



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

**Alan Ferreira da Silva**

**Amanda Andrade Lopes**

**Angelica Sofia Nieves**

**Estevão Moura Rodrigues**

**Yael Joaquim Nobre Dias**

**PROJETO INFRAESTRUTURA DE REDES**

**Belo Horizonte 2024**

## **PROJETO 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
1.1 RESPONSABILIDADES .....	6
2. CRONOGRAMA DE ATIVIDADES .....	7
3. PLANEJAMENTO DOS RECURSOS DE REDE.....	8
3.1 DIVISÃO FÍSICA DA REDE.....	9
3.2 PLANILHA DE MATERIAIS .....	10
3.3 DIVISÃO LÓGICA DA REDE.....	11
3.4 PLANILHA LINKS .....	14
4. IMPLEMENTAÇÃO DOS RECURSOS DE REDE .....	15
4.2 IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ .....	19
4.2.1 CONFIGURAÇÃO DA VPC.....	19
4.2.2 CONFIGURAÇÃO SERVIDOR WEB E ISS.....	20
5. GERENCIAMENTO DE RECURSOS DOS SERVIDORES VIA ZABBIX .....	23
5.1 CONFIGURAÇÃO DO PROTOCLO SNMP NOS SERVIDORES .....	23
5.2 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX.....	25
6. APLICAÇÃO WEB PARA CONTROLE E GERENCIAMENTO DO BACK-END .....	29
6.1 REGISTRO DA ESTRUTURA DE TABELAS DA APLICAÇÃO.....	33
7. DOCUMENTO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO .....	35
7.1 CARTILHA DE SEGURANÇA .....	35
8. APÊNDICES .....	1

## 1. TEMA

O grupo optou pela escolha de uma empresa de telemarketing com um quadro de funcionários de aproximadamente 600 colaboradores que prestam serviço, de venda e cobrança, para empresas de diferentes segmentos do mercado.

É fundamental que a empresa disponha de uma infraestrutura robusta capaz de sustentar chamadas telefônicas, transferência de dados e comunicações eficientes, tanto entre os funcionários presentes no local de trabalho quanto os remotos e os clientes em atendimento. Investir em sistemas de telefonia que ofereçam recursos como discagem automática e gravação de chamadas é crucial para otimizar os processos de comunicação.

É importante contar com um setor dedicado à resolução de problemas técnicos enfrentados pelos funcionários remotos, garantindo que eles recebam o suporte necessário para manter a produtividade. Por fim, é imprescindível adotar medidas de segurança para proteger as informações confidenciais durante todas as interações com os clientes, garantindo assim a privacidade e a integridade dos dados.

Empresas de grande porte possuem estruturas altamente complexas que requerem organização precisa para operar de forma eficiente. Tipicamente, essas organizações são compostas por diversos departamentos e setores que precisam estar interconectados. A seguir, destacamos alguns dos principais aspectos dessa estrutura:

1. **Departamento de TI:** Responsável por gerenciar e manter a infraestrutura tecnológica da empresa, incluindo redes de comunicação, sistemas de telefonia, servidores e outras soluções tecnológicas necessárias para operações eficientes. Eles também cuidam da segurança da informação e da integridade dos dados.
2. **Qualidade, desenvolvimento e segurança:** Encarregado de garantir a qualidade dos serviços prestados pela empresa de telemarketing, através do monitoramento das interações com os clientes e da implementação de treinamentos para os operadores. Também é responsável pelo desenvolvimento de novas estratégias e processos para aprimorar a eficiência e a satisfação do cliente, além de cuidar da segurança das operações.

3. **Marketing e vendas:** responsável por desenvolver estratégias eficazes de marketing para promover os produtos ou serviços da empresa. Isso pode incluir a identificação do público-alvo, análise de mercado, pesquisa de concorrência e definição de mensagens e posicionamento de marca.
4. **Produção:** Responsável por supervisionar o processo de produção das campanhas de telemarketing, incluindo a criação de scripts, a distribuição de leads para os operadores, o monitoramento do desempenho das campanhas e a análise dos resultados.
5. **Departamento de Operações Regionais:** Encarregado de coordenar as operações da empresa em diferentes regiões geográficas, garantindo a consistência e a eficiência das atividades de telemarketing em cada localidade.
6. **Departamento de Vendas Regionais:** Responsável por desenvolver e implementar estratégias de vendas específicas para cada região, visando atingir as metas de vendas estabelecidas pela empresa.
7. **Departamento de Suporte Técnico Regional:** Encarregado de fornecer suporte técnico e assistência aos clientes e operadores de telemarketing em cada região, solucionando problemas técnicos e garantindo a continuidade das operações.
8. **Recursos Humanos:** Responsável pela gestão do capital humano da empresa, incluindo recrutamento, seleção, treinamento, desenvolvimento e gerenciamento de pessoal. Eles cuidam de questões relacionadas aos funcionários, como folha de pagamento, benefícios, avaliação de desempenho e resolução de conflitos.
9. **Financeiro e contábil:** Encarregado de gerenciar as finanças e contabilidade da empresa, incluindo orçamento, controle de despesas, faturamento, cobrança, análise financeira e elaboração de relatórios contábeis. Eles garantem a sustentabilidade financeira da empresa e cumprem as obrigações fiscais e regulatórias.

Dessa forma, entende-se que uma estrutura de rede bem-sucedida é um componente crítico para garantir a eficiência operacional, a qualidade do produto/serviço e a competitividade de uma empresa. Ela permite uma integração eficaz de todos os aspectos da operação promovendo a excelência nos negócios.

## 1.1 RESPONSABILIDADES

Nome	Papel	Responsabilidade
Yael	Prazo e controle de qualidade;	<ul style="list-style-type: none"><li>- Realizar a contextualização das demandas do projeto, compreendendo as necessidades e objetivos;</li><li>- Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades;</li></ul>
Amanda	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>
Angelica	Redatora/editora	<ul style="list-style-type: none"><li>- Coletar, organizar e documentar dados relevantes para o projeto, garantindo a disponibilidade de informações para subsidiar as atividades.</li><li>- Participar das reuniões periódicas de acompanhamento do projeto;</li></ul>
Estevão	Comunicador	<ul style="list-style-type: none"><li>- Realizar levantamento de requisitos;</li><li>- Definir objetivos e metas alinhados com as demandas de rede.</li><li>- Coordenar a planilha de Recursos e Redes.</li></ul>

Alan	Programador	<ul style="list-style-type: none"> <li>- Participar das reuniões periódicas de acompanhamento do projeto;</li> <li>- Coordenar o Protótipo da rede no Simulador da Cisco Packet Tracer.</li> <li>- Definir objetivos e metas alinhados com as demandas de rede.</li> </ul>
------	-------------	--

## 2. CRONOGRAMA DE ATIVIDADES

Semana	Dias de dedicação	Atividades
<b><u>Etapa 1</u></b> 06/02/24 a 24/03/24	47	<ul style="list-style-type: none"> <li>• Organização dos grupos (formados nos encontros online).</li> <li>• Definição do tema e planejamento inicial dos mecanismos de rede. <ul style="list-style-type: none"> <li>• Planilha de Recursos de Rede.</li> </ul> </li> <li>• Arquivo do Protótipo no Simulador de Redes Cisco Packet Trace.</li> </ul>
<b><u>Etapa 2</u></b> 25/03/24 a 28/04/24	34	<ul style="list-style-type: none"> <li>• Organização dos grupos (formados nos encontros online). <ul style="list-style-type: none"> <li>• Criação do servidor Local via máquina Virtual.</li> </ul> </li> <li>• Criação do Servidor Web via AWS.</li> </ul>
<b><u>Etapa 3</u></b> 29/04/24 a 26/05/24	27	<ul style="list-style-type: none"> <li>• Organização dos grupos (formados nos encontros online). <ul style="list-style-type: none"> <li>• Criação do Servidor Zabbix.</li> </ul> </li> <li>• Configuração do Servidor local e Web no Zabbix</li> </ul>
<b><u>Etapa 4</u></b> 27/05/24 a 16/06/24	20	<ul style="list-style-type: none"> <li>• Organização dos grupos (formados nos encontros online).</li> <li>• Criação do documento de Política de Segurança da Informação.</li> <li>• Criação da Cartilha de Segurança. <ul style="list-style-type: none"> <li>• Criação da aplicação Back-End com webservice e App Front.</li> </ul> </li> </ul>

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

Cenário: a rede será composta da matriz da empresa em Belo Horizonte (MG) que se liga com as suas 2 filiais sediadas em São Paulo (SP) e Rio de Janeiro (RJ).

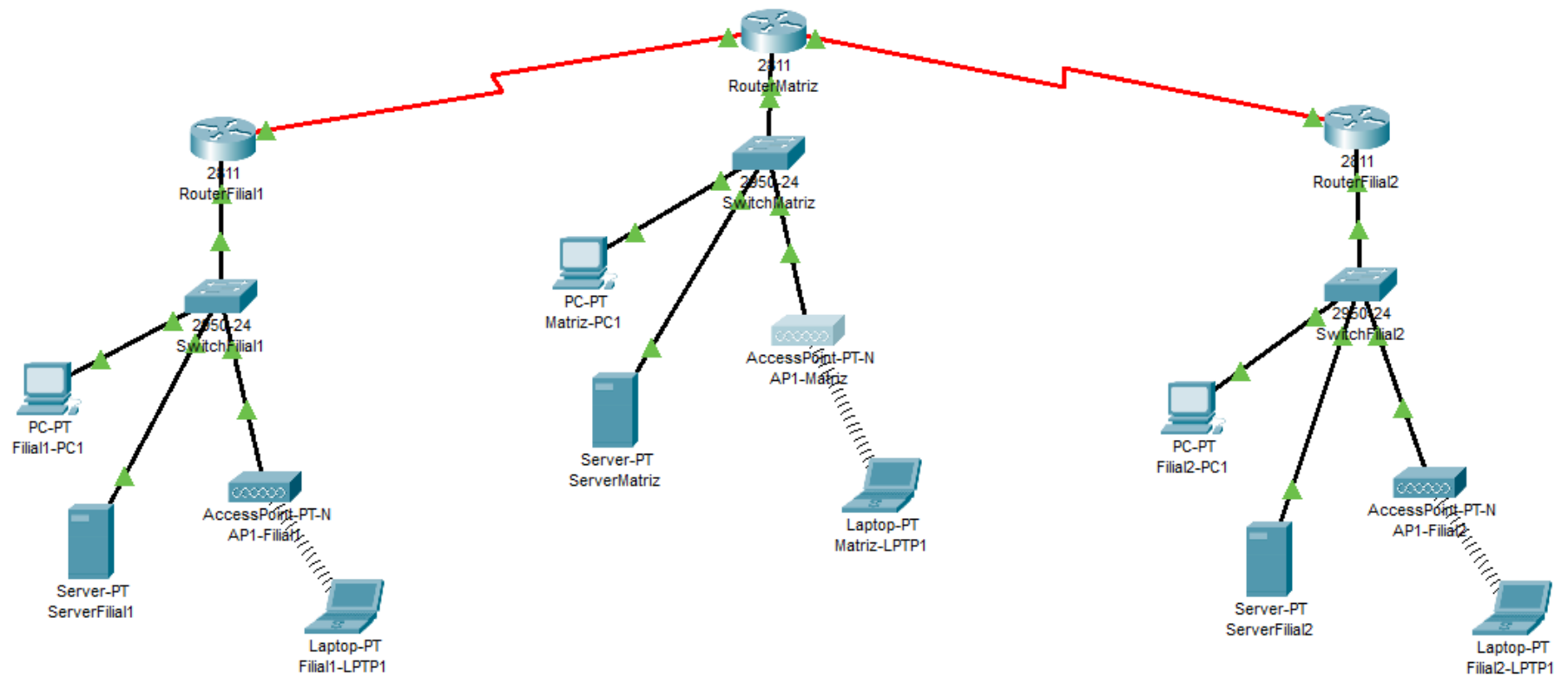
Segue algumas características de cada local da rede:

- Matriz (Belo Horizonte, MG)
  - Diretoria Executiva
  - Departamento de TI
  - Departamento de Marketing e Vendas
  - Departamento de Recursos Humanos
  - Departamento Financeiro e Contábil
  - Departamento de Produção
  - Departamento de Qualidade, Desenvolvimento e Segurança
  
- Filiais (Cada uma das filiais possuíra os departamentos abaixo)
  - Departamento de Operações Regionais
  - Departamento de Vendas Regionais
  - Departamento de Suporte Técnico Regional



### 3.1 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.



### 3.2 PLANILHA DE MATERIAIS

A tabela a seguir reflete a lista de materiais que serão empregados no projeto bem como seus valores correspondentes. A final é demonstrado o valor orçado que será necessário para a Matriz (2.707.478,52 ), Filial 1 (R\$ 1.450.834,26) e Filial 2 (R\$ 1.450.834,26). O total geral estimado para este projeto é de R\$ 5.609.147,04

		Matriz		Filial 1		Filial 2	
		250		125		125	
Apps	LB (kbps)	Qtd	LB	Qtd	LB	Qtd	LB
Web	100	250	25000	125	12500	125	12500
E-mail	50	250	12500	125	6250	125	6250
Helpdesk	250	10	2500	5	1250	5	1250
Videoconferência	300	22	6600	12	3600	12	3600
Monitoramento	100	5	500	5	500	5	500
Sistema de Gestão de Operações	60	20	1200	10	600	10	600
Sistema de Gestão de Vendas	50	12	600	10	500	10	500
Voip	87	160	13920	100	8700	100	8700
		Total	62820	Total	33900	Total	33900
		Matriz		Filial 1		Filial 2	
Internet		58020		31050		31050	
Total Internet		120120					

### 3.3 DIVISÃO LÓGICA DA REDE

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

Dispositivos	Nome	Portas / Endereçamento
Roteador	RouterMatriz	<pre> Device Name: RouterMatriz Custom Device Model: 2811 IOS15 Hostname: RouterMatriz  Port          Link   VLAN   IP Address FastEthernet0/0 Up    --    192.168.0.1/24 FastEthernet0/1 Down  --    &lt;not set&gt; Serial0/2/0   Up    --    192.168.51.1/24 Serial0/2/1   Up    --    192.168.52.1/24 Serial0/3/0   Down  --    &lt;not set&gt; Serial0/3/1   Down  --    &lt;not set&gt; Vlan1         Down  1     &lt;not set&gt;           </pre>
Roteador	RouterFilial1	<pre> Device Name: RouterFilial1 Custom Device Model: 2811 IOS15 Hostname: RouterFilial1  Port          Link   VLAN   IP Address FastEthernet0/0 Up    --    192.168.1.1/24 FastEthernet0/1 Down  --    &lt;not set&gt; Serial0/2/0   Up    --    192.168.51.2/24 Serial0/2/1   Down  --    &lt;not set&gt; Serial0/3/0   Down  --    &lt;not set&gt; Serial0/3/1   Down  --    &lt;not set&gt; Vlan1         Down  1     &lt;not set&gt;           </pre>
Roteador	RouterFilial2	<pre> Device Name: RouterFilial2 Custom Device Model: 2811 IOS15 Hostname: RouterFilial2  Port          Link   VLAN   IP Address FastEthernet0/0 Up    --    192.168.2.1/24 FastEthernet0/1 Down  --    &lt;not set&gt; Serial0/2/0   Down  --    &lt;not set&gt; Serial0/2/1   Up    --    192.168.52.2/24 Serial0/3/0   Down  --    &lt;not set&gt; Serial0/3/1   Down  --    &lt;not set&gt; Vlan1         Down  1     &lt;not set&gt;           </pre>
Switch	SwitchMatriz	<pre> Device Name: SwitchMatriz Device Model: 2950-24 Hostname: SwitchMatriz  Port          Link   VLAN   IP Address FastEthernet0/1 Up    --    -- FastEthernet0/2 Up    --    -- FastEthernet0/3 Up    --    -- FastEthernet0/4 Up    --    -- FastEthernet0/5 Down  --    --           </pre>

Switch	SwitchFilial1	<div>Device Name: SwitchFilial1</div> <div>Device Model: 2950-24</div> <div>Hostname: SwitchFilial1</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/4</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/5</td><td>Down</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Up	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--	FastEthernet0/4	Up	--	--	FastEthernet0/5	Down	--	--
Port	Link	VLAN	IP Address																							
FastEthernet0/1	Up	--	--																							
FastEthernet0/2	Up	--	--																							
FastEthernet0/3	Up	--	--																							
FastEthernet0/4	Up	--	--																							
FastEthernet0/5	Down	--	--																							
Switch	SwitchFilial2	<div>Device Name: SwitchFilial2</div> <div>Device Model: 2950-24</div> <div>Hostname: SwitchFilial2</div> <table><thead><tr><th>Port</th><th>Link</th><th>VLAN</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0/1</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/2</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/3</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/4</td><td>Up</td><td>--</td><td>--</td></tr><tr><td>FastEthernet0/5</td><td>Down</td><td>--</td><td>--</td></tr></tbody></table>	Port	Link	VLAN	IP Address	FastEthernet0/1	Up	--	--	FastEthernet0/2	Up	--	--	FastEthernet0/3	Up	--	--	FastEthernet0/4	Up	--	--	FastEthernet0/5	Down	--	--
Port	Link	VLAN	IP Address																							
FastEthernet0/1	Up	--	--																							
FastEthernet0/2	Up	--	--																							
FastEthernet0/3	Up	--	--																							
FastEthernet0/4	Up	--	--																							
FastEthernet0/5	Down	--	--																							
Servidor	ServerMatriz	<div>Device Name: ServerMatriz</div> <div>Device Model: Server-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>192.168.0.2/24</td></tr></tbody></table> <div>Gateway: 192.168.0.1</div> <div>DNS Server: 192.168.0.2</div> <div>Line Number: &lt;not set&gt;</div>	Port	Link	IP Address	FastEthernet0	Up	192.168.0.2/24																		
Port	Link	IP Address																								
FastEthernet0	Up	192.168.0.2/24																								
Servidor	ServerFilial1	<div>Device Name: ServerFilial1</div> <div>Device Model: Server-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>192.168.1.2/24</td></tr></tbody></table> <div>Gateway: 192.168.1.1</div> <div>DNS Server: 192.168.1.2</div> <div>Line Number: &lt;not set&gt;</div>	Port	Link	IP Address	FastEthernet0	Up	192.168.1.2/24																		
Port	Link	IP Address																								
FastEthernet0	Up	192.168.1.2/24																								
Servidor	ServerFilial2	<div>Device Name: ServerFilial2</div> <div>Device Model: Server-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>192.168.2.2/24</td></tr></tbody></table> <div>Gateway: 192.168.2.1</div> <div>DNS Server: 192.168.2.2</div> <div>Line Number: &lt;not set&gt;</div>	Port	Link	IP Address	FastEthernet0	Up	192.168.2.2/24																		
Port	Link	IP Address																								
FastEthernet0	Up	192.168.2.2/24																								
Computador	Matriz- PC1	<div>Device Name: Matriz-PC1</div> <div>Device Model: PC-PT</div> <table><thead><tr><th>Port</th><th>Link</th><th>IP Address</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>Up</td><td>192.168.0.11/24</td></tr><tr><td>Bluetooth</td><td>Down</td><td>&lt;not set&gt;</td></tr></tbody></table> <div>Gateway: 192.168.0.1</div> <div>DNS Server: 192.168.0.2</div> <div>Line Number: &lt;not set&gt;</div>	Port	Link	IP Address	FastEthernet0	Up	192.168.0.11/24	Bluetooth	Down	<not set>															
Port	Link	IP Address																								
FastEthernet0	Up	192.168.0.11/24																								
Bluetooth	Down	<not set>																								

Computador	Filial1- PC1	Device Name: Filial1-PC1 Device Model: PC-PT  <table> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> <tr> <td>FastEthernet0</td><td>Up</td><td>192.168.1.11/24</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td>&lt;not set&gt;</td></tr> </table> Gateway: 192.168.1.1 DNS Server: 192.168.1.2 Line Number: <not set>	Port	Link	IP Address	FastEthernet0	Up	192.168.1.11/24	Bluetooth	Down	<not set>
Port	Link	IP Address									
FastEthernet0	Up	192.168.1.11/24									
Bluetooth	Down	<not set>									
Computador	Filial2- PC1	Device Name: Filial2-PC1 Device Model: PC-PT  <table> <tr> <th>Port</th><th>Link</th><th>IP Address</th></tr> <tr> <td>FastEthernet0</td><td>Up</td><td>192.168.2.11/24</td></tr> <tr> <td>Bluetooth</td><td>Down</td><td>&lt;not set&gt;</td></tr> </table> Gateway: 192.168.2.1 DNS Server: 192.168.2.2 Line Number: <not set>	Port	Link	IP Address	FastEthernet0	Up	192.168.2.11/24	Bluetooth	Down	<not set>
Port	Link	IP Address									
FastEthernet0	Up	192.168.2.11/24									
Bluetooth	Down	<not set>									

### 3.4 PLANILHA LINKS

A tabela abaixo contém informações correspondentes a divisão de colaboradores por cada localidade dentro da estrutura da empresa e da utilização da estrutura de rede quanto a aplicações e serviços. A matriz conta com um número abrangente de 250 colaboradores por ser a sede de teleatendimento e as filias compartilham estruturas locais centralizadas com 125 colaboradores cada. Além dos colaboradores em loco, todas as unidades possuem também colaboradores em regime de homeoffice sendo de 50 para matriz e 25 para cada filial.

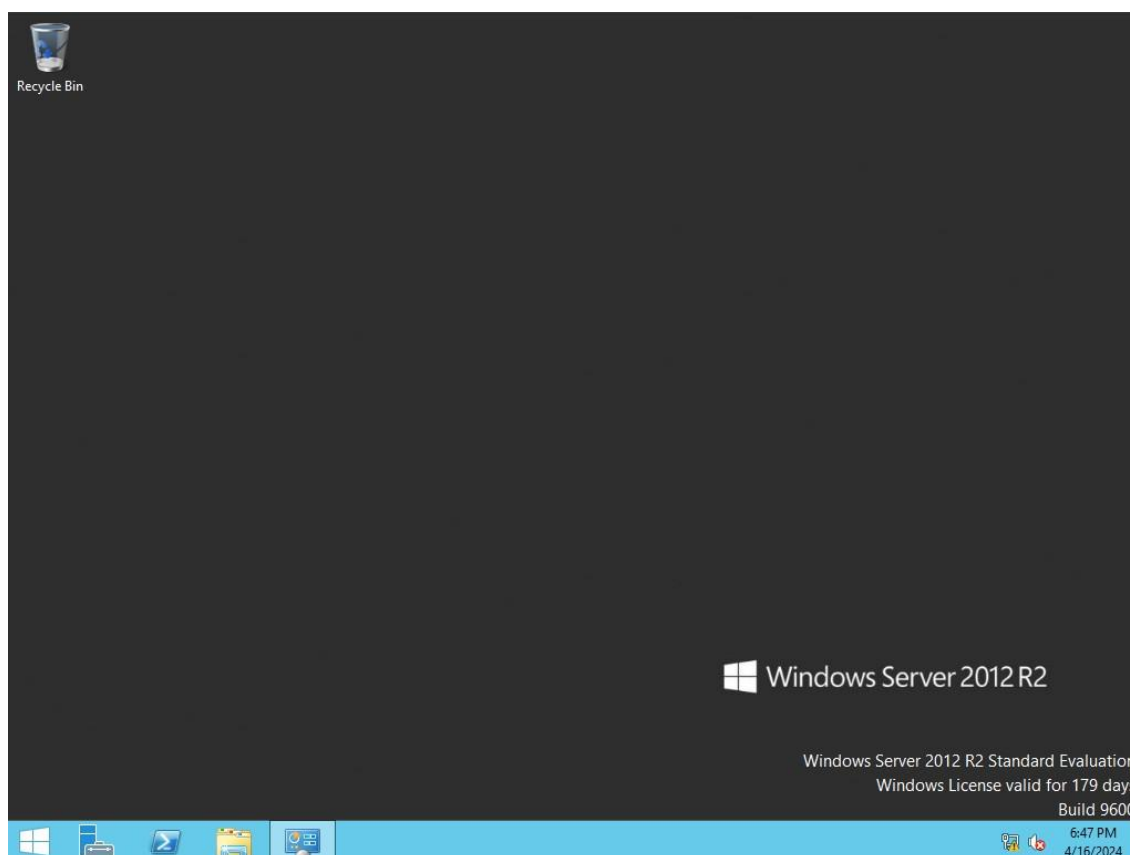
		Matriz		Filial 1		Filial 2	
		250		125		125	
Apps	LB (kbps)	Qtd	LB	Qtd	LB	Qtd	LB
Web	100	250	25000	125	12500	125	12500
E-mail	50	250	12500	125	6250	125	6250
Helpdesk	250	10	2500	5	1250	5	1250
Videoconferência	300	22	6600	12	3600	12	3600
Monitoramento	100	5	500	5	500	5	500
Sistema de Gestão de Operações	60	20	1200	10	600	10	600
Sistema de Gestão de Vendas	50	12	600	10	500	10	500
Voip	87	160	13920	100	8700	100	8700
		Total	62820	Total	33900	Total	33900
		Matriz		Filial 1		Filial 2	
Internet		58020		31050		31050	
Total Internet		120120					

## 4. IMPLEMENTAÇÃO DOS RECURSOS DE REDE

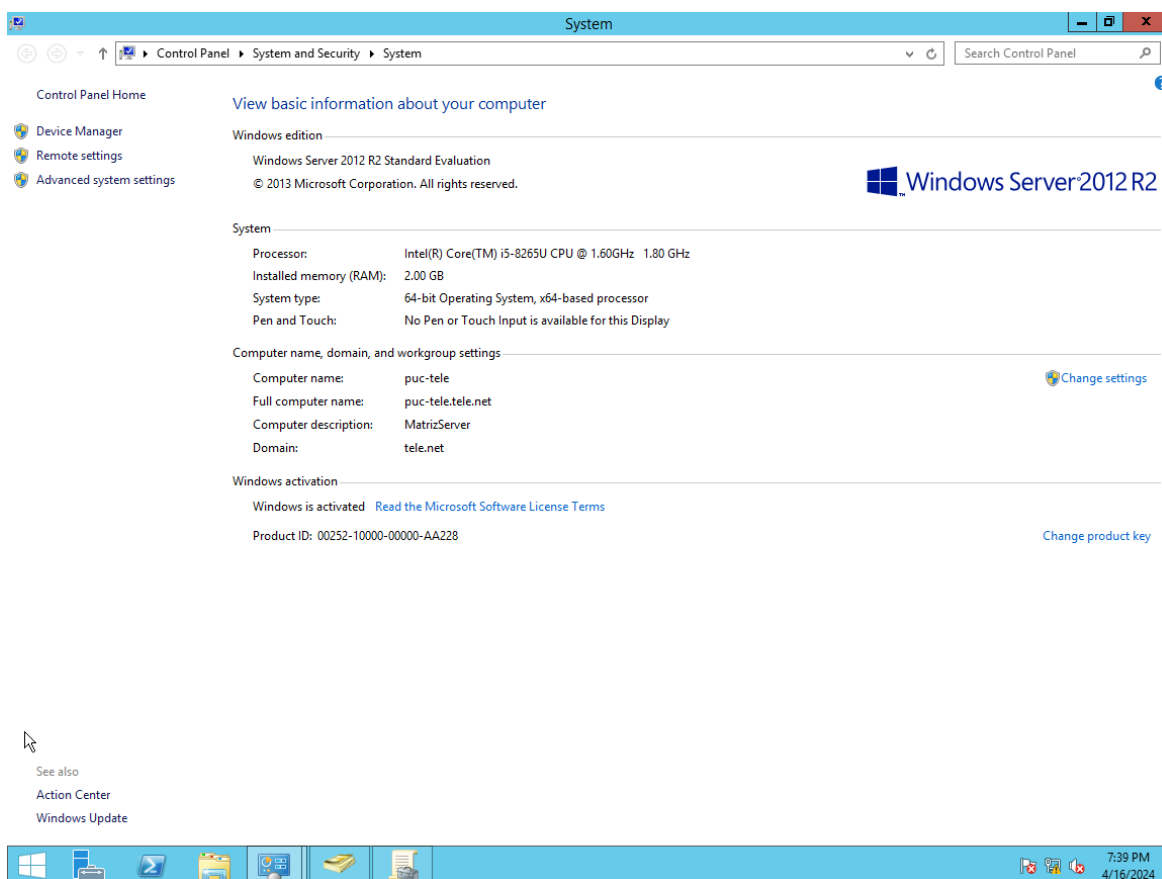
A implementação de uma infraestrutura de TI geralmente envolve a configuração de servidores com propósitos distintos para otimizar o desempenho e a segurança. Neste contexto, foi necessário a criação de um servidor na nuvem dedicado a serviços online, como hospedagem de um site no Internet Information Services (IIS), e um servidor local focado no gerenciamento de identidades e acessos através do Active Directory (AD), permitindo que a organização se beneficie da flexibilidade e escalabilidade da nuvem, enquanto mantém controle rigoroso e seguro sobre a gestão de identidades e acessos internamente

### 4.1 IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ

Foi implementado servidor local com o sistema operacional Windows Server 2012 R2, e um hardware seja suficientemente robusto para suportar o Active Directory e suas operações, considerando também futuras expansões.



*Tela de acesso Inicial do Servidor Local (Windows Server 2012 R2).*



#### 4.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO ACTIVE DIRECTORY

O Active Directory(AD) pode ser instalado através do Gerenciador do Servidor, por meio da adição de funções. O AD pode ser estruturado de forma a refletir a organização física e funcional da empresa, facilitando a gestão de usuários e máquinas em diferentes locais. Depois de instalado, é necessário configurar o domínio, que irá gerenciar as contas de usuários e políticas de segurança dentro da organização.

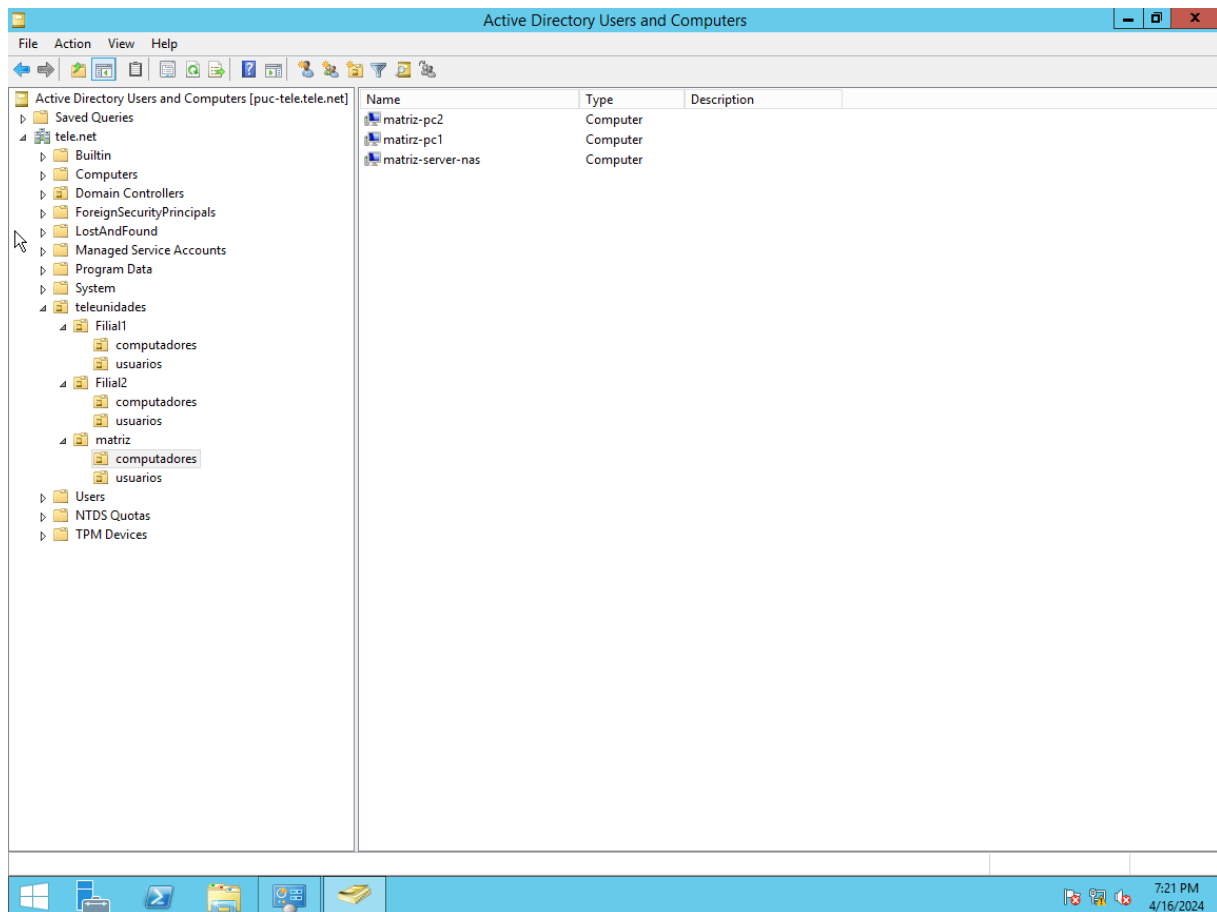
Primeiramente, é criado um domínio principal que será o núcleo da estrutura do AD. Este domínio abrigará as contas de todos os usuários, grupos e computadores da organização. Tendo como domínio principal **tele.net**.

Dentro do domínio, as Unidades Organizacionais são criadas para refletir a estrutura hierárquica da empresa. Foram criadas para a matriz e uma separada para cada filial, sendo assim **Matriz, Filial1 e Filial2**. Isso permite a delegação de controle e a aplicação de políticas de forma mais granular.

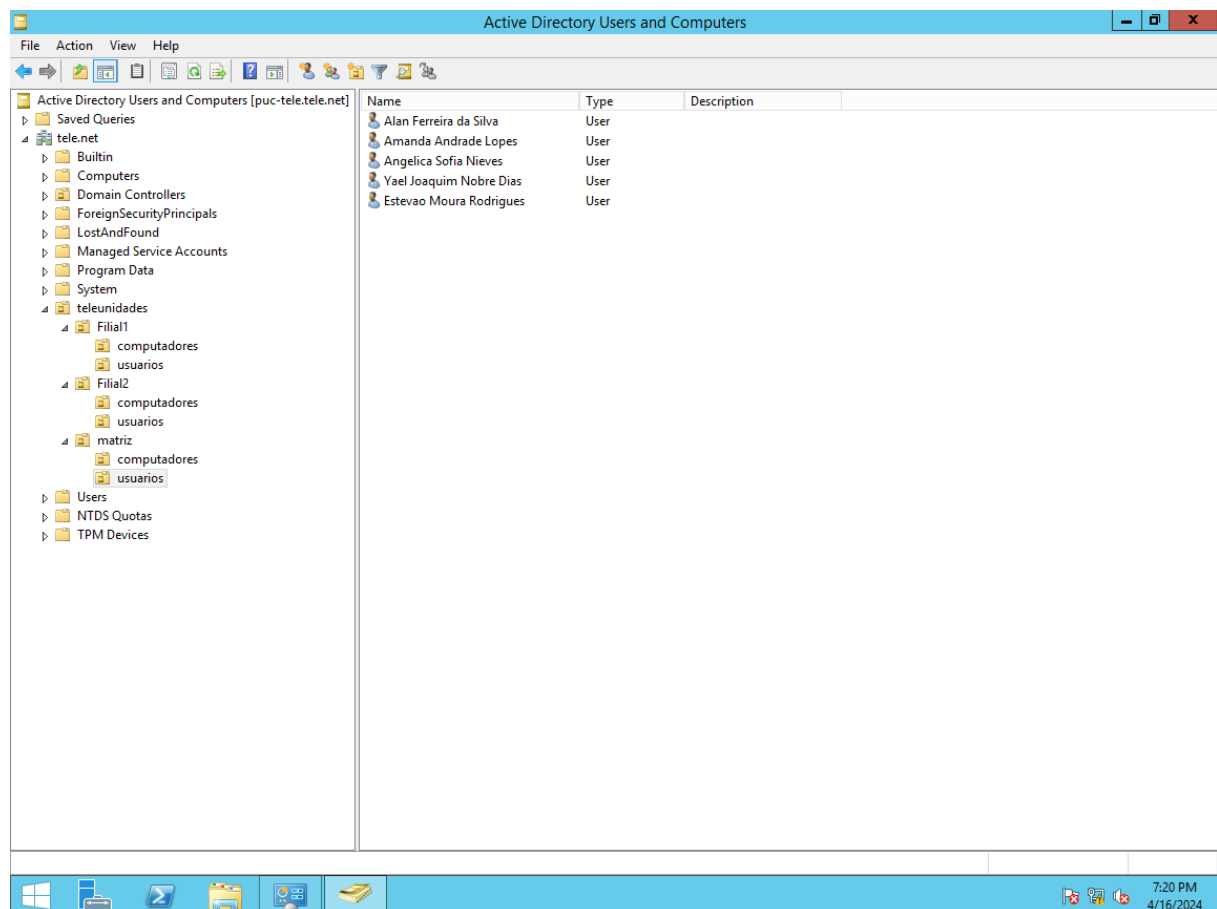
**Matriz:** Contém contas de usuários, grupos e computadores localizados na sede central.

**Filial1 e Filial2:** Similarmente, cada filial terá sua própria , contendo seus respectivos usuários, grupos e recursos de computador.





*Configuração da hierarquia de domínios no Active Directory, e lista de commputadores a Matriz*

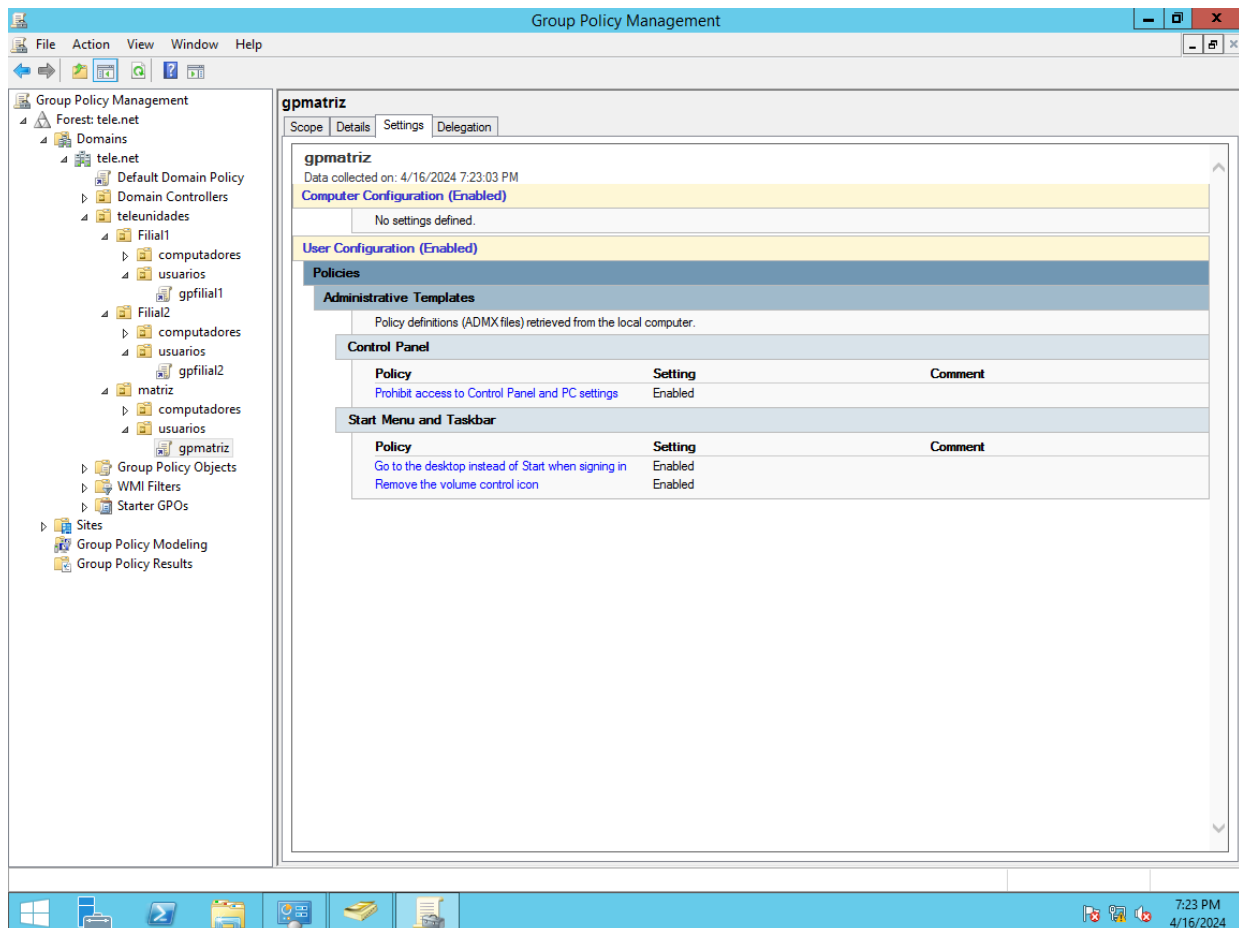


*Active Directory - Lista de usuários na Matriz*

### 4.1.2 CONFIGURAÇÃO DAS POLÍTICAS DE GRUPO

As Políticas de Grupo são usadas para gerenciar configurações de segurança, a implantação de software, e as configurações do sistema operacional em todos os computadores da rede. GPOs podem ser aplicadas em diferentes níveis, incluindo domínio e grupos específicos. As políticas de segurança que foram ser aplicadas tanto na Matriz, quanto nas filiais foram as seguintes.

- 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.



Configuração das Políticas de Grupo do Servidor

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

A primeira etapa envolve selecionar um provedor de serviços na nuvem que ofereça Windows Server como opção de sistema operacional o Amazon Web Services (AWS), foi o escolhido. Após a escolha do provedor, foi dado seguimento com a criação de uma instância de máquina virtual (VM) com Windows Server 2016, garantindo o acesso às últimas atualizações de segurança e funcionalidades. Para esse fim dentro do AWS são necessárias algumas configurações adicionais.

### 4.2.1 CONFIGURAÇÃO DA VPC

Primeiramente, foi configurada um Virtual Private Cloud (VPC) nomeada **puctele-vpc**. Dentro dessa VPC, você foram criadas quatro subredes: duas subredes públicas que terão acesso direto à Internet através de um Internet Gateway, e duas subredes privadas, que são isoladas de acesso direto à Internet para garantir maior segurança para recursos que não necessitam de exposição direta.

vpc-05ca0d6cc35330cd4 / puctele-vpc Ações ▼

**Detalhes** Informações

ID da VPC vpc-05ca0d6cc35330cd4	Estado 🟢 Available	Nomes de host DNS Habilitado	Resolução de DNS Habilitado
Localização Default	Conjunto de opções de DHCP dopt-0161685ae100e3cdb	Tabela de rota principal rtb-06252339d7b9ae151	Network ACL principal acl-0d64e018e9c1627ad
VPC padrão Não	CIDR IPv4 10.0.0.0/16	Grupo IPv6 -	CIDR IPv6 (Grupo de borda de rede) -
Métricas de uso do endereço de rede Desabilitado	Grupos de regras do Firewall de DNS do resolvidor do Route 53 <span>❌ Falha ao carregar grupos de regras</span>	ID do proprietário 094256802884	

**Mapa de recursos** CIDRs Logs de fluxos Tags Integrações

**Mapa de recursos** Informações

VPC [Mostrar detalhes](#)  
Sua rede virtual da AWS

puctele-vpc

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

**us-east-1a**

- 🟢 puctele-subnet-public1-us-east-1a
- 🟢 puctele-subnet-private1-us-east-1a

**us-east-1b**

- 🟢 puctele-subnet-public2-us-east-1b
- 🟢 puctele-subnet-private2-us-east-1b

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

- rtb-06252339d7b9ae151
- puctele-rtb-private2-us-east-1b
- puctele-rtb-public
- puctele-rtb-private1-us-east-1a

Conexões de rede (1)  
Conexões com outras redes

puctele-igw

*Detalhes das configurações da instância de VPC no AWS*

Tabelas de rotas (5) Informações							
Find resources by attribute or tag							
<input type="checkbox"/>	Name	ID da tabela de rotas	Associações explícitas...	Associações de ...	Princ...	VPC	ID do proprietário
<input type="checkbox"/>	-	rtb-06252339d7b9ae151	-	-	Sim	vpc-05ca0d6cc35330cd4   puct...	094256802884
<input type="checkbox"/>	puctele-rtb-private2-us-east-1b	rtb-0d9bcecf26820c1c	-	-	Não	vpc-05ca0d6cc35330cd4   puct...	094256802884
<input type="checkbox"/>	-	rtb-0c232c2339ea770e7	-	-	Sim	vpc-0b1628b8b5e056c22	094256802884
<input type="checkbox"/>	puctele-rtb-public	rtb-0d2fef6cb761c8735	2 sub-redes	-	Não	vpc-05ca0d6cc35330cd4   puct...	094256802884
<input type="checkbox"/>	puctele-rtb-private1-us-east-1a	rtb-0e6343a492ecd1f80	2 sub-redes	-	Não	vpc-05ca0d6cc35330cd4   puct...	094256802884

### Tabelas de rotas da VPC

Além disso, foi criado um grupo de segurança que funciona como firewall virtual para controlar o acesso às instâncias nas subredes. Neste caso, com regras específicas para permitir tráfego HTTP (porta 80) e RDP (porta 3389), garantindo que apenas clientes autorizados possam acessar os serviços por essas portas.

sg-0008494914ea225db - PucTele

Ações

Detalhes

Nome do grupo de segurança

PucTele

ID do grupo de segurança

sg-0008494914ea225db

Descrição

Web Terminal remoto

ID da VPC

vpc-05ca0d6cc35330cd4

Proprietário

094256802884

Número de regras de entrada

2 Entradas de permissão

Número de regras de saída

1 Entrada de permissão

Regras de entrada

Regras de saída

Tags

Regras de entrada (2)

Pesquisar

Gerenciar tags

Editar regras de entrada

< 1 >

	Name	ID da regra do grup...	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
<input type="checkbox"/>	-	sgr-01beccb507cb4028b	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web
<input type="checkbox"/>	-	sgr-0f56d5522edcbd87	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso Terminal Remoto

### Regras de Entrada do Grupo de Segurança da VPC

## 4.2.2 CONFIGURAÇÃO SERVIDOR WEB E ISS

Foi criada uma instância de servidor no Amazon EC2 com Windows Server 2016, denominada **PucTeleWebServer**, com uma Amazon Machine Image (AMI) contendo o *Windows Server 2016 Base*. Buscando uma configuração melhor se adapte às necessidades de desempenho e orçamento do servidor, foi escolhida a instância de tipo t2.large.

Seguindo com a implementação a instância foi incluída na VPC **puctele-vpc** e sendo submetida às suas configurações de grupos de segurança, para controle de acesso à instância através das portas específicas.

Com a VM operacional, o próximo passo foi a instalação do IIS, que é o serviço de web server integrado ao Windows Server. Esta instalação pode ser realizada através do Gerenciador do Servidor, adicionando as funções e recursos necessários

para suportar as aplicações web que serão hospedadas no mesmo.

Resumo da instância para i-017763af93f1d28f5 (PucTeleWebServer) Informações

Conectar

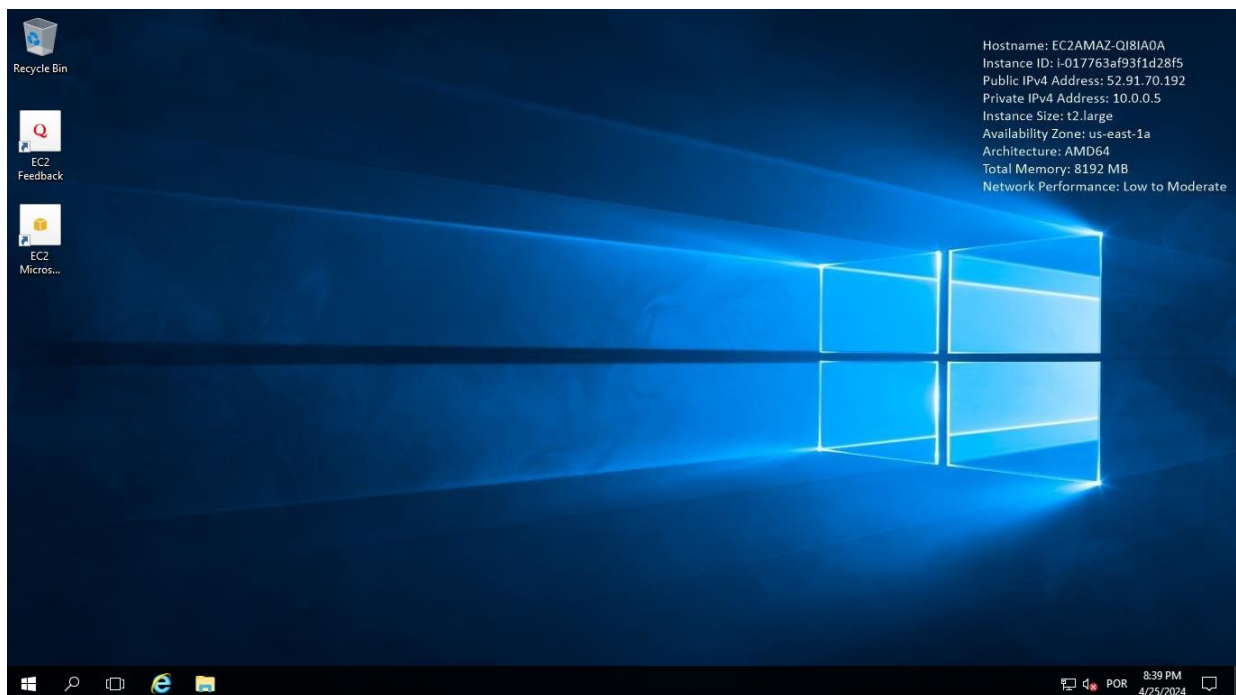
Estado da instância ▼

Ações ▼

Atualizado há 2 minutos

<div>ID da instância</div> <div><div></div><div>i-017763af93f1d28f5 (PucTeleWebServer)</div></div>	<div>Endereço IPv4 público</div> <div><div></div><div>18.206.39.111   <a href="#">endereço aberto</a></div></div>	<div>Endereços IPv4 privados</div> <div><div></div><div>10.0.0.5</div></div>
<div>Endereço IPv6</div> <div><div></div><div>—</div></div>	<div>Estado da instância</div> <div><div></div><div>Executando</div></div>	<div>DNS IPv4 público</div> <div><div></div><div>ec2-18-206-39-111.compute-1.amazonaws.com   <a href="#">endereço aberto</a></div></div>
<div>Tipo de nome do host</div> <div><div></div><div>Nome do IP: ip-10-0-0-5.ec2.internal</div></div>	<div>Nome do DNS de IP privado (somente IPv4)</div> <div><div></div><div>ip-10-0-0-5.ec2.internal</div></div>	
<div>Nome do DNS do recurso privado de resposta</div> <div><div></div><div>—</div></div>	<div>Tipo de instância</div> <div><div></div><div>t2.large</div></div>	<div>Endereços IP elásticos</div> <div><div></div><div>—</div></div>
<div>Endereço IP atribuído automaticamente</div> <div><div></div><div>18.206.39.111 [IP público]</div></div>	<div>ID da VPC</div> <div><div></div><div>vpc-05ca0d6cc35330cd4 (puctele-vpc) <a href="#">↗</a></div></div>	<div>Descoberta do AWS Compute Optimizer</div> <div><div></div><div>Opte por participar do AWS Compute Optimizer para obter recomendações.</div></div>
<div>Função do IAM</div> <div><div></div><div>—</div></div>	<div>ID da sub-rede</div> <div><div></div><div>subnet-0a8759fe3ea433d63 (puctele-subnet-public1-us-east-1a) <a href="#">↗</a></div></div>	<div>Nome do Grupo do Auto Scaling</div> <div><div></div><div>—</div></div>
<div>IMDSv2</div> <div><div></div><div>Required</div></div>		<div><a href="#">Saiba mais</a> <a href="#">↗</a></div>

Detalhes das configurações da instância do Servidor Web no EC2 da AWS



Tela Inicial de acesso do Servidor Web

Após o processo de configuração do IIS, obten-se um site, o caminho físico para os arquivos no servidor (diretório onde os arquivos HTML, CSS e outros estão armazenados), e a porta pela qual o site será acessado. Uma vez configurado e habilitado, o site fica acessível via navegador web na porta especificada, permitindo que usuários visitem e interajam com o conteúdo hospedado no servidor IIS.

The screenshot displays a web browser window with the address bar showing `http://52.91.70.192/`. The website has a header with the PUC Minas logo. The main content area is titled "Projeto Infraestrutura - Telemarketing G12" and contains several paragraphs of text. A sidebar on the left lists a "Conteúdo" (Content) table of contents. A right sidebar provides details about the "Grupo" (Group) and the "Professor" (Professor).

**Projeto Infraestrutura - Telemarketing G12**

O grupo optou pela escolha de uma empresa de telemarketing com um quadro de funcionários de aproximadamente 600 colaboradores que prestam serviço, de venda e cobrança, para empresas de diferentes segmentos do mercado.

É fundamental que a empresa disponha de uma infraestrutura robusta capaz de sustentar chamadas telefônicas, transferência de dados e comunicações eficientes, tanto entre os funcionários presentes no local de trabalho quanto os remotos e os clientes em atendimento. Investir em sistemas de telefonia que ofereçam recursos como discagem automática e gravação de chamadas é crucial para otimizar os processos de comunicação.

É importante contar com um setor dedicado à resolução de problemas técnicos enfrentados pelos funcionários remotos, garantindo que eles recebam o suporte necessário para manter a produtividade. Por fim, é imprescindível adotar medidas de segurança para proteger as informações confidenciais durante todas as interações com os clientes, garantindo assim a privacidade e a integridade dos dados.

**Conteúdo**

- 1 Estrutura
  - 1 Departamento de TI
  - 2 Qualidade, desenvolvimento e segurança
  - 3 Marketing e vendas
  - 4 Produção
  - 5 Departamento de Operações Regionais
  - 6 Departamento de Vendas Regionais
  - 7 Departamento de Suporte Técnico Regional
  - 8 Recursos Humanos
  - 9 Financeiro e contábil

**Grupo**

- Alan Ferreira da Silva
- Amanda Andrade Lopes
- Angelica Sofia Nieves
- Estevão Moura Rodrigues
- Yael Joaquim Nobre Dias

**Professor**

- Alexandre Teixeira

**Instituição**

- PUC Minas

Página Inicial do Site configurado no IIS.

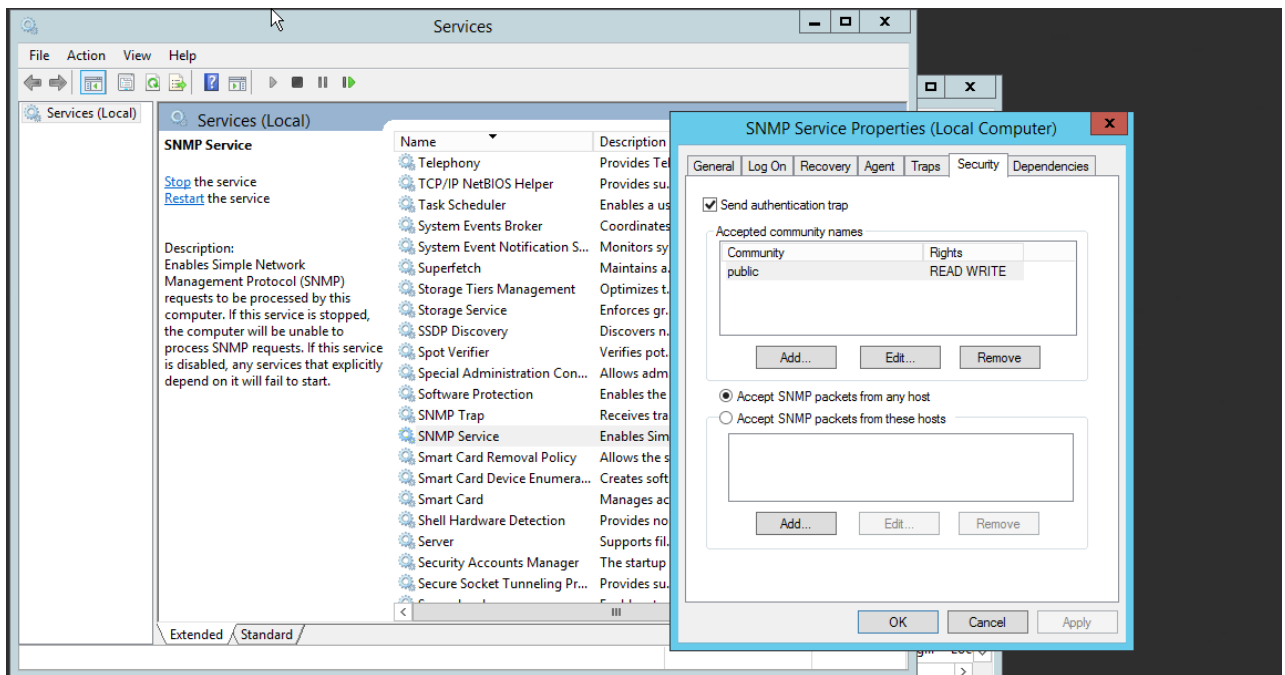
## **5. GERENCIAMENTO DE RECURSOS DOS SERVIDORES VIA ZABBIX**

O Zabbix é uma plataforma de monitoramento de código aberto altamente escalável e flexível, projetada para monitorar e rastrear o desempenho de diversos serviços de rede, servidores, e outros dispositivos de rede. Dentre suas funcionalidades podemos destacar, Coleta de Dados, Monitoramento de Desempenho da performance e a disponibilidade dos recursos, Alertas e Notificações de erros e problemas na rede, Visualização por meio de gráficos, mapas, telas e relatórios que ajudam a visualizar dados de monitoramento, suporte a scripts e automações para tarefas de administração.

O Zabbix suporta monitoramento via SNMP, o que permite coletar dados de diversos dispositivos de rede que utilizam este protocolo. SNMP é um protocolo padrão da internet usado para gerenciar e monitorar dispositivos conectados em redes IP. É amplamente suportado por diversos dispositivos, incluindo roteadores, switches, servidores e impressoras. Seu funcionamento básico consiste nos Agentes SNMP, Software que roda no dispositivo monitorado, coletando dados de gestão e resposta às solicitações de um gerenciador. O Zabbix atuando como Gerente SNMP que envia solicitações aos agentes SNMP e processa as informações recebidas.

### **5.1 CONFIGURAÇÃO DO PROTOCOLO SNMP NOS SERVIDORES**

Visando a comunicação do Zabbix com as máquinas virtuais do servidor local e cloud, foram necessárias algumas configurações nos services e firewall, incluindo a instalação do serviço SNMP e a configuração das suas propriedades. Configurando na aba de segurança adicionando a community com string public (para acesso somente de leitura) e a liberação de pacotes de hosts externos. A liberação das portas 161 e 162 sob o protocolo UDP(utilizadas na comunicação via SNMP) no firewall .



Configuração de segurança do Serviço SNMP no servidor Local

No servidor Cloud além da configuração do Serviço SNMP, também foram necessárias algumas mudanças na regras de segurança da VPC a qual a máquina virtual está submissa. Liberando as portas utilizadas pelo SNMP sob o protocolo UDP além do protocolo ICMP utilizado pelo Zabbix na comunicação inicial com os agentes.

Regras de saída (2)						
<div> <div>Pesquisar</div> <div>Gerenciar tags</div> <div>Editar regras de saída</div> </div>						
Name	ID da regra do grup...	Tipo	Protocolo	Intervalo de portas	Descrição	
-	sgr-0ae052b83aae141f5	Todo o tráfego	Tudo	Tudo	-	
SNMP	sgr-0468c4f3a582716ad	UDP personalizado	UDP	161 - 162	SNMP	

Exibição da configuração da segurança das Regras de saída da VPC

Regras de entrada (5)						
<div> <div>Pesquisar</div> <div>Gerenciar tags</div> <div>Editar regras de entrada</div> </div>						
Name	ID da regra do grup...	Tipo	Protocolo	Intervalo de portas	Descrição	
-	sgr-01beccb507cb4028b	HTTP	TCP	80	Acesso Web	
-	sgr-0f56d5522edcbd87	RDP	TCP	3389	Acesso Terminal Remoto	
SNMP	sgr-00310df35c590cb40	UDP personalizado	UDP	161 - 162	SNMP	
-	sgr-0b5164a0721940...	TCP personalizado	TCP	21	Acesso FTP	
-	sgr-064a4cfe65c49d5b9	Todos os ICMPs - IPv4	ICMP	Tudo	ICMP	

Exibição da configuração da segurança das Regras de saída da VPC



## 5.2 VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX

Com a configuração realizada nos servidores local e na nuvem, o Zabbix já estava apto a monitorá-los. Verificamos na ferramenta que a comunicação com ambos os hosts está sendo executada sem qualquer falha. Havendo a necessidade de atualização dos endereços IP na configuração dos hosts caso haja alguma alteração.

Hosts Create host Import

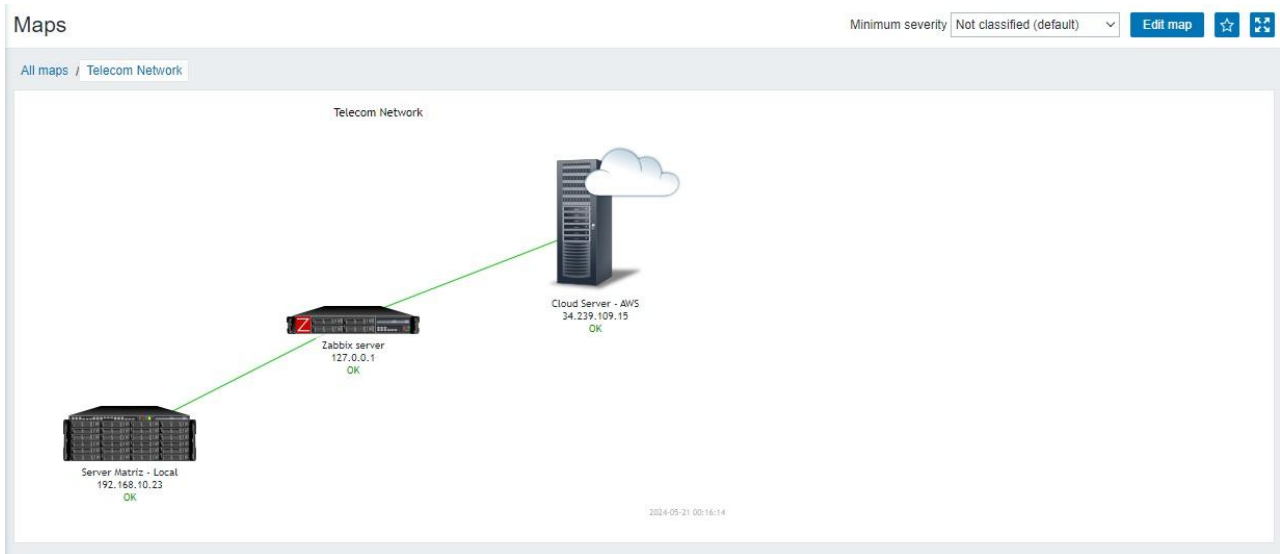
Filter

<input type="checkbox"/>	Name ▲	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
<input type="checkbox"/>	Cloud Server - AWS	Items 28	Triggers 14	Graphs 4	Discovery 3	Web	34.239.109.15:161		Windows by SNMP	Enabled	SNMP	None		
<input type="checkbox"/>	Server Matriz - Local	Items 28	Triggers 14	Graphs 4	Discovery 3	Web	192.168.10.23:161		Windows by SNMP	Enabled	SNMP	None		
<input type="checkbox"/>	Zabbix server	Items 133	Triggers 77	Graphs 27	Discovery 4	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None		

Displaying 3 of 3 found

Lista de Hosts do Zabbix, exibindo os servidores adicionados sem falhas de conexão

O Zabbix também permite a visualização da nossa infraestrutura de rede monitorada por meio de um mapa, exibindo e sua integração com o servidor local e o servidor na nuvem.

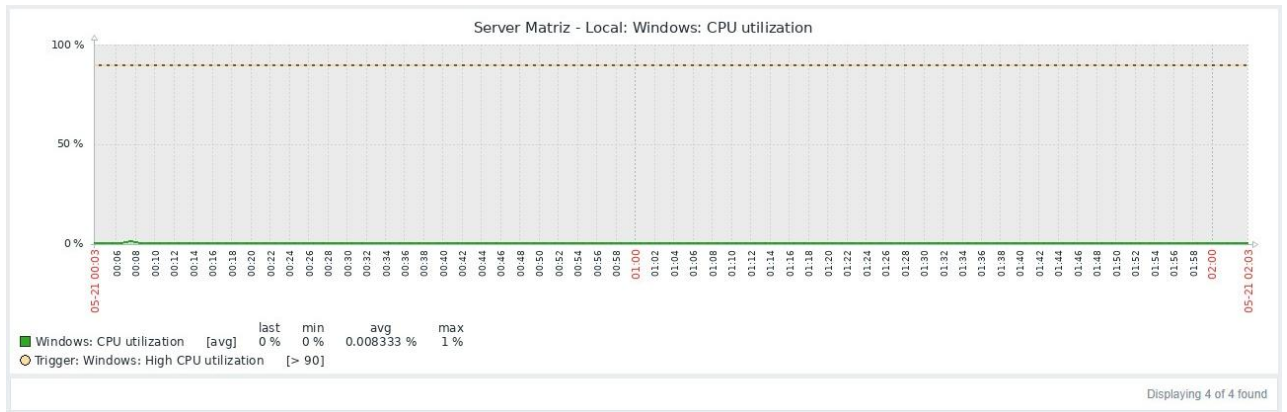


Exibição do mapa de hosts conectados ao Zabbix

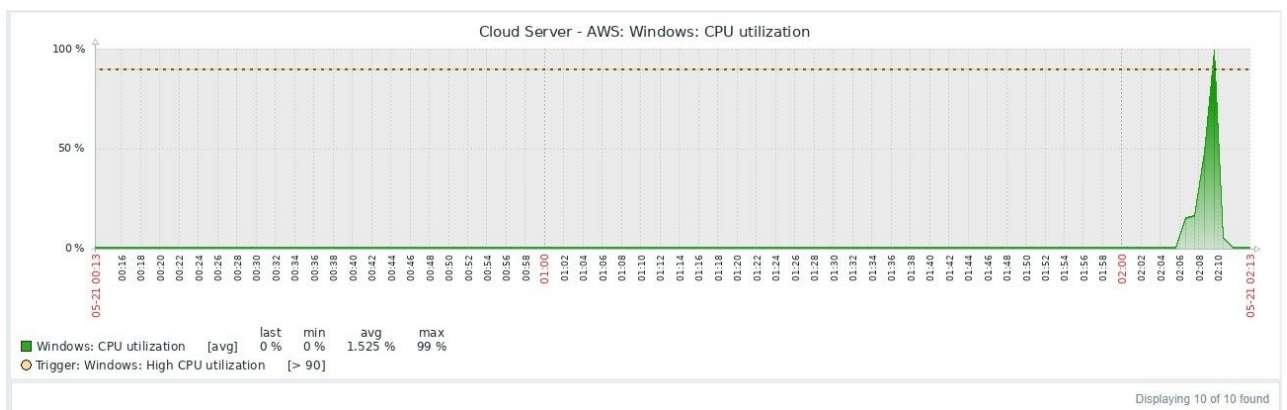
Com o Zabbix, é possível visualizar o desempenho e a saúde da infraestrutura por meio de gráficos integrados em uma interface centralizada, proporcionando uma visão abrangente e detalhada. Esses gráficos de monitoramento de recursos de servidores em rede são ferramentas essenciais para a gestão e manutenção de sistemas de TI, oferecendo uma representação visual em tempo real de diversos

parâmetros críticos, como uso da CPU, memória, disco e rede. Isso facilita a detecção precoce de problemas, permitindo uma resposta rápida e informada, garantindo a continuidade e a eficiência dos serviços.

Gráficos de uso da CPU no Zabbix mostram a carga de processamento que cada servidor está enfrentando, ajudando a identificar picos de utilização que podem indicar a necessidade de otimização ou aumento de capacidade.

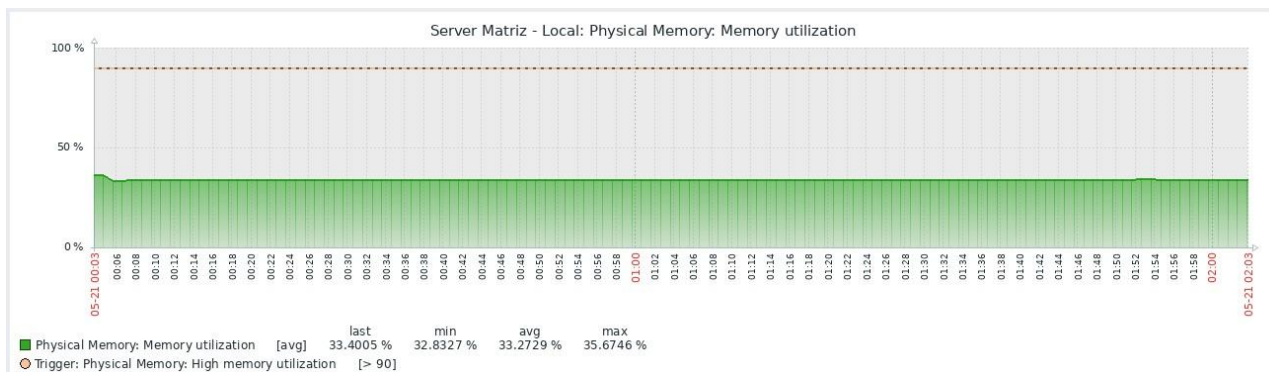


*Servidor Local: Gráfico de Uso de CPU*

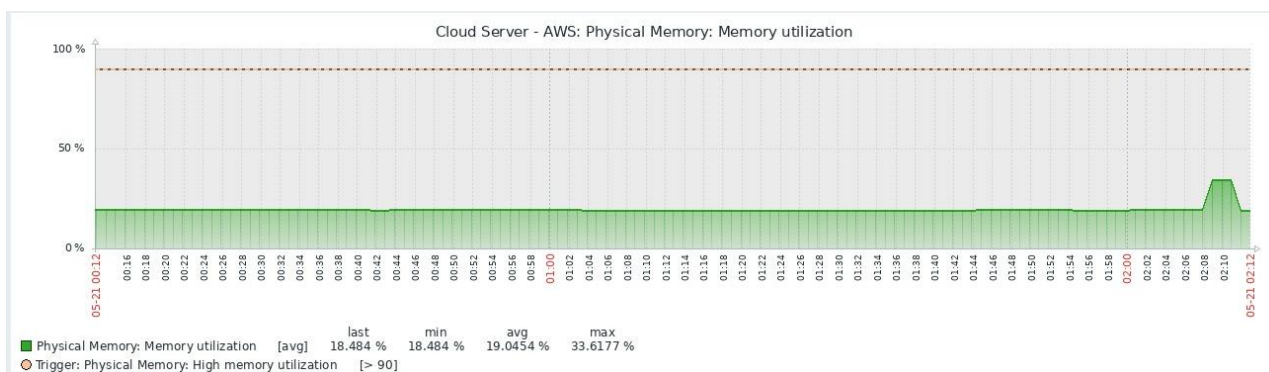


*Servidor Cloud (AWS): Gráfico de Uso de CPU*

Gráficos de uso da memória revelam quanta memória RAM está sendo consumida, possibilitando a detecção de possíveis vazamentos de memória ou a necessidade de expansão para suportar aplicações mais exigentes.

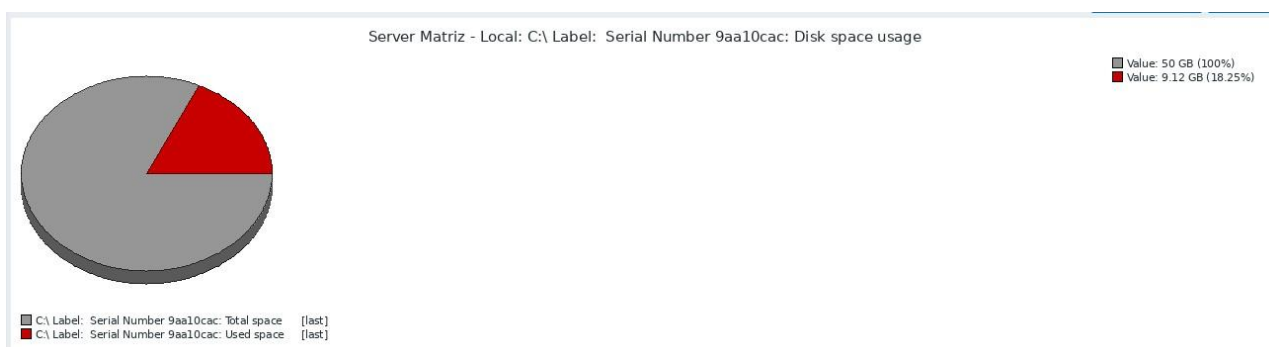


Servidor Local: Gráfico de Uso da memória

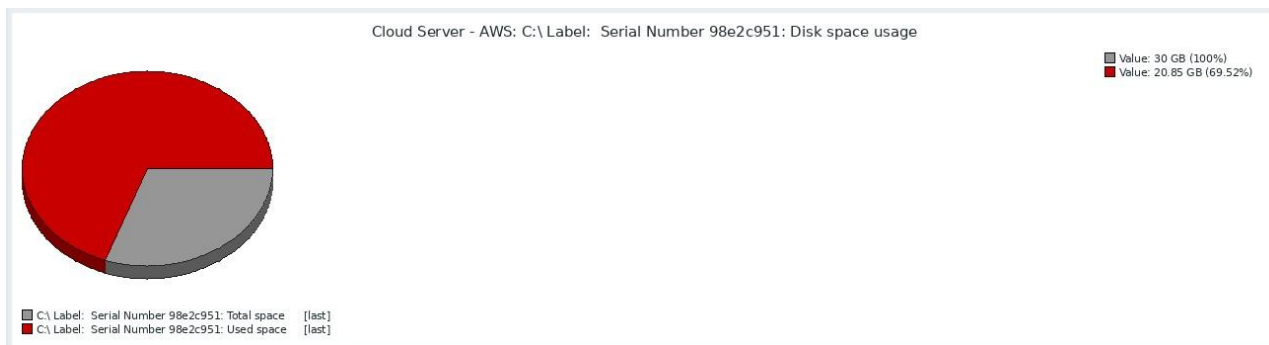


Servidor Cloud (AWS): Gráfico de Uso da memória

Gráficos de uso do disco monitoram a quantidade de espaço utilizado e a taxa de leitura/escrita, ajudando a prever quando o armazenamento poderá se tornar um gargalo ou a identificar problemas de desempenho relacionados ao disco.

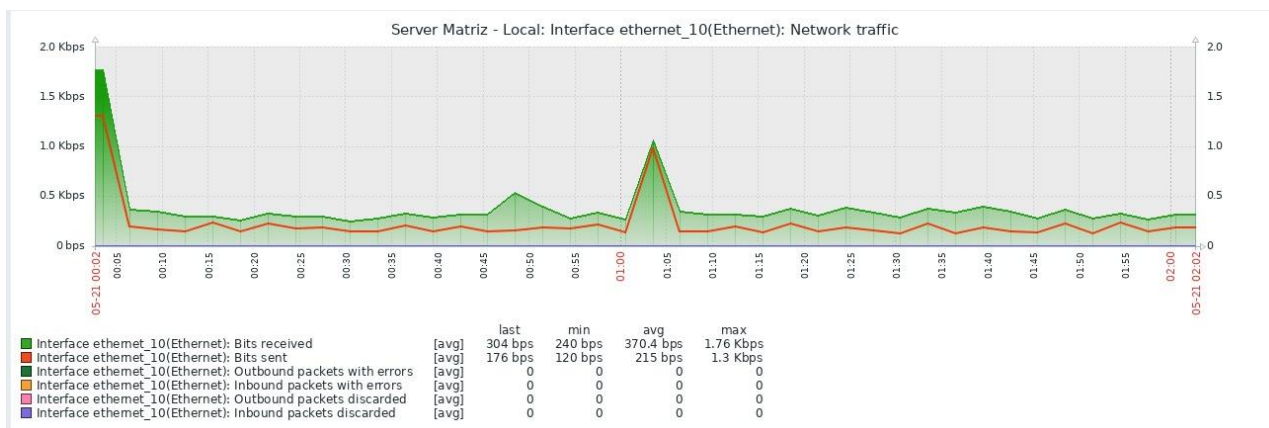


Servidor Local: Gráfico de Uso do Espaço de Disco

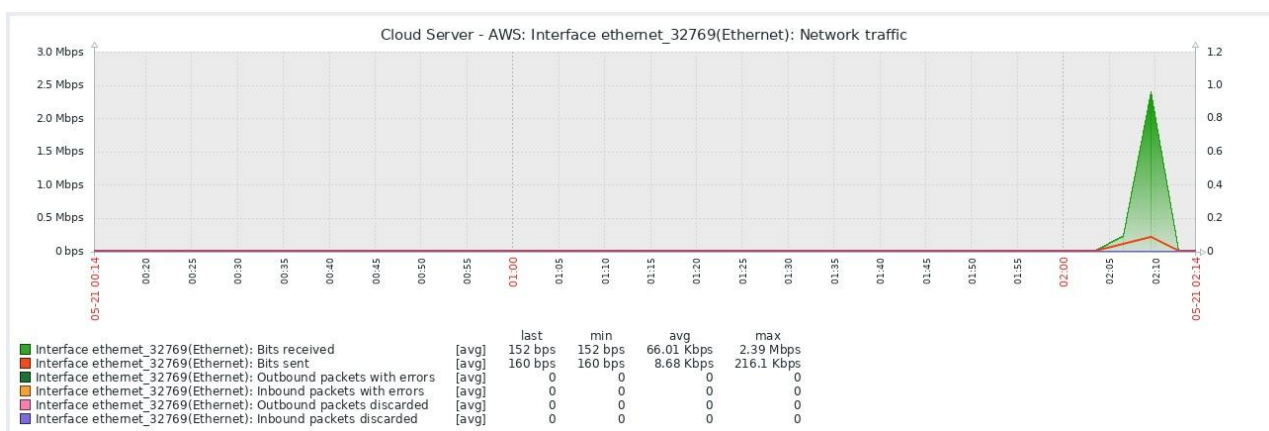


Servidor Cloud (AWS): Gráfico de Uso do Espaço de Disco

Gráficos de uso da rede exibem o tráfego de dados entre os servidores e a rede, permitindo a identificação de congestionamentos, falhas de comunicação ou possíveis ataques de rede.



Servidor Local: Gráfico de Uso do Tráfego de Rede



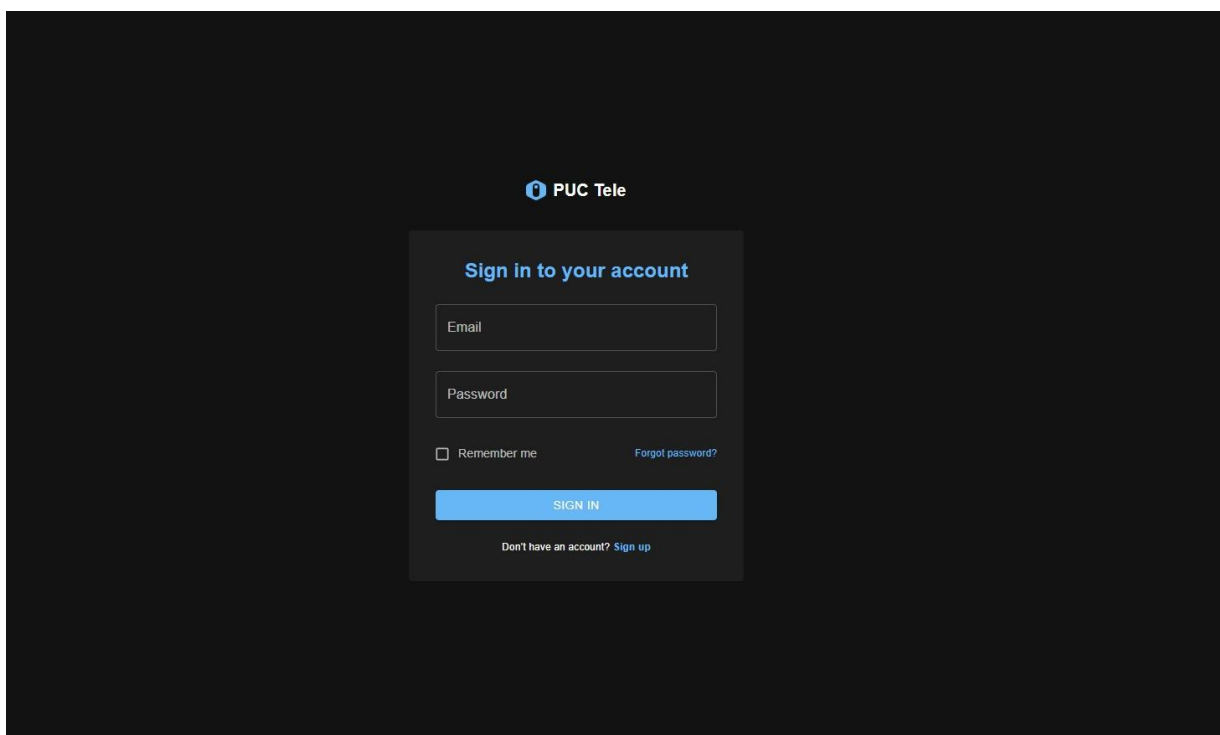
Servidor Cloud (AWS): Gráfico de Uso do Tráfego de Rede

## 6. APLICAÇÃO WEB PARA CONTROLE E GERENCIAMENTO DO BACK-END

As aplicações web são essenciais no contexto atual, pois permitem acesso a funcionalidades complexas diretamente pelo navegador, sem a necessidade de instalação de softwares adicionais. Isso facilita a manutenção, atualização e distribuição de novas funcionalidades.

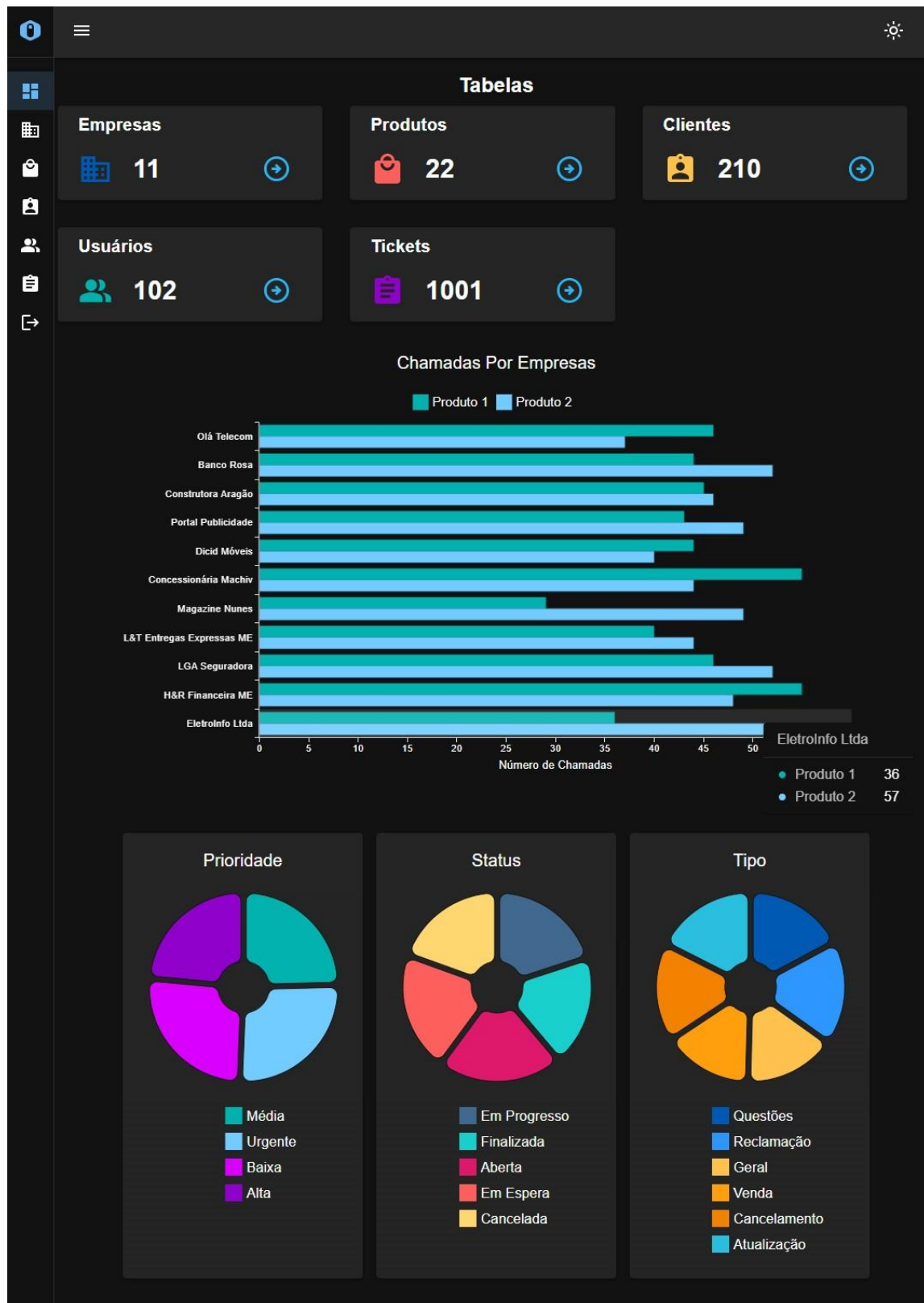
Para garantir eficiência e escalabilidade, foi implementada uma aplicação web desenvolvida na plataforma Node.js. A interface de usuário foi construída com Next.js, um framework React que suporta renderização no servidor (SSR) e geração de sites estáticos. Isso garante carregamento rápido das páginas e excelente performance. O backend da aplicação foi desenvolvido com Express.js, um framework leve e flexível, ideal para criar servidores web e APIs robustas. Ele oferece uma ampla gama de funcionalidades através de middlewares, facilitando o gerenciamento de rotas, autenticação, validação de dados e comunicação com o banco de dados.

Foi utilizado PostgreSQL, um sistema de banco de dados relacional poderoso e escalável, para armazenar e gerenciar os dados críticos da empresa. PostgreSQL é conhecido por sua conformidade com o padrão SQL, extensibilidade e forte foco em integridade dos dados.



*Aplicação Web: Tela de login para controle de acesso a aplicação.*

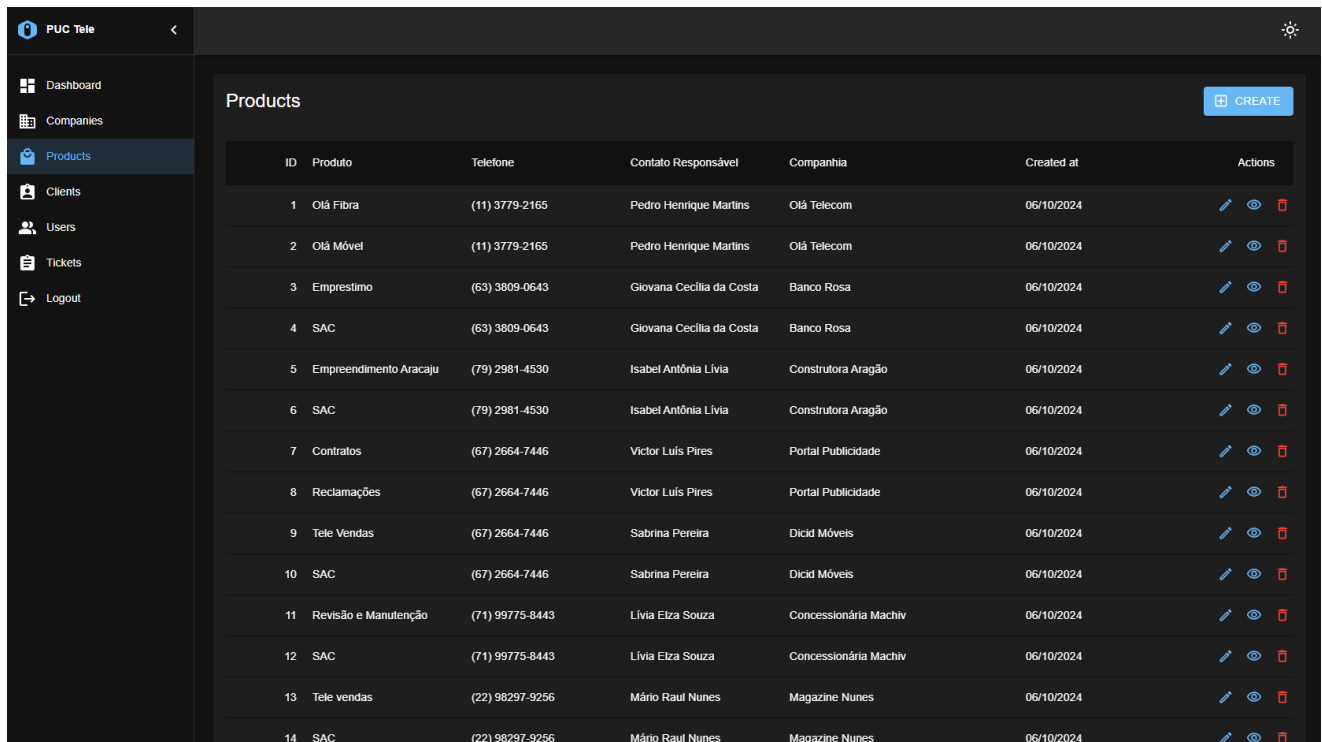
Foi criado um sistema de controle de acesso utilizando Tokens para autenticação e autorização de usuários. Apenas usuários autenticados e autorizados podem acessar a aplicação, garantindo que informações sensíveis sejam protegidas.













































Aplicação Web: Tela de principal com exibição e gráficos e cards com informações das tabelas



A aplicação inclui um dashboard interativo que exibe informações críticas de forma visual e intuitiva, com gráficos para mostra o número de tickets abertos, fechados e pendentes ao longo do tempo, permitindo monitorar o desempenho do suporte ao cliente. Além de informações como distribuição dos tickets para as empresas e seus respectivos produtos e números dos registros nas tabelas.

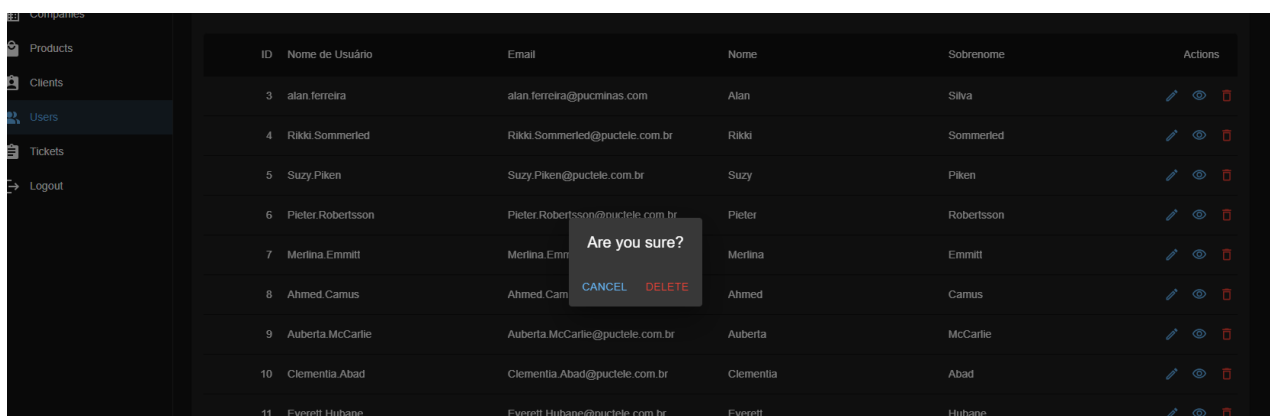


The screenshot shows the 'Products' section of the PUC Tele application. A sidebar on the left contains navigation links: Dashboard, Companies, Products (selected), Clients, Users, Tickets, and Logout. The main area displays a table with 14 rows of product data. Each row includes an ID, product name, phone number, contact person, company, creation date, and action icons (edit, view, delete). A 'CREATE' button is located in the top right corner of the table area.




























ID	Produto	Telefone	Contato Responsável	Companhia	Created at	Actions
1	Olá Fibra	(11) 3779-2165	Pedro Henrique Martins	Olá Telecom	06/10/2024	  
2	Olá Móvel	(11) 3779-2165	Pedro Henrique Martins	Olá Telecom	06/10/2024	  
3	Emprestimo	(63) 3809-0643	Giovana Cecilia da Costa	Banco Rosa	06/10/2024	  
4	SAC	(63) 3809-0643	Giovana Cecilia da Costa	Banco Rosa	06/10/2024	  
5	Empreendimento Aracaju	(79) 2981-4530	Isabel Antônia Livia	Construtora Aragão	06/10/2024	  
6	SAC	(79) 2981-4530	Isabel Antônia Livia	Construtora Aragão	06/10/2024	  
7	Contratos	(67) 2664-7446	Victor Luis Pires	Portal Publicidade	06/10/2024	  
8	Reclamações	(67) 2664-7446	Victor Luis Pires	Portal Publicidade	06/10/2024	  
9	Tele Vendas	(67) 2664-7446	Sabrina Pereira	Dicid Móveis	06/10/2024	  
10	SAC	(67) 2664-7446	Sabrina Pereira	Dicid Móveis	06/10/2024	  
11	Revisão e Manutenção	(71) 99775-8443	Livia Elza Souza	Concessionária Machiv	06/10/2024	  
12	SAC	(71) 99775-8443	Livia Elza Souza	Concessionária Machiv	06/10/2024	  
13	Tele vendas	(22) 98297-9256	Mário Raul Nunes	Magazine Nunes	06/10/2024	  
14	SAC	(22) 98297-9256	Mário Raul Nunes	Magazine Nunes	06/10/2024	  

Aplicação Web: Tela de com listagem dos dados da tabela de produtos.

É possível listar todos os dados das tabelas registradas no banco de dados através de uma requisição à API REST, utilizando paginação para acelerar a aquisição dos dados e facilitar a leitura. Além disso, são exibidas opções de ações para cada registro, como a criação de um novo registro, a exibição detalhada dos dados, a edição de registros existentes e a exclusão.

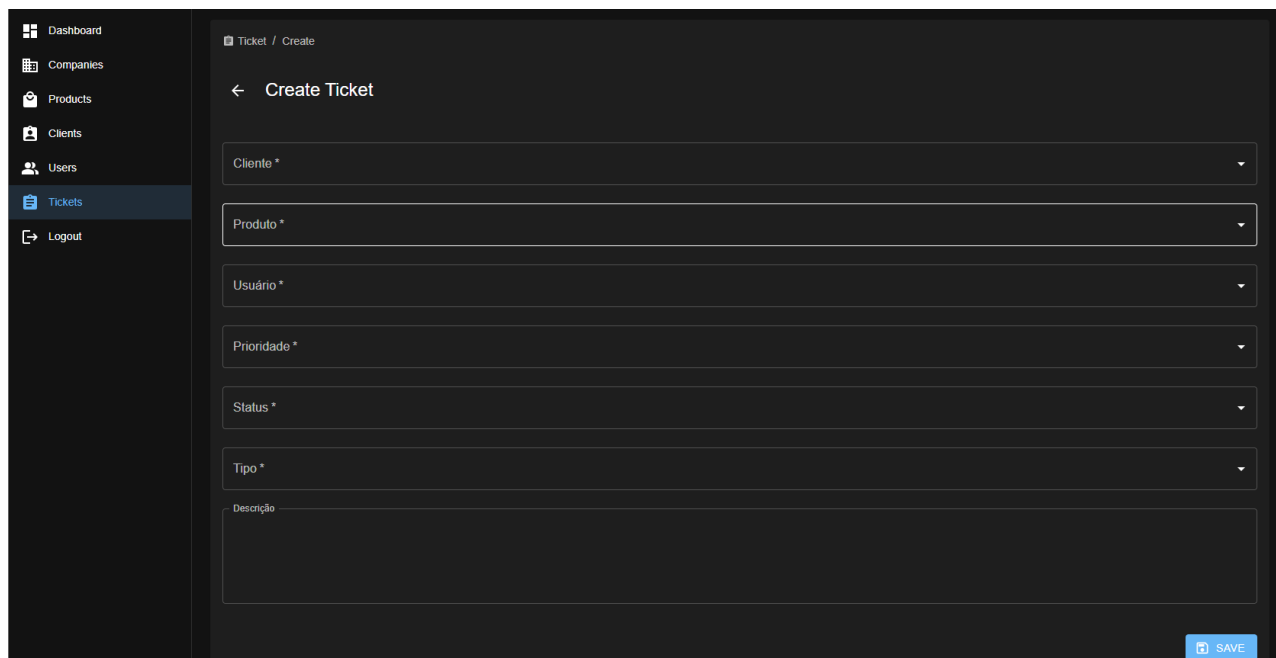


The screenshot shows the 'Users' section of the PUC Tele application. A sidebar on the left contains navigation links: Products, Clients, Users (selected), Tickets, and Logout. The main area displays a table with 11 rows of user data. Each row includes an ID, user name, email, first name, last name, and action icons (edit, view, delete). A confirmation dialog box with the text 'Are you sure?' and buttons 'CANCEL' and 'DELETE' is overlaid on the table, indicating a delete action is being performed.

ID	Nome de Usuário	Email	Nome	Sobrenome	Actions
3	alan.ferreira	alan.ferreira@pucminas.com	Alan	Silva	  
4	Rikdi.Sommerled	Rikdi.Sommerled@puctele.com.br	Rikdi	Sommerled	  
5	Suzy.Piken	Suzy.Piken@puctele.com.br	Suzy	Piken	  
6	Pieter.Robertsson	Pieter.Robertsson@puctele.com.br	Pieter	Robertsson	  
7	Merlina.Emmitt	Merlina.Emmitt@puctele.com.br	Merlina	Emmitt	  
8	Ahmed Camus	Ahmed.Camus@puctele.com.br	Ahmed	Camus	  
9	Auberta.McCarlie	Auberta.McCarlie@puctele.com.br	Auberta	McCarlie	  
10	Clementia.Abad	Clementia.Abad@puctele.com.br	Clementia	Abad	  
11	Everett.Hubane	Everett.Hubane@puctele.com.br	Everett	Hubane	  

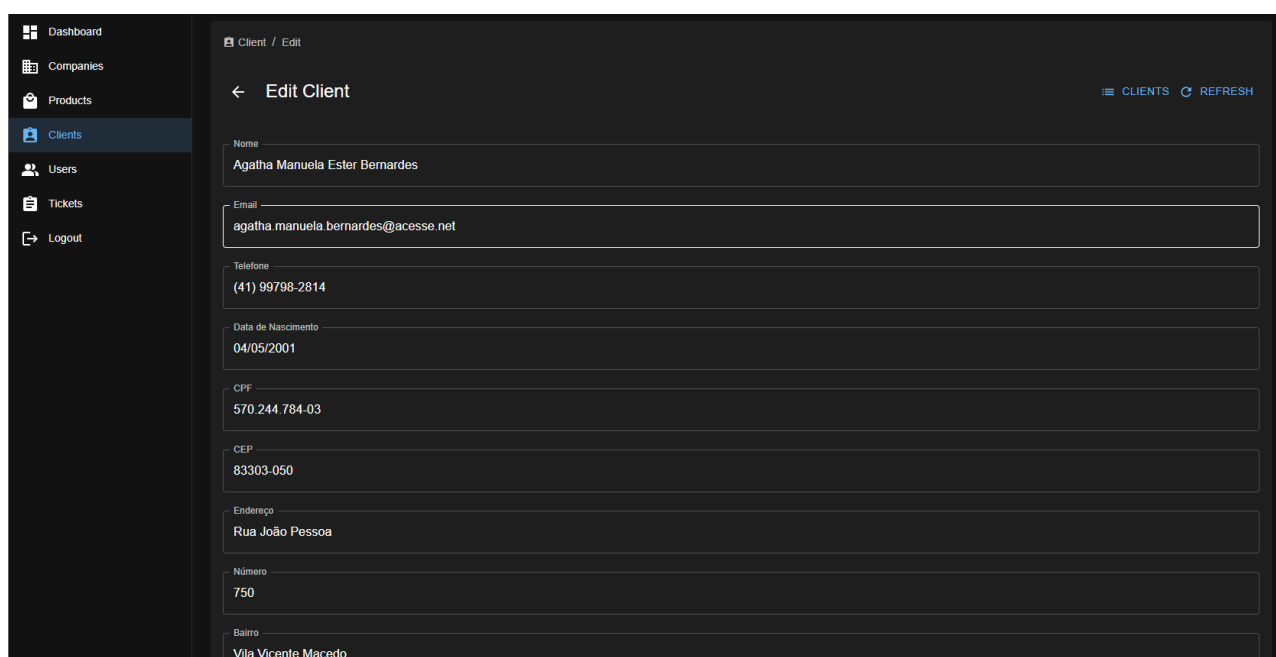
Aplicação Web: Tela de com listagem da tabela de usuários, exemplo de uma ação de exclusão.

É possível a criação de tickets de registro de chamadas através da aplicação. Esses tickets são registrados na tabela de tickets, permitindo que a equipe de visualize e gerencie as solicitações de forma eficiente.



Aplicação Web: Tela de criação de tickets, com seletores de produtos, usuários e clientes além de outros campos.

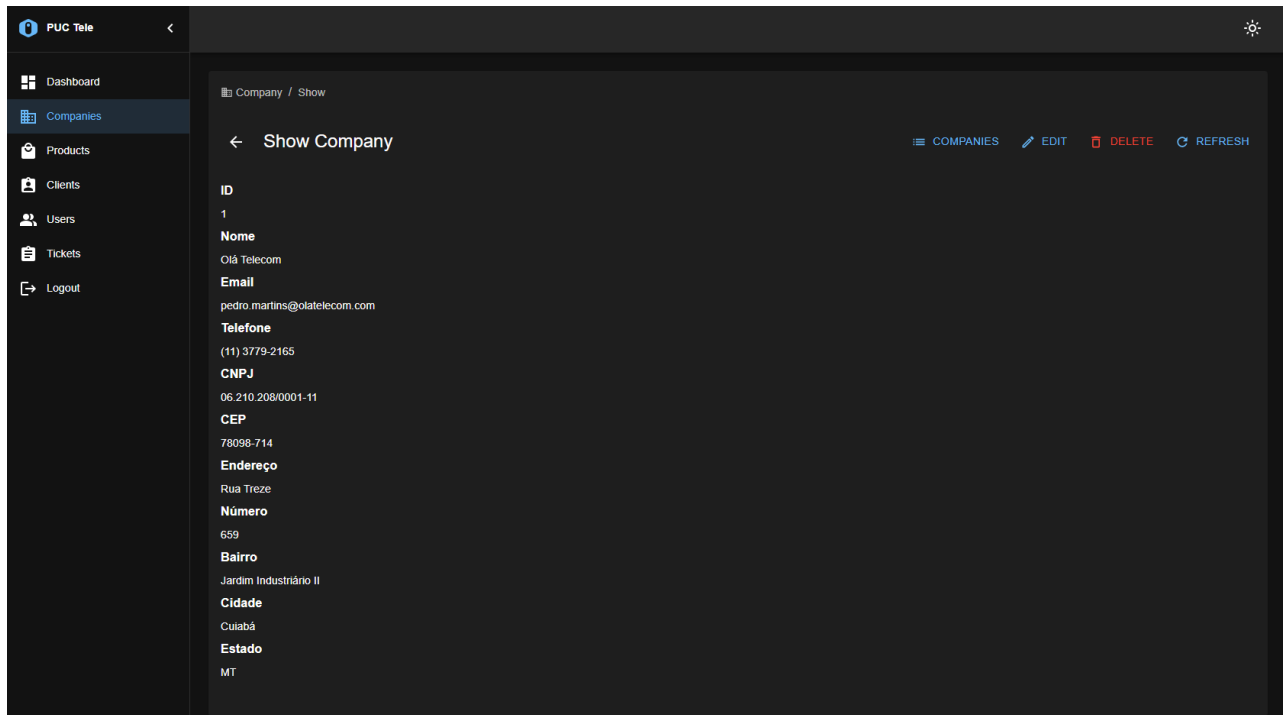
Administradores podem adicionar, editar ou remover todo e qualquer registro nas suas respectivas tabelas. A gestão de clientes é realizada através da tabela de clientes, onde é possível visualizar e atualizar os dados dos clientes.



Aplicação Web: Tela de edição de clientes, com persistência dos dados registrados.



Também é possível a visualização de um registro com informações mais detalhadas. Todas as operações exibidas podem ser executadas igualmente em qualquer objeto ou tabela.



*Aplicação Web: Tela de exibição de uma empresa registrada, com informações mais detalhadas, a listagem das tabelas possui menos dados para melhor visualização.*

## 6.1 REGISTRO DA ESTRUTURA DE TABELAS DA APLICAÇÃO

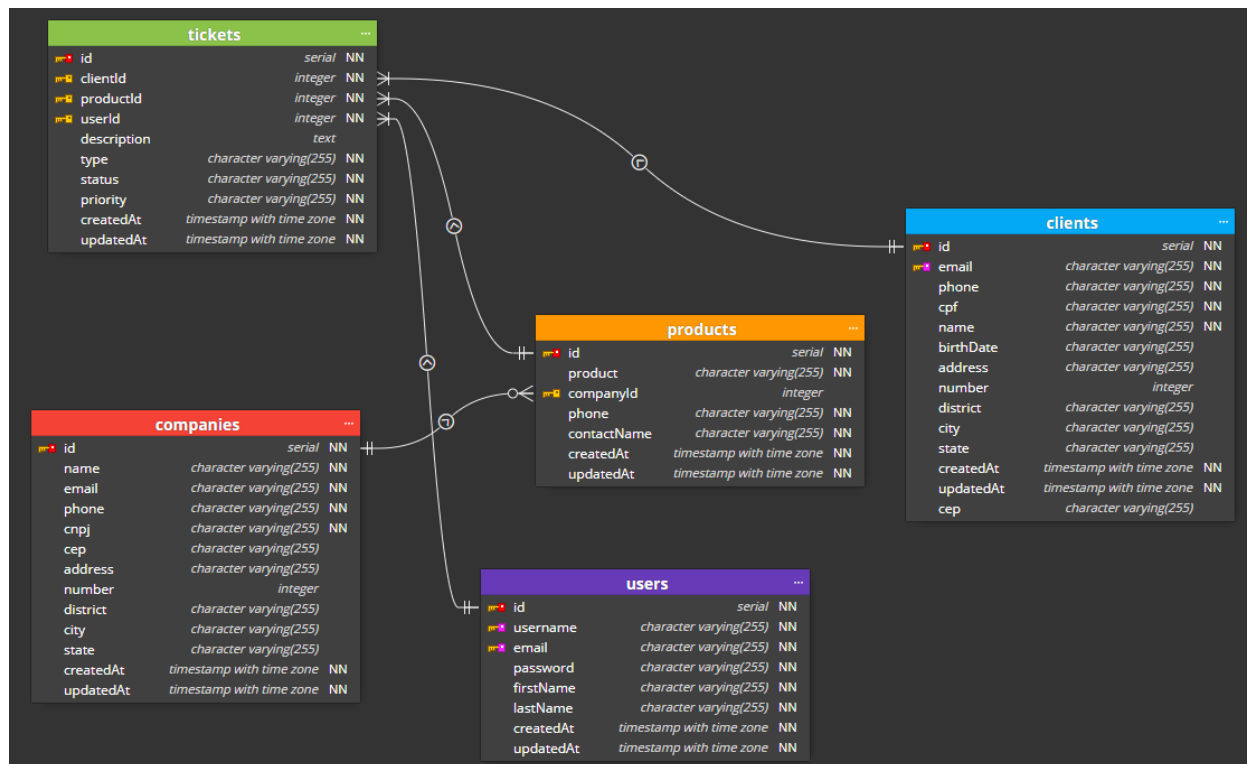
Para o funcionamento da aplicação foi necessária a criação de uma estrutura de tabelas no banco de dados SQL. A tabela de *Users*, *Clients*, *Companies*, *Products* e *Tickets*. Seguindo o funcionamento geral da aplicação:

- Clientes fazem uma ligação para suporte, compras ou outras interações.
- Usuários do sistema (como funcionários de suporte) criam e gerenciam esses tickets.
- Cada ticket faz referência a um produto específico.
- Cada produto é oferecido por uma empresa.

Possuindo as seguintes relações:

- *clients* a *tickets*: Um para muitos (um cliente pode ter vários tickets).
- *users* a *tickets*: Um para muitos (um usuário pode criar e gerenciar vários tickets).
- *companies* a *products*: Um para muitos (uma empresa pode oferecer vários produtos).
- *products* a *tickets*: Um para muitos (um produto pode ser referenciado em vários

tickets).



Tabelas da aplicação Web: Mapeamento de atributos e relações entre as tabelas do banco de dados.

Link da aplicação Web: <https://pmv-si-2024-1-pe5-t2-telemarketing-g12-1.onrender.com>

## **7. DOCUMENTO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

No ambiente atual das empresas em geral, especialmente as de telecomunicações, a segurança da informação é uma prioridade fundamental. Com a constante evolução das ameaças, garantir a integridade, confidencialidade e disponibilidade dos dados tornou-se um desafio crítico.


O documento de política de segurança da informação (apêndice A) abrange várias áreas, incluindo a gestão de acessos, proteção contra malware, gestão de incidentes, e conformidade com regulamentações. Eles servem como a base para a implementação de controles técnicos e administrativos que mitigam os riscos e asseguram a continuidade dos negócios em caso de incidentes de segurança.

Esses documentos estabelecem um conjunto de diretrizes, normas e procedimentos que visam proteger os ativos de informação contra acessos não autorizados, divulgações, alterações ou destruições. Eles são projetados para garantir que todos os colaboradores, desde a diretoria até os operadores de atendimento, compreendam e cumpram as práticas de segurança estabelecidas. Em uma empresa de telecomunicações, onde a infraestrutura de rede e os dados dos clientes são extremamente sensíveis, essas políticas são essenciais.

### **7.1 CARTILHA DE SEGURANÇA**

Complementando as políticas de segurança, as cartilhas de segurança (apêndice B) são ferramentas educacionais essenciais que visam aumentar a conscientização dos funcionários sobre as melhores práticas de segurança. Elas são geralmente mais acessíveis e práticas, oferecendo orientações claras e diretas sobre como identificar e responder a ameaças de segurança no dia a dia.

Enquanto os documentos de política de segurança da informação estabelecem o framework e as diretrizes para proteger os ativos da empresa, as cartilhas de segurança atuam como uma extensão educacional prática, garantindo que todos os membros da organização estejam preparados e informados para lidar com os desafios de segurança da informação. Juntos, esses instrumentos são essenciais para a proteção eficaz dos dados e sistemas em uma empresa de telecomunicações.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024


## 8. APÊNDICES

# TELEPUC – TELEMARKETING 2024

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### Sumário

<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO .....</b>	<b>1</b>
<b>1. INTRODUÇÃO.....</b>	<b>1</b>
<b>2. OBJETIVOS.....</b>	<b>1</b>
<b>3. ABRANGÊNCIA .....</b>	<b>3</b>
<b>4. DIRETRIZES GERAIS .....</b>	<b>4</b>
Interpretação .....	4
Propriedade .....	4
Classificação da Informação .....	4
Controle de Acesso .....	5
Segurança Física.....	5
Internet 5	
Correio Eletrônico .....	5
Rede Sem Fio (Wi-Fi).....	6
Recursos de TIC Institucionais .....	6
Dispositivos Móveis Institucionais .....	6
Recursos de TIC Particulares .....	6
Armazenamento de Informações.....	6
Repositórios Digitais .....	6
Mídias Sociais.....	7
Mesa Limpa e Tela Limpa .....	7
Áudio, Vídeos e Fotos .....	7
Uso de Imagem, Som da Voz e Nome .....	7
Aplicativos de Comunicação.....	7
Monitoramento .....	7
Combate ao Preconceito e Discriminação .....	7
Incidentes de Segurança .....	8
Código de Ética .....	8
Boas Práticas .....	8
Revisão e Atualização .....	8
<b>5. PAPÉIS E RESPONSABILIDADES .....</b>	<b>9</b>
Responsabilidades Gerais.....	9
Responsabilidades Específicas .....	9
<b>6. DISPOSIÇÕES FINAIS.....</b>	<b>10</b>
<b>7. DOCUMENTOS DE REFERÊNCIA .....</b>	<b>11</b>
APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES .....	13

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

## 1. INTRODUÇÃO

A TelePuc é uma empresa de telemarketing comprometida em fornecer serviços de atendimento ao cliente de alta qualidade, valorizando a segurança e a privacidade das informações. No mundo digital altamente interconectado de hoje, garantir a proteção das informações é essencial para manter a confiança dos nossos clientes e parceiros, além de proteger os nossos ativos tangíveis e intangíveis.

Para alcançar este objetivo, a TelePuc reconhece a importância de uma gestão rigorosa e eficaz da segurança da informação. A natureza da nossa atividade, que envolve o manuseio de grandes volumes de dados pessoais e sensíveis, exige uma abordagem robusta e sistemática para prevenir incidentes que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações.

Neste contexto, a segurança da informação se torna uma atividade crucial para a proteção de todos os nossos ativos, incluindo a imagem, a reputação, o patrimônio e, principalmente, a informação que é o coração das nossas operações. É vital que todos os colaboradores, independentemente de seu papel ou nível hierárquico, pratiquem e disseminem boas práticas de segurança da informação.


Em resposta a essas necessidades, estamos implementando o Sistema de Gestão de Segurança da Informação (SGSI), que tem como diretriz principal a Política de Segurança da Informação (PSI). Este sistema foi desenvolvido para atender às necessidades específicas do setor de telemarketing e garantir que nossas operações estejam em conformidade com as melhores práticas de segurança e regulamentações aplicáveis.

Para que a TelePuc alcance o objetivo de proteger seus ativos e continuar oferecendo serviços de excelência, é fundamental que todas as regras e procedimentos descritos nesta política sejam seguidos por todos os colaboradores. A colaboração e o compromisso de cada membro da equipe são essenciais para garantir um ambiente seguro e protegido para a nossa informação e a de nossos clientes.

## 2. OBJETIVOS

A Política de Segurança da Informação (PSI) da TelePuc é aplicável a todos os ambientes e operações da empresa de telemarketing, com os seguintes objetivos:


- **Estabelecer Diretrizes Estratégicas:** Definir diretrizes e princípios estratégicos para

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

a proteção de ativos tangíveis e intangíveis, como imagem, reputação, marca, propriedade intelectual, bancos de dados e conhecimento, além dos recursos de tecnologia da informação e comunicação (TIC) e das informações dos clientes.

- **Nortear a Tomada de Decisão:** Orientar a tomada de decisão e a execução das atividades profissionais de todos os colaboradores da TelePuc, em ambientes presenciais ou digitais, em conformidade com as normas internas, legislação vigente e boas práticas.
- **Promover a Segurança Operacional:** Estabelecer princípios para o desenvolvimento de operações seguras, prevenindo danos à reputação e à continuidade dos negócios da TelePuc.
- **Construir uma Cultura de Segurança:** Fomentar uma cultura de uso seguro da informação, capacitando os colaboradores a agir com responsabilidade e segurança no ambiente digital.
- **Preservar os Pilares Básicos de Segurança da Informação:** Garantir a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e dos recursos de TIC, assegurando que os dados estejam protegidos contra acessos não autorizados, alterações indevidas e indisponibilidade.
- **Nortear Normas e Procedimentos:** Orientar a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para garantir a conformidade e a eficácia das medidas de segurança.

Esses objetivos são essenciais para assegurar que a TelePuc possa operar de maneira segura e eficiente, protegendo as informações críticas e fornecendo um serviço confiável e de alta qualidade aos nossos clientes.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024


### 3. ABRANGÊNCIA

Esta Política de Segurança da Informação (PSI) é um normativo interno com valor jurídico e aplicabilidade imediata e irrestrita a todos os colaboradores e prestadores de serviços da TelePuc. Ela abrange todos os ambientes operacionais e administrativos da empresa, incluindo qualquer situação em que haja acesso ou uso de informações, recursos de tecnologia da informação e comunicação (TIC), e demais ativos tangíveis ou intangíveis da TelePuc.

Esta política se aplica a:

1. **Todos os colaboradores:** Incluindo funcionários permanentes, temporários e terceirizados, em todos os níveis hierárquicos.
2. **Prestadores de serviços e parceiros:** Qualquer entidade externa que tenha acesso aos sistemas de informação e recursos tecnológicos da TelePuc.
3. **Ambientes operacionais e administrativos:** Qualquer local ou contexto, físico ou digital, onde as operações da TelePuc sejam realizadas e onde seus recursos e informações sejam acessados ou utilizados.

A aplicação desta política é essencial para garantir a proteção adequada das informações e ativos da TelePuc, assegurando a continuidade e a integridade dos serviços prestados.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

## 4. DIRETRIZES GERAIS

### Interpretação

Para efeito desta Política de Segurança da Informação (PSI), são adotadas as siglas, os termos e definições constantes no Apêndice A. 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 Gerência de Segurança da Informação (GSI). 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 GSI e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

### Propriedade

As informações geradas, acessadas, recebidas, manuseadas ou armazenadas pela TelePuc, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis, são de propriedade exclusiva da empresa. Os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela TelePuc para o desenvolvimento de atividades profissionais são de propriedade da empresa ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e devem ser utilizados apenas para o cumprimento da finalidade a que se propõem. A utilização das marcas, identidade visual e demais sinais distintivos da TelePuc 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. Colaboradores podem mencionar a marca em conteúdos e materiais, para citação do local de trabalho, mas não podem criar perfis em mídias sociais em nome da instituição e/ou se fazendo passar por ela.

### Classificação da Informação


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.

**Informação Pública:** Informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à empresa e aos colaboradores.

**Informação Interna:** Informação que pode ser divulgada para os colaboradores da empresa, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

**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 empresa ou causar impactos graves, sob o aspecto financeiro, legal e normativo.



	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

**Rotulagem da Informação:** Informações não públicas devem ser rotuladas quando forem geradas, armazenadas ou disponibilizadas. Informações em mídias removíveis ou papel devem ser identificadas com carimbo, etiqueta ou texto padronizado. Para informações em ambientes lógicos, utilizar documentação específica para definir o nível de classificação.

Todos os colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato. 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 empresa, incluindo a internet e mídias sociais, sem prévia e expressa autorização da GSI.

### **Controle de Acesso**

Cada colaborador recebe uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC da TelePuc. A identidade digital é monitorada e controlada pela empresa. O colaborador é responsável pelo uso e sigilo de sua identidade digital. Não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros. Todos devem estar devidamente identificados, portando o crachá individual de forma visível, enquanto estiverem nas dependências físicas da empresa. O crachá de identificação é de uso individual e não pode ser compartilhado.

### **Segurança Física**


A TelePuc deve estabelecer espaços físicos seguros para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas. Os ativos críticos devem estar protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar sua contínua integridade e disponibilidade.

### **Internet**

Os recursos de conectividade são fornecidos para atender ao propósito profissional. O acesso à internet é concedido aos colaboradores por meio de identidade digital pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

### **Correio Eletrônico**

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. O uso de correio eletrônico particular é permitido apenas para a transmissão ou recebimento de conteúdo ou informações particulares, sem prioridade sobre as atividades profissionais e sem efeitos negativos para a rede corporativa.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

### **Rede Sem Fio (Wi-Fi)**

A TelePuc oferece rede sem fio (Wi-Fi) própria para finalidades profissionais, disponível nos ambientes autorizados e limitados ao perímetro físico da empresa. Somente os colaboradores autorizados podem ter acesso à rede sem fio e devem comprometer-se a fazer uso seguro desse recurso. Visitantes e fornecedores poderão ter acesso à rede sem fio com prévia autorização.

### **Recursos de TIC Institucionais**

Os recursos de TIC da TelePuc são destinados a finalidades estritamente profissionais. É vedado o armazenamento de arquivos pessoais nos recursos de TIC da empresa. Para a proteção das informações, os arquivos digitais devem ser armazenados nos servidores específicos, com acesso restrito. A TelePuc não se responsabiliza pelos arquivos digitais armazenados nas estações de trabalho, notebooks, tablets e smartphones disponibilizados pela empresa. Em casos de desligamento, os arquivos digitais serão apagados. Todos os recursos de TIC devem ser inventariados e identificados. Apenas é permitida a utilização de softwares e hardwares legítimos, previamente homologados ou autorizados.

### **Dispositivos Móveis Institucionais**

O uso de dispositivos móveis da TelePuc não é permitido por terceiros. Em casos de roubo, perda ou furto do dispositivo móvel institucional, o colaborador deve registrar um Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GSI.

### **Recursos de TIC Particulares**


É vedada a conexão dos recursos de TIC particulares na rede corporativa da TelePuc. Os colaboradores autorizados podem utilizar recursos de TIC particulares conectados à rede corporativa exclusivamente para suas funções profissionais. Todos os recursos particulares devem ser protegidos com métodos de segurança, como antivírus e firewall. A TelePuc não se responsabiliza pela utilização dos softwares, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos colaboradores.

### **Armazenamento de Informações**

As informações da TelePuc devem ser armazenadas no local apropriado e destinado a esse fim. Informações digitais devem ser armazenadas nos servidores da rede corporativa, com controle de acesso e cópia de segurança. Informações físicas devem ser guardadas em locais seguros. A TelePuc pode solicitar a remoção de conteúdos que ofereçam riscos à empresa e seus colaboradores, sejam contrários à legislação ou possam causar danos à instituição.

### **Repositórios Digitais**

Os repositórios digitais para uso institucional são destinados ao armazenamento, criação, compartilhamento e transmissão de arquivos, desde que previamente autorizados. É vedado o armazenamento de arquivos pessoais nos repositórios digitais institucionais. Os repositórios para

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

uso educacional ou acadêmico podem ser utilizados com autorização. É vedado armazenar, criar, compartilhar ou transmitir arquivos ilegais ou que comprometam a segurança da informação.

### **Mídias Sociais**

Os colaboradores devem adotar um comportamento seguro nas mídias sociais, em conformidade com os direitos e deveres estabelecidos. A participação institucional deve ser diretamente relacionada à função profissional e aos objetivos da empresa, sendo o colaborador responsável por suas ações e omissões.

### **Mesa Limpa e Tela Limpa**

Os papéis contendo informações da TelePuc não devem ficar expostos em locais públicos ou de trânsito de pessoas. Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando.

### **Áudio, Vídeos e Fotos**

Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da TelePuc sem prévia autorização. Situações previamente autorizadas, como eventos institucionais, são exceções. Colaboradores devem obter autorização para captar ou reproduzir imagens dentro da empresa e utilizá-las apenas para fins pessoais, sem compartilhamento público.

### **Uso de Imagem, Som da Voz e Nome**

A TelePuc pode utilizar a imagem dos colaboradores para fins de identificação, autenticação, segurança, registro de atividades, uso institucional e educacional. O uso de imagem, som da voz e nome deve respeitar a integridade e reputação dos colaboradores, conforme as leis vigentes.

### **Aplicativos de Comunicação**


O uso de aplicativos de comunicação para compartilhar informações deve ser feito de forma responsável para evitar riscos à empresa. Informações institucionais devem ser compartilhadas respeitando o sigilo e as normas de segurança.

### **Monitoramento**

A TelePuc realiza o registro e monitoramento de atividades (logs) em seus ambientes físicos e lógicos, com captura de imagens, áudio ou vídeo, para proteção do patrimônio e da reputação da empresa, e para colaborar com as autoridades em caso de investigação.

### **Combate ao Preconceito e Discriminação**

Todos os colaboradores devem participar de campanhas de conscientização contra atos de preconceito e discriminação, e cooperar em situações críticas, fornecendo informações de segurança sempre que necessário.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

### **Incidentes de Segurança**

Incidentes de segurança devem ser reportados imediatamente ao gestor e à GSI para investigação e adoção de medidas corretivas e preventivas.

### **Código de Ética**


Todos os colaboradores da TelePuc devem respeitar a PSI e o Código de Ética e Conduta da empresa, sendo responsáveis por suas ações e omissões.

### **Boas Práticas**

Todos devem adotar boas práticas de segurança da informação, incluindo o uso de senhas fortes, proteção dos recursos de TIC, atualização de software e hardware, além de participar de treinamentos e campanhas de conscientização.

### **Revisão e Atualização**

Esta PSI deve ser revisada e atualizada periodicamente para atender às necessidades e ao contexto da TelePuc, levando em consideração as mudanças na legislação, tecnologias e ambiente de negócio. As atualizações devem ser comunicadas a todos os colaboradores e demais interessados.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

## 5. PAPÉIS E RESPONSABILIDADES


### Responsabilidades Gerais

Todos os colaboradores da TelePuc devem validar, ler e assinar a Política de Segurança da Informação no momento da contratação, garantindo que sua eficácia tenha início desde a integração do novo funcionário. O setor de Segurança da Informação (SI) é responsável por garantir a atualização da Política sempre que houver alterações ou necessidade de melhoria nos processos.

### Responsabilidades Específicas

#### Todos os Colaboradores

- **Conhecimento e Disseminação:** Conhecer e disseminar as regras e boas práticas mencionadas nesta Política.
- **Preservação e Proteção:** Preservar e proteger os ativos físicos e não físicos de propriedade ou sob a custódia da TelePuc, incluindo todas as suas informações e conteúdos, contra qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.
- **Recursos Institucionais:** Zelar pela proteção dos recursos institucionais, da marca, reputação, conhecimento e propriedade intelectual da TelePuc.
- **Uso Responsável:** Usar com responsabilidade os recursos físicos e lógicos fornecidos pela empresa.
- **Exposição de Informações:** Evitar a exposição desnecessária de informações, projetos, trabalhos e dependências da TelePuc, incluindo mídias sociais e internet, e agir com responsabilidade no uso dos recursos de TIC e das informações.
- **Prevenção de Incidentes:** Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.
- **Conformidade:** Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da TelePuc.
- **Proteção de Informações:** Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados.
- **Combate a Discriminação e ao Preconceito :** Adotar medidas preventivas e reativas para combater a discriminação e o preconceito, e conscientizar sobre a necessidade de coibir e conter toda forma de violência.
- **Relato de Incidentes:** Reportar imediatamente quaisquer incidentes que possam impactar na segurança das informações da TelePuc através do endereço de contato designado pela empresa.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

### Gestores e Coordenadores

- **Orientação e Disseminação:** Orientar constantemente suas equipes sobre o uso seguro dos ativos tangíveis e intangíveis, e disseminar os valores adotados pela TelePuc.
- **Delegação de Funções:** Suportar todas as consequências das funções e atividades delegadas a outros colaboradores.
- **Cumprimento da Política:** Assegurar o cumprimento desta Política e das demais regulações pelos colaboradores sob sua supervisão.
- **Investigação de Incidentes:** Participar da investigação de incidentes de segurança relacionados às informações, ativos e colaboradores sob sua responsabilidade.
- **Participação no Comitê de Segurança da Informação:** Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

### Colaboradores


- **Sigilo e Exposição Pessoal:** Ser cauteloso quanto à exposição de sua vida particular e preservar o sigilo profissional nas mídias sociais, protegendo a imagem e reputação da TelePuc.
- **Comunicação Adequada:** Utilizar linguagem respeitosa e adequada nas comunicações, evitando termos dúbios, abusos de poder, perseguição, discriminação, assédio moral ou sexual.
- **Uso de Mídias Sociais:** Utilizar as mídias sociais de forma que evite exposição excessiva e riscos para sua própria imagem e reputação, bem como para a instituição.

## 6. DISPOSIÇÕES FINAIS

Este documento deverá ser interpretado com base nas definições disponíveis no apêndice e nas leis brasileiras.

As atitudes ou ações adversas previstas, não autorizadas ou até mesmo ilícitas baseadas nesta Política de Segurança da Informação, já serão consideradas violações. Haverá avaliação pela equipe de segurança, baseado no Regimento Geral contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição, sobre o risco e a sanção específica do colaborador que descumpra a Política.

A PSI e as demais normas de segurança, incluindo folders educativos sobre como se proteger na internet, poderão ser consultados assim que solicitados para a equipe de segurança através do e-mail: [seguranca@telepuc.com.br](mailto:seguranca@telepuc.com.br), bem como estará disponível para acesso na intranet corporativa.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024


Em caso de eventuais dúvidas, estas devem ser mandadas por e-mail com o assunto: [DÚVIDA PSI] para: [seguranca@telepuc.com.br](mailto:seguranca@telepuc.com.br).

Em caso de dúvidas sobre possíveis phishings, potenciais incidentes, denúncias ou quebra de conduta, deverão ser encaminhados por meio do endereço: [abuse@telepuc.com.br](mailto:abuse@telepuc.com.br) ou deverão ser comunicados imediatamente para a equipe de segurança da informação via chat homologado.

## 7. DOCUMENTOS DE REFERÊNCIA

A elaboração da Política de Segurança da Informação (PSI) da TelePuc foi fundamentada em uma série de documentos de referência reconhecidos internacionalmente e alinhados com as melhores práticas de segurança da informação. Estes documentos são essenciais para garantir que a PSI esteja em conformidade com padrões, leis e regulamentações relevantes. A seguir, estão listados os principais documentos de referência utilizados:

1. **ISO/IEC 27001:2013** - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos:
  - Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) no contexto dos riscos de segurança da informação gerais da organização.
2. **ISO/IEC 27002:2013** - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação:
  - Fornece diretrizes para as melhores práticas de gestão da segurança da informação e para a implementação dos controles de segurança especificados na ISO/IEC 27001.
3. **Lei Geral de Proteção de Dados (LGPD) - Lei n.º 13.709/2018:**
  - Regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
4. **NIST SP 800-53** - Security and Privacy Controls for Federal Information Systems and Organizations:
  - Publicação do Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, que fornece um catálogo de controles de segurança e privacidade para todas as organizações.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

5. **COBIT 5** - Control Objectives for Information and Related Technology:

- Um framework para a governança e gestão de TI da ISACA, que ajuda as organizações a criar valor a partir da TI, mantendo um equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e uso de recursos.

6. **PCI-DSS** - Payment Card Industry Data Security Standard:

- Conjunto de requisitos de segurança projetado para garantir que todas as empresas que aceitam, processam, armazenam ou transmitem informações de cartão de crédito mantenham um ambiente seguro.

7. **Norma ABNT NBR ISO/IEC 27005:2011** - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos em Segurança da Informação:

- Fornece diretrizes para a gestão de riscos em segurança da informação, suportando os requisitos do sistema de gestão de segurança da informação (SGSI) especificados na ISO/IEC 27001.

8. **Resolução n.º 4.658/2018 do Banco Central do Brasil** - Dispõe sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras.


9. **Marco Civil da Internet - Lei n.º 12.965/2014:**

- Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

10. **Diretivas Internas da TelePuc:**

- Conjunto de políticas, normas e procedimentos internos específicos da TelePuc que complementam e detalham as diretrizes gerais da PSI.



	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

## 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, como 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, como a reputação, imagem, marca e conhecimento.

**Ativo tangível:** Bens de propriedade da instituição que são concretos e que podem ser tocados, como 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 de proteção que detecta e elimina programas espiões (spywares) que observam e roubam 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 ou menor aprendiz da instituição.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2024</b>
		Versão: 1.0
	Classificação: interna	Última Revisão: 19/06/2024

## D

**Dado pessoal:** Qualquer informação relacionada a uma pessoa natural identificada ou identificável.

**Dado sensível:** Categoria especial de dados pessoais que revelem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

## E

**Engenharia social:** Técnica usada para enganar pessoas para que revelem informações confidenciais ou realizem ações que comprometam a segurança da informação.

## I

**Incidente de segurança:** Qualquer evento que tenha potencial de comprometer a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

**Integridade:** Propriedade que assegura que a informação não foi alterada ou destruída de maneira não autorizada.

## P

**Phishing:** Técnica de fraude em que um atacante se faz passar por uma entidade confiável para obter informações sensíveis, como senhas e dados de cartão de crédito, através de comunicações eletrônicas enganosas.

## R

**Ransomware:** Tipo de software malicioso que restringe o acesso ao sistema infectado e exige um resgate para que o acesso seja restabelecido.

## S

**Segurança da informação:** Conjunto de medidas que visam proteger a informação contra acessos não autorizados, garantindo sua confidencialidade, integridade e disponibilidade.

## T

**TelePuc:** Empresa de telemarketing especializada em serviços de atendimento ao cliente, que valoriza a segurança e a privacidade das informações.



**TelePuc**  
Telemarketing

# Cartilha de Segurança

Seja bem-vindo à Cartilha de Segurança da TelePuc! Aqui, você encontrará orientações importantes para proteger as informações e os recursos da nossa empresa. Vamos lá!



## Principais orientações de segurança



### Propriedade

Todas as informações geradas, acessadas, recebidas ou armazenadas pela TelePuc são propriedade exclusiva da empresa. Isso inclui nossas marcas, reputação e ativos tangíveis e intangíveis. Lembre-se sempre de utilizar os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela TelePuc apenas para atividades profissionais e com autorização prévia para o uso de nossas marcas em qualquer veículo de comunicação.



### Classificação da Informação

- Informação Pública: Pode ser divulgada sem causar danos à empresa.
- Informação Interna: Destinada apenas aos colaboradores da TelePuc e seu acesso não autorizado pode causar impactos institucionais.
- Informação Confidencial: Exclusiva e requer tratamento especial, sua divulgação pode afetar nossa reputação e imagem, além de causar impactos financeiros, legais e normativos.



### Controle de Acesso

Cada colaborador recebe uma identidade digital para acessar os recursos da TelePuc, que não deve ser compartilhada. É obrigatório portar o crachá de identificação nas dependências da empresa.



### Segurança Física

Estabelecemos espaços físicos seguros para proteger áreas que criam, desenvolvem, processam ou armazenam informações críticas. É fundamental garantir a integridade e disponibilidade desses ativos.



### Internet e Correio Eletrônico

O acesso à internet e o uso do correio eletrônico corporativo devem ser estritamente profissionais, respeitando as regras de direitos autorais e privacidade.



### Redes Sem Fio (Wi-Fi)

O acesso à rede sem fio é restrito aos colaboradores autorizados e limitado ao perímetro da empresa. Visitantes e fornecedores poderão ter acesso à rede sem fio com prévia autorização.



### Recursos de TIC

Os recursos de TIC são destinados apenas a fins profissionais e não devem ser utilizados para armazenamento de arquivos pessoais.



### Dispositivos Móveis

O uso de dispositivos móveis da TelePuc não é permitido por terceiros. Em casos de roubo, perda ou furto do dispositivo móvel institucional, o colaborador deve registrar um Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GSI.





## Armazenamento de Informações

As informações devem ser armazenadas de forma segura nos locais apropriados. Informações digitais devem ser armazenadas nos servidores da rede corporativa, com controle de acesso e cópia de segurança.



## Mídias Sociais

O comportamento nas mídias sociais deve ser compatível com os objetivos da empresa.



## Segurança de Informação

Os colaboradores devem adotar medidas de segurança, como uso de senhas fortes e atualização de software.



## Monitoramento e Incidentes de Segurança

A empresa monitora atividades para proteção do patrimônio e colabora com investigações em caso de incidentes de segurança.



## Combate ao Preconceito e Discriminação

Todos os colaboradores devem participar de campanhas contra preconceito e discriminação, e cooperar em situações críticas, fornecendo informações de segurança sempre que necessário.



## Código de Ética

Todos os colaboradores da TelePuc devem respeitar a PSI e o Código de Ética e Conduta da empresa, sendo responsáveis por suas ações e omissões.



## Boas Práticas

Todos devem adotar boas práticas de segurança da informação, incluindo o uso de senhas fortes, proteção dos recursos de TIC, atualização de software e hardware, além de participar de treinamentos e campanhas de conscientização.



## Boas Práticas

Esta PSI deve ser revisada e atualizada periodicamente para atender às necessidades e ao contexto da TelePuc, levando em consideração as mudanças na legislação, tecnologias e ambiente de negócio. As atualizações devem ser comunicadas a todos os colaboradores e demais interessados.



**Seguindo essas orientações, contribuímos para manter um ambiente seguro e protegido para todos na TelePuc. Juntos, podemos garantir a confidencialidade, integridade e disponibilidade das nossas informações e recursos.**