades profissionais ou acadêmicas, não gere efeitos negativos para outros usuários, não viole ou prejudique a rede corporativa e acadêmica, e não infrinja as normas vigentes do Instituto Reciclar.

#### **4.6.3.1**

O correio eletrônico particular deve ser usado exclusivamente para interesses particulares do usuário e não pode ser utilizado para o envio ou recebimento de informações do Instituto Reciclar. Este tipo de comunicação deve ser estritamente separado das atividades institucionais, garantindo a segurança e integridade dos dados e informações da organização.

### **4.7    Rede sem fio (Wi-Fi)**

#### **4.7.1**

O Instituto Reciclar, sempre que possível, oferece à comunidade acadêmica e administrativa uma rede sem fio (Wi-Fi) própria, disponível em ambientes autorizados e limitados ao perímetro físico da instituição. Essa rede é destinada exclusivamente para finalidades educacionais e administrativas.

#### **4.7.2**

Apenas os alunos e colaboradores expressamente autorizados têm permissão para acessar a rede sem fio (Wi-Fi) da instituição e devem comprometer-se a utilizar esse recurso de forma segura e responsável.

### **4.8 Recursos de TIC institucionais**

#### **4.8.1**

Os recursos de Tecnologia da Informação e Comunicação (TIC) do Instituto Reciclar são destinados exclusivamente a finalidades profissionais e educacionais, reservadas às atividades e permissões designadas para os usuários.

#### **4.8.2**

É proibido o armazenamento de arquivos pessoais nos recursos de TIC do Instituto Reciclar.

#### **4.8.3**

Para garantir a segurança das informações, os arquivos digitais contendo dados do Instituto Reciclar devem ser armazenados em servidores de arquivos específicos, com acesso restrito. Isso se deve à necessidade de proteger tais informações contra ameaças externas, como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas.

#### **4.8.3.1**

Os colaboradores devem armazenar os arquivos digitais nos servidores de arquivos

específicos e com acesso restrito disponibilizados na rede corporativa.

#### **4.8.3.2**

A Gestão de Tecnologia da Informação (GTI) e o Comitê de Revisão de Contas (CRC) são responsáveis por realizar cópias de segurança (backup) dos arquivos digitais armazenados nos servidores específicos do Instituto Reciclar.

#### **4.8.3.3**

O Instituto Reciclar não se responsabiliza pelos arquivos digitais armazenados em dispositivos individuais, como estações de trabalho, notebooks, tablets e smartphones. Em casos de desligamento ou rescisão contratual, os arquivos digitais serão removidos.

#### **4.8.4**

Todos os recursos de TIC do Instituto Reciclar, incluindo software, devem ser inventariados e identificados pela GTI.

#### **4.8.5**

A utilização de softwares e hardwares só é permitida se forem legítimos, previamente homologados ou autorizados pela GTI, independentemente de serem onerosos, gratuitos, livres ou licenciados.

#### **4.8.6**

O desenvolvimento, manutenção ou aquisição de aplicativos e sistemas no mercado são de responsabilidade da GTI e do CRC. Esses processos devem atender aos requisitos de segurança em todas as etapas para garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

#### **4.8.7**

Todas as modificações nos recursos de TIC do Instituto Reciclar, principalmente em sistemas e infraestrutura tecnológica, devem ser realizadas ou autorizadas pela GTI ou pelo CRC. Essas modificações devem ser controladas para identificar possíveis riscos e prevenir impactos na instituição, garantindo a disponibilidade dos recursos e a possibilidade de restauração do ambiente original em caso de incidentes.

#### **4.8.8**

A utilização dos recursos de TIC deve ser monitorada pela GTI e pelo CRC, que devem realizar projeções constantes para garantir que esses recursos atendam às necessidades tecnológicas futuras.

#### **4.8.9**

É proibido o uso dos recursos de TIC do Instituto Reciclar para acessar, baixar, utilizar, armazenar ou divulgar conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com as finalidades profissionais e educacionais da instituição, bem como com as diretrizes estabelecidas.

#### **4.8.10**

Todos os recursos de TIC de propriedade do Instituto Reciclar, incluindo dispositivos móveis, devem utilizar recursos de segurança, como senha de bloqueio automático, antivírus, antispyware, firewall e mecanismos de controle de softwares maliciosos.

#### **4.8.11**

A retirada de qualquer equipamento, banco de dados ou software das instalações do Instituto Reciclar, ou de sua infraestrutura tecnológica, deve ser realizada pela GTI e pelo CRC, mediante prévia e formal autorização do gestor imediato ou por necessidade da GTI ou do CRC.

#### **4.8.12 Dispositivos Móveis Institucionais**

##### **4.12.1**

O uso de dispositivos móveis de propriedade do Instituto Reciclar não é permitido para terceiros, prestadores de serviços e visitantes.

##### **4.8.12.2**

Os dispositivos móveis institucionais devem conter a menor quantidade possível de informações do Instituto Reciclar. Arquivos digitais com informações da instituição, principalmente sobre alunos, devem ser armazenados em servidores específicos para esse fim.

##### **4.8.12.3**

Em caso de roubo, perda ou furto do dispositivo móvel institucional contendo informações do Instituto Reciclar, o colaborador deve registrar o incidente e tomar as medidas necessárias para garantir a segurança das informações.

### **4.9 Recursos de TIC particulares**

#### **4.9.1**

A conexão dos recursos de Tecnologia da Informação e Comunicação (TIC) particulares na rede do Instituto Reciclar é estritamente proibida.

##### **4.9.1.1**

Os docentes têm autorização para utilizar recursos de TIC particulares conectados à rede acadêmica exclusivamente para suas funções educacionais, em conformidade com os princípios desta Política.

##### **4.9.1.2**

O Instituto Reciclar não assume qualquer responsabilidade sobre a utilização de softwares, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos docentes.

#### **4.9.2**

Os recursos de TIC particulares autorizados a acessar os conteúdos e serviços fornecidos pelo Instituto Reciclar devem ser protegidos com métodos de bloqueio de acesso e ferramentas de segurança, como antivírus e firewall, para mitigar os riscos de exposição da instituição a ameaças.

#### **4.9.3**

Todo recurso de TIC particular trazido para as dependências do Instituto Reciclar é de

inteira responsabilidade de seu proprietário, incluindo os dados e softwares nele armazenados ou instalados.

**4.9.4** O Instituto Reciclar não será responsabilizado por qualquer perda, furto ou dano aos recursos de TIC particulares.

#### **4.9.5 Dispositivos Móveis Particulares**

##### **4.9.5.1**

O uso de dispositivos móveis particulares é permitido dentro do perímetro físico do Instituto Reciclar, desde que não interfira nas atividades profissionais e educacionais e esteja em conformidade com as leis em vigor.

##### **4.9.5.2**

Dentro do perímetro físico e lógico onde informações confidenciais são armazenadas ou processadas, o Instituto Reciclar deve restringir a entrada e circulação de dispositivos móveis particulares.

##### **4.9.5.3**

É recomendável que o uso de dispositivos móveis particulares pelos alunos dentro da sala de aula seja para finalidades educacionais e didáticas. Caso contrário, o uso deve ocorrer com o prévio conhecimento do docente.

### **4.10 Armazenamento de informações**

#### **4.10.1**

É fundamental que todas as informações do Instituto Reciclar e das mantidas sejam armazenadas nos locais apropriados designados para esse fim.

#### **4.10.2**

Os colaboradores têm a responsabilidade de armazenar as informações digitais do Instituto Reciclar e das mantidas nos servidores da rede corporativa, os quais possuem controle de acesso e cópia de segurança. Já as informações físicas devem ser guardadas em gavetas, armários trancados ou em locais apropriados e seguros quando não estiverem em uso, especialmente quando envolverem documentação de identificação de alunos, provas ou trabalhos educacionais.

#### **4.10.3**

O Instituto Reciclar deve solicitar o apagamento e/ou remoção de conteúdos presentes em dispositivos móveis particulares, internet, mídias sociais e/ou aplicativos, sempre que esses conteúdos representarem riscos para os alunos, colaboradores e a instituição, estiverem em desacordo com a legislação nacional vigente, prejudicarem o bom relacionamento da comunidade acadêmica ou puderem causar danos à instituição

#### **4.10.4**

Todos devem manter as informações do Instituto Reciclar e mantidas armazenadas no

local apropriado e destinado a esse fim.

#### **4.10.5**

Os colaboradores devem armazenar as informações digitais do Instituto Reciclar e mantidas nos servidores da rede corporativa que possuem controle de acesso e cópia de segurança. As informações físicas devem ser guardadas em gavetas, armários trancados ou local apropriado e seguro quando não estiverem sendo utilizadas, principalmente quando envolver, mas não se limitando a, documentação de identificação de aluno, provas ou trabalhos educacionais.

#### **4.10.6**

O Instituto Reciclar e/ou mantidas devem solicitar o apagamento e/ou a remoção de conteúdos que estejam nos dispositivos móveis particulares, na internet, nas mídias sociais e/ou em aplicativos, sempre que os mesmos oferecerem riscos aos alunos, colaboradores e à instituição, que forem contrários à legislação nacional vigente, que afetem o bom relacionamento da comunidade acadêmica ou possam configurar algum tipo de dano à instituição.

### **4.11 Reppositórios digitais**

#### **4.11.1 Uso Institucional**

##### **4.11.1.1**

Os repositórios digitais destinados ao uso institucional são projetados para armazenar, criar, compartilhar e transmitir arquivos de informações do Instituto Reciclar ou de suas mantidas, desde que tenham sido previamente autorizados, homologados e disponibilizados pela GTI.

##### **4.11.1.2**

A utilização dos repositórios digitais para o uso institucional deve seguir os requisitos de segurança descritos nesta Política. É proibido o armazenamento de arquivos digitais pessoais nos repositórios digitais para uso institucional.

#### **4.11.2 Uso Educacional ou Acadêmico**

Os repositórios digitais destinados ao uso educacional ou acadêmico, para fins de aprendizado, avaliação ou testes, podem ser utilizados desde que tenham sido previamente autorizados e homologados pelo CRC.

#### **4.11.3 Restrições**

É estritamente proibido armazenar, criar, compartilhar ou transmitir arquivos contendo informações do Instituto Reciclar e mantidas para repositórios digitais particulares, especialmente informações sobre alunos e dados pessoais dos colaboradores.

### **4.12 Áudio, Vídeo e Fotos**

#### **4.11.1 Restrições Gerais**

Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens do Instituto Reciclar e suas mantidas, seja dentro da sala de aula, nos pátios, corredores, banheiros, vestiários ou qualquer outro local pertencente ao perímetro físico, assim como de alunos e colaboradores, sem prévia autorização.

#### **4.11.2. Exceções**

Exceto para situações já previamente comunicadas e autorizadas, como eventos educacionais, administrativos, sociais e/ou esportivos, de natureza pública e compartilhamento de informações, desde que o conteúdo não exponha ao ridículo ou cause constrangimento aos envolvidos.

#### **4.11.3 Alunos**

Os alunos devem obter autorização prévia expressa do docente para captar ou reproduzir qualquer imagem, vídeo ou som de dentro da sala de aula, inclusive para registrar a lousa ou o próprio docente, limitando o uso para fins pessoais e proibindo seu compartilhamento público, seja pela internet ou outros meios tecnológicos, além da divulgação/reprodução do conteúdo a terceiros não pertencentes à instituição.

#### **4.11.4. Exceções**

Salvo em situações já previamente comunicadas e autorizadas, como eventos educacionais, sociais e/ou esportivos, passeios, excursões e campeonatos.

#### **4.11.5 Colaboradores**

Os colaboradores do Instituto Reciclar e suas mantidas não devem captar, reproduzir ou compartilhar, por meio de qualquer tecnologia, incluindo a internet, imagens, vídeos ou sons que possam comprometer a segurança dos alunos, outros colaboradores e do ambiente educacional, acadêmico ou administrativo; violar o sigilo das informações; ou envolver diretamente a imagem de alunos, outros colaboradores, visitantes, prestadores de serviços e fornecedores, sem sua prévia e expressa autorização ou do gestor responsável, exceto quando autorizados por sua função ou em situações já previamente comunicadas e autorizadas, como eventos educacionais, sociais e/ou esportivos, passeios, excursões e campeonatos, de natureza pública e compartilhamento de informações.

### **4.13 Uso de imagem, som da voz e nome**

#### **4.12.1 Uso Institucional da Imagem dos Alunos**

O Instituto Reciclar e suas mantidas podem capturar, armazenar, manipular, editar e utilizar a imagem dos alunos para fins de identificação, autenticação, segurança, registro de atividades, acervo histórico, uso institucional, educativo e social. Isso inclui eventos promovidos pela instituição, bem como seu uso em perfis oficiais nas mídias sociais, websites, intranet, quadro de avisos, revistas, jornais universitários, vídeos educacionais, entre outros conteúdos. Essas imagens, devido à natureza técnica da internet, podem ter alcance global e prazo indeterminado, podendo até mesmo serem replicadas em sites e outros ambientes digitais externos.

#### **4.12.2 Respeito aos Direitos do Aluno**

No uso da imagem, som da voz e nome dos alunos, a instituição ressalva os direitos à integridade da honra, reputação, boa fama ou respeitabilidade dos alunos. Portanto, esses recursos são utilizados dentro dos limites acordados e sem expor o aluno ao ridículo ou situações constrangedoras, em conformidade com as leis brasileiras vigentes.

### **4.13. Aplicativos de Comunicação**

#### **4.13.1 Uso Responsável por Alunos e Docentes**

O uso de aplicativos de comunicação no ambiente educacional deve ser feito de maneira responsável pelos alunos e docentes, seja por recursos institucionais ou particulares, para evitar riscos desnecessários que possam comprometer atividades, projetos ou a própria instituição.

#### **4.13.2 Respeito às Normas e Sigilo por Colaboradores**

Os colaboradores do Instituto Reciclar e mantidas, ao utilizarem aplicativos de comunicação, devem respeitar o sigilo da informação, atender aos requisitos de segurança estabelecidos nesta política e respeitar as leis nacionais em vigor para evitar riscos relacionados ao vazamento de informações que possam comprometer a instituição.

### **4.14. Monitoramento**

#### **4.14.1 Registro e Armazenamento de Atividades**

O Instituto Reciclar e suas mantidas registram e armazenam atividades (logs) e monitoram seus ambientes físicos e lógicos, incluindo captura de imagens, áudio ou vídeo, visando proteger seu patrimônio e reputação, bem como a segurança daqueles relacionados à instituição.

#### **4.14.2 Utilização dos Dados Monitorados**

Os dados monitorados são utilizados para fins administrativos e legais, colaborando com as autoridades em caso de investigação.

#### **4.14.3 Cooperação em Casos de Incidentes**

Em casos de incidentes de segurança ou eventos que comprometam a integridade física e lógica dos alunos e colaboradores, o Instituto Reciclar e suas mantidas têm o dever de fornecer informações ao órgão competente para apuração, além de disponibilizar provas que estejam em seu poder ou de cuja existência tenham conhecimento.

### **4.15 Combate à Intimidação Sistemática (Bullying)**

#### **4.15.1 Conscientização e Cooperação**

Todos os alunos e colaboradores devem participar de campanhas de conscientização contra o bullying promovidas pela instituição, cooperando em situações críticas para

aplicação de medidas preventivas e reativas. Além disso devem contribuir para a identificação de casos de bullying fornecendo depoimentos e provas quando necessário.

#### **4.16 Segurança da informação**

4.16.1 Ao repassar ou transmitir informações da ONG Reciclar e/ou suas mantidas ou sob sua responsabilidade seja de forma presencial via telefone comunicadores instantâneos mensagens eletrônicas ou mídias sociais os alunos e colaboradores devem agir com cautela confirmando antes a identidade do solicitante e a real necessidade do compartilhamento da informação solicitada.

4.16.2 Os alunos e colaboradores devem ter cautela ao acessar softwares, informações e conteúdos disponibilizados gratuitamente na internet, a exemplo de aplicativos, músicas, vídeos, trabalhos completos, livros físicos digitalizados e e-mails com propostas suspeitas, pois podem ser vetores de ataques criminosos.

4.16.3 As informações confidenciais, assim como os recursos de TIC que as contenham, quando descartados, devem passar por procedimento de destruição que impossibilite sua recuperação e o acesso às informações armazenadas por pessoas não autorizadas.

4.16.4 A ONG Reciclar está comprometida com o dever de orientar constantemente seus alunos e colaboradores no uso seguro das informações e da tecnologia. Por isso, podem realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança no instituto.

### **5 PAPÉIS E RESPONSABILIDADES**

#### **5.1 Todos**

##### **5.1.1 Conhecimento e Disseminação da Política de Privacidade**

Todos os membros e colaboradores do Instituto Reciclar devem estar cientes e promover a compreensão das regras e princípios estabelecidos na Política de Privacidade da organização.

##### **5.1.2 Preservação e Proteção dos Ativos Tangíveis e Intangíveis**

É responsabilidade de todos preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia do Instituto Reciclar, incluindo todas as informações e conteúdos, contra qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.

##### **5.1.3 Zelo pela Proteção do Patrimônio e da Reputação**

Os membros e colaboradores devem zelar pela proteção do patrimônio e da reputação do Instituto Reciclar, utilizando com responsabilidade os recursos físicos e lógicos fornecidos pela organização.

**5.1.4 Evitar Exposição Desnecessária de Informações**

É fundamental evitar a exposição desnecessária das informações, projetos, trabalhos e dependências do Instituto Reciclar, inclusive nas mídias sociais e na internet, e agir com responsabilidade no uso dos recursos de Tecnologia da Informação e Comunicação (TIC) e das informações.

**5.1.5 Preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia do Instituto Reciclar e mantidas, inclusive todas as suas informações e conteúdos, independentemente do formato ou suporte utilizado, contra todo e qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.**

**5.1.6 Preservar e proteger os recursos institucionais, a marca, a reputação, o conhecimento, a propriedade intelectual do Instituto Reciclar e mantidas, principalmente todas as suas informações e conteúdos.**

**5.1.7 Zelar pela proteção do patrimônio do Instituto Reciclar e mantidas, usando com responsabilidade os recursos físicos e lógicos fornecidos;**

**5.1.8 Evitar a exposição desnecessária das informações, projetos, trabalhos e dependências do Instituto Reciclar e mantidas, inclusive nas mídias sociais e na internet, além de agir com responsabilidade no uso dos recursos de TIC e das informações.**

**5.1.9 Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.**

**5.1.10 Reportar os incidentes que possam impactar na segurança das informações do Instituto Reciclar e mantidas, imediatamente, por meio do endereço [contatos@reciclar.org.br](mailto:contatos@reciclar.org.br)**

**5.1.11 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela ONG Reciclar e mantidas.**

## **5.2 Gestores e coordenadores**

**5.2.1** Orientar constantemente suas equipes quanto ao uso seguro dos ativos tangíveis e intangíveis, e dos valores adotados pela ONG Reciclar e mantidas, instruindo-as, inclusive, a disseminar a cultura para os demais colaboradores.

**5.2.2** Suportar todas as consequências das funções e atividades que delegar a outros colaboradores.

**5.2.3** Assegurar o cumprimento desta Política e das demais regulações por parte dos colaboradores supervisionados.

**5.2.4** Participar da investigação de incidentes de segurança relacionados às informações, ativos e aos colaboradores sob sua responsabilidade.

**5.2.5** Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

## **5.3 Colaboradores**

**5.3.1** Ser cauteloso em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contatos e intimidades, além do dever de sempre preservar o sigilo profissional nas mídias sociais, a imagem e reputação da instituição.

**5.3.2** Durante a comunicação, presencial ou digital, com demais colaboradores, alunos, visitantes, fornecedores, prestadores de serviços e outros profissionais, utilizar linguagem respeitosa e adequada, condizente com o ambiente estudantil, acadêmico e administrativo, sem o uso de termos dúbios, com dupla interpretação, que exponham a intimidade ou que denotem excesso de intimidade, abuso de poder, perseguição, discriminação, algum tipo de assédio moral ou sexual.

**5.3.3** Utilizar as mídias sociais evitando excessos de exposição e riscos para a sua própria imagem e reputação, bem como para a instituição.

## **6 DISPOSIÇÕES FINAIS**

O presente documento deve ser interpretado de acordo com as leis brasileiras, em língua portuguesa, em conjunto com outras normas e procedimentos aplicáveis pela ONG Instituto Reciclar.

Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da

informação do Instituto Reciclar serão consideradas violações por si só e estarão sujeitas às sanções previstas no Regimento Interno, contratos de prestação de serviços, contratos de trabalho e em outras normas da organização.

A Política de Privacidade, bem como outras normas de segurança da informação do Instituto Reciclar, encontram-se disponíveis no site oficial da organização ou podem ser solicitadas através do endereço de e-mail [contatos@reciclar.org.br](mailto:contatos@reciclar.org.br)

Em caso de dúvidas sobre esta Política ou outros procedimentos de segurança da informação do Instituto Reciclar, os membros e colaboradores podem solicitar esclarecimentos pelo e-mail: [contatos@reciclar.org.br](mailto:contatos@reciclar.org.br).

Os casos de incidentes, infrações ou suspeitas dessas ocorrências devem ser comunicados imediatamente, pessoalmente ou através do endereço de e-mail [contatos@reciclar.org.br](mailto:contatos@reciclar.org.br).

## 6 DOCUMENTOS DE REFERÊNCIA

O presente documento será complementado pelos Procedimentos, Códigos e Normas de Segurança da Informação da ONG Reciclar e está em consonância com os seguintes documentos:

- Política de Segurança da Informação da Sociedade Mineira de Cultura, versão 1.1;
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;

- COBIT 5® Foundation

**Anexo II - Cartilha da Política de Segurança da Informação**





**Cartilha**  
da Política de Segurança da  
Informação - ONG Reciclar

### Três Pilares da segurança da informação



#### Integridade

Está associada a veracidade e confiabilidade da informação, garantindo à preservação dos dados. Ela deve garantir que as informações estejam livres de qualquer alteração sem autorização, se mantendo conforme foram criadas.



#### Confidencialidade

Está relacionada a privacidade dos dados. Seu objetivo é restringir o acesso às informações, garantindo que ela chegue apenas às pessoas autorizadas.



#### Disponibilidade

Tem o foco de garantir que dados e sistemas ficarão acessíveis sempre que necessário, sem interrupções, podendo ser acessados por qualquer pessoa ou processo autorizado quando for preciso, bem como ter meios de solicitar a portabilidade dos dados para outro fornecedor de produto ou serviço.

### O que é um Incidente de Segurança da Informação e como Reporta-lo?

Um incidente de segurança refere-se a qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade de dados e informações em um sistema de informação. Esses incidentes podem ocorrer de diversas formas e têm o potencial de causar danos significativos às organizações, indivíduos ou sistemas.

#### Caso Perceba!



- Comportamentos estranhos em seu computador ou em qualquer recurso tecnológico;
- Comportamento suspeito de terceiros ou Funcionários;
- Políticas e normas de segurança não sendo seguidas

Notifique o fato imediatamente há coordenação de Tecnologia da Informação ou entre em contato pelo e-mail: [reciclar@ongreciclar.org.br](mailto:reciclar@ongreciclar.org.br)



[www.ongreciclar.com.br](http://www.ongreciclar.com.br)



**Cartilha**  
da Política de Segurança da  
Informação - ONG Reciclar

#### Controle de Acesso



Para cada aluno e professor será fornecida uma identidade digital de uso individual e intransferível. Todos são responsáveis pelo uso e sigilo de sua identidade digital. Não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

#### Preservação e Proteção dos Ativos Tangíveis e Intangíveis

É responsabilidade de todos preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia do Instituto Reciclar, incluindo todas as informações e conteúdos, contra qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.



#### Internet



No entanto, é imprescindível que os alunos e colaboradores utilizem a internet em estrita observância das leis em vigor. Qualquer uso inadequado ou ilícito da internet será de responsabilidade individual do usuário, que responderá por eventuais infrações ou danos causados.

#### Rede sem fio (Wi-Fi)

Essa rede é destinada exclusivamente para fins educacionais e administrativos, sendo acessível apenas para alunos e colaboradores autorizados, que devem utilizá-la de forma segura e responsável.





**Cartilha**  
da Política de Segurança da  
Informação - ONG Reciclar

## Práticas de Segurança da Informação



### Usar senhas fortes

Na hora de criá-las, é importante inserir letras, números e símbolos, assim ficará mais difícil de alguém descobrir. Mas, não é só isso! Você também não pode esquecer de criar senhas diferentes para cada acesso.



### Fazer cópias de segurança

As cópias de segurança são indispensáveis para evitar que todo o trabalho dos colaboradores seja perdido, seja por falta de energia na hora da elaboração de um documento, ação de algum vírus, entre outras causas.



### Atualizar softwares

Você nunca deve negligenciar a atualização que o aplicativo costuma solicitar. Assim, conseguirá reduzir o risco da plataforma ser atingida por algum vírus, por exemplo, e terceiros acessar dados confidenciais da instituição de ensino e dos alunos.

## Minhas Responsabilidades Como Usuário



Informar imediatamente ao canal de comunicação disponível qualquer incidente ou violação de segurança



Entender, respeitar e fazer cumprir a política de segurança;



Utilizar as informações apenas para os propósitos do negócio;



Comunicar sobre qualquer indício ou falha relacionada à Segurança da Informação.



**Cartilha**  
da Política de Segurança da  
Informação - ONG Reciclar

## Bullying

Define como ato de “intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais”.



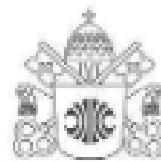
## Bullying é Crime

Punição do crime de bullying:  
O bullying pode ensejar pena de multa (erradicamente cominada pelo legislador) e o cyberbullying, pena de reclusão de dois a quatro anos, e multa, se a conduta não constituir crime mais grave

## Formas de Prevenção ao Bullying

1. Seja gentil ao se comunicar com a criança mesmo que ela tenha feito algo errado
2. Conversar com os alunos e escutar atentamente reclamações ou sugestões
3. Estimular os estudantes a informar os casos
4. Reconhecer e valorizar as atitudes da garotada no combate ao problema
5. Criar com os estudantes regras de disciplina para a classe em coerência com o regimento da instituição
6. Estimular lideranças positivas entre os alunos, prevenindo futuros casos
7. Interferir diretamente nos grupos, o quanto antes, para quebrar a dinâmica do bullying





**PUC Minas**

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

