PROJETO DE INFRA

EIXO 5: Projeto: Infraestrutura de Rede
CURSO: Sistemas de Informação EAD
Prof. Alexandre Teixeira

ALUNOS

Andre Alves Leocadio (andrealvesleocadio17@gmail.com),
Izabele Ribeiro Lima de Oliveira (izahhoran8@gmail.com),
Lucas Brito de Paula (lucasbrito775823@gmail.com),
Renato Donizeti da Silva Junior (rrenatosilva.rs@gmail.com),
Ricky Ramos de Oliveira (contactricky@zoho.com),
Sânzio de Oliveira Carmo (sanzio.carmo@gmail.com).

TÍTULO DO PROJETO: ONG

1- RESUMO

Este projeto do curso de Sistemas de Informação EAD, sob a orientação do Prof. Alexandre Teixeira, tem como objetivo a criação e implementação de uma infraestrutura de rede para uma Organização Não Governamental (ONG).

2- SITUAÇÃO PROBLEMA

A ONG, cuja sede está localizada em São Paulo (SP), enfrenta desafios no que diz respeito à sua infraestrutura de rede, devido à expansão que inclui três filiais nas cidades de Belo Horizonte, Contagem e Betim. As necessidades abrangem a implementação de serviços web, e-mail, bankline, suporte técnico, videoconferência, impressão e a configuração de um servidor de arquivos. Isso visa assegurar uma comunicação eficiente e a partilha de recursos entre todas as unidades da organização.

		Matriz (SP)		Belo Horizonte		Contagem		Betim		Link Internet		Link Internet	
		20		15		10		13					
APPs	LB (kbps)	Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB				
Web	100	20	2000	15	1500	10	1000	13	1300	3800		2000	
e-mail	50	20	1000	15	750	10	500	13	650	1900		1000	
Bankline	100	5	500	2	200	0	0	0	0	200		500	
Suporte	80	5	400	8	640	2	160	2	160				
Videoconferência	500	10	5000	8	4000	5	2500	5	2500				
Impressão	30	10	300	8	240	5	150	5	150				
Servidor de Arquivos	50	20	1000	15	750	10	500	13	650				
		Total BH - SP	12400	Total RC BH	5630	Total RC C	3310	Total RC B	3460				
						Total	4810	Total	5410				
										5900	Internet BH	3500	Internet SP

A necessidade dos links é:

Link de Internet de São Paulo 3500 kbps
Link de Internet de Belo Horizonte 5900 kbps
Link de Belo Horizonte para Contagem 4810 kbps
Link de Belo Horizonte para Contagem 5410 kbps

3- JUSTIFICATIVA

A necessidade de estabelecer uma infraestrutura de rede eficiente apresenta como um desafio significativo para ONGs, considerando ainda a situação problema proposta em que a matriz se situa em São Paulo (SP) e há três filiais localizadas em Belo Horizonte, Contagem e Betim.

Assim, faz-se necessário o desenvolvimento de um projeto que atenda às necessidades de segurança e comunicação entre as filiais, bem como a importância de assegurar que o custo total da realização do projeto seja acessível, ou pelo menos, o menor possível.

4 - OBJETIVO GERAL

Projetar e implementar um projeto de rede para a situação problema proposta, dentro de um orçamento pequeno.

5 - ANÁLISE DOS CUSTOS

		Matriz (SP)		Filial 1 (BH)		Filial 2 (Contagem)		Filial3 (Betim)		
		20		15		10		13		
Item	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	TOTAL GERAL
Nutanix HPC	R$ 6.098,00	1	R$ 6.068,00	1	R$ 6.068,00	1	R$ 6.068,00	1	R$ 6.068,00	R$ 24.272,00
Estação Dell	R$ 2.649,00	20	R$ 52.980,00	15	R$ 39.735,00	10	R$ 26.490,00	13	R$ 34.437,00	R$ 153.642,00
Roteador CISCO	R$ 4.300,00	1	R$ 4.300,00	1	R$ 4.300,00	1	R$ 4.300,00	1	R$ 4.300,00	R$ 17.200,00
Serial CISCO	R$ 1.000,00	2	R$ 2.000,00	4	R$ 4.000,00	1	R$ 1.000,00	1	R$ 1.000,00	R$ 8.000,00
Switch Dell 24p	R$ 10.709,15	2	R$ 21.418,30	2	R$ 21.418,30	1	R$ 10.709,15	1	R$ 10.709,15	R$ 64.254,90
Cabo UTP CAT6 cx	R$ 4.500,00	2	R$ 9.000,00	2	R$ 9.000,00	1	R$ 4.500,00	1	R$ 4.500,00	R$ 27.000,00
RJ45 f Cat6	R$ 60,00	24	R$ 1.440,00	17	R$ 1.020,00	13	R$ 780,00	15	R$ 900,00	R$ 4.140,00
Patch Cord CAT 6	R$ 60,00	48	R$ 2.880,00	34	R$ 2.040,00	26	R$ 1.560,00	30	R$ 1.800,00	R$ 8.280,00
Patch Panel CAT 6	R$ 1.500,00	2	R$ 3.000,00	2	R$ 3.000,00	1	R$ 1.500,00	1	R$ 1.500,00	R$ 9.000,00
Rack 44 U	R$ 2.398,68	1	R$ 2.398,68	1	R$ 2.398,68	1	R$ 2.398,68	1	R$ 2.398,68	R$ 9.594,72
Cx + placa	R$ 40,00	24	R$ 960,00	17	R$ 680,00	13	R$ 520,00	15	R$ 600,00	R$ 2.760,00
AP Rukus WiFi 6	R$ 1.597,35	1	R$ 1.597,35	1	R$ 1.597,35	1	R$ 1.597,35	1	R$ 1.597,35	R$ 6.389,40
Organizador de Cabo	R$ 54,98	2	R$ 109,96	2	R$ 109,96	1	R$ 54,98	1	R$ 54,98	R$ 329,88
Impressora	R$ 2.159,00	1	R$ 2.159,00	1	R$ 2.159,00	1	R$ 2.159,00	1	R$ 2.159,00	R$ 8.636,00
Nobreak	R$ 4.969,90	1	R$ 4.969,90	1	R$ 4.969,90	1	R$ 4.969,90	1	R$ 4.969,90	R$ 19.879,60
Mesa + Cadeira	R$ 649,90	20	R$ 12.998,00	15	R$ 9.748,50	10	R$ 6.499,00	13	R$ 8.448,70	R$ 37.694,20
		Total	R$ 128.279,19	Total	R$ 112.244,69	Total	R$ 75.106,06	Total	R$ 85.442,76	R$ 401.072,70

O custo estimado do projeto é de R$ 401.072,70. Ficando a maior parte de custo em infraestrutura distribuído da seguinte forma:

Descrição	Composição do valor final do Orçamento em %
Estação Dell	38,31%
Switch Dell 24p	16,02%
Mesa + Cadeira	9,40%
Cabo UTP CAT6 cx	6,73%
Nutanix HPC	6,05%
Nobreak	4,96%
Outros	18,53%

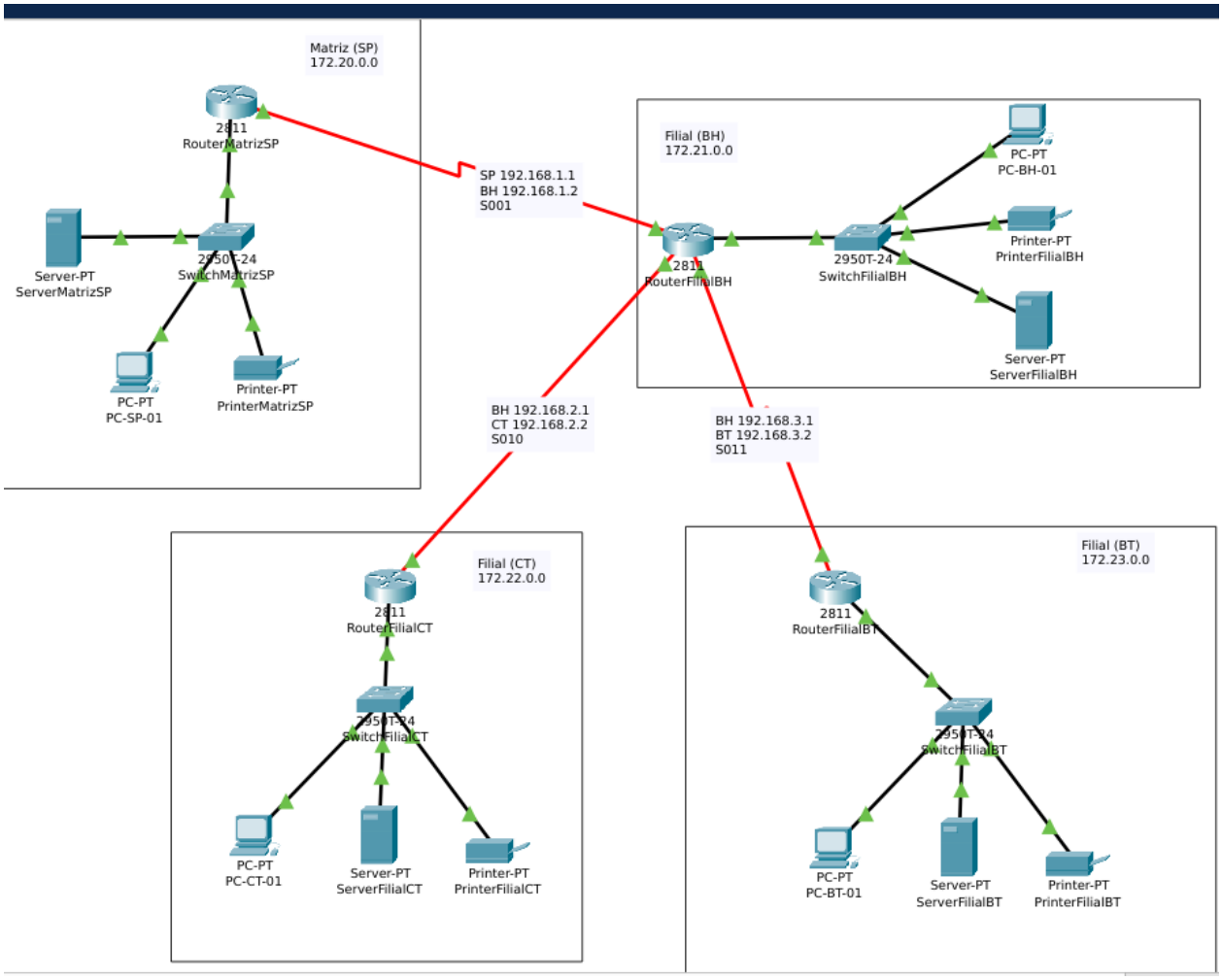
E a distribuição do custo por localidade:

Local	Matriz (SP)	Filial BH	Filial Contagem	Filial Betim
Valor	R$ 128.279,19	R$ 112.244,69	R$ 75.106,06	R$ 85.442,76
Composição em %	31,98%	27,99%	18,73%	21,30%

As referências de custos estão no final deste documento para consulta.

6 – RESULTADOS

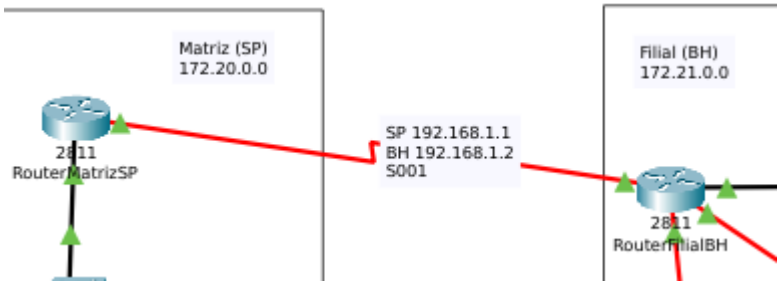
Com as necessidades mapeadas a seguinte rede foi projetada.



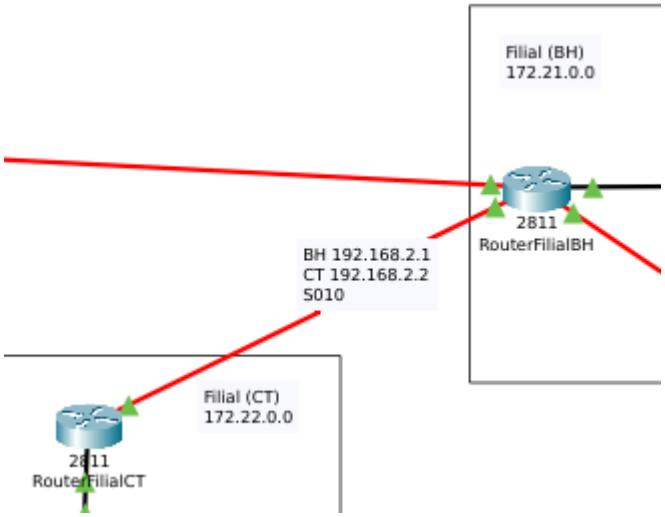
Endereçamentos de IP

As redes entre os roteadores usam a faixa 192.168.x.x/24, sendo:

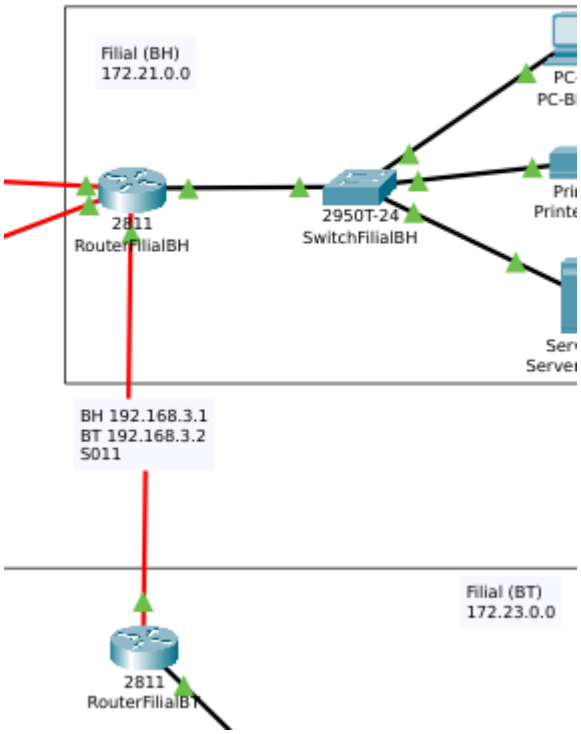
- 192.168.1.1 - 192.168.1.2 a ligação entre São Paulo e Belo Horizonte, utilizando as portas seriais 001.



- 192.168.2.1 - 192.168.2.2 a ligação entre Belo Horizonte e Contagem, utilizando as portas seriais 010.



- 192.168.3.1 - 192.168.3.2 a ligação entre Belo Horizonte e Betim, utilizando as portas seriais 011.



Já as filiais utilizam a faixa de IP 172.X.X.X/16, sendo:

- Matriz de São Paulo 172.20.X.X
- Filial de Belo Horizonte 172.21.X.X
- Filial de Contagem 172.22.X.X
- Filial de Betim 172.23.X.X

Padrões de endereço para rede interna

- 172.X.0.1 -> Roteador

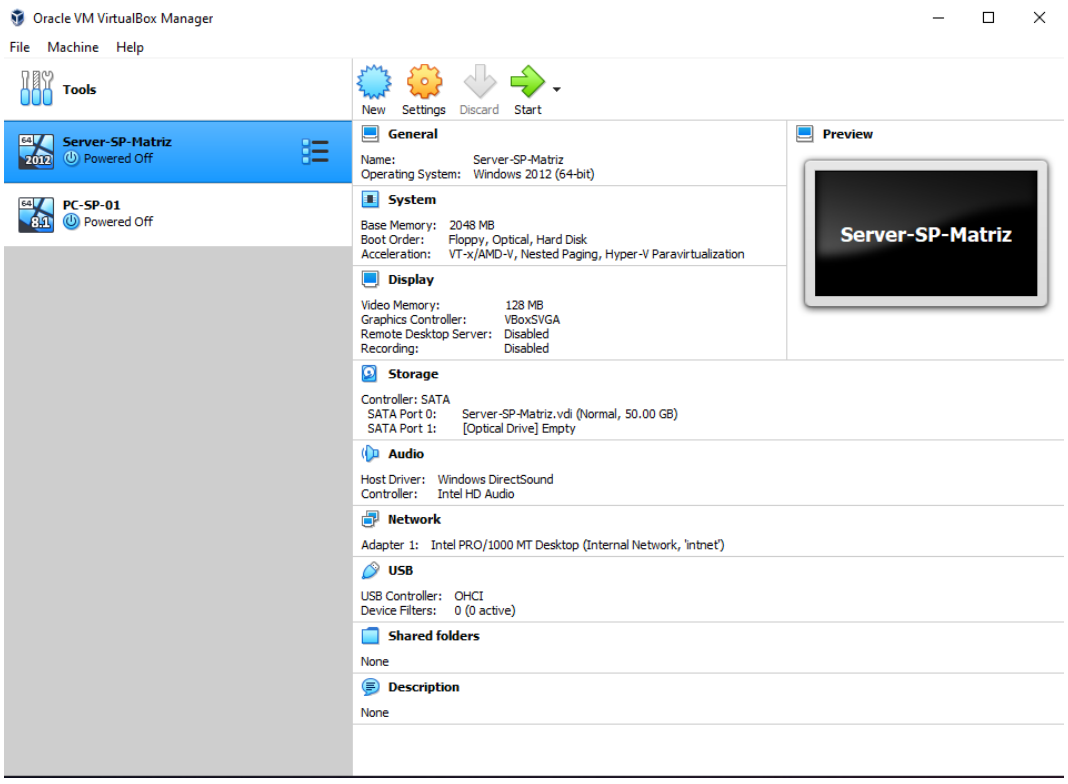
- 172.X.0.2 -> Servidor
- 172.X.0.3 -> Impressora
- 172.X.0.4 - 10 -> Reservado

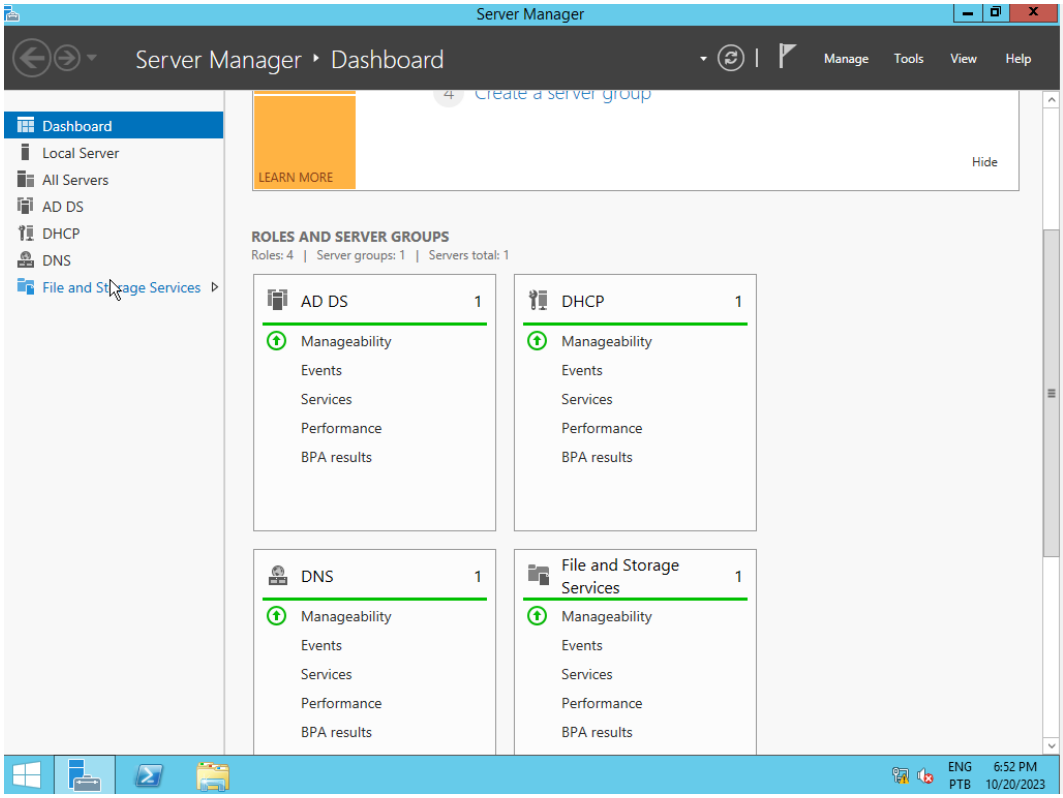
Nomenclaturas

- Para roteadores é utilizado o padrão **Router[Matriz|Filial][Sigla da filial]**
- Para servidores é utilizado o padrão **Server[Matriz|Filial][Sigla da filial]**
- Para impressoras é utilizado o padrão **Printer[Matriz|Filial][Sigla da filial]**
- Para computadores é utilizado o padrão **PC-[Sigla da filial]-[Número sequêncial]**

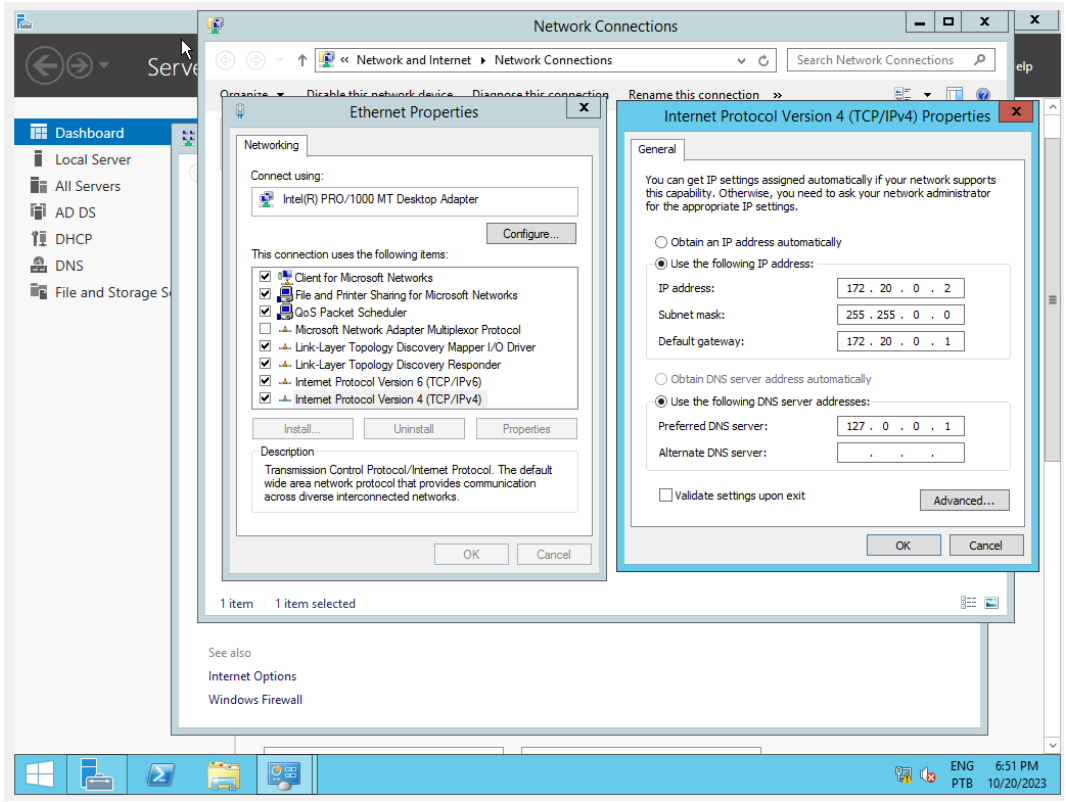
VM LOCAL E VM CLOUD

VM LOCAL



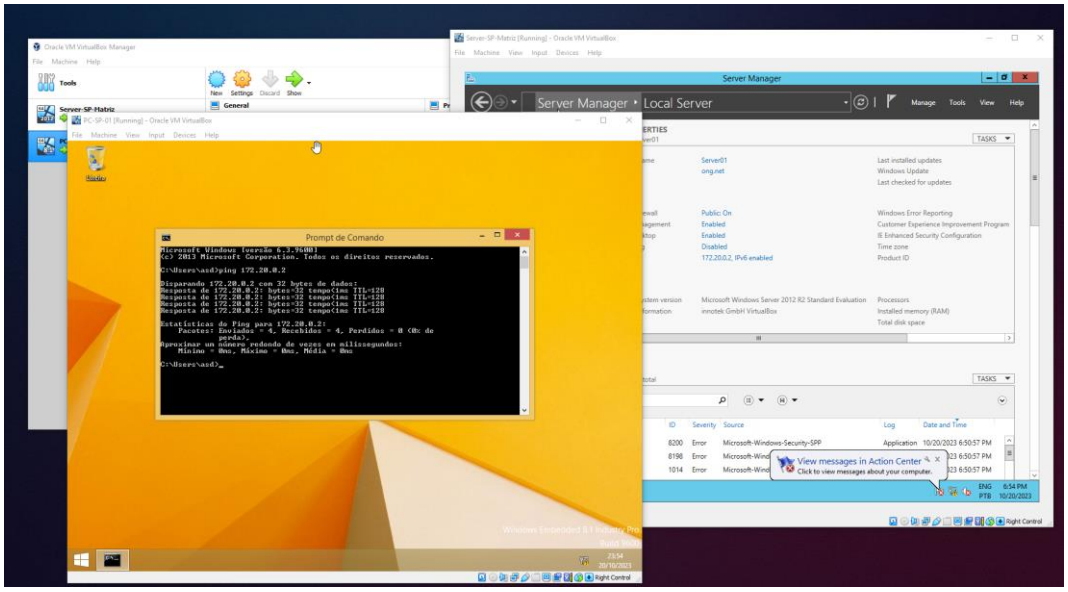


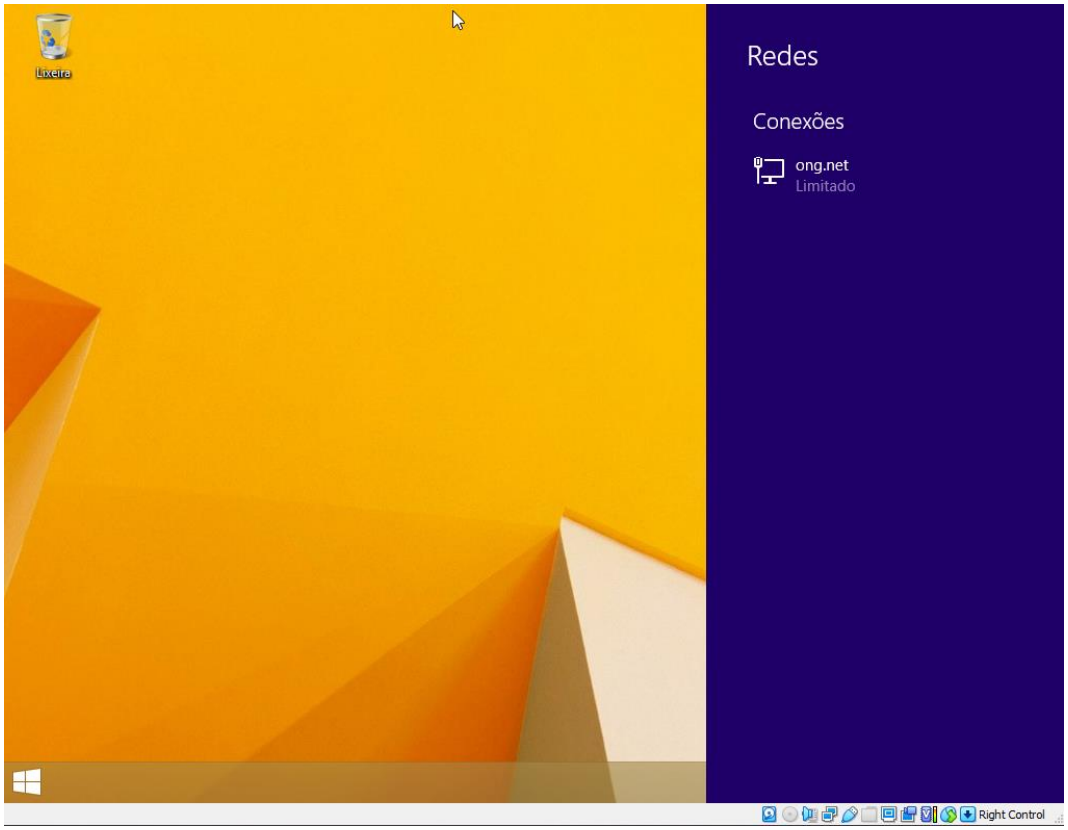
- Acima podemos ver as especificações da imagem da máquina virtual criada para servir de servidor da matriz de São Paulo da ONG e o dashboard inicial do servidor rodando Windows server 2012 bem como uma prévia dos principais serviços utilizados.



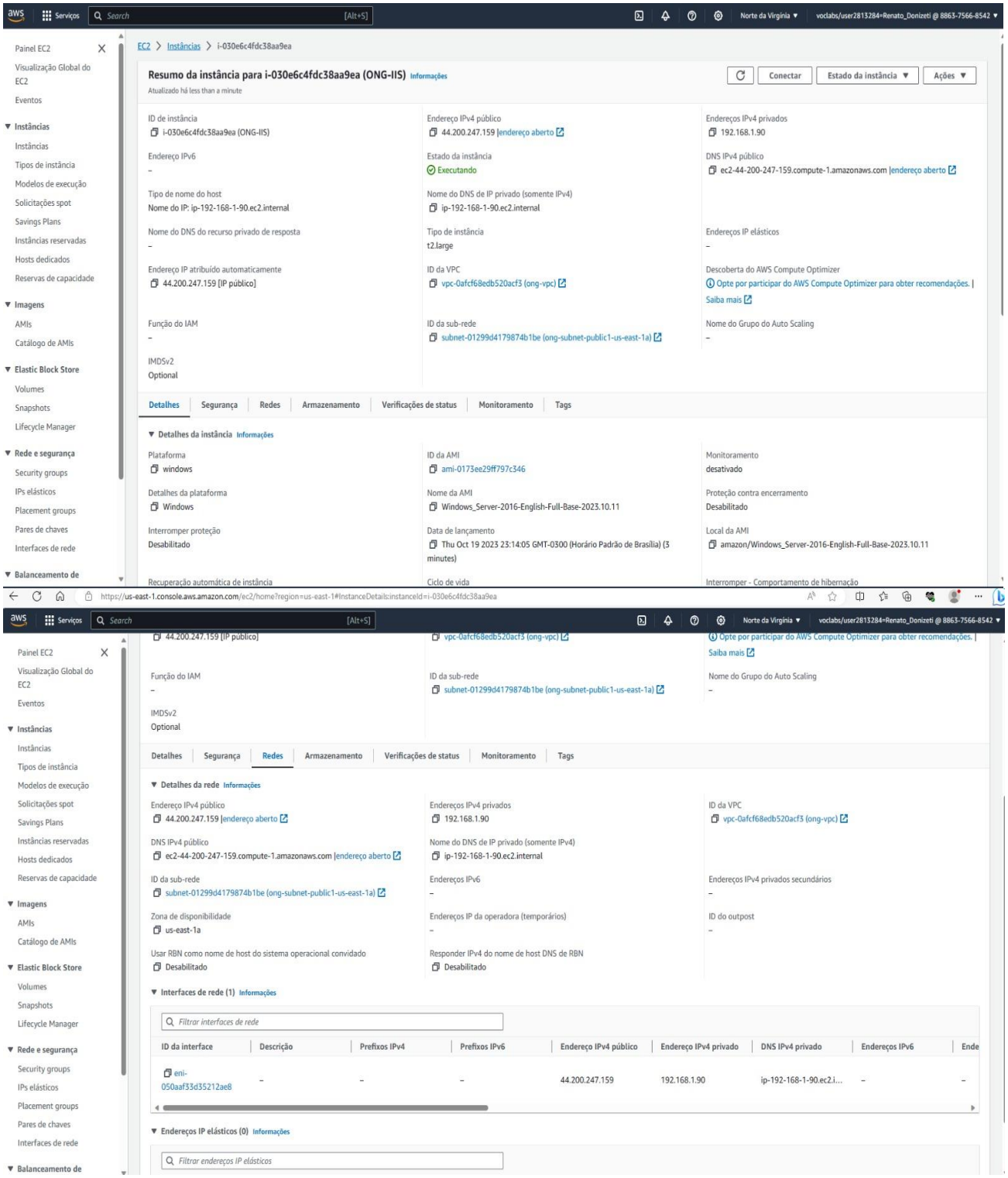
- O servidor matriz segue as configurações de IP estático descritas acima para e de acordo com o definido no planejamento do projeto.

- Foi criado uma máquina virtual para simular uma estação de trabalho inserida no domínio do servidor matriz. Como podemos ver a seguir a máquina consegue conectar ao domínio “ong.net” e para tirar a prova de maneira prática realizamos um ping entre as duas máquinas.

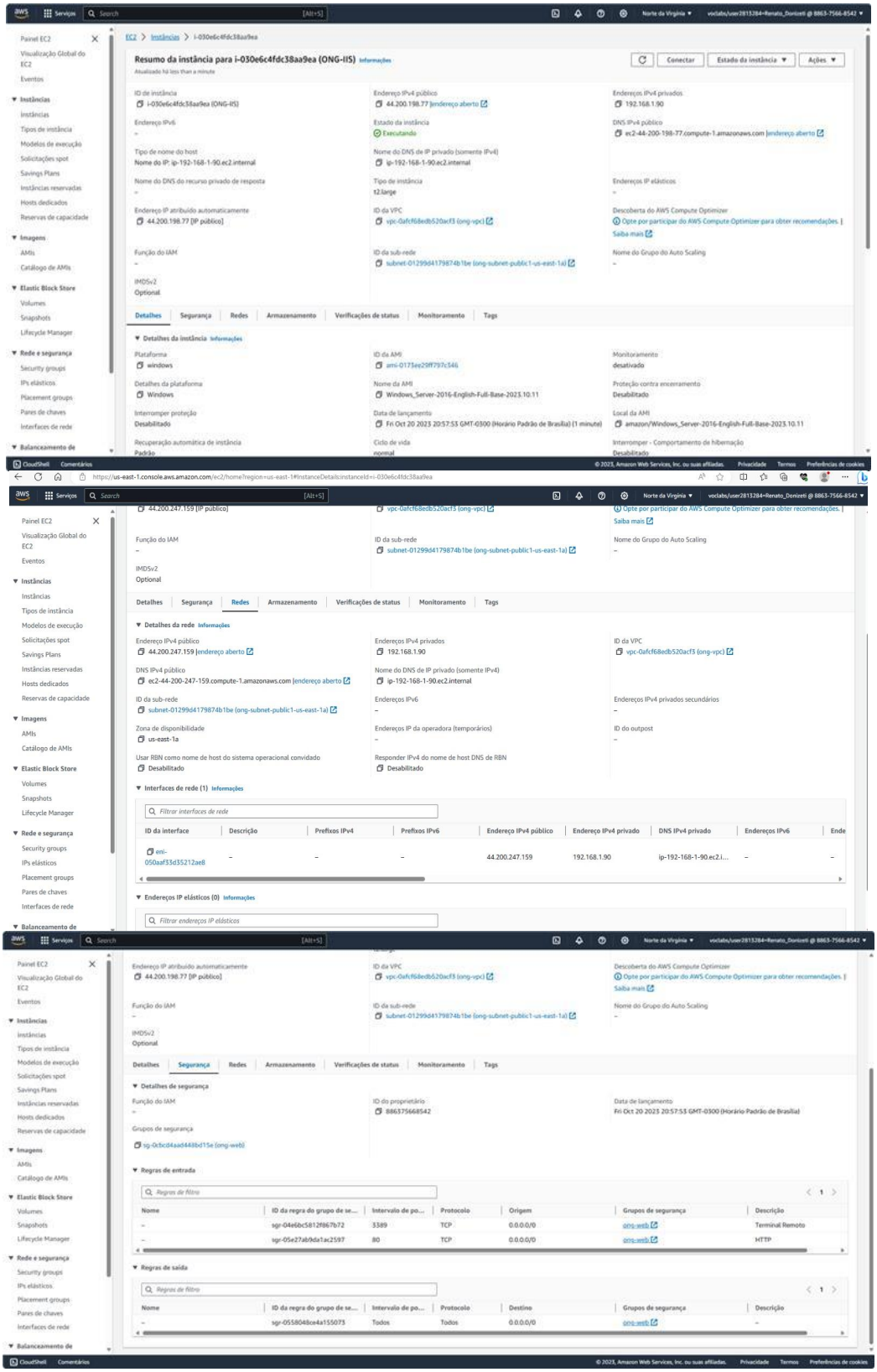




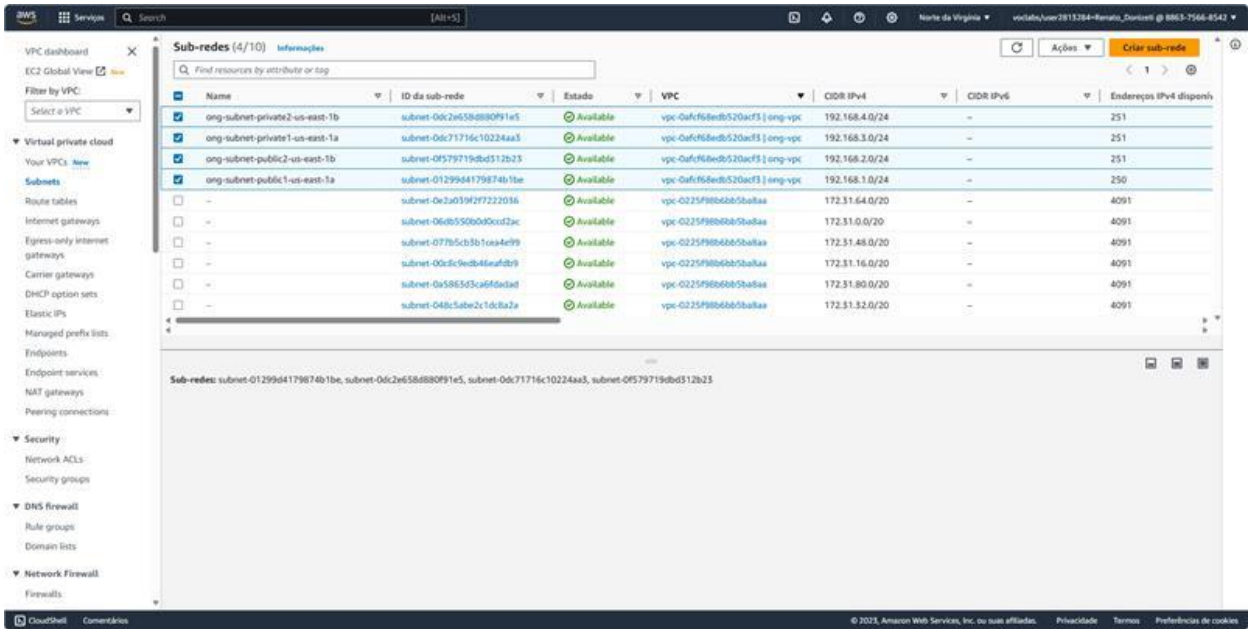
VM CLOUD



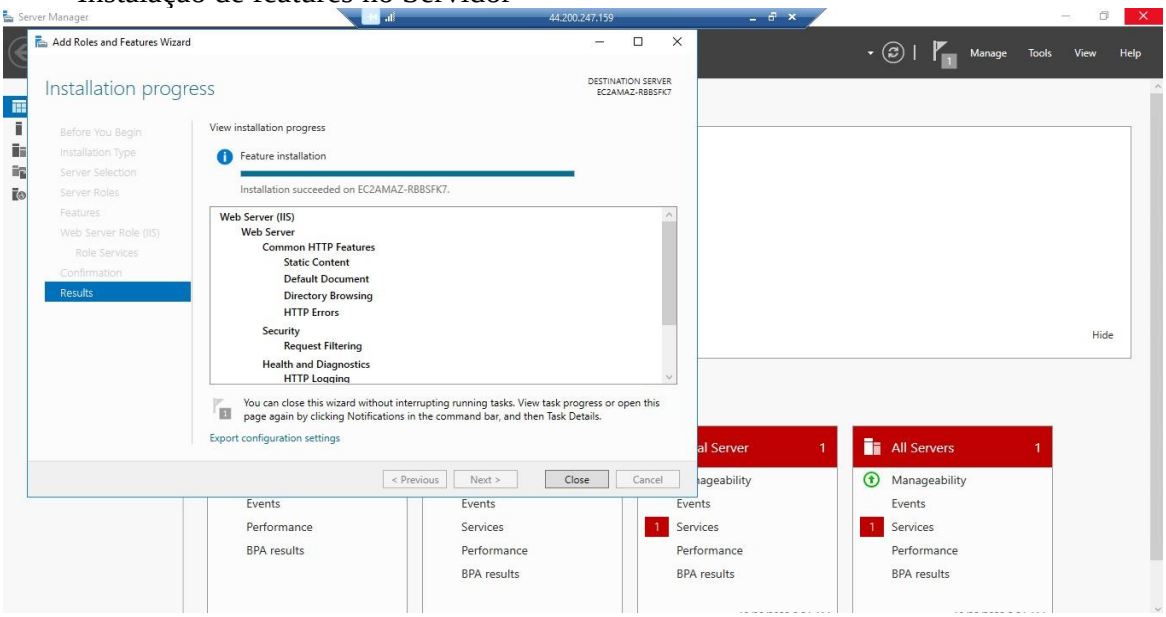
- Acima podemos ver especificações do mesmo estilo de ambiente de servidor matriz criado localmente, porém desta vez criado na nuvem disponibilizada pela AWS.
- As prints a seguir temos detalhes das instâncias e das configurações de rede utilizadas.



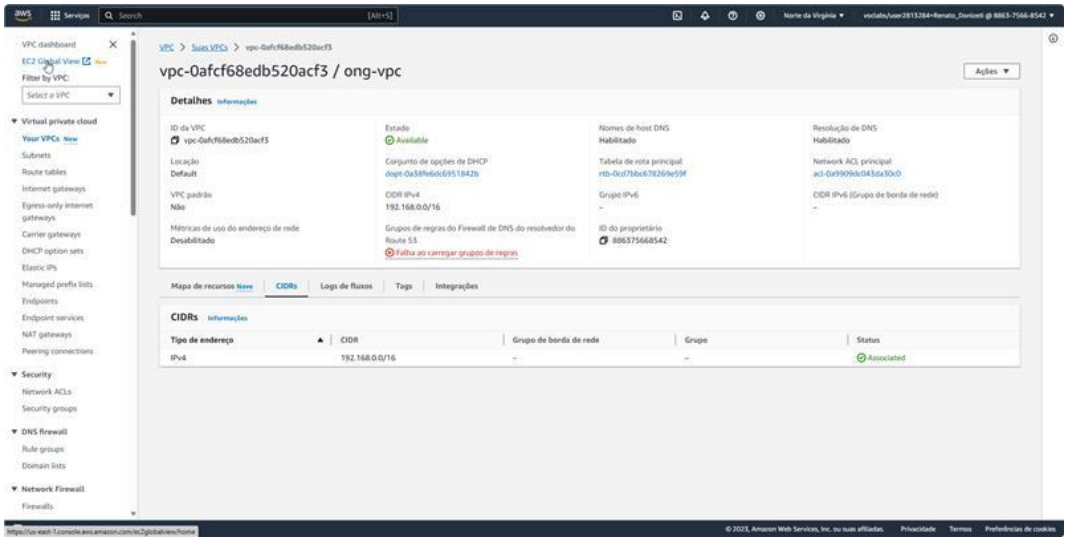
- Abaixo temos um apanhado das sub redes utilizadas na cloud.

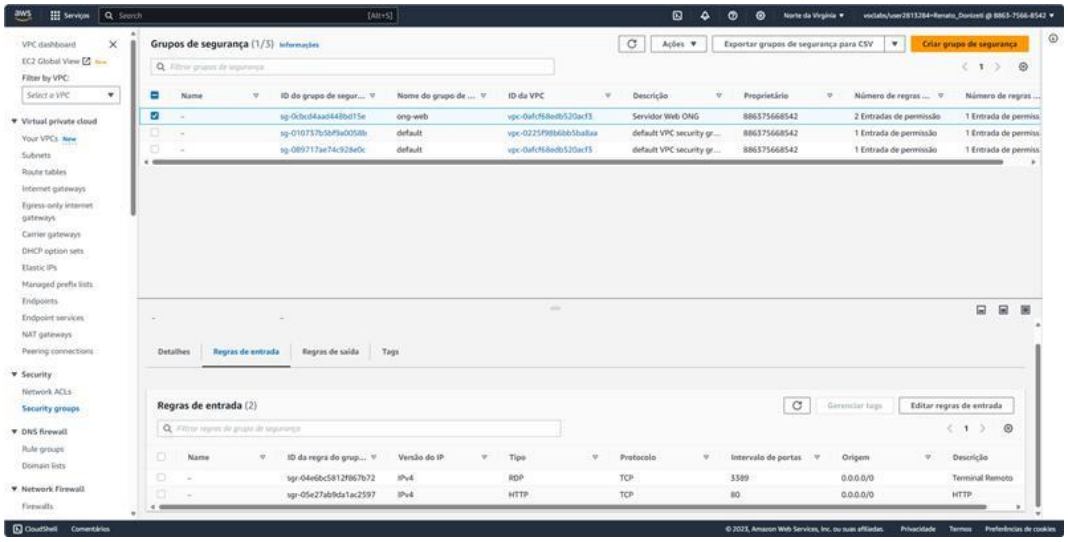


- Instalação de features no Servidor



- Dados de VPC das instâncias criadas.



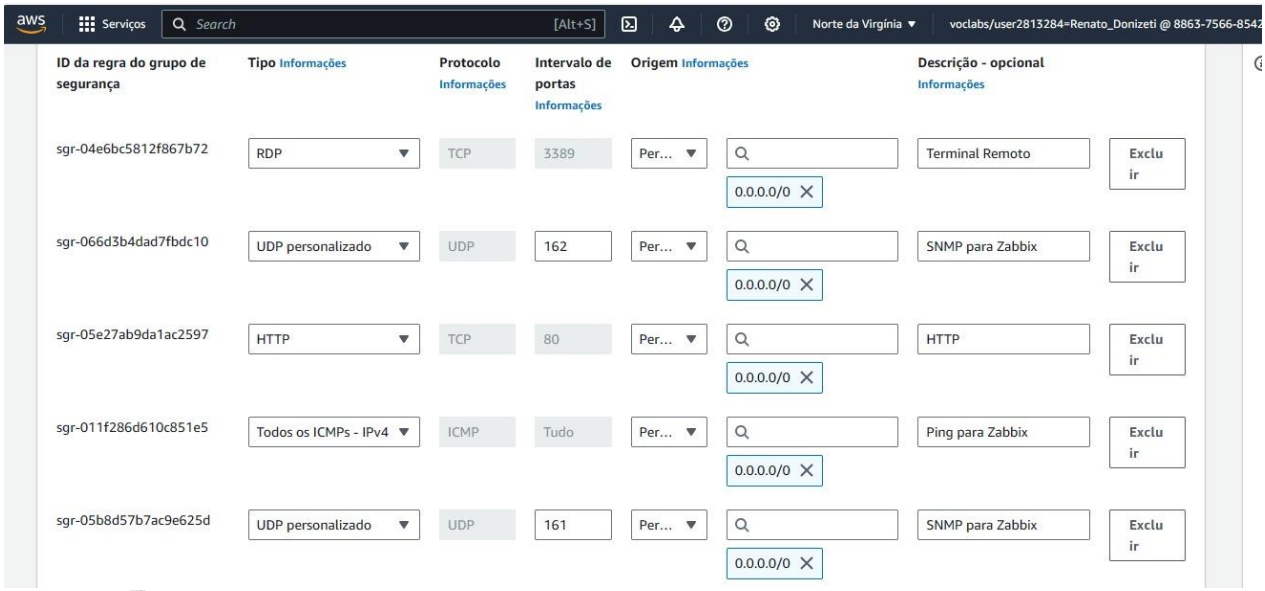


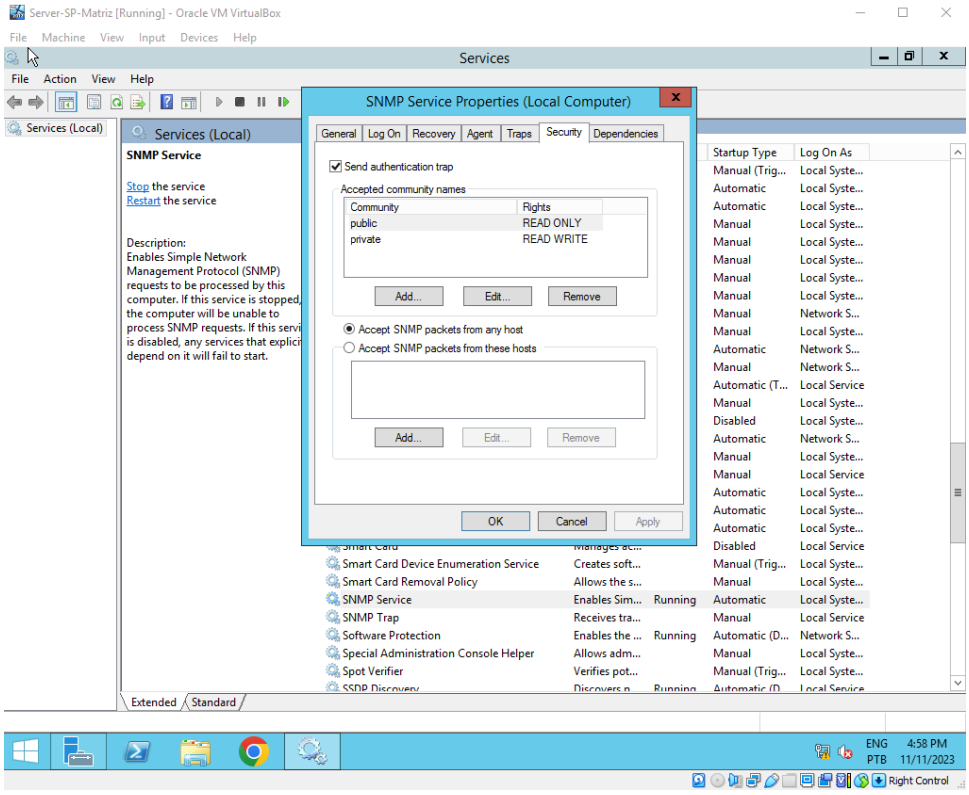
- IP Público: 107.23.83.234

- IP VPC: 192.168.0.0/16

- SUBNET Pública 1: 192.168.1.0/24
- SUBNET Privada1: 192.168.3.0/24
- SUBNET Pública 2: 192.168.2.0/24
- SUBNET Privada 2: 192.168.4.0/24

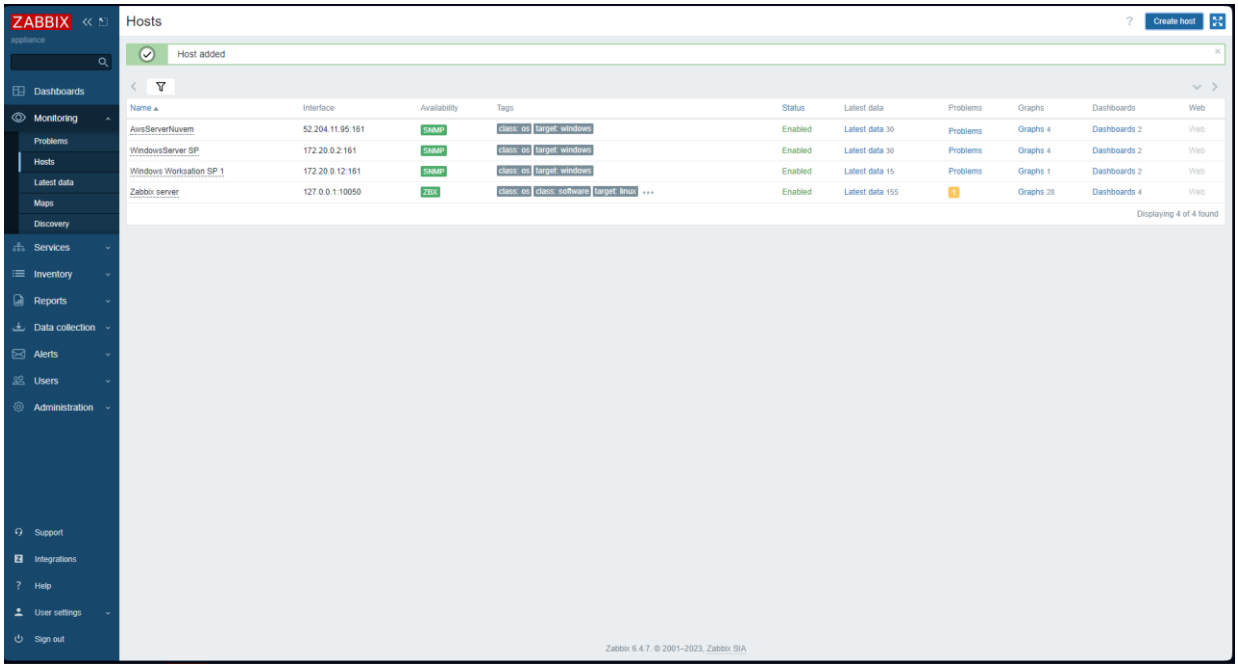
- A seguir podemos ver como estão organizados os grupos de segurança na nuvem e no servidor local.



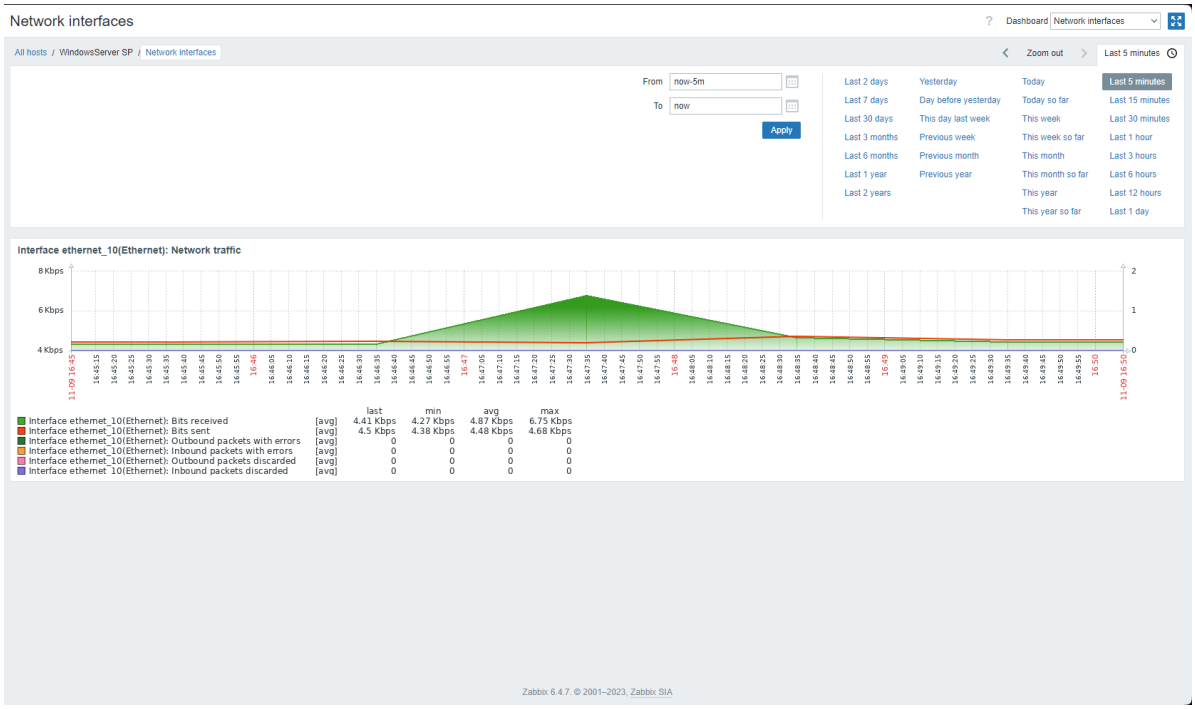


ZABBIX

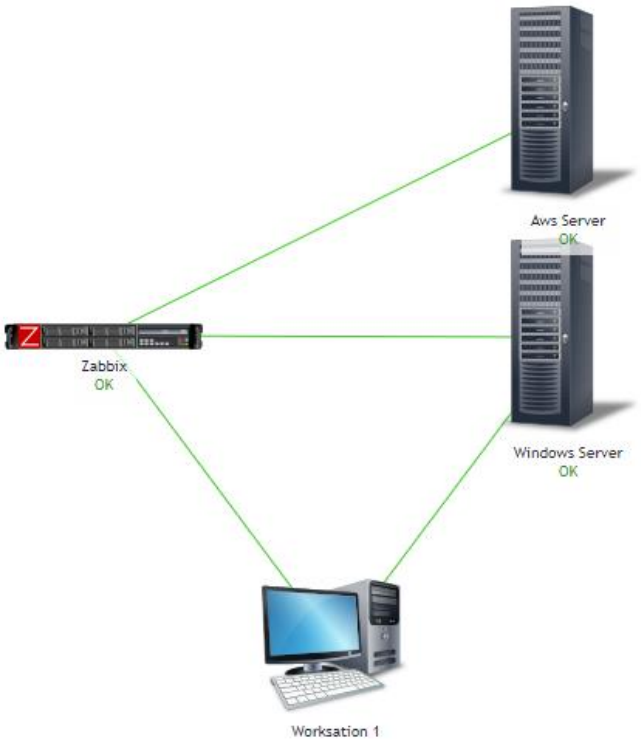
- Abaixo temos os hosts tanto das máquinas locais quanto das máquinas na nuvem, inseridos e monitorados com sucesso no Zabbix.



- Monitoramento de rede da máquina de servidor matriz (local)



- Mapa simples da Rede



- Acima podemos ver que a rede pode aumentar na vertical com mais links de servidores e na horizontal com mais computadores conforme a necessidade de mais workstations.

7 - Aplicação desenvolvida internamente

7.1 - Configurações do servidor

Implementamos um ambiente de hospedagem do back-end utilizando um servidor na Amazon Web Services (AWS) com a distribuição Ubuntu. O processo de setup foi realizado seguindo as etapas recomendadas pela AWS para provisionamento de instâncias EC2. Para garantir uma infraestrutura altamente escalável e modular, optamos por empregar o Docker Compose para a gestão dos contêineres que compõem o ambiente do servidor. Isso nos permitiu definir e orquestrar facilmente múltiplos contêineres.

Para que o back-end funcionasse em nosso ambiente, foram configurados dois containers, um container NGINX e outro de PHP-fpm, conforme é possível ver:

```
version: '3.9'

services:
  nginx:
    image: nginx:latest
    ports:
      - '3000:80'
    volumes:
      - ./src:/var/www/html
      - ./default.conf:/etc/nginx/nginx.conf
    links:
      - php-fpm
    depends_on:
      - php-fpm
  php-fpm:
    image: php:8-fpm-alpine
    volumes:
      - ./src:/var/www/html
```

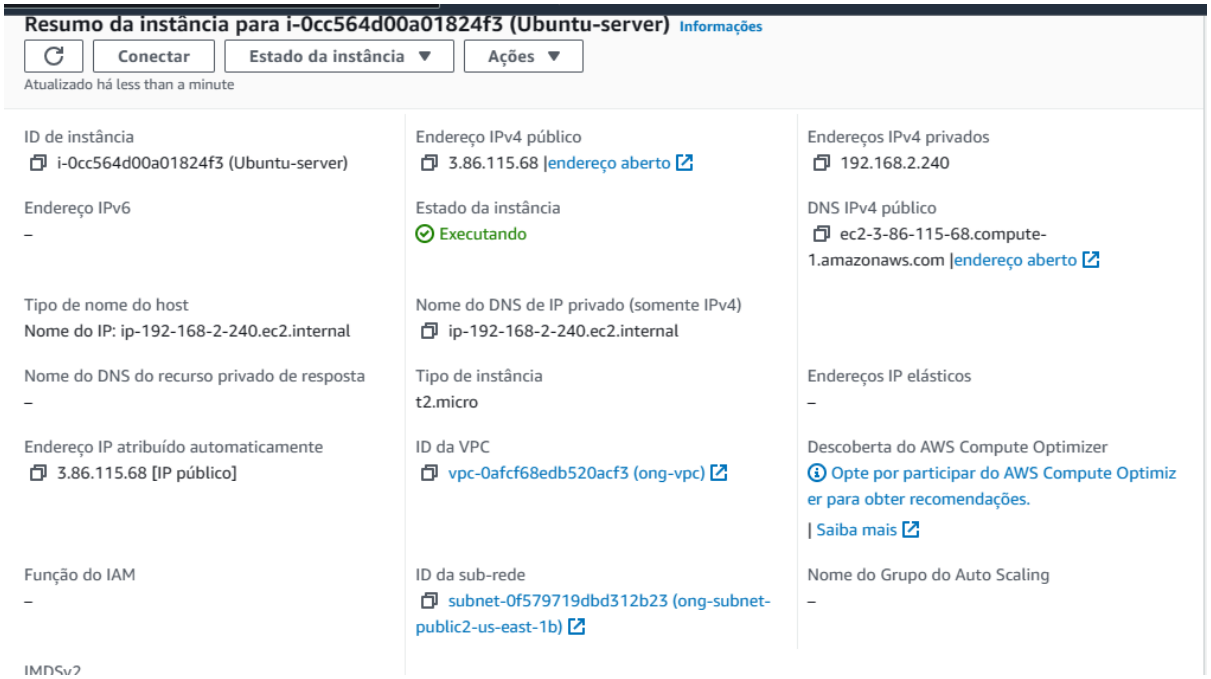
A escolha do Docker Compose como ferramenta de orquestração se deu pela sua capacidade de simplificar a configuração e o gerenciamento dos serviços, garantindo a padronização do ambiente e facilitando o deploy e a manutenção do back-end da aplicação. Utilizamos arquivos de composição (YAML) para definir os serviços, redes e volumes necessários para a execução eficiente do sistema, possibilitando uma arquitetura mais flexível e robusta.

As configurações do NGINX para se comunicar com o PHP-fpm são as seguintes:

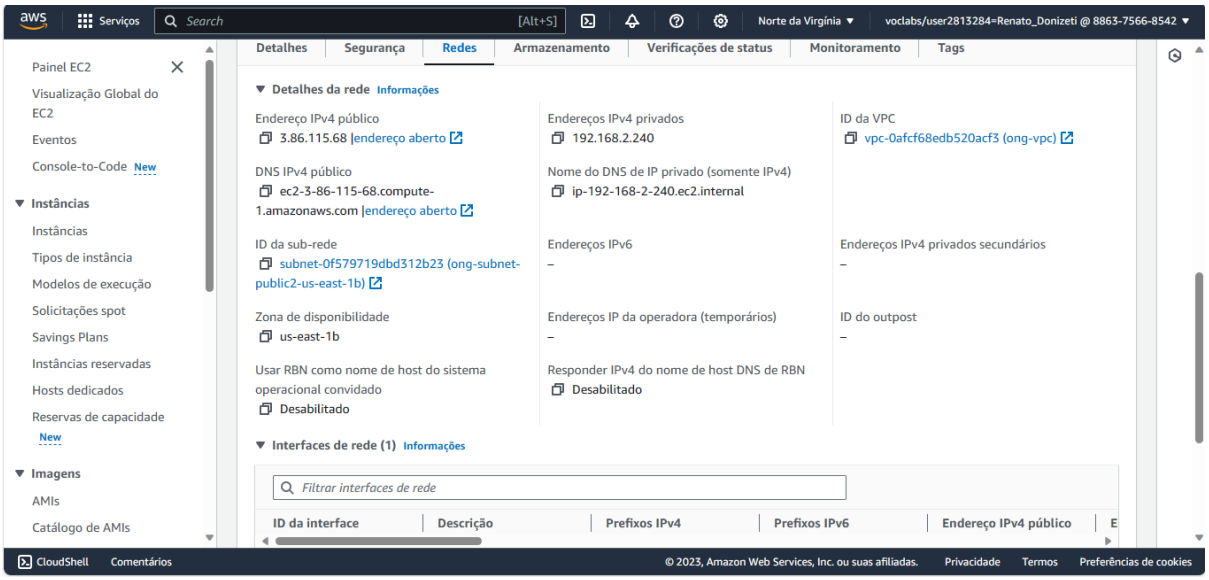
```
worker_processes auto;

events {
```

```
  worker_connections 1024;
}

http {
  include /etc/nginx/mime.types;

  server {
    listen 80 default_server;
    listen [::]:80 default_server;

    charset utf-8;
    root /var/www/html;
    server_name _;

    location / {
      index index.php index.html index.htm;
      try_files $uri $uri/ /index.php$is_args$args;
    }

    location ~ [^/]\.php(/|$) {
      include /etc/nginx/mime.types;
      include /etc/nginx/modules-enabled/*.conf;
      include fastcgi_params;
      fastcgi_param REQUEST_METHOD $request_method;
      fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
      fastcgi_split_path_info ^(.+\.php)(/.+)$;
      if (!-f $document_root$fastcgi_script_name) {
        return 404;
      }

      fastcgi_intercept_errors on;
      fastcgi_pass php-fpm:9000;
    }

    location ~ /\.ht {
      deny all;
    }
  }
}
```

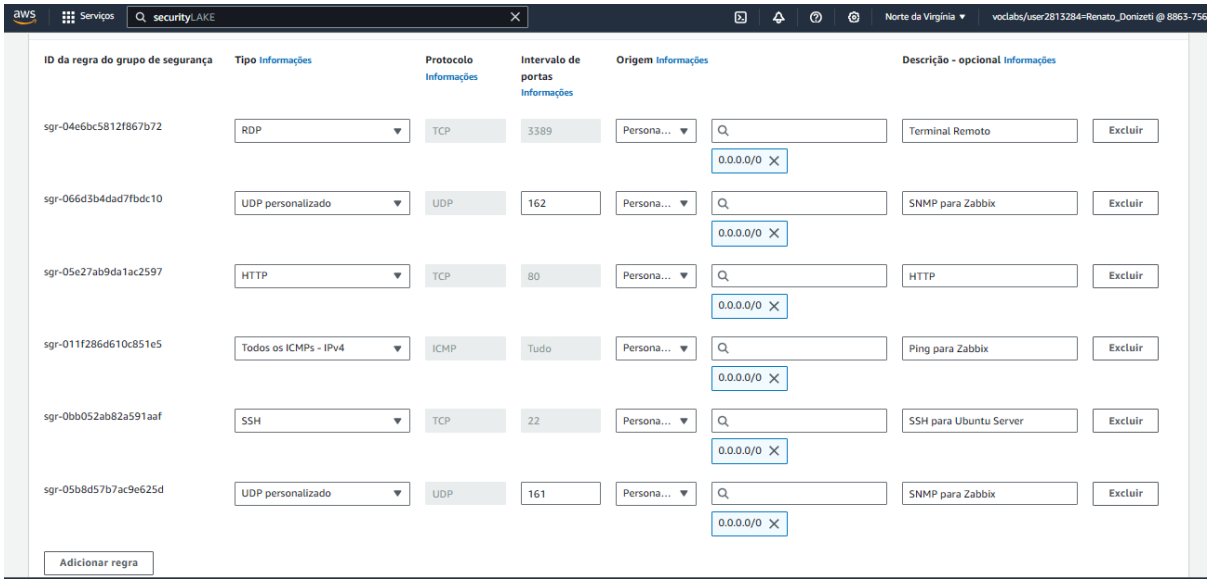
Falando sobre as configurações do Servidor na AWS, foi criado uma máquina do tipo EC2 de Shape t2.micro instalado Ubuntu Server. Foi necessário liberar a porta 22 para permitir acesso SSH. Como mostra as imagens:



Nesta imagem é possível observar o IP público atribuído ao servidor, a rede VPC, a sub-rede em que foi atribuído e o shape do servidor.



Nesta imagem é possível observar as configurações de rede da máquina.



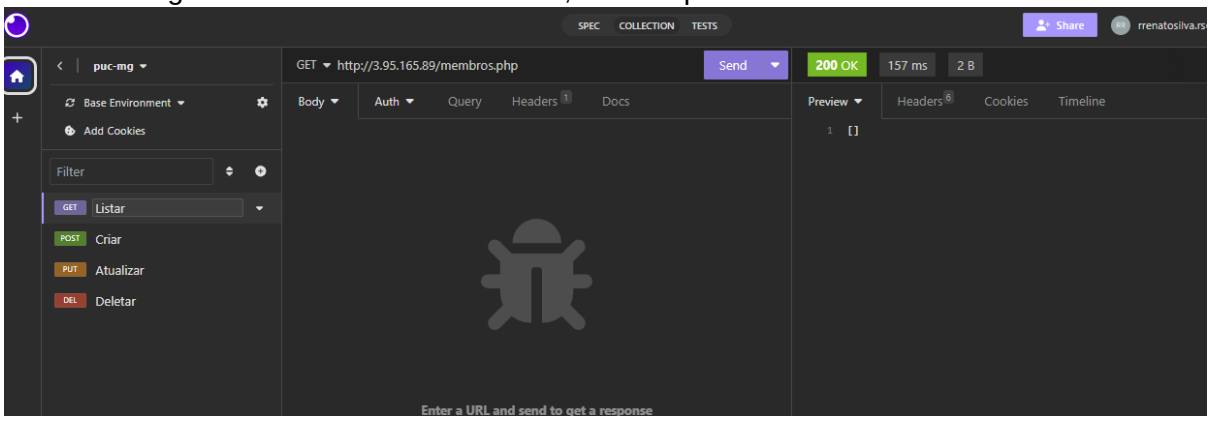
Nesta imagem é possível observar as configurações do grupo de segurança e que foi necessário habilitar a porta 22.

7.2 - Serviços fornecidos

A aplicação criada e mantida pela ONG será um conjunto de endpoints para gerenciar os membros. O serviço fornecido é uma *Application Programming Interface* (API), para realizar operações nos registros de membros, exposta através de *Hypertext Transfer Protocol* (HTTP).

7.2.1 - Listagem de membros

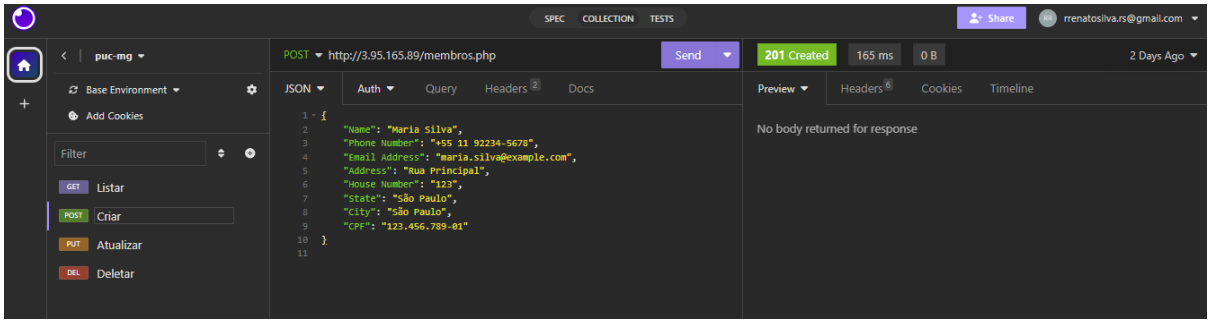
O endpoint de listagem utiliza o método GET na rota /membros.php e retorna em formato JSON a listagem de membros cadastrados, com resposta válida HTTP 200.



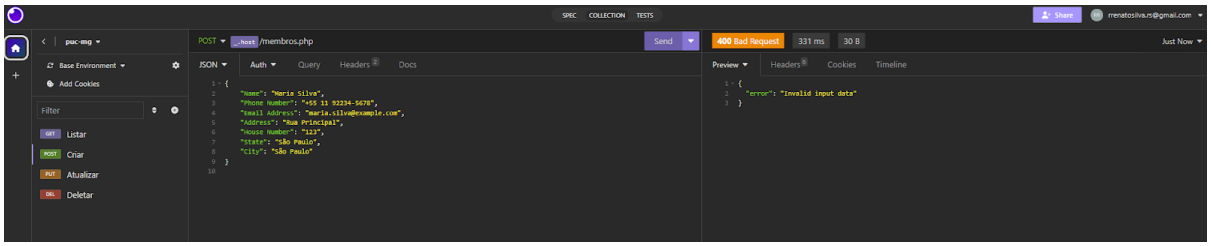
Sucesso ao listar membros.

7.2.2 - Cadastro de membros

O endpoint de criação de membros utiliza o método POST na rota /membros.php e retorna HTTP 201 ao criar um novo membro com sucesso ou HTTP 400 em caso de falha.



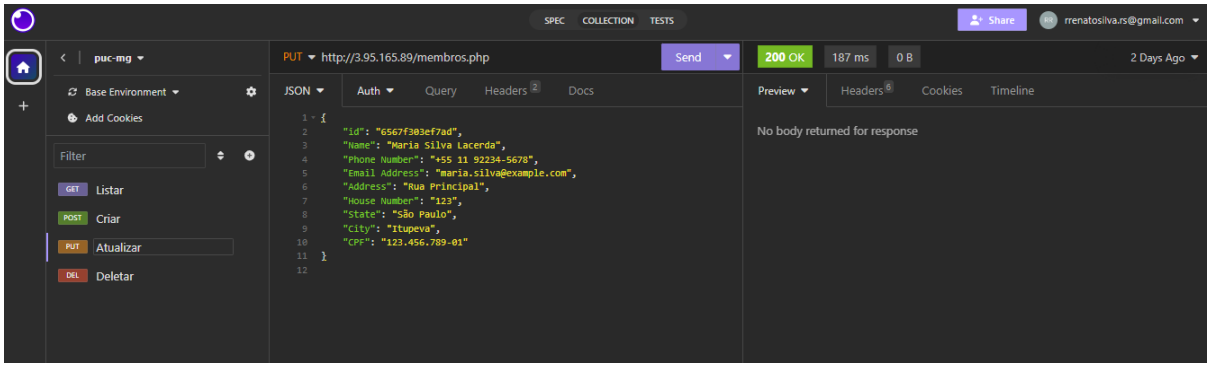
Sucesso ao cadastrar membro.



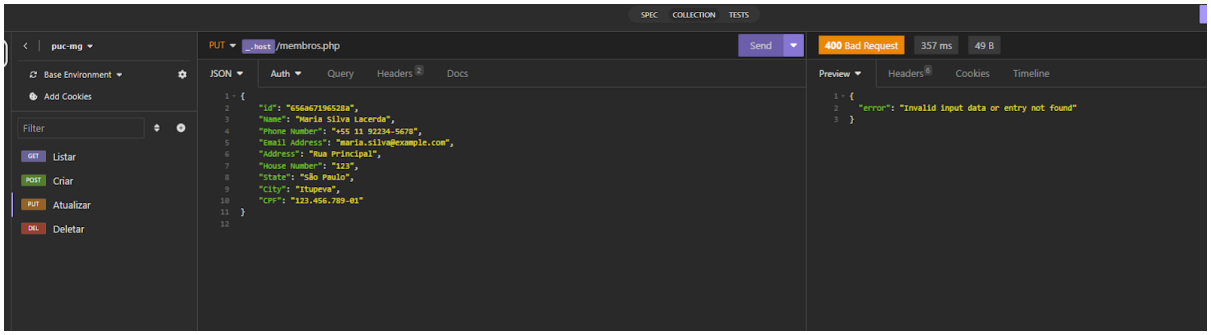
Falha ao cadastrar membro, a requisição informada não contém todos os campos necessários ou algum campo se encontra no formato incorreto.

7.2.3 - Atualização de membros

O endpoint de atualizar dados de membros utiliza o método PUT na rota /membros.php e retorna HTTP 200 ao atualizar os dados com sucesso ou HTTP 400 em caso de falha.



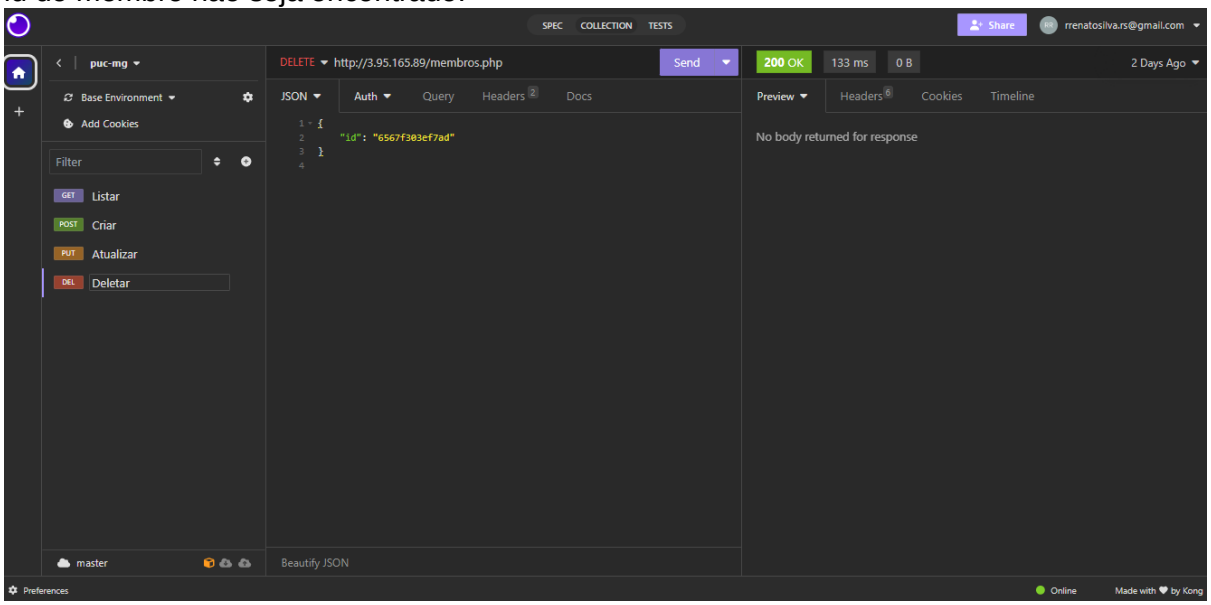
Sucesso ao editar membro.



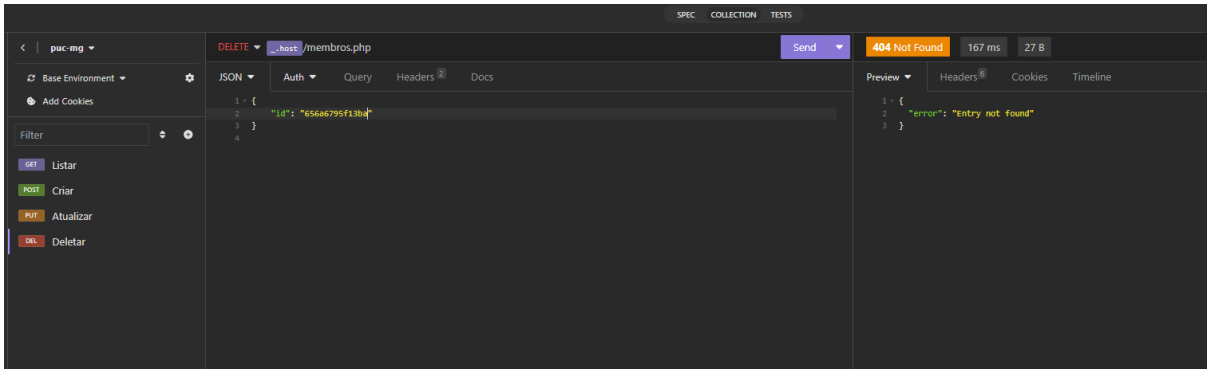
Falha ao editar membro, a requisição informada não contém todos os campos necessários ou algum campo se encontra no formato incorreto.

7.2.4 - Exclusão de membros

O endpoint de exclusão de dados de membros utiliza o método DELETE na rota /membros.php e retorna HTTP 200 ao atualizar os dados com sucesso ou HTTP 404 caso o id do membro não seja encontrado.



Sucesso ao excluir membro.



Falha ao excluir membro, usuário não existe.

8 - REFERÊNCIAS

Dell. **Precision 3660 Workstation.** Disponível em: https://www.dell.com/pt-br/shop/cty/pdp/spd/precision-3660-workstation/xcto01p3660mtrplbcc_p11?gacd=9657105-15015-5761040-275878141-0&dgc=ST&cid=71700000112393939&gclid=Cj0KCQjwgNanBhDUARIsAAeIcAteZMe65c6Y9jlFo_VCNZBa1WK5W0mfT8AD4u8P0MzdZ52VGxBEApwaAt0ZEALw_wcB&gclsrc=aw.ds&configurationid=9250193a-2565-4bf3-a536-848b2992de4d. Acesso em 02/09/2023.

Dell. Vostro Small Desktop. Disponível em: https://www.dell.com/pt-br/shop/computadores-all-in-ones-e-workstations/vostro-small-desktop/spd/vostro-3710-desktop/v3710w6505w. Acesso em 02/09/2023.

Mercado Livre. **Roteadores e Sistemas Sem Fios Cisco C1121-4P**. Disponível em: https://www.mercadolivre.com.br/roteadores-e-sistemas-sem-fios-cisco-c1121-4p-router-sem-fios-gigabit-ethernet-dual-band-24-ghz-5-ghz-branco-100v240v/p/MLB21971695?from=gshop&matt_tool=76735400&matt_word=&matt_source=google&matt_campaign_id=14303413823&matt_ad_group_id=125956126719&matt_match_type=&matt_network=g&matt_device=c&matt_creative=543112166789&matt_keyword=&matt_ad_position=&matt_ad_type=pla&matt_merchant_id=735098660&matt_product_id=MLB21971695-product&matt_product_partition_id=435661999394&matt_target_id=pla-435661999394&gclid=Cj0KCQjwgNanBhDUARIsAAeIcAu6FlnjGIIFt8geUtCKrhBQt_QOHMJfzZqb353-3lQr8M_EEDeMxcUaAvQPEALw_wcB. Acesso em 02/09/2023.

Mercado Livre. **Cabo Console Serial Cisco Original RJ45 DB9 Macho 72-3383-01**. Disponível em: https://produto.mercadolivre.com.br/MLB-2944023914-cabo-console-serial-cisco-original-rj45-db9-macho-72-3383-01-_JM?matt_tool=76735400&matt_word=&matt_source=google&matt_campaign_id=14303413823&matt_ad_group_id=125956126719&matt_match_type=&matt_network=g&matt_device=c&matt_creative=543112166789&matt_keyword=&matt_ad_position=&matt_ad_type=pla&matt_merchant_id=5082133997&matt_product_id=MLB2944023914&matt_product_partition_id=435661999394&matt_target_id=pla-435661999394&gclid=Cj0KCQjwgNanBhDUARIsAAeIcAuyeWMTpYcIR7f8VJ6NbU22Yu3Ve6SZsFmA5v3oUGqNfXLX56Y4st4aAg9kEALw_wcB. Acesso em 02/09/2023.

FourServ. **Switch Dell N1524 24 Portas Gigabit 4x SFP Layer 3 Gerenciável**. Disponível em: https://www.fourserv.com.br/produto/switch-dell-n1524-24-portas-gigabit-4x-sfp-layer-3-gerenciavel-mpn-210-asnf/468793?utm_source=google-pmax&utm_medium=cpc&utm_campaign=pmax-switches&gclid=Cj0KCQjwgNanBhDUARIsAAeIcAuf5AJoPCnbZ332YApFYgYptizuVa6Bs15BDjX9fDu9ii_Uj-nFAE8aAm_NEALw_wcB. Acesso em 02/09/2023.

Amazon. **FURUKAWA SOHOPLUS - Caixa de Cobre Cinza**. Disponível em: https://www.amazon.com.br/FURUKAWA-SOHOPLUS-Caixa-Cobre-Cinza/dp/B081VSRPFQ/ref=asc_df_B081VSRPFQ/?tag=googleshopp00-20&linkCode=df0&hvadid=379726213612&hvpos=&hvnetw=g&hvrand=3586566409474997790&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1031483&hvtargid=pla-929242871190&psc=1. Acesso em 02/09/2023.

Cirilo Cabos. **Kit com 50 Conectores RJ45 Cat6 Seccon 901920**. Disponível em: https://www.cirilocabos.com.br/kit-com-50-conectores-rj45-cat6-seccon-901920/p. Acesso em 02/09/2023.

Cirilo Cabos. **Patch Cord Cat 6 Furukawa**. Disponível em: https://www.cirilocabos.com.br/patch-cord-cat-6-furukawa/p?skuId=1285753540. Acesso em 02/09/2023.

Loja Elétrica. **Patch Panel Cat6 24 Posições 19" 568AB SOHOPLUS 35050402 Furukawa**. Disponível em: http://www.lojaeletrica.com.br/patch-panel-cat6-24-posicoes-19-568ab-sohoplus-35050402-furukawa,product,2521101380511,dept,999999.aspx. Acesso em 02/09/2023.

Loja Elétrica. **Rack Fechado 44U 215x57x057cm ACR-PR**. Disponível em: http://www.lojaeletrica.com.br/rack-fech44u-215x57x057cm-acr-pr----contato,product,2520823990497,dept,999999.aspx. Acesso em 02/09/2023.

Amazon. **Tomada RJ45 com Placa Tramontina**. Disponível em: https://www.amazon.com.br/Tomada-RJ45-com-Placa-Tramontina/dp/B077TXFRBR/ref=asc_df_B077TXFRBR/?tag=googleshopp00-20&linkCode=df0&hvadid=379727323120&hvpos=&hvnetw=g&hvrand=15699767760088099075&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=1001655&hvlocphy=1031483&hvtargid=pla-1038417730315&psc=1. Acesso em 02/09/2023.

Amazon. **Ponto de Acesso Ubiquiti U6-LITE UniFi**. Disponível em: https://www.amazon.com.br/Ponto-acesso-Ubiquiti-U6-LITE-UniFi/dp/B08T6CKG5B/ref=asc_df_B08T6CKG5B/?tag=googleshopp00-20&linkCode=df0&hvadid=379720709908&hvpos=&hvnetw=g&hvrand=16150431801728275540&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9101113&hvtargid=pla-1182964561905&psc=1. Acesso em 02/09/2023.

Amazon. **Guia de Cabo 1U Fechado Preto**. Disponível em: https://www.amazon.com.br/Guia-Cabo-1u-Fechado-preto/dp/B0891RY8C5/ref=asc_df_B0891RY8C5/?tag=googleshopp00-20&linkCode=df0&hvadid=379787216837&hvpos=&hvnetw=g&hvrand=14220512271108259022&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1031483&hvtargid=pla-1410918484505&psc=1. Acesso em 02/09/2023.

HP. **Impressora Multifuncional HP LaserJet Tank 1602w**. Disponível em: https://www.hp.com/br-pt/shop/impressora-multifuncional-hp-laserjet-tank-1602w-2r3e8a.html. Acesso em 02/09/2023.

Amazon. **Nobreak Senoidal Intelbras SNB 3000VA**. Disponível em: https://www.amazon.com.br/Nobreak-Senoidal-Intelbras-SNB-3000VA/dp/B09MKP79L2/ref=asc_df_B09MKP79L2/?tag=googleshopp00-20&linkCode=df0&hvadid=379749544033&hvpos=&hvnetw=g&hvrand=5672864949990135327&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1031483&hvtargid=pla-1853523943090&psc=1. Acesso em 02/09/2023.

MadeiraMadeira. **Conjunto Home Office 2 Peças Escrivaninha Notável com Cadeira para Escritório Madri**. Disponível em: https://www.madeiramadeira.com.br/conjunto-home-office-2-pecas-escrivaninha-notavel-com-cadeira-para-escritorio-madri-3031524.html?index=vr-prod-poc-madeira-listings-best-seller-desc. Acesso em 02/09/2023.

9 - ANEXOS

9.1 - Política de segurança da informação

É com grande comprometimento com a integridade, confidencialidade e disponibilidade de dados que apresentamos a nossa Política de Segurança da Informação. Reconhecemos a importância vital que a segurança da informação desempenha na proteção dos ativos digitais da organização e na garantia da confiança de nossos colaboradores, parceiros e clientes.

Esta política é uma expressão tangível do nosso compromisso em estabelecer e manter práticas seguras em todas as áreas que envolvem o manuseio de informações sensíveis. A segurança da informação não é apenas uma responsabilidade, mas sim um valor intrínseco que permeia todos os aspectos de nossas operações.

Neste documento, delineamos diretrizes claras, normas e procedimentos que visam proteger contra ameaças digitais, garantindo que os dados sejam tratados com a máxima responsabilidade e cuidado. Ao implementar esta política, aspiramos a um ambiente digital resiliente, que inspire confiança e esteja alinhado com as melhores práticas globais de segurança da informação.

Cada membro de nossa organização é peça fundamental na execução efetiva desta política. Incentivamos a leitura atenta e a adesão integral aos princípios aqui estabelecidos, a fim de construirmos juntos um ambiente digital seguro, robusto e confiável.

Agradecemos a todos pelo comprometimento contínuo com a segurança da informação e confiança depositada em nossa equipe para preservar a integridade dos dados que nos foram confiados.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO..... 2
2. OBJETIVOS..... 2
3. ABRANGÊNCIA..... 3
4. DIRETRIZES GERAIS..... 3
4.1 Interpretação..... 3
4.2 Propriedade..... 4
4.3 Classificação da informação..... 4
4.4 Controle de acesso..... 6
4.5 Internet..... 7
4.6 Correio eletrônico..... 7
4.7 Rede sem fio (Wi-Fi)..... 7
4.8 Recursos de TIC institucionais..... 8
4.9 Recursos de TIC particulares..... 10
4.10 Armazenamento de informações..... 11
4.11 Repositórios digitais..... 11
4.12 Mídias sociais..... 12
4.13 Mesa limpa e tela limpa..... 12
4.14 Áudio, vídeos e fotos..... 12
4.15 Uso de imagem, som da voz e nome..... 13
4.16 Aplicativos de comunicação..... 14
4.17 Monitoramento..... 14
4.18 Combate à intimidação sistemática (bullying)..... 15
4.19 Contratos de trabalho e de prestação de serviços..... 15
4.20 Segurança da informação..... 16
5. PAPÉIS E RESPONSABILIDADES..... 17
5.1 Todos..... 17
5.2 Gestores e coordenadores..... 18
5.3 Colaboradores..... 18
6. DISPOSIÇÕES FINAIS..... 19
7. DOCUMENTOS DE REFERÊNCIA..... 19
APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES..... 20

1. INTRODUÇÃO

A Organização não governamental (ONG), na forma do seu Estatuto, é uma associação civil de fins não econômicos e beneficentes de assistência social. Tem por finalidade, dentre outras, manter campanhas de arrecadação para causas que julgar nobre.

A ONG utiliza a tecnologia e a internet de forma a garantir a disseminação e promoção de campanhas e eventos para tornar público e/ou reforçar causas. No entanto, a mobilidade e a ausência de perímetros físicos e de fronteiras claras que caracterizam a sociedade atual, permitidas pelos avanços tecnológicos, exigem muito mais cuidado para se evitar incidentes que possam colocar em risco seus colaboradores.

Nesse contexto, a segurança da informação é uma atividade essencial de proteção de todos os ativos tangíveis e intangíveis da ONG, a exemplo de imagem, reputação, conhecimento, patrimônio e a própria informação. Desse modo, é fundamental que todos os integrantes pratiquem e disseminem a segurança digital.

Em resposta a essas novas necessidades, está sendo implementado o Sistema de Gestão de Segurança da Informação (SGSI), que possui como diretriz principal a Política de Segurança da Informação (PSI), para atender às peculiaridades do segmento.

Para que a ONG alcance o resultado de proteger seus ativos na produção e compartilhamento de conhecimento, essas novas regras devem ser cumpridas por todos.

2. OBJETIVOS

A Política de Segurança da Informação (PSI) é aplicável ao ambiente administrativo e tem por objetivos:

- Estabelecer as diretrizes estratégicas e os princípios para a proteção dos ativos tangíveis e intangíveis, a exemplo da imagem, reputação, marca, propriedade intelectual, bancos de dados e conhecimento, e dos recursos de tecnologia da informação e comunicação (recursos de TIC) da ONG, além das informações dos colaboradores;

- Nortear a tomada de decisão e a realização das atividades profissionais de todos os colaboradores da ONG, em ambientes presenciais ou digitais, sempre de acordo com as normas da instituição e a legislação nacional vigente;
- Construir uma cultura de uso seguro das informações, formando indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital;
- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações e dos recursos de TIC da ONG;
- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

3. ABRANGÊNCIA

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os colaboradores, para o ambiente administrativo, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da ONG.

4. DIRETRIZES GERAIS

4.1 Interpretação

4.1.1 Para efeito desta PSI, são adotadas as siglas, os termos e definições constantes no Apêndice A.

4.1.2 Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da ONG.

4.1.2.1 Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da ONG e com

duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

4.2 Propriedade

4.2.1 As informações geradas, acessadas, recebidas, manuseadas e/ou armazenadas, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis da ONG, são de propriedade coletiva do grupo.

4.2.2 Os recursos de TIC fornecidos pela ONG, para o desenvolvimento de atividades, são de propriedade de cada unidade ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e, por isso, devem ser utilizados apenas para o cumprimento da finalidade a que se propõem.

4.2.3 Todos os ativos tangíveis e intangíveis da ONG só podem ser utilizados para o cumprimento das atividades profissionais, limitados à função do colaborador.

4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da ONG, atuais e futuros, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais, quando prévia e expressamente autorizada.

4.2.5 Todos os colaboradores poderão fazer menção da marca em conteúdos e materiais, para citação do local onde trabalha, mas, em hipótese alguma, poderá a marca ser utilizada para criação de perfis em mídias sociais em nome da instituição e/ou se fazendo passar por ela.

4.3 Classificação da informação

4.3.1 Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

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 alunos.

4.3.1.2 Informação interna: informação que pode ser divulgada para os colaboradores da instituição, enquanto estiverem desempenhando atividades. Sua

divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

4.3.1.3 Informação confidencial: informação exclusiva a quem se destina. 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 o aspecto financeiro, legal e normativo.

4.3.2 Rotulagem da informação: quando se tratar de 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, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.

4.3.2.2 Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados e Plano Diretor de Segurança, Políticas de Uso.

4.3.3 Em respeito à classificação da informação, os colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.

4.3.3.1 Em caso de dúvida, todos deverão tratar a informação 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 da ONG.

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

4.3.5 A 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 colaborador é fornecida uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC da ONG.

4.4.1.1 A identidade digital é monitorada e controlada pela ONG.

4.4.1.2 O colaborador é responsável pelo uso e sigilo de sua identidade digital. No caso de uso não autorizado, não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

4.4.2 Quando a identidade for disponibilizada e fornecida pela unidade, todos os colaboradores, prestadores de serviços e visitantes, enquanto presentes nas dependências físicas da instituição, precisam 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 o seu uso fora das dependências da ONG.

4.4.3 Para a segurança física, a ONG deve estabelecer espaço físico seguro para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas e que contenham ativos críticos para a instituição, a exemplo de, mas não se limitando à, data centers, salas de documentação crítica etc.

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

4.5 Internet

4.5.1 Os recursos de conectividade são fornecidos para atender ao propósito administrativo, visto que o acesso à internet é um direito essencial para o exercício da cidadania no Brasil. No entanto, os colaboradores devem fazer uso da internet em estrita observância das leis em vigor, respondendo pelo seu descumprimento.

4.5.2 O acesso à internet é concedido aos usuários e colaboradores por meio da identidade digital (*login* e senha) pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

4.6 Correio eletrônico

4.6.1 A utilização do correio eletrônico corporativo deve se ater à execução das atividades profissionais, respeitando as regras de direitos autorais, licenciamento de *software*, direitos de propriedade e privacidade.

4.6.2 O correio eletrônico corporativo pode ser utilizado no dispositivo móvel particular, porém o acesso às mensagens e às informações institucionais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, visto que pode ocorrer por ato de liberalidade e/ou conveniência sem a 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, e desde que não lhe seja dada prioridade sobre as atividades profissionais, não provoque efeitos negativos para qualquer outro usuário, não viole ou prejudique a rede corporativa e não viole norma vigente da ONG.

4.6.3.1 O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da ONG.

4.7 Rede sem fio (Wi-Fi)

4.7.1 A ONG, quando possível, oferece à comunidade administrativa, nos ambientes autorizados e limitados ao perímetro físico da instituição, uma rede sem fio (Wi-Fi) própria para finalidades administrativas.

4.7.2 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.

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

4.8 Recursos de TIC institucionais

4.8.1 Os recursos de TIC da ONG são destinados a finalidades estritamente profissionais e educacionais, reservadas às atividades e permissões designadas para os usuários.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da ONG.

4.8.3 Para a proteção das informações, os arquivos digitais contendo informações da ONG devem ser armazenados nos servidores de arquivos destinados às áreas e setores específicos, com acesso restrito, considerando que ameaças externas, tais como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas podem afetar a segurança de tais informações.

4.8.3.1 Quando disponíveis, 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 GTI é responsável por realizar as cópias de segurança dos arquivos digitais (*backup*) armazenados nos servidores de arquivos específicos da ONG.

4.8.3.3 A ONG não se responsabiliza pelos arquivos digitais armazenados nas estações de trabalho, nos *notebooks*, *tablets* e *smartphones* disponibilizados pela instituição. Em casos de desligamento ou rescisão, os arquivos digitais serão apagados.

4.8.4 Todos os recursos de TIC da ONG, incluindo os *softwares*, devem ser inventariados e identificados pela GTI.

4.8.5 Só é permitida a utilização de *softwares* e *hardwares* legítimos, previamente homologados ou autorizados pela GTI, sejam eles onerosos, gratuitos, livres ou licenciados.

4.8.6 O desenvolvimento, a manutenção ou definição de aquisição de aplicativos e de sistemas no mercado são de responsabilidade da GTI e precisa atender aos requisitos de segurança em todas as etapas dos processos, a fim de garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

4.8.7 Todas as modificações nos recursos de TIC da ONG, principalmente em sistemas e na infraestrutura tecnológica, devem ser realizadas e/ou autorizadas pela GTI, e de maneira controlada para identificar os possíveis riscos e prevenir impactos à instituição, além de garantir a disponibilidade dos recursos de TIC e a possibilidade de restauração do ambiente original em caso de incidentes não previstos.

4.8.8 A utilização de recursos deve ser monitorada pela GTI, aos quais cabe realizar projeções constantes para que os recursos de TIC suportem necessidades tecnológicas futuras.

4.8.9 É vedado o uso de recurso de TIC da ONG para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com o propósito profissional e as diretrizes da ONG.

4.8.10 Todo recurso de TIC de propriedade da ONG, incluindo os 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 Dispositivos móveis institucionais

4.8.11.1 O uso de dispositivos móveis de propriedade da ONG não é permitido por terceiros, prestadores de serviços e visitantes.

4.8.11.2 Os dispositivos móveis institucionais devem conter a menor quantidade possível de informações da ONG. Arquivos digitais com informações da ONG, devem ser armazenados em servidores específicos para esse fim.

4.8.11.3 Em casos de roubo, perda ou furto do dispositivo móvel institucional que contenha informações da ONG, o colaborador deve registrar o Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GTI.

4.9 Recursos de TIC particulares

4.9.1 É vedada a conexão dos recursos de TIC particulares na rede corporativa da ONG.

4.9.1.1 Os colaboradores são autorizados a utilizar os recursos de TIC particulares, conectados à rede, exclusivamente para as suas funções, atendendo aos princípios desta Política.

4.9.1.2 A ONG não tem qualquer responsabilidade sobre a utilização dos *softwares*, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos docentes.

4.9.2 Os recursos de TIC particulares previamente autorizados a acessar os conteúdos e serviços fornecidos pela ONG devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança, como antivírus e *firewall*, a fim de mitigar os riscos de exposição da instituição a ameaças.

4.9.3 Todo recurso de TIC particular trazido para as dependências da ONG é de inteira responsabilidade de seu proprietário, incluindo os dados e *softwares* nele armazenados ou instalados.

4.9.4 A ONG não será responsabilizada por qualquer perda, furto ou avaria dos 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 da ONG, desde que não interfira nas atividades profissionais e esteja de acordo com as leis em vigor.

4.9.5.2 Dentro do perímetro físico e lógico em que informações confidenciais são armazenadas ou processadas, a ONG deve restringir a entrada e circulação de dispositivos móveis particulares.

4.10 Armazenamento de informações

4.10.1 Todos devem manter as informações da ONG armazenadas no local apropriado e destinado a esse fim.

4.10.2 Os colaboradores devem armazenar as informações digitais da ONG 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.

4.10.3 A ONG deve 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 colaboradores, instituição e/ou terceiros relacionados, que forem contrários à legislação nacional vigente, ou possam configurar algum tipo de dano à instituição.

4.11 Repositórios digitais

4.11.1 Os repositórios digitais para o uso institucional são destinados ao armazenamento, à criação, ao compartilhamento e à transmissão de arquivos (*upload*) de informações da ONG, desde que previamente autorizados, homologados e disponibilizados pela GTI.

4.11.1.1 A utilização dos repositórios digitais para o uso institucional deve estar de acordo com os requisitos de segurança descritos nesta Política.

4.11.1.2 É vedado o armazenamento de arquivos digitais pessoais nos repositórios digitais para uso institucional.

4.11.2 É vedado armazenar, criar, compartilhar ou transmitir arquivos (upload) contendo informações da ONG para repositórios digitais particulares.

4.11.3 Nos repositórios digitais de uso institucional é vedada a criação, o armazenamento, o compartilhamento e a transmissão de arquivos (upload) de informações referentes a qualquer tipo de atividade ilegal, como pornografia infantil, jogos de azar, pirataria, violação dos direitos autorais, marcas comerciais ou outras leis de propriedade intelectual.

4.11.4 É vedado disponibilizar a identidade digital a terceiros para acessar os repositórios digitais de uso institucional.

4.12 Mídias sociais

4.12.1 A participação institucional do colaborador, por meio de acesso e/ou conexão a mídias sociais a partir do ambiente da instituição e durante o horário de trabalho, deve ser diretamente relacionada à sua função profissional e aos objetivos da ONG, sendo o colaborador responsável por qualquer ação ou omissão resultante de sua postura e comportamento.

4.13 Mesa limpa e tela limpa

4.13.1 Os papéis contendo informações da ONG não devem ficar expostos em impressoras, fax, *scanner*, pátios, telas de computadores, áreas comuns, locais de trânsito de pessoas, elevador, refeitório e nas salas de reunião, principalmente quando não estiverem sendo utilizados.

4.13.2 Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando, especialmente da sua estação de trabalho ou dispositivo móvel.

4.14 Áudio, vídeos e fotos

4.14.1 Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da ONG pertencente ao perímetro físico, e também dos colaboradores, sem prévia autorização.

4.14.1.1 Exceto para situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos administrativos, sociais e/ou esportivos, por sua natureza pública e de compartilhamento de informações e desde que o teor do conteúdo não exponha ao ridículo ou gere constrangimento aos envolvidos.

4.14.2 Os colaboradores da ONG não devem captar, reproduzir ou compartilhar por meio de qualquer meio tecnológico, inclusive na internet, quaisquer imagens, vídeos ou sons que:

a) Possam comprometer a segurança de outros colaboradores e do ambiente administrativo;

b) Possam comprometer o sigilo das informações;

c) Envolvam diretamente a de outros colaboradores, visitantes, prestadores de serviço e fornecedores, sem a prévia e expressa anuência desses ou do gestor responsável, exceto quando autorizados em razão da sua função ou em situações já previamente avisadas e autorizadas a exemplo de, mas não se limitando a, eventos sociais e/ou esportivos, passeios, excursões, campeonatos, por sua natureza pública e de compartilhamento de informações.

4.15 Uso de imagem, som da voz e nome

4.15.1 A ONG pode capturar, guardar, manipular, editar e usar a imagem dos colaboradores e prestadores de serviços para fins de identificação, autenticação, segurança, registro de atividades, acervo histórico, uso institucional e social, o que inclui os eventos promovidos pela instituição, inclusive em seus perfis oficiais nas mídias sociais, *website*,

intranet, quadro de avisos ou similar, vídeos educacionais, entre outros conteúdos que possam ser criados ou produzidos em razão da atividade educacional, tendo, por isso, pela própria característica técnica da internet, alcance global e prazo indeterminado, podendo inclusive alcançar *sites* e outros ambientes digitais externos.

4.15.2 Para o uso de imagem, som da voz e nome dos colaboradores, estão ressalvados os direitos sobre a integridade da sua honra, sua reputação, boa fama ou respeitabilidade, sendo feito apenas nos limites acordados, sem, de forma alguma, expor o colaborador ao ridículo ou a situações constrangedoras, atendendo às leis em vigor no Brasil.

4.16 Aplicativos de comunicação

4.16.1 O uso de aplicativos de comunicação pelos alunos ou docentes, a partir de recursos institucionais ou particulares, para compartilhar informações, deve ser feito de forma responsável para evitar riscos desnecessários que comprometam atividades ou a própria instituição.

4.16.2 O uso de aplicativos de comunicação no ambiente de trabalho ou fora dele, pelos colaboradores da ONG, a partir dos recursos institucionais ou particulares, para compartilhar informações institucionais, deve respeitar sempre o sigilo da informação, atender aos requisitos de segurança previstos nesta Política e respeitar as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a instituição.

4.17 Monitoramento

4.17.1 A ONG realiza o registro e armazenamento de atividades (*logs*) e monitoram seus ambientes lógicos, com a finalidade de proteção de seu patrimônio e reputação, assim como a proteção daqueles com os quais se relacionam de alguma forma.

4.17.2 O armazenamento dos dados monitorados é utilizado para fins administrativos e legais, além de colaborar com as autoridades em caso de investigação.

4.17.3 Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica, a ONG tem o dever de fornecer informações ao órgão competente para apuração, e quando necessário, disponibilizar provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

4.18 Combate à intimidação sistemática (bullying)

4.18.1. Responsabilidade do Usuário: Todos os usuários são responsáveis por manter um ambiente online seguro e respeitoso. Devem se abster de participar de qualquer forma de intimidação sistemática e relatar prontamente qualquer incidente que testemunhem ou experimentem.

4.18.2. Canais de Denúncia: Forneceremos canais seguros e confidenciais para denúncias, permitindo que os usuários relatem incidentes sem receio de retaliação. As denúncias serão tratadas de forma rápida e eficaz.

4.18.3. Privacidade e Confidencialidade: Garantimos a privacidade e confidencialidade dos envolvidos durante investigações, protegendo informações sensíveis relacionadas aos incidentes. A divulgação de informações só será feita quando estritamente necessário.

4.18.4. Monitoramento de Atividades Online: Implementaremos medidas de monitoramento para identificar padrões de intimidação sistemática. Isso nos permitirá tomar medidas preventivas e corretivas, protegendo proactivamente nossa comunidade.

4.18.5. Colaboração com Autoridades Competentes: Colaboraremos com autoridades competentes, conforme necessário, para lidar com casos mais graves de intimidação sistemática que possam violar leis locais. A segurança e o bem-estar de nossa comunidade são prioridades fundamentais.

4.19 Contratos de trabalho e de prestação de serviços

4.19.1 O mero porte de dispositivos institucionais e o acesso aos recursos de TIC e/ou às informações institucionais, inclusive de forma remota, fora do horário normal do expediente, em qualquer meio ou canal, incluindo, mas não se limitando a, mensagens de colaboradores em mídias sociais, mensagens SMS, correio eletrônico institucional, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da instituição.

4.19.2 Em casos de desligamento, rescisão contratual ou término do contrato, a GTI deve desativar todas as identidades digitais do colaborador em todos os sistemas e ambientes da ONG.

4.19.2.1 Nesse caso, o colaborador deve excluir todas as informações e contas da ONG, disponíveis no dispositivo móvel particular, caso tenham sido cadastradas.

4.20 Segurança da informação

4.20.1 Ao repassar ou transmitir informações da ONG 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.

4.20.2 Os 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.

4.20.3 A GTI deve manter um processo de salvaguarda e restauração dos arquivos digitais críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

4.20.4 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.

4.20.5 Para a proteção das informações e recursos de TIC críticos, a GTI deve elaborar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

4.20.6 A ONG está comprometida com o dever de orientar constantemente seus 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 na instituição.

5. PAPÉIS E RESPONSABILIDADES

5.1 Todos

5.1.1 Conhecer e disseminar as regras e princípios da Política de Segurança da Informação.

5.1.2 Preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia da ONG, 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 autorizada.

5.1.3 Preservar e proteger os recursos institucionais, a marca, a reputação, o conhecimento, a propriedade intelectual da ONG, principalmente todas as suas informações e conteúdos.

5.1.4 Zelar pela proteção do patrimônio da ONG, usando com responsabilidade os recursos físicos e lógicos fornecidos;

5.1.5 Evitar a exposição desnecessária das informações, projetos, trabalhos e dependências da ONG, inclusive nas mídias sociais e na internet, além de agir com responsabilidade no uso dos recursos de TIC e das informações.

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

5.1.7 Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da ONG.

5.1.8 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela ONG.

5.1.9 Reportar os incidentes que possam impactar na segurança das informações da ONG, imediatamente para o gestor.

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, 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, visitantes, fornecedores, prestadores de serviços e outros profissionais, utilizar linguagem respeitosa e adequada, condizente com o ambiente 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 lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela ONG.

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 da ONG serão consideradas violações por si só e estarão sujeitas às sanções previstas no Regimento Geral, contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição.

A PSI, bem como as demais normas de segurança da informação da ONG podem ser solicitadas ao gestor.

Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação da ONG, os colaboradores podem solicitar os esclarecimentos necessários para o GTI.

Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente, pessoalmente para o GTI.

7. DOCUMENTOS DE REFERÊNCIA

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

- 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.

APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES

A

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano à instituição.

Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de *Whatsapp*, *Telegram* e *Snapchat*.

Ativo: Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.

Ativos críticos: Todos os recursos considerados essenciais para a instituição que, se não estiverem intactos, disponíveis ou acessíveis, poderão acarretar danos graves à instituição.

Ativo intangível: Todo elemento que possui valor para a instituição e que esteja em meio digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à, reputação, imagem, marca e conhecimento.

Ativo tangível: Bens de propriedade da instituição que são concretos, que podem ser tocados, a exemplo, mas não se limitando a computadores, imóveis, móveis.

Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.

Antispyware: Programa espião de computador que tem o objetivo de observar e roubar informações pessoais do usuário, transmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

Autenticidade: Garantia de que as informações sejam procedentes e fidedignas, bem como capazes de gerar evidências não repudiáveis da identificação de quem as criou, editou ou emitiu.

B

Backup: Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

C

Colaborador: Empregado, estagiário, voluntário ou menor aprendiz da instituição.

Correio eletrônico: Também denominado e-mail, é um recurso que permite compor, enviar e receber mensagens através de programas eletrônicos de comunicação.

Correio eletrônico corporativo: Destinado a alunos, docentes e colaboradores da instituição, dentro do domínio de cada instituição (Exemplo: joao@ong.net).

Correio eletrônico particular: Estrutura de correio eletrônico particular não mantido pela instituição (Exemplo: jose@gmail.com).

Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.

Criptografia: Mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos etc.) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem.

D

Dados: Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processados ou agrupados, produzem informações.

Datacenter: Ambiente altamente crítico, projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como *switches*, roteadores e outros.

Disponibilidade: Garantia de que as informações e/ou recursos estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido à sua portabilidade. Exemplos: smartphone, notebook, tablet, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.

F

Firewall: Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

G

GTI: Gerência de Tecnologia da Informação.

I

Identidade digital: Identificação do usuário em ambientes lógicos, sendo composta por *login* e senha ou por outros mecanismos de identificação e autenticação, como crachá magnético, certificado digital, *token* e biometria.

Incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação e levando à perda de um ou mais princípios básicos de confidencialidade, integridade e disponibilidade.

Informação: Conjunto de dados que, processados ou não, pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato.

Internet: Rede mundial de computadores em que o usuário pode, a partir de um dispositivo, caso tenha acesso e autorização, obter informação de qualquer outro dispositivo também conectado à rede.

Integridade: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.

Intimidação sistemática (*bullying*): Todo ato de violência física ou psicológica, intencional e repetitivo, que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la(s) ou agredi-la(s), causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas.

L

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor no Brasil.

Login: Nome da identificação única dos usuários para acessarem sistemas computacionais ou recursos tecnológicos.

R

Recursos de tecnologia de informação e comunicação (recursos de TIC): Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Exemplos: computadores, *notebooks*, *smartphones*, *tablets*, discos externos, mídias, impressoras, *scanners*, entre outros.

Rede corporativa ou administrativa: Conjunto de recursos de conexão (rede local, rede internet e rede sem fio) para provimento de serviços internos à instituição, disponível para colaboradores, mantida e administrada pela GTI.

Repositórios digitais: Coleções de informação digital ou serviços de armazenamento, que podem ser mantidos internamente ou armazenados na internet, a exemplo de, mas não se limitando a, Wikipédia, *Microsoft Onedrive*, *Google Drive*, *SkyDrive*, *Dropbox*, *iCloud*.

Risco: Possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo para prejudicar a instituição.

S

Sala de Telecom: Ambiente para armazenar equipamentos de telecomunicações, de conexão e instalações de aterramento e de proteção de rede.

Segurança da informação: Preservação da confidencialidade, integridade e disponibilidade da informação na instituição.

SMS: Sigla de *Short Message Service* (Serviço de Mensagens Curtas). Serviço muito utilizado para o envio de mensagens de textos curtos, através de telefones celulares.

T

TIC: Tecnologia da Informação e Comunicação.

V

Violação: Qualquer atividade que desrespeite as diretrizes estabelecidas na política de segurança da informação ou em quaisquer das demais normas que as complementam.

W

Wi-Fi: Abreviação de *Wireless Fidelity*, que significa fidelidade sem fio, em português. *Wi-fi*, ou *wireless*, é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc