



**PUC Minas**

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS  
GERAIS INSTITUTO DE CIÊNCIAS EXATAS E  
INFORMÁTICA**

**Bacharelado em Sistemas de Informação**

**Douglas Evangelista dos Santos**

**Lucas Marcio Nascimento Costa Lima**

**Luiz Flávio Ferreira**

**Marcos Antonio Ferreira Filho**

**Sarah Moura Miranda**

**PROJETO INFRAESTRUTURA DE REDES**

Belo Horizonte

2024

## **PROJETO INFRAESTRUTURA DE TELEMARKETING**

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)	36

## 1. TEMA

Nosso tema é voltado para a área de telemarketing, mais especificamente em como funciona a rede e a infraestrutura em uma empresa de grande porte atuando no país. Estamos focando em três cidades chaves, sendo elas: Rio de Janeiro, São Paulo e Belo Horizonte., além de uma escala de trabalho home office.

Vendo como o mundo atual está na época da conexão, esse segmento não só utiliza de máquinas físicas, mas também de ferramentas virtuais como nuvem e outros, o que causa um grande impacto no uso de redes.

Uma empresa de call center possui uma estrutura e infraestrutura imensa e complexa, o que pede uma organização operacional completa, tornando inviável citar todo campo administrativo. A seguir, alguns exemplos:

1. **Escritórios:** A empresa terá um ou vários escritórios para alocar seus funcionários. Esses espaços podem ser divididos em áreas de trabalho individuais ou compartilhadas, dependendo do tamanho da equipe.
2. **Estações de trabalho:** Cada funcionário terá uma estação de trabalho com um computador, telefone e fones de ouvido. Essas estações são configuradas para permitir que os operadores façam chamadas telefônicas e tenham acesso aos sistemas e softwares necessários para realizar suas tarefas.
3. **Sala de supervisão:** Geralmente, há uma sala onde os supervisores monitoram as chamadas dos operadores, oferecem suporte e fornecem feedback aos funcionários. Nessa sala, também podem estar presentes monitores adicionais, sistemas de gravação de chamadas e outros recursos técnicos para auxiliar no gerenciamento das operações.
4. **Sala de treinamento:** Uma área reservada para treinamentos internos, onde novos operadores são capacitados antes de começarem a trabalhar nas operações ativas.
5. **Sala de descanso/refeitório:** Um espaço reservado para que os funcionários possam descansar durante os intervalos ou fazer refeições.
6. **Setor técnico/infraestrutura:** Pode haver uma área dedicada à equipe técnica

responsável pela manutenção dos equipamentos, atualização dos sistemas e solução de problemas relacionados às telecomunicações e tecnologia da informação utilizados pela empresa.

7. **Salas administrativas:** A empresa também pode contar com salas administrativas onde são realizadas atividades como gestão financeira, recursos humanos, marketing e outras funções relacionadas ao gerenciamento do negócio.
8. **Central telefônica/pabx:** Esse é o sistema central responsável por rotear as chamadas telefônicas entre os clientes externos e os operadores internos da empresa.
9. **Infraestrutura tecnológica:** A empresa precisará contar com servidores, computadores em rede, equipamentos telefônicos, softwares específicos (para discagem automática por exemplo), sistemas CRM (gerenciamento do relacionamento com o cliente) entre outros recursos tecnológicos necessários para o desempenho das atividades do telemarketing.

Termos aqui que salientar novamente o quanto complexo é uma empresa de telemarketing e como é impossível mensurar todos os setores da sua estrutura.

Nosso exemplo será focado em como funciona uma infraestrutura de uma empresa de grande porte, levando em consideração tecnologias que são imprescindíveis para o trabalho diário. Uma infraestrutura bem feita equivale a:

- Segurança de dados públicos de clientes e colaboradores;
- Expansão de área de atuação;
- Acesso remoto e trabalho interno conectados;
- Comunicação entre matriz e filiais em quaisquer estados;
- Automação de processos;
- Gestão e manutenção de processos;
- Gestão de dados de clientes ou possíveis clientes.

Não existe hoje empresa que não vise uma estrutura de redes, seja pequena ou grande porte. Para uma empresa voltada ao telemarketing, é crucial o investimento em tecnologias e no aperfeiçoamento em comunicação de rede.

## 2. RESPONSABILIDADES

Nome	Papel	Responsabilidade
Todo o grupo	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>
Todo o grupo		<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>
Todo o grupo	Redatora/editora	<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>
Todo o grupo	Comunicador	<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>

Todo o grupo	Programadora	<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>
Todo o grupo	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>
Todo o grupo	Pesquisador	<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 04/03/2024	Cinco dias	<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 09/03/2024	Cinco dias	- Definição do tema e planejamento inicial da proposta; - Curso do Cisco Packet Tracer;
Semana 3 14/03/2024	Cinco dias	- Planilha de Recursos de Rede; - Protótipo da rede no Simulador da Cisco Packet Tracer.
Semana 4 19/03/2024	Cinco dias	- Dúvidas finais com o professor; - Revisão e entrega da Entrega 1 (Primeira Etapa).

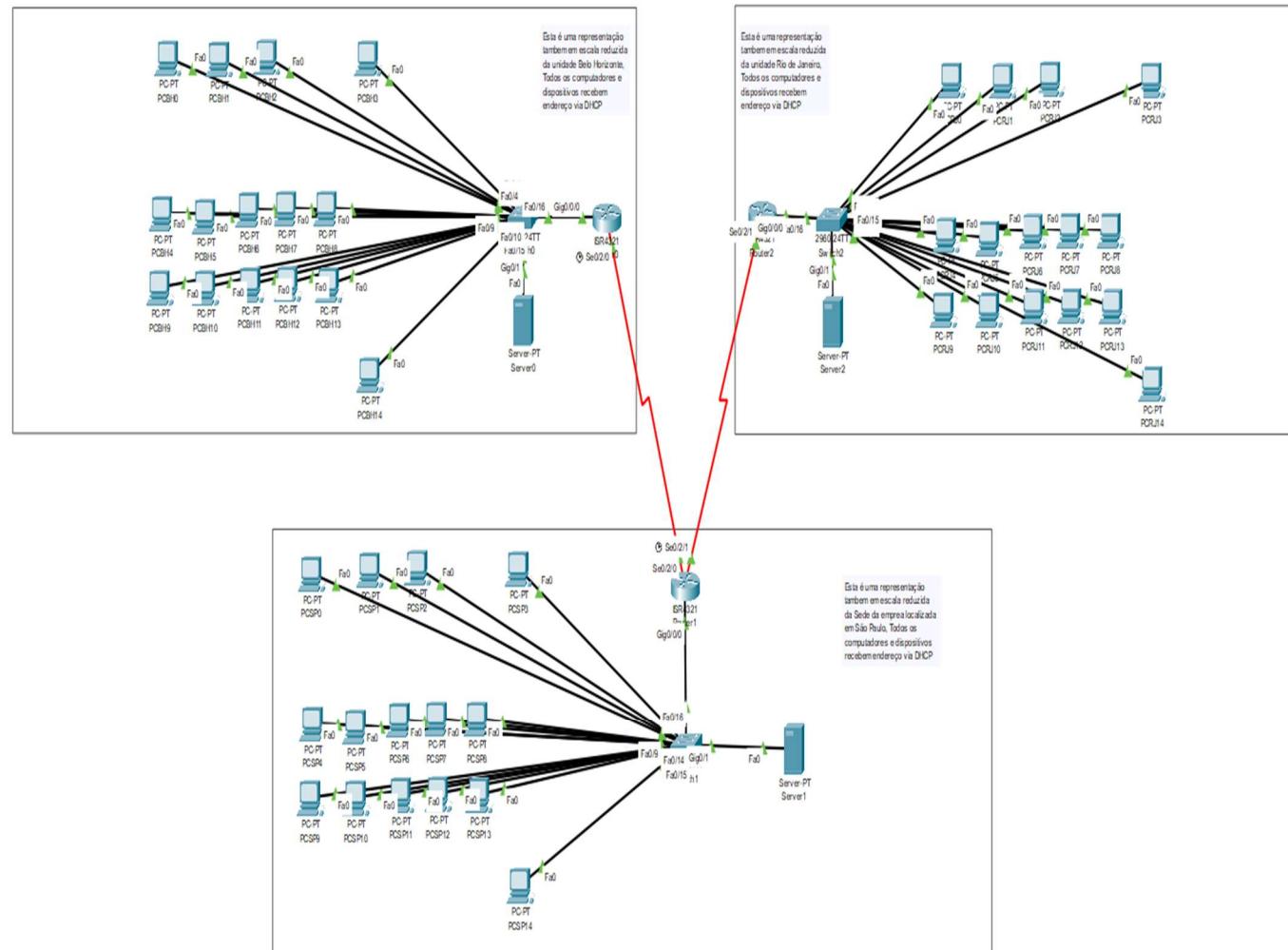
#### **4. PLANEJAMENTO DOS RECURSOS DE REDE**

Cenário: a rede será composta da matriz da empresa em São Paulo (SP) que se liga com uma filial em Belo Horizonte (MG) e uma filial no Rio de Janeiro (RJ). Além disso, a empresa também contará com um sistema de trabalho home office para comportar terceirizados e outros colaboradores.

- Matriz (São Paulo, SP)
  - Escritórios de superintendência;
  - Diretoria geral;
  - Estações de trabalho presencial para atendimento a colaboradores;
  - Departamento de segurança da informação;
  - Contabilidade;
  - Contas a pagar e contas a receber;
  - Departamento de Logística;
  - Gestão de projetos.
- Filial 1: Planejamento e estratégia (Belo Horizonte, MG)
  - Diretoria Executiva;
  - Estações de trabalho para busca ativa de clientes;
  - Departamento de qualidade.
- Filial 3: Escritório de Desenvolvimento de Mercado (Rio de Janeiro, RJ)
  - Departamento de Marketing e Vendas;
  - Departamento de Recursos Humanos;
  - Departamento Financeiro e Contábil.
- Home office
  - Departamento de Vendas;
  - Departamento de infraestrutura;
  - Suporte técnico virtual;
  - Equipe de desenvolvimento;
  - Departamento jurídico e de contratos;

## 4.1 DIVISÃO FÍSICA DA REDE

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



Fonte: Cisco Packet Tracer10

## 4.2 PLANILHA DE MATERIAIS

A tabela a seguir reflete a lista de materiais que serão empregados no projeto bem como seus valores correspondentes. A tabela abaixo é demonstrado o valor orçado que será necessário para a Matriz (São Paulo) (R\$ 1.205.249,90), Belo Horizonte (R\$ 918.172,90), Rio de Janeiro (R\$ 851.008,90), HOME OFFICE ( R\$ 740.700,00), O total geral estimado para este projeto é de R\$ 3.715.131,70.

		BELO HORIZONTE		SÃO PAULO		RIO DE JANEIRO		HOME OFFICE	
		200		250		180		300	
Item	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
Nutanix HPC - SERVIDOR OLHAR VALOR		0	0	0					
Estação DELL	R\$ 2.469,00	200	493.800,00	250	R\$ 617.250,00	180	444.420,00	300	R\$ 740.700,00
Roteador CISCO	R\$ 2.451,00	1	R\$ 2.451,00	1	R\$ 2.451,00	1	R\$ 2.451,00	0	R\$ -
Serial CISCO	R\$ 245,00	2	R\$ 490,00	2	R\$ 490,00	2	R\$ 490,00	0	R\$ -
Switch Dell 24p	R\$ 17.740,00	10	R\$ 177.400,00	15	R\$ 266.100,00	10	R\$ 177.400,00	0	R\$ -
Cabo UTP CAT6 cx	R\$ 1.349,10	20	R\$ 26.982,00	30	R\$ 40.473,00	20	R\$ 26.982,00	0	R\$ -
RJ45 f Cat6	R\$ 23,32	210	R\$ 4.897,20	260	R\$ 6.063,20	190	R\$ 4.430,80	0	R\$ -
Patch Cord CAT 6	R\$ 68,82	400	R\$ 27.528,00	500	R\$ 34.410,00	360	R\$ 24.775,20	0	R\$ -
Patch Panel CAT 6	R\$ 806,55	10	R\$ 8.065,50	20	R\$ 16.131,00	10	R\$ 8.065,50	0	R\$ -
Rack 44 U	R\$ 2.231,00	2	R\$ 4.462,00	2	R\$ 4.462,00	2	R\$ 4.462,00	0	R\$ -
CX + placa	R\$ 69,34	210	R\$ 14.561,40	260	R\$ 18.028,40	190	R\$ 13.174,60	0	R\$ -
AP Rukus WIFI 6	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	0	R\$ -
Organizador de cabo	R\$ 388,00	10	R\$ 3.880,00	15	R\$ 5.820,00	10	R\$ 3.880,00	0	R\$ -
Impressora	R\$ 1.394,10	10	R\$ 13.941,00	15	R\$ 20.911,50	10	R\$ 13.941,00	0	R\$ -
Nobreak	R\$ 1.434,80	1	R\$ 1.434,80	1	R\$ 1.434,80	1	R\$ 1.434,80	0	R\$ -
Mesa + Cadeira	R\$ 658,90	200	R\$ 131.780,00	250	R\$ 164.725,00	180	R\$ 118.602,00	0	R\$ -
		Total	R\$ 918.172,90	Total	R\$ 1.205.249,90	Total	R\$ 851.008,90	Total	R\$ 740.700,00
		TOTAL GERAL							R\$ 3.715.131,70

#### 4.3 DIVISÃO LÓGICA DA REDE

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

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

		<pre>Device Name: RouterFilial1 Custom Device Model: 2811 IOS15 Hostname: RouterFilial1  Port          Link  VLAN   IP Address FastEthernet0/0 Up    --     172.23.0.1/16 FastEthernet0/1 Down  --     &lt;not set&gt; Serial0/0/0    Down  --     &lt;not set&gt; Serial0/0/1    Down  --     &lt;not set&gt; Serial0/1/0    Down  --     &lt;not set&gt; Serial0/1/1    Up    --     192.168.3.2/24 Vlan1         Down  1      &lt;not set&gt;</pre>
		<pre>Device Name: RouterFilial2 Custom Device Model: 2811 IOS15 Hostname: RouterFilial2  Port          Link  VLAN   IP Address FastEthernet0/0 Up    --     172.24.0.1/16 FastEthernet0/1 Down  --     &lt;not set&gt; Serial0/0/0    Down  --     &lt;not set&gt; Serial0/0/1    Down  --     &lt;not set&gt; Serial0/1/0    Down  --     &lt;not set&gt; Serial0/1/1    Up    --     192.168.4.2/24 Serial0/2/0    Down  --     &lt;not set&gt; Serial0/2/1    Down  --     &lt;not set&gt; Vlan1         Down  1      &lt;not set&gt;</pre>
		<pre>Device Name: RouterFilial3 Custom Device Model: 2811 IOS15 Hostname: RouterFilial3  Port          Link  VLAN   IP Address FastEthernet0/0 Up    --     172.25.0.1/16 FastEthernet0/1 Down  --     &lt;not set&gt; Serial0/0/0    Down  --     &lt;not set&gt; Serial0/0/1    Down  --     &lt;not set&gt; Serial0/1/0    Down  --     &lt;not set&gt; Serial0/1/1    Up    --     192.168.5.2/24 Serial0/2/0    Down  --     &lt;not set&gt; Serial0/2/1    Down  --     &lt;not set&gt; Vlan1         Down  1      &lt;not set&gt;</pre>
		<pre>Device Name: SwitchMatrix Device Model: 2950T-24 Hostname: Switch  Port          Link  VLAN   IP Address FastEthernet0/1 Up    --     -- FastEthernet0/2 Up    --     -- FastEthernet0/3 Up    --     --</pre>
		<pre>Device Name: SwitchEsc1 Device Model: 2950T-24 Hostname: Switch  Port          Link  VLAN   IP Address FastEthernet0/1 Down  --     -- FastEthernet0/2 Up    --     -- FastEthernet0/3 Up    --     --</pre>
		<pre>Device Name: SwitchEsc2 Device Model: 2950T-24 Hostname: Switch  Port          Link  VLAN   IP Address FastEthernet0/1 Down  --     -- FastEthernet0/2 Up    --     -- FastEthernet0/3 Up    --     --</pre>

Switch	SwitchSP	<p>Device Name: SwitchFilial1 Device Model: 2950T-24 Hostname: Switch</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Switch	SwitchBH	<p>Device Name: SwitchFilial2 Device Model: 2950T-24 Hostname: Switch</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Switch	SwitchRJ	<p>Device Name: SwitchFilial3 Device Model: 2950T-24 Hostname: Switch</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0/1</td><td>Down</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr> <tr> <td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr> </tbody> </table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Down	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--
Port	Link	VLAN	IP Address															
FastEthernet0/1	Down	--	--															
FastEthernet0/2	Up	--	--															
FastEthernet0/3	Up	--	--															
Servidor	ServerSP	<p>Device Name: ServerMatriz Device Model: Server-PT</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>172.20.0.2/16</td></tr> </tbody> </table> <p>Gateway: 172.20.0.1 DNS Server: 172.20.0.2 Line Number: &lt;not set&gt;</p>	Port	Link	IP Address	FastEthernet0	Up	172.20.0.2/16										
Port	Link	IP Address																
FastEthernet0	Up	172.20.0.2/16																
Computador	PCSP	<p>Device Name: PCMatriz Device Model: PC-PT</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>172.20.2.11/16</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td>&lt;not set&gt;</td></tr> </tbody> </table> <p>Gateway: 172.20.0.1 DNS Server: 172.20.0.2 Line Number: &lt;not set&gt;</p>	Port	Link	IP Address	FastEthernet0	Up	172.20.2.11/16	Bluetooth	Down	<not set>							
Port	Link	IP Address																
FastEthernet0	Up	172.20.2.11/16																
Bluetooth	Down	<not set>																
Computador	PC2SP	IPv4 Address: 172.20.2.12/16 (Notação CIDR)																
Computador	PC1Esc1	<p>Device Name: PCEsc1 Device Model: PC-PT</p> <table border="1"> <thead> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>FastEthernet0</td><td>Up</td><td>172.21.0.11/16</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td>&lt;not set&gt;</td></tr> </tbody> </table> <p>Gateway: 172.21.0.1 DNS Server: 172.21.0.2 Line Number: &lt;not set&gt;</p>	Port	Link	IP Address	FastEthernet0	Up	172.21.0.11/16	Bluetooth	Down	<not set>							
Port	Link	IP Address																
FastEthernet0	Up	172.21.0.11/16																
Bluetooth	Down	<not set>																
Computador	PC2Esc1	IPv4 Address: 172.21.0.12/16 (Notação CIDR)																

Computador	PC1Esc2	<pre>Device Name: PCEsc2 Device Model: PC-PT  Port           Link   IP Address FastEthernet0  Up     172.22.0.11/16 Bluetooth      Down   &lt;not set&gt;  Gateway: 172.22.0.1 DNS Server: 172.22.0.2 Line Number: &lt;not set&gt;</pre>
------------	---------	--

Computador	PC2Esc2	IPv4 Address: 172.22.0.12/16 (Notação CIDR)
Computador	PC1BH	<pre> Device Name: PCFilial1 Device Model: PC-PT  Port          Link   IP Address FastEthernet0 Up    172.23.0.11/16 Bluetooth     Down  &lt;not set&gt;  Gateway: 172.23.0.1 DNS Server: 172.23.0.2 Line Number: &lt;not set&gt; </pre>
Computador	PC2BH	IPv4 Address: 172.23.0.12/16 (Notação CIDR)
Computador	PCRJ	<pre> Device Name: PCFilial2 Device Model: PC-PT  Port          Link   IP Address FastEthernet0 Up    172.24.0.11/16 Bluetooth     Down  &lt;not set&gt;  Gateway: 172.24.0.1 DNS Server: 172.24.0.2 Line Number: &lt;not set&gt; </pre>
Computador	PCRJ	IPv4 Address: 172.24.0.12/16 (Notação CIDR)
Computador	PCSP	<pre> Device Name: PCFilial3 Device Model: PC-PT  Port          Link   IP Address FastEthernet0 Up    172.25.0.11/16 Bluetooth     Down  &lt;not set&gt;  Gateway: 172.25.0.1 DNS Server: 172.25.0.2 Line Number: &lt;not set&gt; </pre>
Computador	PCBH	IPv4 Address: 172.25.0.12/16 (Notação CIDR)

#### 4.4 PLANILHA LINKS

A tabela abaixo contém informações correspondentes a divisão de colaboradores por cada localidade dentro da estrutura da empresa e da utilização da estrutura de rede quanto a aplicações e serviços. Atualmente, home office conta com a maior parte dos colaboradores, sendo 300 pessoas e não gerando custos de rede para a empresa; São Paulo conta com 250 colaboradores, Belo Horizonte com 200 e no Rio de Janeiro temos 180.

APPs	LB (kbps)	BELO HORIZONTE		SÃO PAULO		RIO DE JANEIRO		HOME OFFICE	
		Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB
Web	100	200	20000	250	25000	180	18000	0	0
E-mail	50	200	10000	250	12500	180	9000	0	0
Bankline	100	20	2000	20	2000	20	2000	0	0
Suporte	80	3	240	3	240	3	240	0	0
Videoconferência	500	20	10000	20	10000	20	10000	0	0
AWS	100	200	20000	250	25000	180	18000	0	0
<hr/>									
ERP	50	20	1000	20	1000	20	1000	0	0
CRM	50	23	1150	23	1150	23	1150	0	0
Sistema Operativo	90	200	18000	250	22500	180	16200	0	0
Sistema de Gestão de Operações	60	20	1200	20	1200	20	1200	0	0
Sistema para Gestão de Vendas	50	0	0	0	0	0	0	0	0
Recrutamento e Seleção e Admissão	40	0	0	0	0	0	0	0	0
<b>TOTAL LINK INTERNET</b>		<b>62240</b>		<b>74740</b>		<b>57240</b>		<b>0</b>	
<b>TOTAL LINK DE DADOS</b>		<b>21350</b>		<b>25850</b>		<b>19550</b>		<b>0</b>	
<b>TOTAL</b>		<b>83590</b>		<b>100590</b>		<b>76790</b>		<b>0</b>	
		<b>BH</b>		<b>SP</b>		<b>RJ</b>		<b>HOME OFFICE</b>	

## 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:

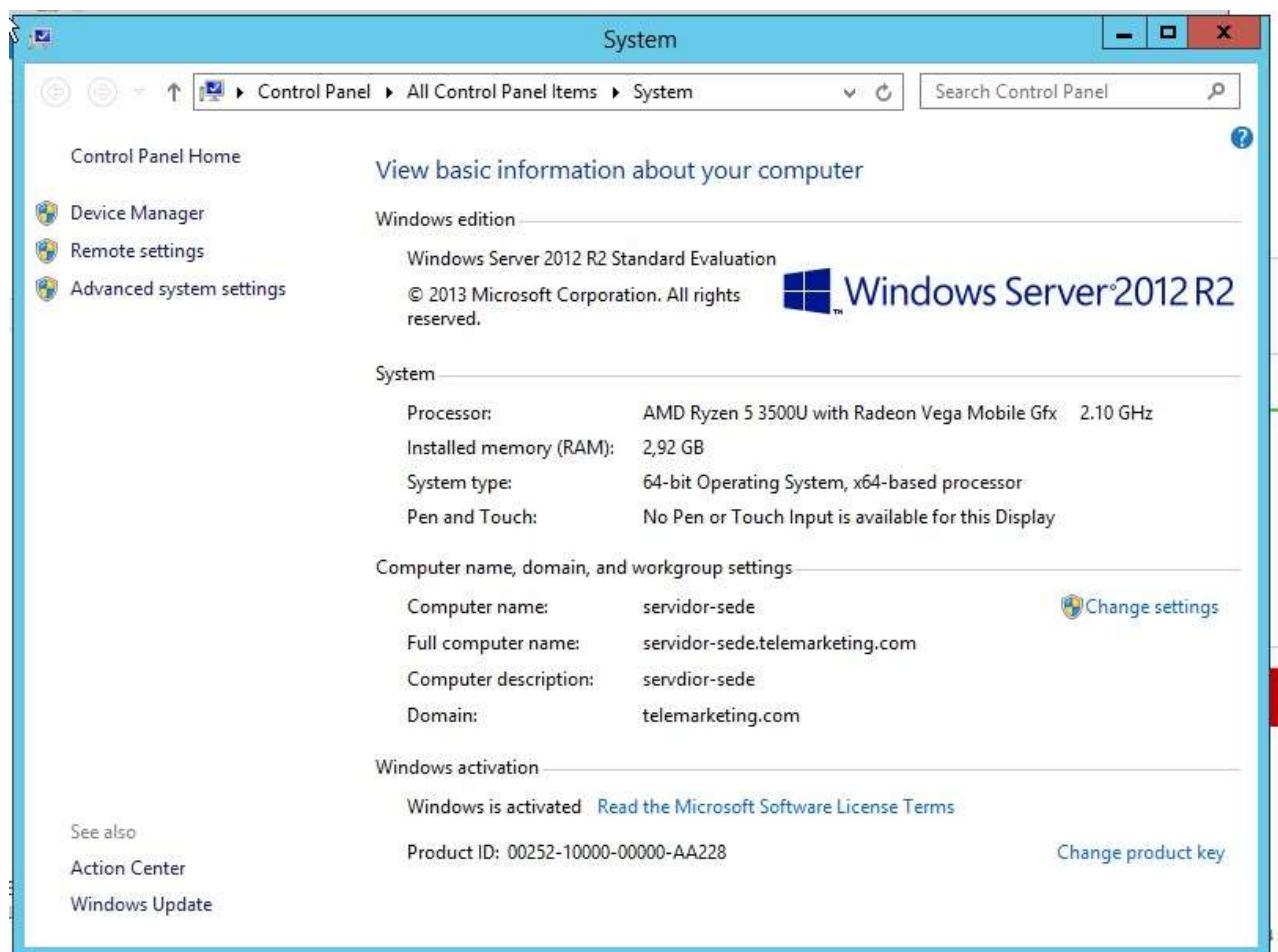
Sistema Operacional: Windows Server 2012 R2 64 bits

CPU: AMD Ryzen 5 3500 U 2.10 GHz

Memória RAM: 2,92GB

Nome do servidor: ServerMatrizLoc01

Domínio: telemarketing.com >



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

#### Credenciais de acesso:

**Usuário:** Administrador

**Senha:** puc@2024

**Dashboard**

- Local Server
- All Servers
- AD DS
- DHCP
- DNS
- File and Storage Services
- IIS
- Remote Access

## WELCOME TO SERVER MANAGER



1 Configure this local server

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group



Hide

## ROLES AND SERVER GROUPS

Roles: 6 | Server groups: 1 | Servers total: 1

AD DS 1 Manageability Events Services Performance BPA results	DHCP 1 Manageability Events Services Performance BPA results	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services 1 Manageability Events Services Performance BPA results
IIS 1 Manageability	Remote Access 1 Manageability	Local Server 1 Manageability	All Servers 1 Manageability

## Internet Protocol Version 4 (TCP/IPv4) Properties

## General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

 Obtain an IP address automatically Use the following IP address:

IP address: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

 Obtain DNS server address automatically Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 2

Alternate DNS server: . . .

 Validate settings upon exit

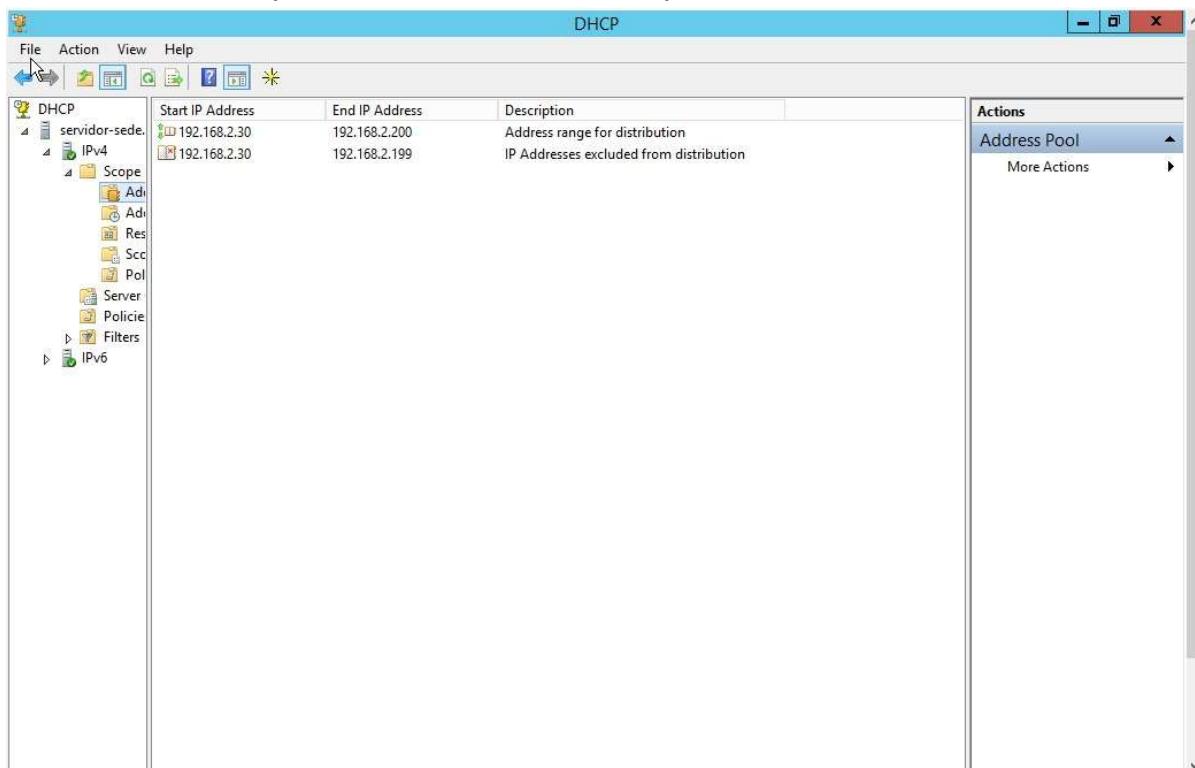
Advanced...

OK

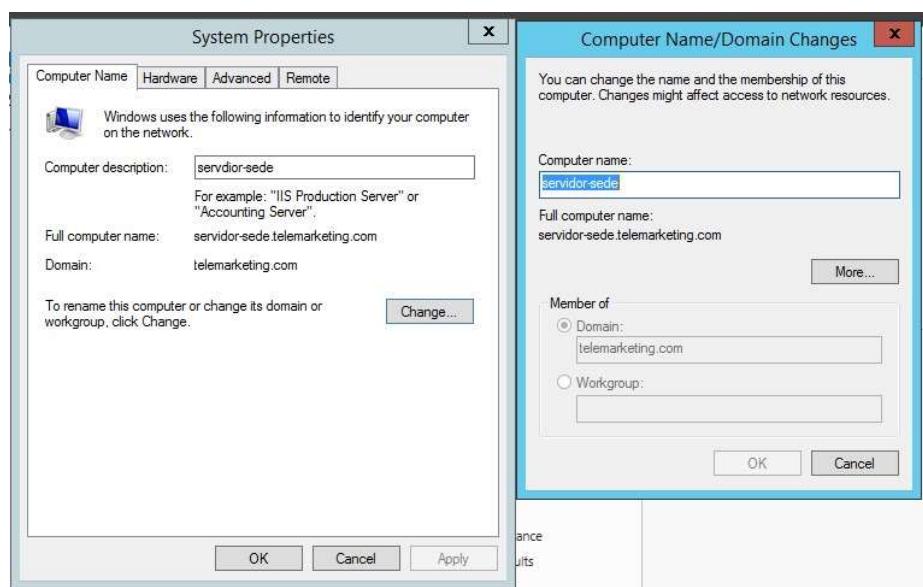
Cancel

### 5.1.1 CONFIGURAÇÃO DO IP

Foi configurado os primeiros IP'S para serem da gerencia e com a mascara 255.255.255.224 para não serem acessíveis pelo service desk



Fonte: autoria própria



File Action View Help



Active Directory Users and Computers
Saved Queries
telemarketing.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
home office
usuarios
computadores
Managed Service Accounts
sede-sp
usuarios
computadores
unidade-bh
computadores
usuario
unidade-rj
computadores
usuarios
Users

Name	Type	Description
------	------	-------------

servicedesk-...	Computer
server-bh	Computer
gerencia-bh	Computer



Usuários ativos. Fonte: autoria própria

Usuários ativos. Fonte: autoria própria

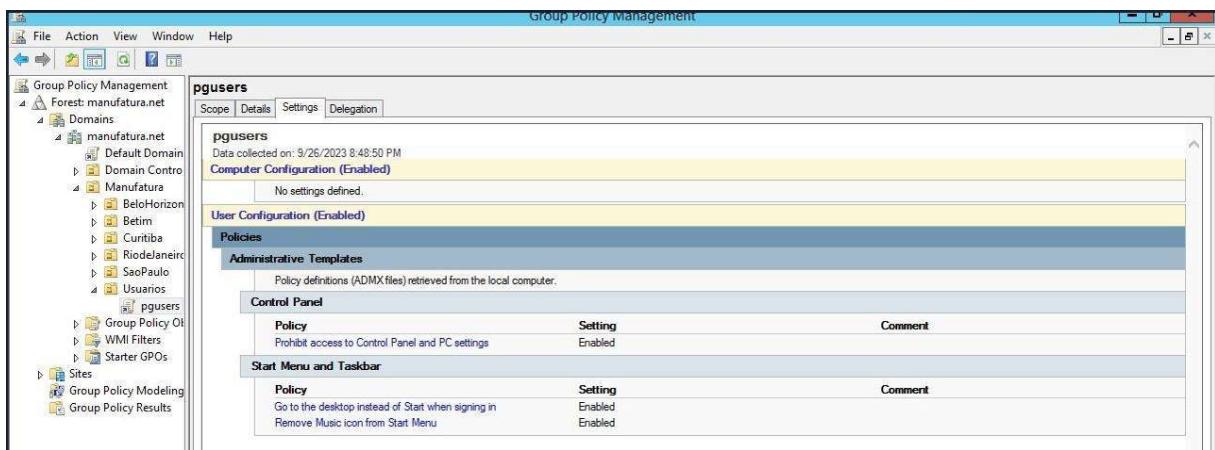
The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'telemarketing.com'. The right pane shows a table of active users:

Name	Type	Description
funcionario ...	User	
gerente bh.	User	
receppcionist...	User	

### 5.1.2 POLÍTICAS DE GRUPO APLICADAS

Foram aplicadas as políticas abaixo:

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



Políticas Aplicadas. Fonte: autoria própria

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

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

Na 1<sup>a</sup> etapa foi a criação de uma rede virtual (VPC) para a configuração dos recursos da rede. A criação da VPC permitirá a alocação do servidor dentro da rede G10-telemarketing-vpc criada.

**Painel EC2**

Visualização Global do EC2

Eventos

Console-to-Code [Prévia](#)

**Instâncias**

- Instâncias
- Tipos de instância
- Modelos de execução
- Solicitações spot
- Savings Plans
- Instâncias reservadas
- Hosts dedicados
- Reservas de capacidade
- [Novo](#)

**Imagens**

- AMIs
- Catálogo de AMIs

**Elastic Block Store**

- Volumes
- Snapshots
- Lifecycle Manager

**Rede e segurança**

- Security groups
- IPs elásticos
- Placement groups
- Pares de chaves
- Interfaces de rede

**Balanceamento de carga**

- Load balancers
- Grupos de destino

**Recursos**

Você está usando os seguintes recursos do Amazon EC2 na Região Leste dos EUA (Norte da Virginia):

Instâncias (em execução)	1	Grupos de posicionamento	0	Grupos de segurança	3
Grupos do Auto Scaling	0	Hosts dedicados	0	Instâncias	1
IPs elásticos	0	Load balancers	0	Pares de chaves	2
Snapshots	0	Volumes	1		

**Executar instância**

Para começar, execute uma instância do Amazon EC2, que é um servidor virtual na nuvem.

[Executar instância](#) [Migrar um servidor](#)

Observação: suas instâncias serão executadas na Região Leste dos EUA (Norte da Virginia)

**Integridade do serviço**

AWS Health Dashboard

Região: Leste dos EUA (Norte da Virginia) Status: Este serviço está funcionando normalmente

**Zonas**

Nome da zona	ID da zona
us-east-1a	use1-az4
us-east-1b	use1-az6
us-east-1c	use1-az1
us-east-1d	use1-az2
us-east-1e	use1-az3
us-east-1f	use1-az5

[Habilitar zonas locais adicionais](#)

**Alarmes de instância**

Exibir no CloudWatch

0 em alarme 0 OK 0 dados insuficientes

**Eventos agendados**

Leste dos EUA (Norte da Virginia)  
Nenhum evento programado

**Migrar um servidor**

**Atributos da conta**

VPC padrão: vpc-075be8d08cc7132

**Configurações**

- Proteção e segurança de dados
- Zonas
- Console serial do EC2
- Especificação de crédito padrão
- Experimentos com o console

**Informações adicionais**

Guia de conceitos básicos Documentação Todos os recursos do EC2 Fóruns Definição de preço Entre em contato conosco

**Painel da VPC**

Visualização global do EC2

Filtrar por VPC: [Selecionar uma VPC](#)

**Nuvem privada virtual**

**Suas VPCs**

- Sub-redes
- Tabelas de rotas
- Gateways da Internet
- Gateways da Internet somente de saída
- Gateways da operadora
- Conjuntos de opções de DHCP
- IPs elásticos
- Listas de prefixos gerenciados
- Endpoints
- Serviços de endpoint
- Gateways NAT
- Conexões de emparelhamento

**Segurança**

- ACLs da rede
- Grupos de segurança

**Firewall de DNS**

- Grupos de regras
- Listas de domínios

**Detalhes**

ID da VPC: [vpc-04a7e10e439b9fada](#) Estado: Available

Locação: Default

VPC padrão: Não

Métricas de uso do endereço de rede: Desabilitado

Estado: Available

Conjunto de opções de DHCP: [dopt-054d7691bb7d72f9ce](#)

CIDR IPv4: 10.0.0.0/16

Grupos de regras do Firewall de DNS do resolvidor do Route 53: Falha ao carregar grupos de regras

Nomes de host DNS: Habilitado

Tabela de rota principal: [rtb-0dec70bd524624d9c](#)

Grupo IPv6: -

ID do proprietário: [788895827698](#)

Resolução de DNS: Habilitado

Network ACL principal: [acl-07d6a7ea5bd9443f](#)

CIDR IPv6 (Grupo de borda de rede): -

**Mapa de recursos**

**VPC** Mostrar detalhes Sua rede virtual da AWS

**Sub-redes (4)** Sub-redes dentro dessa VPC

**us-east-1a**

- G10 - Telemarketing-subnet-public...
- G10 - Telemarketing-subnet-private1-us...

**us-east-1b**

- G10 - Telemarketing-subnet-public...
- G10 - Telemarketing-subnet-private2-us...

**Tabelas de rotas (4)** Rotear o tráfego de rede para recursos

- G10 - Telemarketing-rtb-public
- G10 - Telemarketing-rtb-private1-us...
- G10 - Telemarketing-rtb-private2-us...
- rtb-0dec70bd524624d9c

**Conexões de rede (1)** Conexões com outras redes

G10 - Telemarketing-igw

© 2024, Amazon Web Services, Inc. ou suas afiliadas. [Privacidade](#) [Termos](#) [Preferências de cookies](#)

Screenshot of the AWS EC2 Instance Details page for instance i-0dd8364fa99542cad (G10webServer).

**Instance Summary:**

- ID da instância:** i-0dd8364fa99542cad (G10webServer)
- Endereço IPv4 público:** 3.93.188.52 | endereço aberto
- Estado da instância:** Executando
- Nome do DNS de IP privado (somente IPv4):** ip-10-0-0-174.ec2.internal
- Tipo de instância:** t2.large
- ID da VPC:** vpc-04a7e10e459b9fada (G10 - Telemarketing-vpc)
- Endereço IP atribuído automaticamente:** 3.93.188.52 [IP público]
- ID da sub-rede:** subnet-00ef111dd87c4389d (G10 - Telemarketing-subnet-public1-us-east-1a)

**Details Tab (Selected):**

- Plataforma:** windows
- ID da AMI:** ami-05821768380ccca45
- Nome da AMI:** Windows\_Server-2016-English-Full-Base-2024.04.10
- Data de lançamento:** Tue Apr 23 2024 18:08:28 GMT-0300 (Horário Padrão de Brasília) (5 minutes)
- Monitoramento:** desativado
- Proteção contra encerramento:** Desabilitado
- Local da AMI:** amazon/Windows\_Server-2016-English-Full-Base-2024.04.10

**Navigation:** EC2 > Instâncias > i-0dd8364fa99542cad

Subredes na AWS. Fonte:AWS

A 2<sup>a</sup> etapa consistiu na criação de um grupo de segurança para atuar como um firewall de nossa rede. Criamos 3 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.

Name	ID do grupo de segurança	Nome do grupo de segurança	ID da VPC	Descrição	Proprietário
-	<a href="#">sg-017b91e8a693a9168</a>	default	<a href="#">vpc-04a7e10e439b9fada</a>	default VPC security group	788895827698
-	<a href="#">sg-058edfd54c9d0d517</a>	G10sec	<a href="#">vpc-04a7e10e439b9fada</a>	Web e Terminal remoto	788895827698
-	<a href="#">sg-042a8885bc5826a6c</a>	default	<a href="#">vpc-0975be88d08cc7132</a>	default VPC security group	788895827698

Grupos de Segurança. Fonte: AWS

**Grupos de segurança (3) Informações**

Name	ID do grupo de segurança	Nome do grupo de segurança	ID da VPC	Descrição	Proprietário
-	sg-012b91e8a693a9168	default	vpc-04a7e10e459b9fada	default VPC security group	788895827698
-	sg-058edfd54c9d0517	G10sec	vpc-04a7e10e459b9fada	Web e Terminal remoto	788895827698
-	sg-047a885bc5826a6c	default	vpc-0975be88d08cc7132	default VPC security group	788895827698

**sg-012b91e8a693a9168 - default**

**Regras de entrada (1)**

Name	ID da regra do grupo...	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
-	sgr-09ea8c165ebbf90d	-	Todo o tráfego	Tudo	Tudo	sg-012b91e8a693a91...	-

### 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 G10webServer.

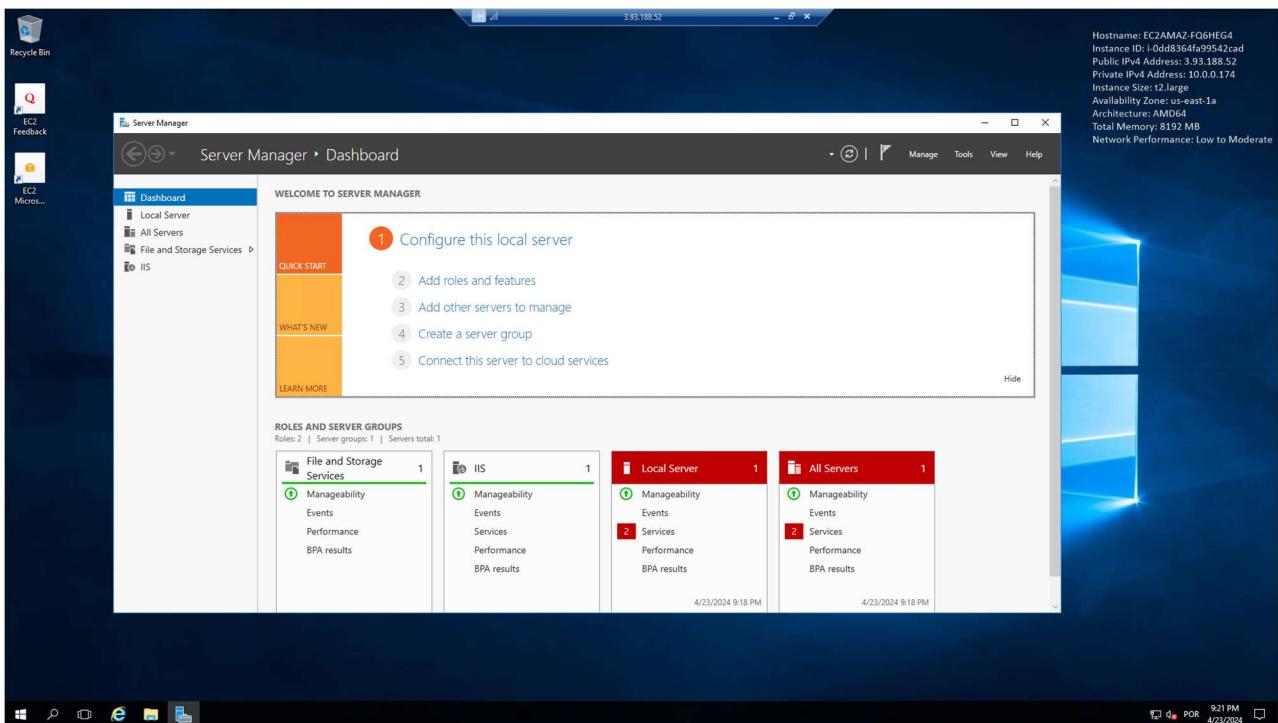
**Instâncias (1) Informações**

Name	ID da instância	Estado da inst...	Tipo de inst...	Verificação de sta...	Status do alarn...	Zona de dispon...	DNS IPv4 público	Endereço IP...	IP elástico
G10webServer	i-0dd8364f995542cad	Executando	t2.large	Inicializando	Exibir alarmes	us-east-1a	ec2-3-93-180-52.comp...	3.93.180.52	-

**Selecionar uma instância**

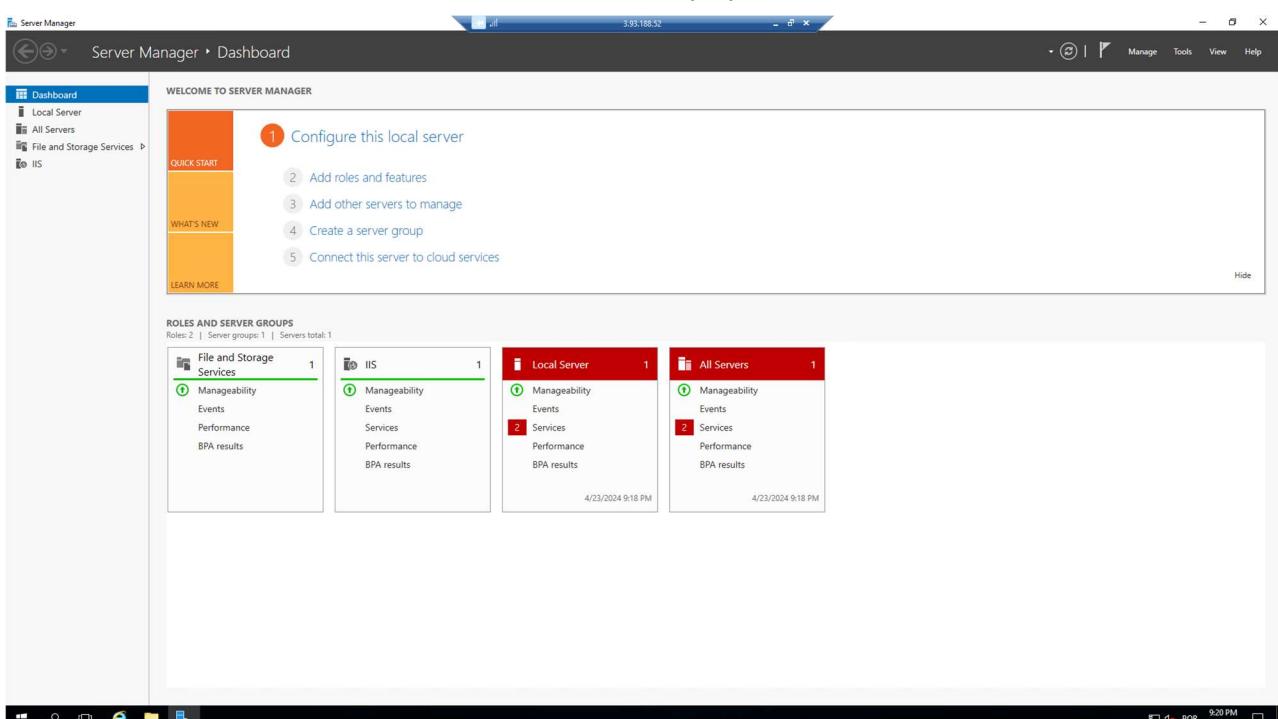
### Instância do Servidor Web. Fonte: AWS

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



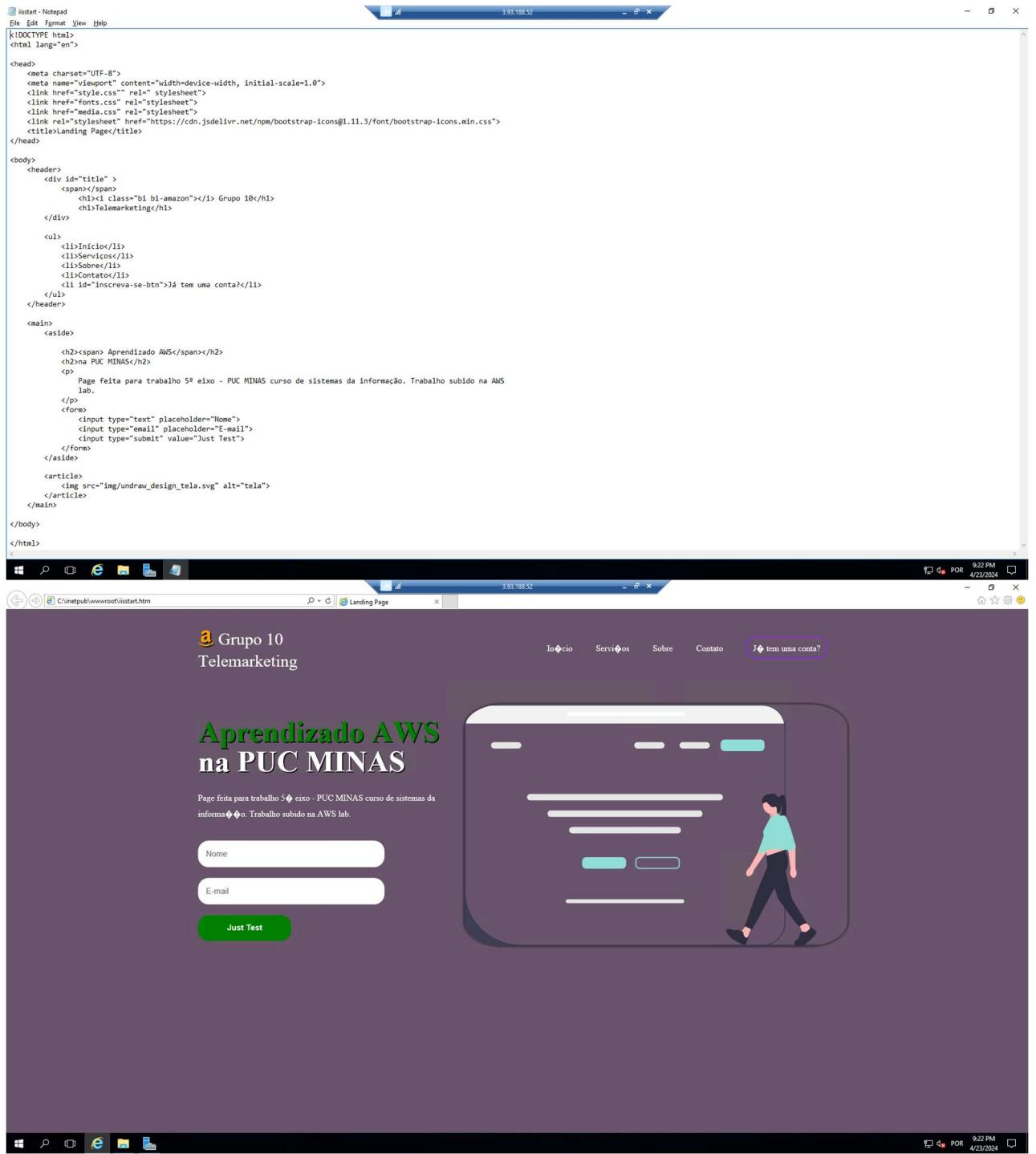
Acesso via RDP ao servidor.

Fonte: autoria própria



Serviço IIS disponível no servidor. Fonte: Autoria própria.

Fizemos a 5ª etapa para a modelagem da página do servidor. Utilizamos as últimas versões do HTML5 e CSS3.



```
Notepad - Notepad
File Edit Format View Help
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="style.css" rel="stylesheet">
    <link href="fonts.css" rel="stylesheet">
    <link href="media.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.min.css">
    <title>Landing Page</title>
</head>
<body>
    <header>
        <div id="title" >
            <span></span>
            <h1>i class="bi bi-amazon"</i> Grupo 10</h1>
            <h1>Telemarketing</h1>
        </div>
        <ul>
            <li>Início</li>
            <li>Serviços</li>
            <li>Sobre</li>
            <li>Contato</li>
            <li id="inscreva-se-btn">Já tem uma conta?</li>
        </ul>
    </header>
    <main>
        <aside>
            <h2><span> Aprendizado AWS</span></h2>
            <h2>PUC MINAS</h2>
            <p>Page feita para trabalho 5º eixo - PUC MINAS curso de sistemas da informação. Trabalho subido na AWS lab.</p>
            </p>
            <form>
                <input type="text" placeholder="Nome">
                <input type="email" placeholder="E-mail">
                <input type="submit" value="Just Test">
            </form>
        </aside>
        <article>
            
    </main>
</body>
</html>
```

The screenshot shows a Windows desktop environment. At the top, there is a Notepad window titled "Notepad" containing the provided HTML code. Below it is a browser window titled "Landing Page" with the URL "C:\inetpub\wwwroot\uisstart.htm". The browser displays a dark-themed landing page for "Grupo 10 Telemarketing". The page features a header with a logo and navigation links for "Início", "Serviços", "Sobre", and "Contato". A prominent call-to-action button labeled "Já tem uma conta?" is highlighted with a purple border. The main content area includes a heading "Aprendizado AWS na PUC MINAS", a brief description, and a form with fields for "Nome" and "E-mail", followed by a green "Just Test" button. To the right of the form is a stylized illustration of a person walking past a smartphone screen displaying a user interface with several input fields and buttons.

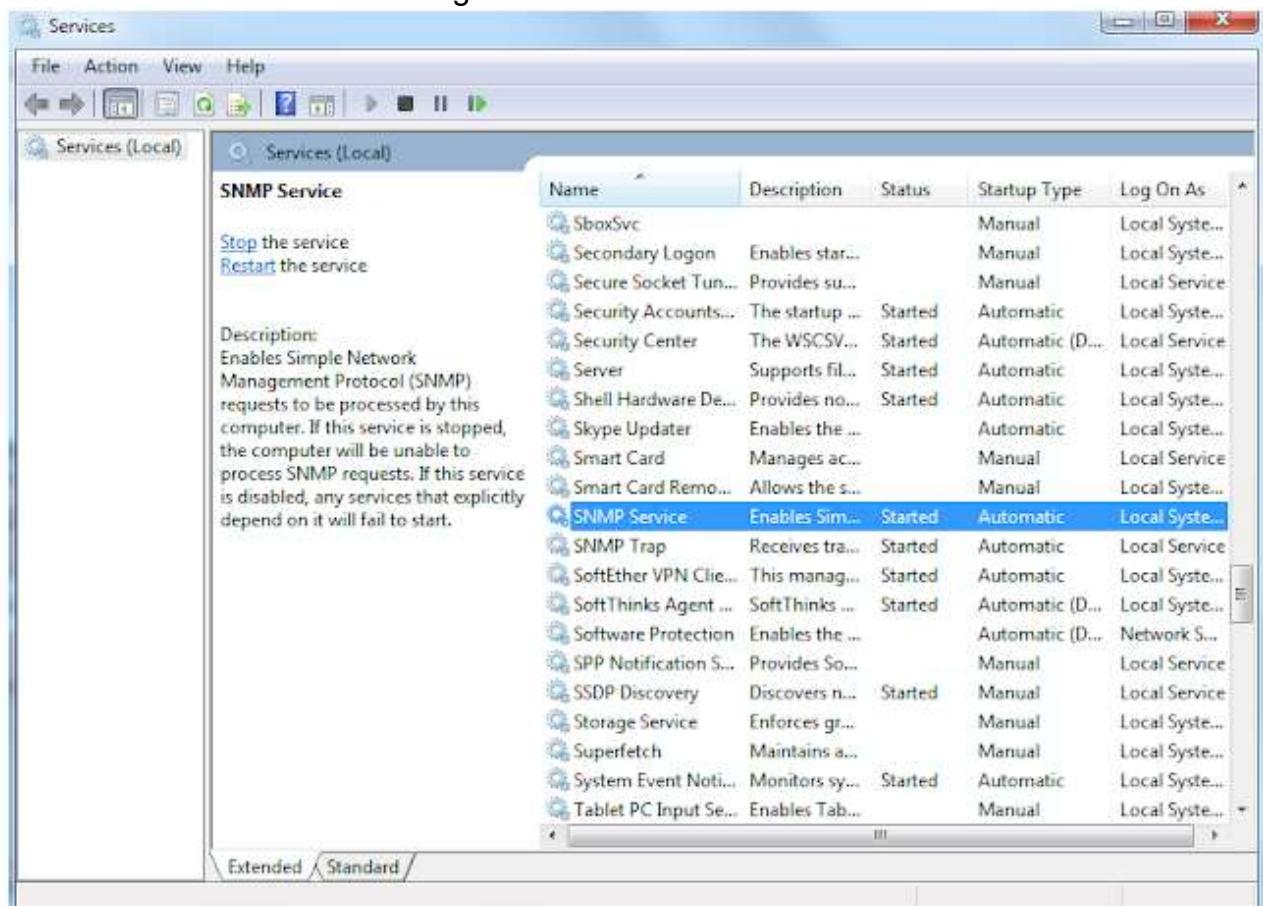
Acesso a página do servidor web pelo navegador. Fonte: autoria própria

## 6. GERENCIAMENTO DOS SERVIDORES NO ZABBIX

### 6.1 GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX

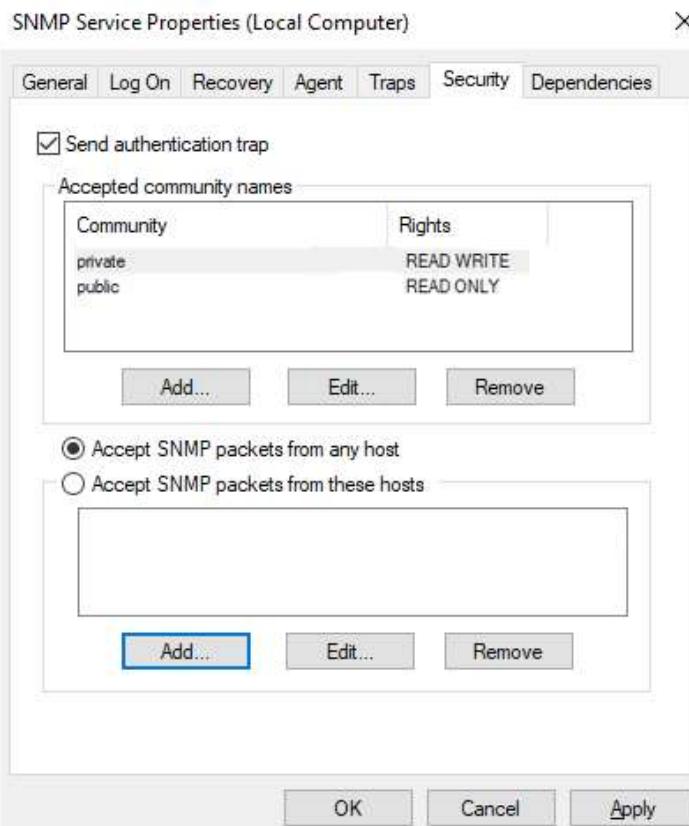
Para habilitarmos o monitoramento do servidor físico na rede, foi essencial integrá-lo ao Zabbix, uma ferramenta de monitoramento de infraestrutura de TI amplamente utilizada. Para essa integração, recorremos ao protocolo SNMP, uma escolha sólida devido à sua capacidade de gerenciar dispositivos em uma rede por meio de seus endereços IP.

Conforme ilustrado na representação abaixo, configuramos o serviço SNMP no servidor local, estabelecendo duas comunidades com distintas strings: "privada" para acesso de leitura e escrita e "pública" para acesso exclusivo de leitura. Essas strings atuam como chaves de acesso, permitindo a conexão do servidor ao software Zabbix, possibilitando um monitoramento eficiente e abrangente de sua infraestrutura.



Serviço de SNMP no servidor local.

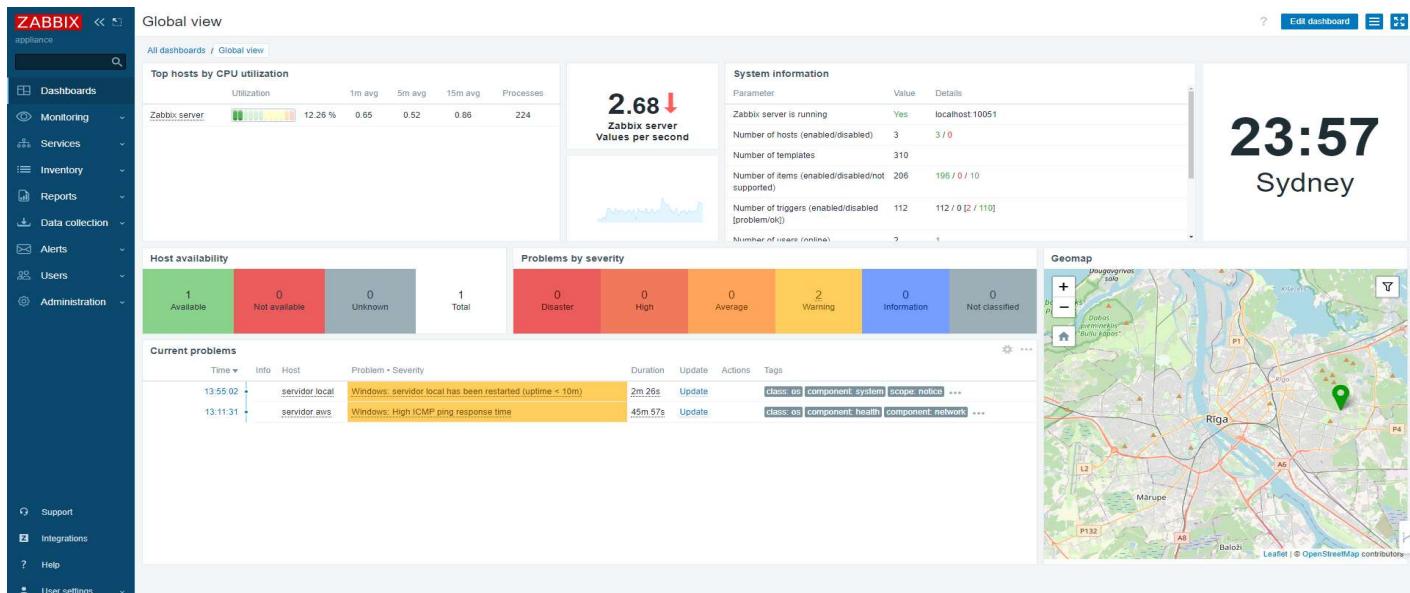
Fonte: autoria própria



Serviço de SNMP no servidor local.

Fonte: autoria própria

Com a configuração realizada tanto no servidor local quanto no servidor da nuvem, o Zabbix já estava operacional, monitorando os servidores. Durante nossa análise na ferramenta, constatamos que todas as comunicações com os hosts estavam sendo executadas sem qualquer falha, conforme evidenciado nas imagens abaixo.



Adição do servidor local na plataforma Zabbix.

Fonte: autoria própria

SNMP no servidor localizado em nuvem

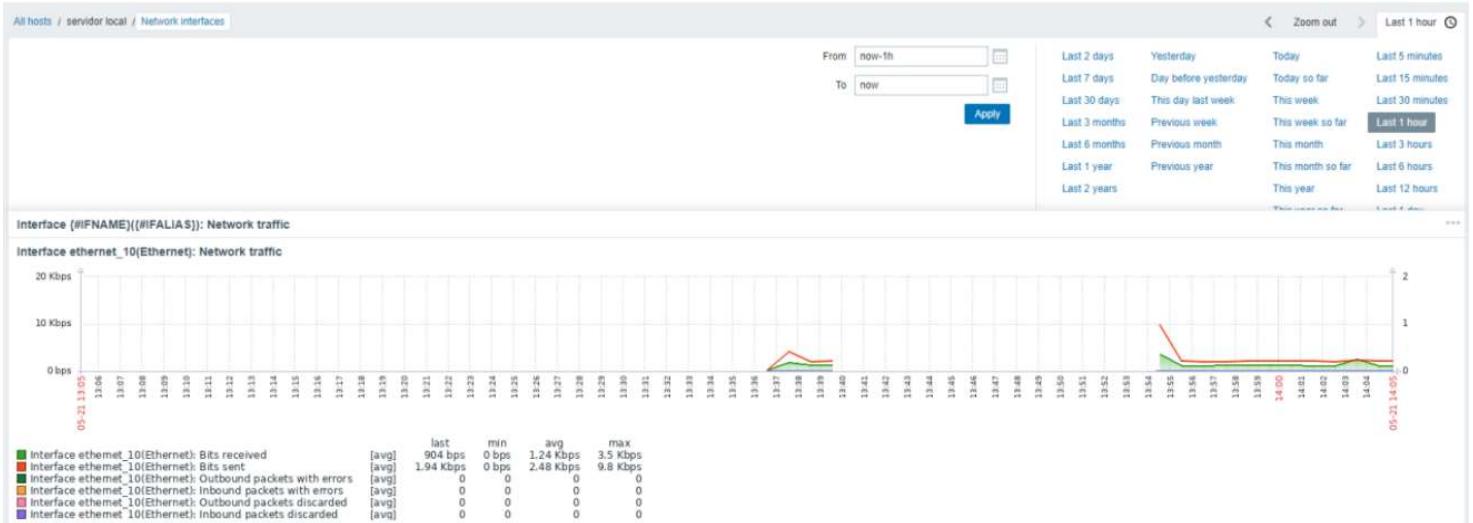
Fonte: Autoria própria

Visualização dos dados coletados e problemas encontrados no Zabbix.

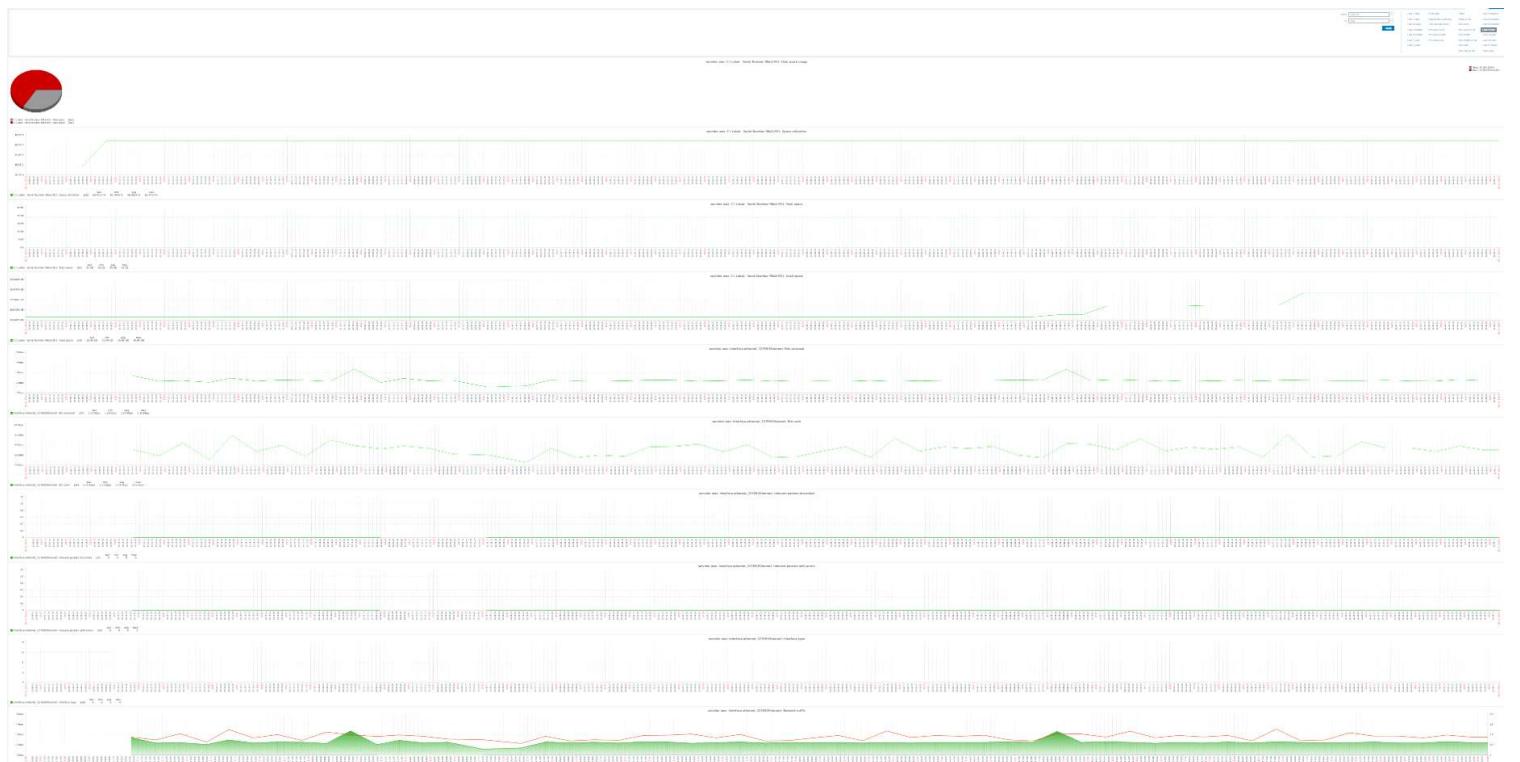
Fonte: Autoria própria

Nos gráficos abaixo, apresentamos os resultados do monitoramento dos dois hosts: o servidor local e o servidor da nuvem. As visualizações mostram a quantidade de tráfego de rede gerada por ambos os servidores ao longo da última hora. Esses dados fornecem uma perspectiva clara sobre o volume de atividade de rede de cada servidor, permitindo uma análise comparativa e a identificação de padrões ou anomalias relevantes para a gestão eficaz da infraestrutura.

## Network interfaces



Monitoramento do tráfego de rede do servidor AWS.  
Fonte: Autoria própria



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

## 6.2 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX

As capturas de tela abaixo ilustram os dados mais recentes recuperados pelo Zabbix. Essas informações fornecem uma visão atualizada do estado de nossos sistemas e recursos monitorados. Ao analisar esses dados no Zabbix, podemos obter insights valiosos sobre o desempenho, a disponibilidade e a saúde de nossos servidores e serviços. Essa visão em tempo real é essencial para garantir a estabilidade e a eficiência de nossa infraestrutura, permitindo-nos tomar medidas proativas para resolver quaisquer problemas que possam surgir.

The screenshot shows the Zabbix interface for monitoring a host named 'Zabbix server'. The left sidebar contains navigation links for Dashboards, Monitoring (selected), Problems, Hosts, Latest data (selected), Maps, Discovery, Services, Inventory, Reports, Data collection, Alerts, Users, and Administration. The main content area is titled 'Latest data' and includes sections for 'HOSTS', 'TAGS', 'TAG VALUES', and 'DATA'. The 'HOSTS' section lists 'servidor\_aws' (30), 'servidor\_local' (30), and 'Zabbix server' (146). The 'TAGS' section lists 'component' (206), 'description' (10), 'disk' (6), 'Filesystem' (30), and 'interface' (27). The 'TAG VALUES' section provides a detailed breakdown of these tags. The 'DATA' section displays a table of recent monitoring data for the 'Zabbix server' host, showing metrics like 'Filesystem is read-only', 'Free inodes in %', 'Get filesystem data', 'Space utilization', 'Total space', 'Used space', and 'Used space /boot'. Each row includes columns for Host, Name, Last check, Last value, Change, Tags, and Info/Graph/Histroy links.

Host	Name	Last check	Last value	Change	Tags	Info
Zabbix server	/: Filesystem is read-only	5s	0		component, storage, Filesystem, /	Graph
Zabbix server	/: Free inodes in %	5s	98.8283 %		component, storage, Filesystem, /	Graph
Zabbix server	/: Get filesystem data	5s	{"filename": "/", "options": "rw,...		component, raw, component, storage, Filesystem, /	History
Zabbix server	/: Space utilization	5s	25.2034 %		component, storage, Filesystem, /	Graph
Zabbix server	/: Total space	5s	3.99 GB		component, storage, Filesystem, /	Graph
Zabbix server	/: Used space	5s	1.01 GB		component, storage, Filesystem, /	Graph
Zabbix server	/boot: Filesystem is read-only	5s	0		component, storage, Filesystem, /boot	Graph

Tabela com retornos mais recentes feitos pelo Zabbix.

Fonte: Autoria própria

<input type="checkbox"/> Host	Name ▾	Last check	Last value	Change	Tags	Graph
Zabbix server	/: Filesystem is read-only	5s	0		component: storage   filesystem: /	Graph
Zabbix server	/: Free inodes in %	5s	98.8283 %		component: storage   filesystem: /	Graph
Zabbix server	/: Get filesystem data	5s	{"fsname": "/", "options": "rw", "type": "ext4"}		component: raw   component: storage   filesystem: /	History
Zabbix server	/: Space utilization	5s	25.2034 %		component: storage   filesystem: /	Graph
Zabbix server	/: Total space	5s	3.99 GB		component: storage   filesystem: /	Graph
Zabbix server	/: Used space	5s	1.01 GB		component: storage   filesystem: /	Graph
Zabbix server	/boot: Filesystem is read-only	5s	0		component: storage   filesystem: /boot	Graph
Zabbix server	/boot: Free inodes in %	5s	99.0417 %		component: storage   filesystem: /boot	Graph
Zabbix server	/boot: Get filesystem data	5s	{"fsname": "/boot", "options": "rw", "type": "ext4"}		component: raw   component: storage   filesystem: /boot	History
Zabbix server	/boot: Space utilization	5s	10.9631 %		component: storage   filesystem: /boot	Graph
Zabbix server	/boot: Total space	5s	487.21 MB		component: storage   filesystem: /boot	Graph
Zabbix server	/boot: Used space	5s	49.48 MB		component: storage   filesystem: /boot	Graph
Zabbix server	/tmp: Filesystem is read-only	5s	0		component: storage   filesystem: /tmp	Graph
Zabbix server	/tmp: Free inodes in %	5s	99.9968 %		component: storage   filesystem: /tmp	Graph
Zabbix server	/tmp: Get filesystem data	5s	{"fsname": "/tmp", "options": "rw,exec"}		component: raw   component: storage   filesystem: /tmp	History
Zabbix server	/tmp: Space utilization	5s	3.8901 %		component: storage   filesystem: /tmp	Graph
Zabbix server	/tmp: Total space	5s	1014 MB		component: storage   filesystem: /tmp	Graph
Zabbix server	/tmp: Used space	5s	39.45 MB		component: storage   filesystem: /tmp	Graph
Zabbix server	/var/lib/mysql: Filesystem is read-only	5s	0		component: storage   filesystem: /var/lib/mysql	Graph
Zabbix server	/var/lib/mysql: Free inodes in %	5s	99.9836 %		component: storage   filesystem: /var/lib/mysql	Graph
Zabbix server	/var/lib/mysql: Get filesystem data	5s	{"fsname": "/var/lib/mysql", "options": "rw,exec"}		component: raw   component: storage   filesystem: /var/lib/mysql	History
Zabbix server	/var/lib/mysql: Space utilization	5s	20.11 %	+0.009519 %	component: storage   filesystem: /var/lib/mysql	Graph
Zabbix server	/var/lib/mysql: Total space	5s	4.49 GB		component: storage   filesystem: /var/lib/mysql	Graph
Zabbix server	/var/lib/mysql: Used space	5s	924.26 MB	+448 KB	component: storage   filesystem: /var/lib/mysql	Graph
servidor aws	C:\Label: Serial Number 98e2c951: Space utilization	4s	66.4723 %		component: storage   filesystem: C:\Label	Graph
servidor aws	C:\Label: Serial Number 98e2c951: Total space	20s	30 GB		component: storage   filesystem: C:\Label	Graph
servidor aws	C:\Label: Serial Number 98e2c951: Used space	20s	19.94 GB		component: storage   filesystem: C:\Label	Graph

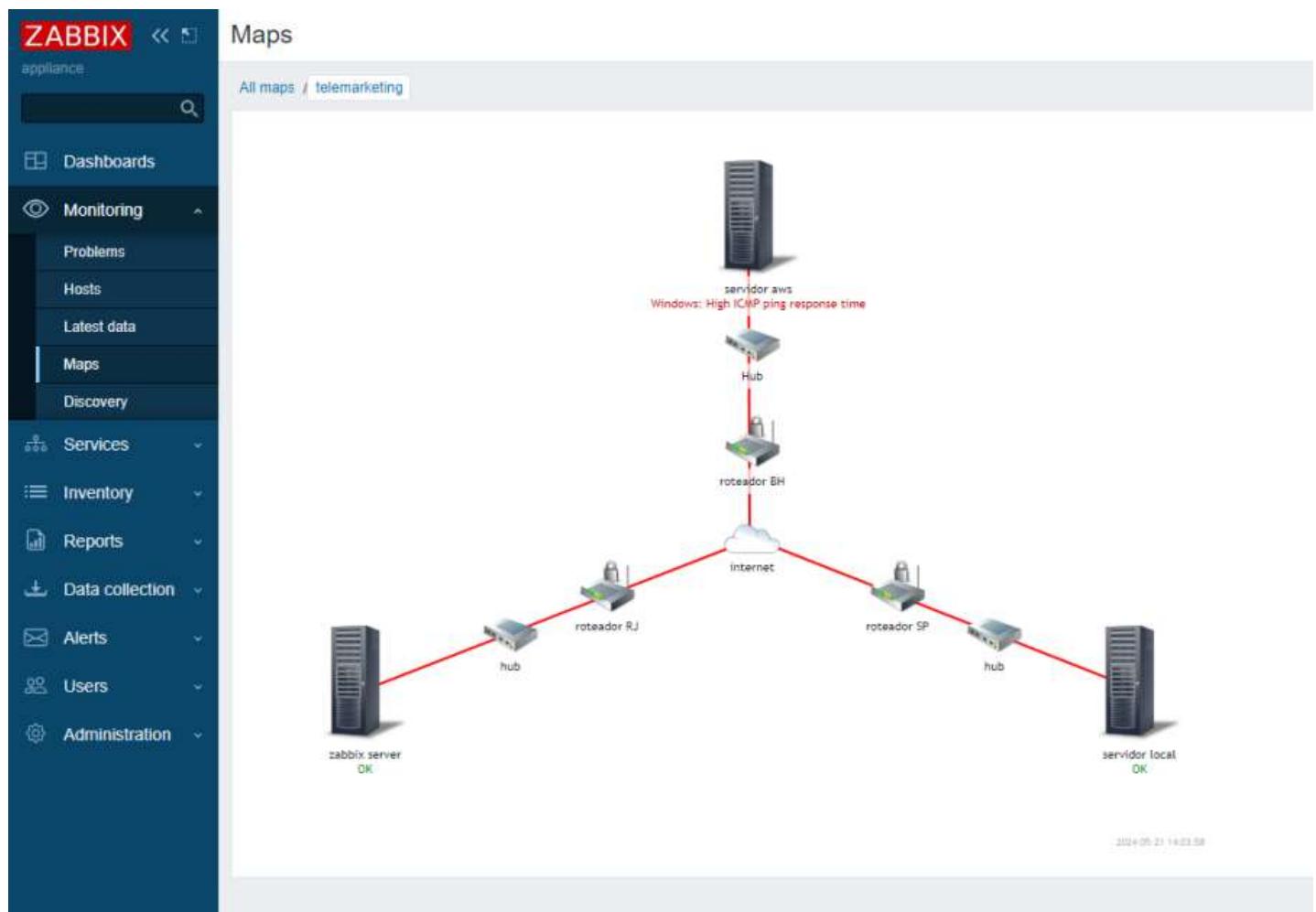
Tabela com retornos mais recentes feitos pelo Zabbix.

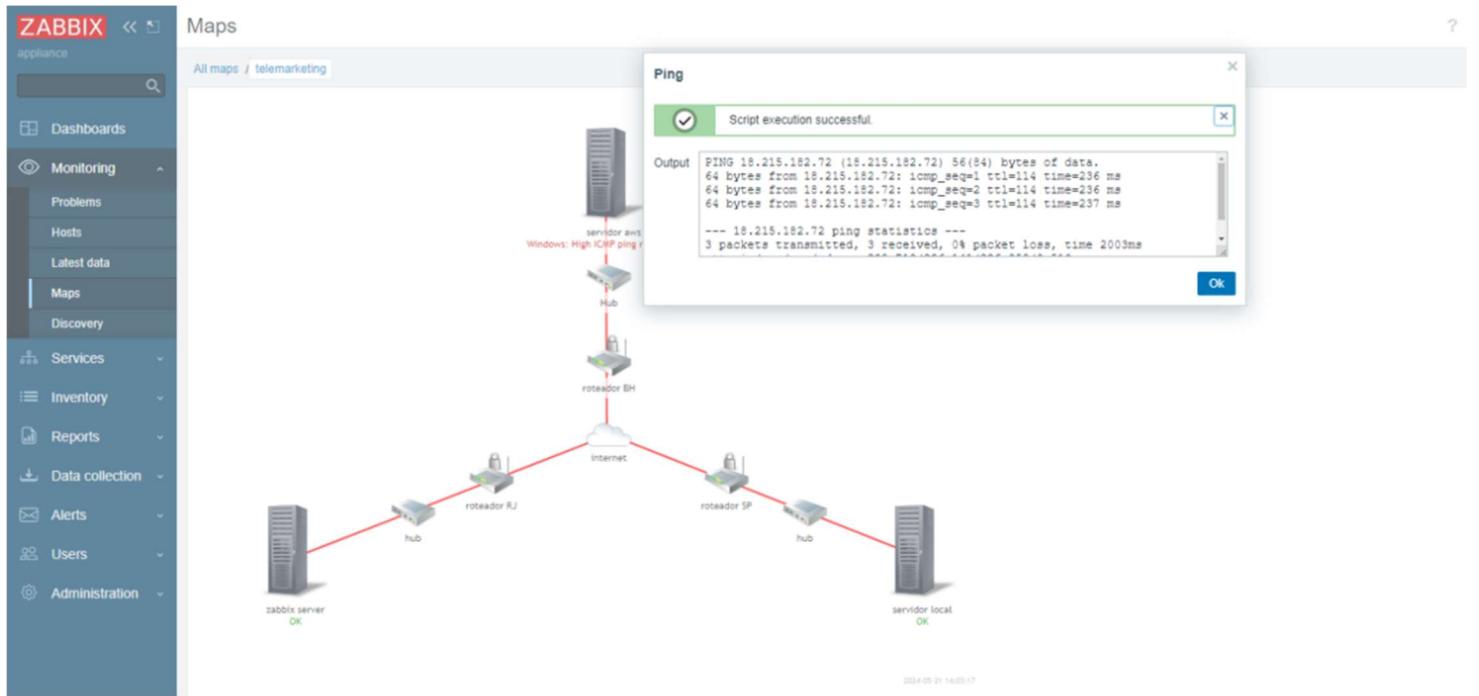
Fonte: Autoria própria

O Zabbix oferece a visualização de mapas da nossa rede monitorada. Na imagem abaixo, vemos o servidor do Zabbix conectado ao servidor local e à nuvem. Esse mapa fornece uma visão clara da arquitetura de rede, destacando as conexões entre os

componentes. É uma ferramenta crucial para identificar e responder rapidamente a problemas em nossos ambientes locais e na nuvem.

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





Mapa de rede da infraestrutura executado com sucesso no Zabbix.  
Fonte: Autoria própria

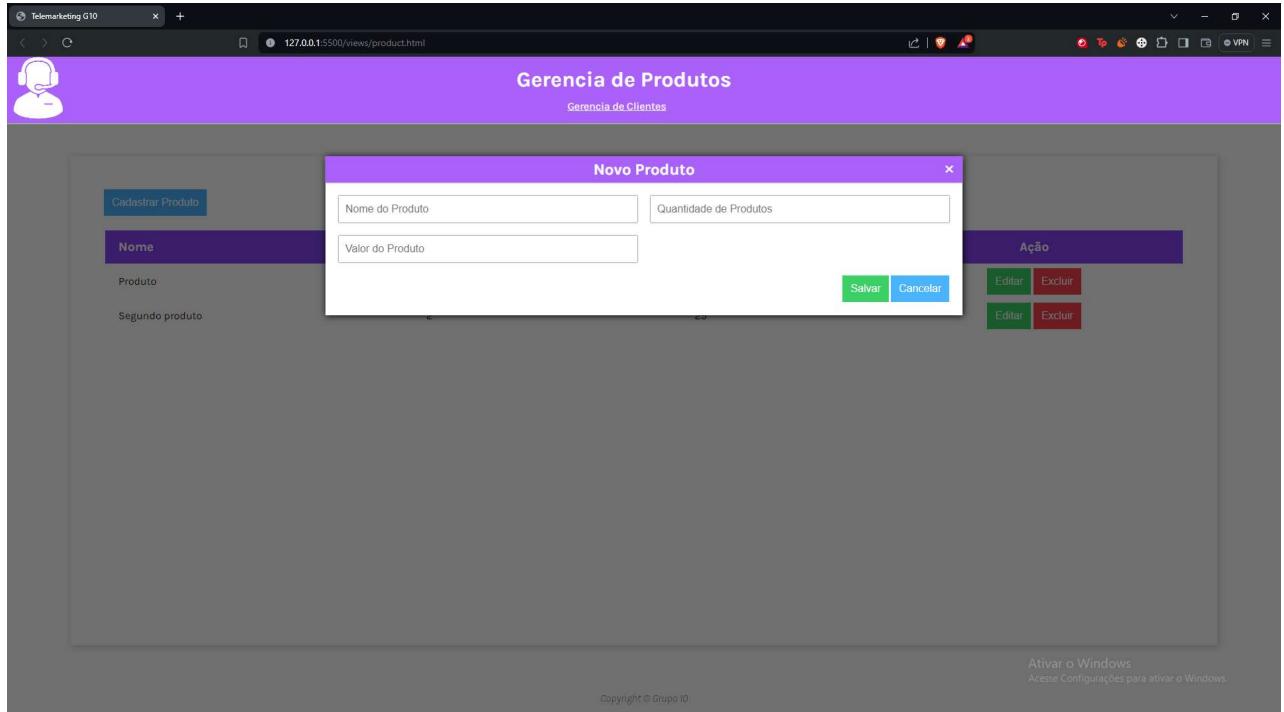
## 7. APLICAÇÃO BACK-END

As capturas de tela abaixo representam a aplicação back-end onde existem 2 CRUDs um para cadastro, edição dos produtos e outro com as mesmas funcionalidades para clientes. Para transicionar da tela de gerência de produtos para tela de gerência de clientes basta clicar no texto “Gerencia de Clientes”

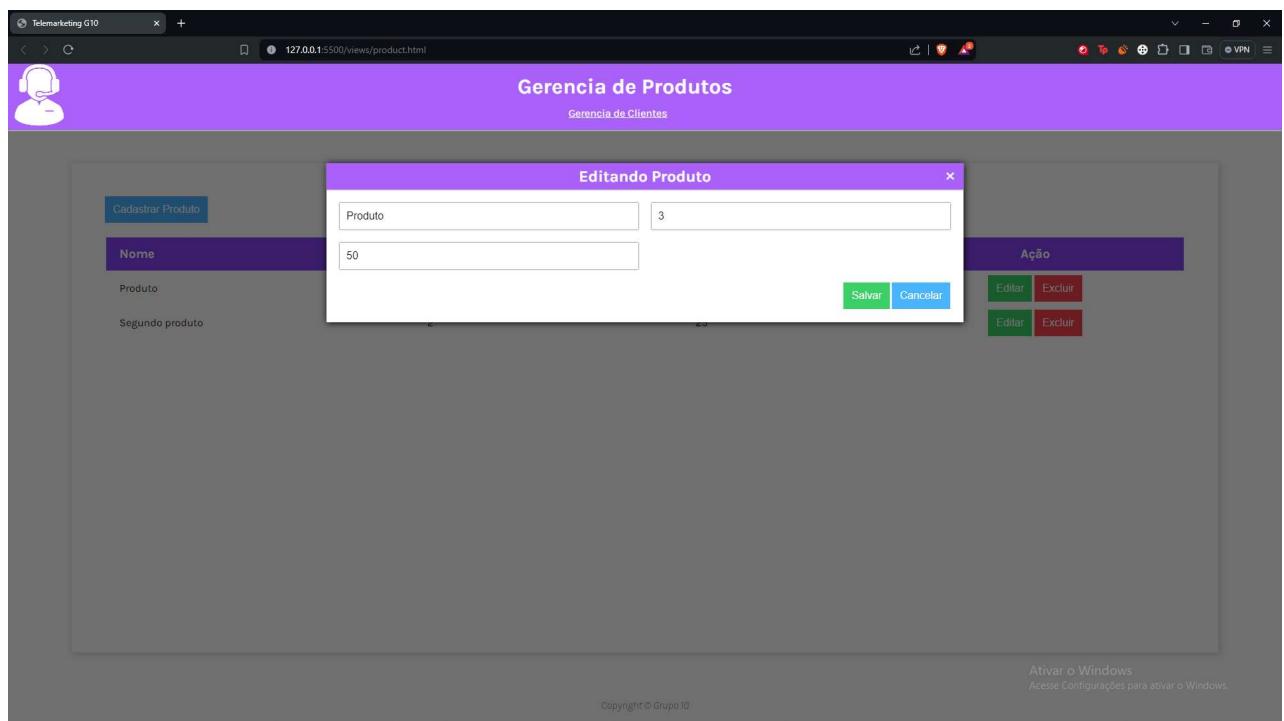
Nome	Quantidade	Valor R\$	Ação
Produto	3	50	<a href="#">Editar</a> <a href="#">Excluir</a>
Segundo produto	2	25	<a href="#">Editar</a> <a href="#">Excluir</a>

Página 01 - Lista de Produtos (Read)

A captura de tela abaixo é referente ao formulário para cadastro de produto, o qual possui campos para o nome do produto, quantidade de produtos e o valor do produto em questão,



Página 02 - Adicionar novo produto (Create)



Página 03 - Editar dados do produto (Update)

A screenshot of a web browser window titled "Telemarketing G10". The address bar shows the URL "127.0.0.1:500/views/product.html". A confirmation dialog box is displayed in the center, asking "Deseja realmente excluir o produto Produto?" with "OK" and "Cancelar" buttons. Below the dialog, a table lists products:

Nome	Quantidade	Valor R\$	Ação
Produto	3	50	<button>Editar</button> <button>Excluir</button>
Segundo produto	2	25	<button>Editar</button> <button>Excluir</button>

Ativar o Windows  
Acesse Configurações para ativar o Windows.

Copyright © Grupo 10

#### Página 04 - Remover um produto (Delete)

A screenshot of a web browser window titled "Telemarketing G10". The address bar shows the URL "127.0.0.1:500/views/client.html". The main title is "Gerencia de Clientes" and the subtitle is "Gerencia de Produtos". A confirmation dialog box is displayed in the center, asking "Deseja realmente excluir o cliente Tallys Winter?" with "OK" and "Cancelar" buttons. Below the dialog, a table lists clients:

Nome	E-mail	Celular	Cidade	Ação
Tallys Winter	winter.tallys@yahoo.com	85988443194	Fortaleza	<button>Editar</button> <button>Excluir</button>
Tally Winter	winter.tallys@yahoo.com	85942042069	Fortaleza	<button>Editar</button> <button>Excluir</button>

Ativar o Windows  
Acesse Configurações para ativar o Windows.

Copyright © Grupo 10

#### Página 05 - Lista de usuários (Read)

A captura de tela abaixo é referente ao formulário para cadastro de cliente, o qual possui campos para o nome do cliente, e-mail do cliente, celular do cliente e cidade do cliente em questão.

The screenshot shows a web application window titled 'Gerencia de Clientes'. A modal dialog box is open with the title 'Novo Cliente'. The form contains four input fields: 'Nome do Cliente' (Name), 'e-mail do Cliente' (Email), 'Celular do Cliente' (Cellular), and 'Cidade do Cliente' (City). Below the form are 'Salvar' (Save) and 'Cancelar' (Cancel) buttons. To the left of the modal, there is a sidebar with a 'Cadastrar Cliente' button and a table showing client data. To the right, there is a toolbar with 'Ação' buttons ('Editar', 'Excluir') and a status bar at the bottom.

Página 06 - Adicionar novo usuário (Create)

The screenshot shows a web application window titled 'Gerencia de Clientes'. A modal dialog box is open with the title 'Editando Tallys Winter'. The form contains four input fields: 'Nome' (Name), 'E-mail' (Email), 'Celular' (Cellular), and 'Cidade' (City). The 'Nome' field has 'Tallys Winter' entered. The 'E-mail' field has 'winter.tallys@yahoo.com' entered. The 'Celular' field has '85988443194' entered. The 'Cidade' field has 'Fortaleza' entered. Below the form are 'Salvar' (Save) and 'Cancelar' (Cancel) buttons. To the left of the modal, there is a sidebar with a 'Cadastrar Cliente' button and a table showing client data. To the right, there is a toolbar with 'Ação' buttons ('Editar', 'Excluir') and a status bar at the bottom.

Página 07 - Editar dados do usuário (Update)

The screenshot shows a web browser window titled "Telemarketing G10" with the URL "127.0.0.1:5001/views/client.html". A confirmation dialog box is displayed in the center, asking "Deseja realmente excluir o cliente Tallys Winter?" (Do you really want to delete the client Tallys Winter?). The dialog has "OK" and "Cancelar" buttons. Below the dialog is a table listing clients. The table has columns: Nome (Name), E-mail (Email), Celular (Cellular), Cidade (City), and Ação (Action). The first row shows "Tallys Winter" with email "winter.tallys@yahoo.com", cellular "85988443194", city "Fortaleza", and action buttons "Editar" (Edit) and "Excluir" (Delete). The second row shows "Tally Winter" with email "winter.tallys@yahoo.com", cellular "85942042069", city "Fortaleza", and action buttons "Editar" (Edit) and "Excluir" (Delete).

Nome	E-mail	Celular	Cidade	Ação
Tallys Winter	winter.tallys@yahoo.com	85988443194	Fortaleza	<button>Editar</button> <button>Excluir</button>
Tally Winter	winter.tallys@yahoo.com	85942042069	Fortaleza	<button>Editar</button> <button>Excluir</button>

Ativar o Windows  
Acesse Configurações para ativar o Windows.

Copyright © Grupo 10

## Página 08 - Remover um usuário (Delete)

## Anexo I

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	PSI-001-2024
		Versão: 1.0
	<b>Grupo Telemarketing 2024</b>	
	<b>Classificação: interna</b>	Última revisão: 04/06/2024

## SUMÁRIO

<b>Introdução.....</b>	<b>39</b>
<b>Escopo .....</b>	<b>39</b>
<b>Sistema de Gestão de Privacidade da Informação (SGSI).....</b>	<b>39</b>
<b>Responsabilidades .....</b>	<b>40</b>
<b>Objetivo.....</b>	<b>41</b>
<b>Termos e Definições .....</b>	<b>41</b>
<b>Diretrizes Estratégicas .....</b>	<b>42</b>
<b>Sanções para o descumprimento da PSI.....</b>	<b>43</b>
<b>Políticas de Combate aos crimes de ódio, bullying e preconceito.....</b>	<b>45</b>
<b>Considerações Adicionais .....</b>	<b>47</b>
<b>Documentos Relacionados: .....</b>	<b>47</b>
<b>Treinamento e Conscientização .....</b>	<b>47</b>
<b>Periodicidade dos Treinamentos .....</b>	<b>48</b>
<b>Mecanismos de Avaliação.....</b>	<b>48</b>
<b>Comunicação.....</b>	<b>48</b>
<b>Atualização da Política .....</b>	<b>48</b>
<b>Conclusão.....</b>	<b>48</b>

## **Introdução**

A presente Política de Segurança da Informação (PSI) estabelece os princípios e diretrizes para proteger a informação confidencial e sensível da empresa de telemarketing Grupo de Estudos Sistema de Informação - Telemarketing - PUC MINAS 2024, denominada aqui como apenas G10T2024, incluindo dados pessoais dos seus clientes e colaboradores. A política está alinhada com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) e com as melhores práticas de segurança da informação.

## **Escopo**

Esta política se aplica a todos os colaboradores, parceiros e fornecedores da G10T2024 que tenham acesso ou que processem informações confidenciais e sensíveis da empresa, incluindo dados pessoais.

## **Liderança**

Os líderes da organização são responsáveis por conhecer e aplicar as políticas de segurança definidas no SGSI, garantindo o total envolvimento no propósito de atingir os objetivos de segurança da organização.

## **Envolvimento de pessoas**

É responsabilidade de todos os níveis de colaboradores conhecer e atender a política do SGSI se envolvendo nas questões relacionadas à segurança, permitindo que as suas habilidades sejam usadas para a garantia e melhoria contínua do SGSI.

## **Processos e melhoria contínua**

É responsabilidade da alta direção, representante da direção e equipe de segurança estar constantemente alerta com relação aos procedimentos e processos estabelecidos no SGSI. Os mesmos devem ser regularmente revisados e melhorados, garantindo a efetividade da política estabelecida no SGSI.

## **Relacionamentos externos**

É responsabilidade da empresa garantir a política em questões internas e em relacionamentos externos quando clientes, fornecedores e outras partes interessadas não possuírem sua própria política de segurança da informação. Quando um cliente ou fornecedor apresentar uma política distinta, o representante da direção junto com a equipe da segurança da informação deve avaliar se a nova política afeta de alguma maneira a segurança e possui a liberdade de adotar neste relacionamento a política terceira.

## **Sistema de Gestão de Privacidade da Informação (SGSI)**

A G10T2024 implementará um SGSI, que possui como diretriz principal a Política de Segurança da Informação (PSI), para atender às peculiaridades do segmento de call center. O SGSI incluirá os seguintes elementos:

**Procedimento de Gestão de Riscos:** Um processo para identificar, avaliar e tratar os riscos à segurança da informação e à privacidade dos dados pessoais.

**Programa de Conscientização:** Um programa para educar e conscientizar os colaboradores sobre a importância da segurança da informação e da proteção da privacidade dos dados pessoais.

**Controles de Segurança:** Medidas técnicas e organizacionais para proteger a informação confidencial e sensível da empresa, incluindo medidas de segurança física, lógica e tecnológica.

**Monitoramento e Auditoria:** Monitoramento contínuo da segurança da informação e auditorias periódicas para verificar a efetividade dos controles de segurança.

## Responsabilidades

Todos os colaboradores, parceiros e fornecedores da empresa são responsáveis pela segurança da informação sob sua custódia:

**Usuário:** Conhecer e cumprir a Política de Segurança da Informação na íntegra; Relatar ocorrências ou suspeitas de incidentes de segurança ao Comitê do SGSI. Zelar pela segurança da informação.

**Gestor:** Ser agente multiplicador, informando, incentivando e conscientizando cada usuário a cumprir a Política de Segurança da Informação e Política de Privacidade da Informação; Garantir que no momento da contratação, o prestador de serviço conheceu e aceitou a Política de Segurança da Informação e Política de Privacidade da Informação.

**Equipe SGSI:** Ser guardião da informação e dados pessoais dentro da empresa; Manter e melhorar o sistema da segurança da informação e proteção de dados pessoais; Revisar e atualizar os documentos que compõem a Política de Segurança da Informação e Política de Privacidade da Informação; Conscientizar e orientar os usuários em relação à Política de Segurança da Informação e Política de Privacidade da Informação; Julgar os incidentes de segurança da informação e comunicar o resultado aos gestores para que as medidas disciplinares cabíveis sejam executadas; Definir o conteúdo das informações que estarão disponíveis para os usuários.

**Diretoria:** A diretoria da empresa é responsável por aprovar e implementar esta política e por garantir que os recursos necessários estejam disponíveis para a gestão da segurança da informação.

**Encarregado do Tratamento de Dados Pessoais (Encarregado):** O Encarregado é responsável por monitorar a conformidade da empresa com a LGPD e por orientar os colaboradores sobre as melhores práticas de proteção dos dados pessoais.

**Colaboradores:** Todos os colaboradores são responsáveis por proteger a informação confidencial e sensível da empresa, seguindo as orientações desta política e dos procedimentos de segurança da informação.

**Fornecedores:** Os fornecedores da empresa devem implementar medidas de segurança adequadas para proteger a informação da empresa sob sua custódia.

## **Objetivo**

O objetivo desta política é:

**Proteger a confidencialidade, integridade e disponibilidade da informação:** Garantir que a informação da empresa esteja protegida contra acesso não autorizado, uso indevido, divulgação, alteração ou destruição.

**Assegurar a conformidade com a LGPD:** Proteger os direitos dos titulares de dados pessoais e garantir que a empresa processe esses dados de forma ética e responsável.

**Promover uma cultura de segurança da informação:** Conscientizar os colaboradores sobre a importância da segurança da informação e capacitar-los para proteger os dados da empresa.

## **Termos e Definições**

**Autenticidade:** Os sistemas e os dados devem ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema; Propriedade que uma entidade é o que afirma ser.

**Informação Confidencial:** Qualquer informação que não seja de conhecimento público e que possa causar prejuízo à empresa se for divulgada sem autorização.

**Informação Sensível:** Informação que se refere a dados pessoais, como nome, endereço, telefone, e-mail, CPF, RG, dados financeiros, dados biométricos, etc.

**Dado Pessoal:** Informação que identifica ou torna identificável uma pessoa natural.

**Titular de Dados Pessoais:** A pessoa natural a quem se referem os dados pessoais.

**Tratamento de Dados Pessoais:** Qualquer operação realizada com dados pessoais, como coleta, produção, armazenamento, consulta, utilização, difusão ou transmissão.

**Eficácia:** Extensão na qual as atividades planejadas são realizadas e os resultados planejados, alcançados.

**Eficiência:** Relação entre o resultado alcançado e os recursos usados.

A segurança da informação da G10T2024 será baseada nos seguintes princípios:

**Confidencialidade:** A informação confidencial e sensível da empresa deve ser mantida em sigilo e acessível apenas às pessoas autorizadas. Os dados privados devem ser apresentados somente aos donos ou a pessoas ou grupo por eles liberados; Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

**Integridade:** A informação deve ser precisa, completa e confiável, devendo ser mantida sua autenticidade e veracidade. Os sistemas e os dados devem estar sempre íntegros e em condições de serem utilizados; Propriedade de salvaguarda da exatidão e completeza dos ativos.

**Disponibilidade:** A informação deve estar disponível para os usuários autorizados quando necessário, de forma confiável e segura. Os sistemas e os dados devem estar disponíveis de forma que quando o usuário necessitar, possa usar.

## Diretrizes Estratégicas

**Estabelecimento de um Programa de Segurança da Informação (PSI):** O PSI deve definir os objetivos, as responsabilidades e as medidas necessárias para proteger a informação da empresa.

**Classificação da Informação:** A informação deve ser classificada de acordo com seu nível de sensibilidade, estabelecendo critérios para o acesso e o tratamento de cada categoria.

**Gestão de Ativos da Informação:** Os ativos associados à informação e aos recursos de processamento da informação estão identificados e inventariados. Para cada ativo da informação está definido um proprietário que é responsável por assegurar que o mesmo seja utilizado conforme política de segurança da empresa. As diretrizes para utilização adequada dos ativos são informadas durante o processo de contratação de pessoas. Ativos específicos possuem como responsável profissional capacitado para manipulação garantindo a devida utilização.

**Softwares e Hardwares:** Todos os recursos de TI da G10T2024, incluindo os softwares, devem ser inventariados e identificados pela GTI. Só é permitida a utilização de softwares e hardwares legítimos, previamente homologados ou autorizados pela equipe responsável, sejam eles onerosos, gratuitos, livres ou licenciados. Todo recurso de TI de propriedade da G10T2024, incluindo os dispositivos móveis, devem utilizar recursos de segurança, como senha de bloqueio automático, antivírus, antispyware, firewall e mecanismos de controle de softwares maliciosos. A retirada de qualquer equipamento, bancos de dados ou software das instalações da empresa, ou da sua infraestrutura tecnológica, deve ser realizada pela equipe responsável, quando prévia e formalmente autorizada pelo gestor imediato ou por necessidade da equipe responsável.

**Controle de Acesso:** O acesso à informação deve ser limitado a usuários autorizados, com base em suas necessidades e responsabilidades funcionais. Controle de acesso é um dos mecanismos utilizados para proteger fisicamente e logicamente o ambiente de TI. O acesso aos ativos de TI deve ser permitido somente a pessoas autorizadas de acordo com os itens desta Política de Segurança da Informação. O direito de uso dos ativos é controlado e cedido no momento da contratação e cessado quando do término do vínculo com a empresa, momento em que os ativos físicos são recolhidos. Caso o contratado tenha a necessidade de acesso a um sistema corporativo específico, este será provido via autorização do gestor da informação envolvida.

**Proteção de Dados Pessoais:** A empresa deve cumprir as leis de proteção de dados, como a LGPD no Brasil, garantindo a privacidade e a segurança dos dados dos clientes e colaboradores.

**Segurança da Rede e dos Sistemas:** medidas de segurança física e lógica para proteger a rede e os sistemas da empresa contra ataques cibernéticos, como firewalls, antivírus e soluções de criptografia. A G10T2024 disponibiliza acesso à internet a funcionários e visitantes, sendo que o acesso a visitantes é feito através de rede específica e apartada da rede corporativa. A internet disponibilizada pela G10T2024 aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que este uso não envolva conteúdo pornográfico, fraudulento, difamatório, racialmente ofensivo, ilegal ou que viole quaisquer normas regulatórias como download de software não legalizado ou cause riscos a infraestrutura. É proibida a divulgação de informações confidenciais da organização em quaisquer grupos de discussão, listas ou bate-papos. A falha em não seguir a política irá resultar em sanções que variam desde procedimentos disciplinares, com avisos verbais ou escritos.

**Políticas de Senhas:** Implementação de políticas rigorosas para a criação e o uso de senhas seguras, incluindo requisitos de complexidade, mudança periódica e proteção contra phishing. O

procedimento de logon deve divulgar apenas as informações necessárias às atividades de determinado funcionário, evitando fornecer a um usuário não autorizado informações indevidas. As mensagens de ajuda do processo de logon não devem possuir dicas capazes de permitir um usuário não autorizado o acesso ao sistema. Todo usuário deverá ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal, e é responsável por qualquer ação executada com o seu login/senha, não é permitido o compartilhamento, divulgação a terceiros ou anotações em papel da identificação pessoal.

**E-mail:** Todos os usuários de correio eletrônico estão habilitados a enviar e receber mensagens externas desde que vinculadas ao trabalho. O padrão para criação de e-mail institucional é nome.sobre@G10T2024.com. Em casos excepcionais, de duplicidade ou que causem constrangimento aos usuários, o padrão deverá ser revisto. A conta de e-mail é disponibilizada exclusivamente para uso institucional, não sendo admitida para uso pessoal.

**Acesso Remoto:** É disponibilizado acesso remoto à infraestrutura, desde que necessário à realização das atividades laborais da empresa através de conexão segura com aprovação do gestor da área e equipe de T.I. As ferramentas que disponibilizamos acesso remoto, são testadas e atendem aos requisitos de segurança. O acesso à informação de clientes é realizado através de conexão segura e protegida por senha. As informações da empresa que são armazenadas remotamente, devem ser feitas via software que garanta a segurança dos dados armazenados e o tráfego da informação. Em todos os casos de acesso remoto, aplicam-se todas as medidas de segurança adotadas pela empresa.

**Conscientização e Treinamento:** Treinamentos periódicos para conscientizar os colaboradores sobre a importância da segurança da informação e sobre as melhores práticas para proteger os dados da empresa.

**Monitoramento e Auditoria:** Monitoramento contínuo da segurança da informação e realização de auditorias periódicas para verificar a efetividade das medidas de segurança.

**Plano de Resposta a Incidentes:** Estabelecimento de um plano para lidar com incidentes de segurança, como vazamentos de dados, ataques cibernéticos ou perda de dispositivos.

**Revisão e Atualização Contínuas:** A política de segurança da informação deve ser revisada e atualizada periodicamente para refletir as mudanças no ambiente de negócios, nas tecnologias de informação e na legislação sobre proteção de dados

## **Sanções para o descumprimento da PSI**

Esta cláusula visa estabelecer as medidas disciplinares a serem aplicadas aos colaboradores que violarem a Política de Segurança da Informação da empresa. O objetivo é garantir a proteção das informações confidenciais da empresa, prevenir danos e promover a cultura de segurança da informação.

### **Abrangência**

Esta cláusula se aplica a todos os colaboradores da empresa, incluindo empregados, terceirizados, estagiários e voluntários, independentemente do cargo ou função.

## **Violações e Punições**

As violações à Política de Segurança da Informação podem ser classificadas em três níveis de gravidade: leve, média e grave. As medidas disciplinares serão aplicadas de acordo com a gravidade da violação e o histórico do colaborador:

### **Violações Leves:**

**Descrição:** Violações que não causam danos significativos à empresa ou comprometem a confidencialidade das informações. Exemplos: acesso não autorizado a recursos de rede, uso indevido de equipamentos da empresa, instalação de software não autorizado.

**Punições:** Advertência verbal, advertência por escrito, treinamento obrigatório sobre segurança da informação.

### **Violações Médias:**

**Descrição:** Violações que causam danos à empresa ou colocam em risco a confidencialidade das informações. Exemplos: divulgação de informações confidenciais, perda ou roubo de equipamentos da empresa, falha em reportar incidentes de segurança.

**Punições:** Suspensão do colaborador por até 5 dias sem remuneração, treinamento obrigatório sobre segurança da informação, reavaliação do acesso a recursos de informação.

### **Violações Graves:**

**Descrição:** Violações que causam danos graves à empresa ou comprometem seriamente a confidencialidade das informações. Exemplos: espionagem industrial, sabotagem, venda de informações confidenciais, crimes descritos na política de combate a crimes de ódio, bullying e preconceito.

**Punições:** Demissão por justa causa, processo judicial, investigação interna para identificar outros envolvidos.

## **Reincidência**

Em caso de reincidência, as medidas disciplinares serão mais rigorosas, podendo levar à demissão por justa causa, mesmo para violações leves ou médias.

## **Apuração das Violações**

As violações à Política de Segurança da Informação serão apuradas por uma comissão composta por membros da equipe de segurança da informação, da área de recursos humanos e da área jurídica da empresa. A comissão terá o dever de investigar o caso de forma imparcial e sigilosa, e recomendar a aplicação da medida disciplinar cabível.

## **Direito de Defesa**

O colaborador acusado de violar a Política de Segurança da Informação terá o direito de se defender perante a comissão de apuração. A comissão ouvirá o colaborador e considerará todas as provas antes de tomar sua decisão.

## **Recursos**

O colaborador que discordar da medida disciplinar aplicada poderá recorrer à área de recursos humanos da empresa. O recurso deverá ser apresentado por escrito no prazo de 5 dias úteis após a notificação da medida disciplinar.

## **Confidencialidade**

Todas as informações relacionadas às violações da Política de Segurança da Informação serão tratadas com confidencialidade.

## **Vigência**

Esta cláusula entra em vigor na data de sua publicação e estará disponível para consulta de todos os colaboradores da empresa.

## **Revisão**

Esta cláusula será revisada periodicamente para garantir que esteja adequada às necessidades da empresa e à legislação vigente.

## **Políticas de Combate aos crimes de ódio, bullying e preconceito**

Todos os alunos e colaboradores devem se comprometer a participar de campanhas de conscientização promovidas pela G10T2024 e/ou suas mantidas contra atos de violência e intimidação sistemática; preconceitos de injúria racial; crimes de ódio, bem como a cooperar de todas as formas em situações críticas para a melhor aplicação de medidas preventivas e reativas, e também contribuir para a apuração de fatos e de pessoas envolvidas em casos de bullying, comprometendo-se inclusive a fornecer depoimentos, quando necessários, e provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

## **Definições**

**Crime de ódio:** Crime motivado por preconceito ou ódio contra uma pessoa ou grupo de pessoas, em função de sua raça, religião, etnia, nacionalidade, orientação sexual, identidade de gênero, entre outros.

**Bullying:** Comportamento agressivo repetido por uma ou mais pessoas contra outra, com o objetivo de intimidar, humilhar ou causar sofrimento físico ou emocional.

**Preconceito:** Opinião ou sentimento preconcebido, geralmente negativo, em relação a um indivíduo ou grupo de pessoas, sem fundamento na realidade.

## **Políticas**

### **Prevenção**

A empresa promoverá a conscientização sobre crimes de ódio, bullying e preconceito através de treinamentos, campanhas informativas e canais de denúncia.

Será criado um ambiente de trabalho inclusivo e acolhedor, onde todos se sintam respeitados e valorizados.

A empresa promoverá a diversidade e a inclusão em todos os níveis da organização.

### **Denúncias**

A organização disponibilizará canais de denúncia seguros e confidenciais para que os colaboradores possam reportar qualquer situação de crime de ódio, bullying ou preconceito, via ramal, whatsapp ou presencial com acompanhamento da equipe de RH e psicólogo(a)..

As denúncias serão investigadas de forma imparcial e sigilosa.

As medidas cabíveis serão tomadas contra os responsáveis, de acordo com a legislação vigente e as normas internas da organização.

### **Medidas Disciplinares**

Qualquer colaborador que cometer crimes de ódio, bullying ou preconceito estará sujeito a medidas disciplinares, que podem incluir advertência verbal ou escrita, suspensão ou demissão por justa causa.

### **Apoio às Vítimas**

A organização oferecerá apoio às vítimas de crimes de ódio, bullying ou preconceito, incluindo acompanhamento psicológico, jurídico e social.

As vítimas terão acesso a canais de comunicação para solicitar ajuda e orientação.

### **Monitoramento e Revisão**

A organização monitorará a efetividade desta política e a revisará periodicamente para garantir que esteja adequada às necessidades da organização e à legislação vigente.

### **Comunicação**

Esta política será divulgada a todos os colaboradores da organização e estará disponível em local de fácil acesso.

Treinamentos serão realizados para conscientizar os colaboradores sobre a importância desta política e como prevenir e combater crimes de ódio, bullying e preconceito.

## Considerações Adicionais

**Responsabilidade Compartilhada:** A segurança da informação é uma responsabilidade compartilhada por todos os colaboradores da empresa.

**Cultura de Segurança:** É fundamental criar uma cultura de segurança na empresa, onde todos os colaboradores estejam conscientes da importância de proteger os dados da empresa.

**Comunicação Aberta:** A empresa deve manter um canal de comunicação aberto com os colaboradores para esclarecer dúvidas sobre a política de segurança da informação e sobre como proteger os dados da empresa.

## Documentos Relacionados:

- Manual do SGSI;
- Política de Privacidade da Informação;
- Política de Controle de Acesso;
- Política de Segurança Física;
- Processo de Contratação de Pessoal;
- Política de Uso Aceitável dos Ativos.

## Treinamento e Conscientização

A G10T2024 realizará treinamentos periódicos para conscientizar os colaboradores sobre a importância da segurança da informação e da proteção da privacidade dos dados pessoais. Os treinamentos abordarão os seguintes tópicos:

**Princípios de segurança da informação:** Confidencialidade, integridade e disponibilidade.

**Lei Geral de Proteção de Dados Pessoais (LGPD):** Direitos dos titulares de dados, princípios do tratamento de dados, medidas de segurança, incidentes de segurança e canais de comunicação com o Encarregado.

**Políticas e procedimentos de segurança da informação da empresa:** Orientações sobre como proteger a informação confidencial e sensível da empresa, incluindo medidas de segurança física, lógica e tecnológica.

**Boas práticas para a proteção da privacidade:** Como proteger os dados pessoais dos clientes e colaboradores, como evitar phishing e outras ameaças cibernéticas, como usar senhas seguras e como descartar documentos com informações confidenciais.

**Canais de comunicação para relatar incidentes de segurança:** Orientações sobre como os colaboradores podem relatar incidentes de segurança, como perda de dados, acessos não autorizados ou ataques cibernéticos.

## Periodicidade dos Treinamentos

Os treinamentos serão realizados periodicamente, pelo menos uma vez por ano, e sempre que houver mudanças significativas na política de segurança da informação ou na LGPD.

## Mecanismos de Avaliação

A empresa realizará avaliações periódicas para verificar a efetividade dos treinamentos e o nível de conscientização dos colaboradores sobre a segurança da informação e a proteção da privacidade dos dados pessoais.

## Comunicação

A empresa manterá um canal de comunicação aberto com os colaboradores para esclarecer dúvidas sobre a política de segurança da informação e a proteção da privacidade dos dados pessoais.

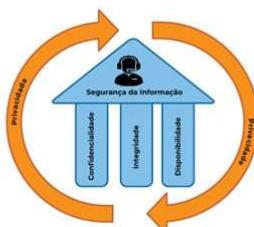
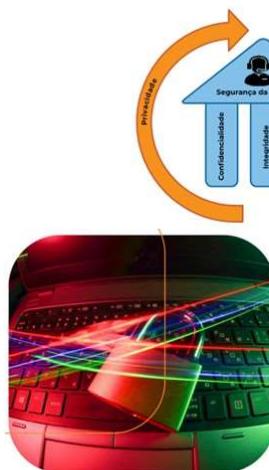
## Atualização da Política

Esta política será revisada e atualizada periodicamente para refletir as mudanças no ambiente de negócios, nas tecnologias de informação e na legislação sobre proteção de dados.

## Conclusão

A segurança da informação e a proteção da privacidade dos dados pessoais são prioridades para a G10T2024.. Através da implementação desta política de segurança da informação e do SGSI, a empresa se compromete a proteger a informação confidencial e sensível da empresa e a garantir a conformidade com a LGPD.

### Cartilha de segurança da informação



**Integridade:** A informação deve ser precisa, completa e confiável, devendo ser mantida sua autenticidade e veracidade.

**Disponibilidade:** A informação deve estar disponível para os usuários autorizados quando necessário, de forma confiável e segura.

**Controle de Acesso:** O acesso à informação deve ser limitado a usuários autorizados, com base em suas necessidades e responsabilidades funcionais.

**Proteção de Dados Pessoais:** Deve se cumprir as leis de proteção de dados, como a LGPD no Brasil, garantindo a privacidade e a segurança dos dados dos clientes e colaboradores.

**Segurança da Rede e dos Sistemas:** Medidas de segurança física e lógica para proteger a rede e os sistemas da empresa contra ataques cibernéticos, como firewalls, antivírus e soluções de criptografia.

**Acesso Remoto:** É disponibilizado acesso remoto à infraestrutura, desde que necessário à realização das atividades laborais da empresa através de conexão segura com aprovação do gestor da área e equipe de TI.

**E-mail:** Todos os usuários de correio eletrônico estão habilitados a enviar e receber mensagens externas desde que vinculadas ao trabalho. O padrão para criação de e-mail institucional é nome.sobre@G10T2024.com.



**Violações e Punições:** As violações à Política de Segurança da Informação podem ser classificadas em três níveis de gravidade: leve, média e grave. As medidas disciplinares serão aplicadas de acordo com a gravidade da violação e o histórico do colaborador.



**Controle de Acesso:** O acesso à informação deve ser limitado a usuários autorizados, com base em suas necessidades e responsabilidades funcionais.



**Conscientização e Treinamento:** Treinamentos periódicos para conscientizar os colaboradores sobre a importância da segurança da informação e sobre as melhores práticas para proteger os dados da empresa.

**Violações Leves:** Violações que não causam danos significativos à empresa ou comprometem a confidencialidade das informações. Exemplos: acesso não autorizado a recursos de rede, uso indevido de equipamentos da empresa, instalação de software não autorizado.

**Violações Médias:** Violações que causam danos à empresa ou colocam em risco a confidencialidade das informações. Exemplos: divulgação de informações confidenciais, perda ou roubo de equipamentos da empresa, falha em reportar incidentes de segurança.



**Violações Graves:** Violações que causam danos graves à empresa ou comprometem seriamente a confidencialidade das informações. Exemplos: espionagem industrial, sabotagem, venda de informações confidenciais, crimes descritos na política de combate a crimes de ódio, bullying e preconceito.

**Apuração das Violações:** As violações à Política de Segurança da Informação serão apuradas por uma comissão composta por membros da equipe de segurança da informação, da área de recursos humanos e da área jurídica da empresa.