Issabel Open Source PABX em Google Cloud Platform

Elaborador:	Guilherme Terribele Leme
Orientador:	Marcus Vinícius Lahr Giraldi

FACULDADE DE TECNOLOGIA DE AMERICANA

Guilherme Terribele Leme

Issabel Open Source PABX em Google Cloud Platform

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.

Área de Concentração: Segurança da Informação

Americana, 20 de Junho de 2022.

Banca Examinadora:

Marcus Vinícius Lahr Giraldi (Presidente)
Especialista
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

Wagner Siqueira Cavalcante (Membro)
Mestre
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

Maria Elizete Luz Saes (Membro)
Mestre
FATEC Faculdade de Tecnologia de Americana – Ralph Biasi

FACULDADE DE TECNOLOGIA DE AMERICANA

SUMÁRIO

Lista de figuras

1 Introdução

O mundo está cada vez mais globalizado. A quantidade de informações processadas pelos computadores têm crescido exponencialmente a cada ano. Deste modo, a necessidade por ferramentas computacionais capazes de atender a esta demanda crescente de tráfego de informações também tem sido incrementada.

Além da alta demanda por processamento de dados, também a informação exigiu melhorias, de modo a modernizar a forma como estas são compartilhadas, demandando-se cada vez mais velocidade destas interações.

A busca por ferramentas que atendem a uma determinada necessidade corporativa (seja ela pública ou privada), sempre impulsionou o mercado de tecnologia, motivando o desenvolvimento de novas formas (ou talvez adaptações) mais eficientes de entregar esses resultados. Como por exemplo, pode-se citar o serviço de telefonia, que surgiu em meados do século XX, em que a voz era convertida em pulsos elétricos e trafegavam por extensas linhas de uma ponta a outra.

Essa tecnologia, em pleno período da Revolução Industrial, teve um papel fundamental na velocidade com que as informações eram transmitidas entre as partes envolvidas. Ao decorrer do século, em decorrência das guerras em escala mundial, a corrida pela supremacia tecnológica era perceptível, e um dos seus maiores legados foi a computação e a Internet, que através de protocolos de redes de computadores, tornou-se possível a comunicação entre dispositivos.

Como citado anteriormente, ferramentas mais eficientes e baratas impulsionam o mercado, e, de modo indireto, o apetite por eficiência que é cada vez maior. Desta maneira, em meados de 1995, pensado em uma maneira de aproveitar as redes de computadores existentes nas mais diversas organizações para realizar o tráfego de voz, assim surgiu o VoIP (***Voice over Internet Protocol***).

Esse relatório técnico visa demonstrar a preparação, instalação e configuração de um ambiente em GCP (***Google Cloud Platform***) de modo a possibilitar a hospedagem de um software *open source*, chamado Issabel, para fornecer serviço de VoIP.

2 Fundamentação teórica

Durante esse capítulo serão abordados conceitos, ferramentas e protocolos referentes à computação em nuvem e VoIP, de forma a facilitar o entendimento dos pontos que serão discutidos no decorrer deste relatório técnico.

2.1 Computação em nuvem

Para um entendimento mais adequado do trabalho, primeiramente é necessário entender o conceito de computação em nuvem, desta maneira, Taurion (2009, p. 02) diz:

> Bem, podemos dizer que a Computação em Nuvem é um termo para descrever um ambiente de computação baseado em uma imensa rede de servidores, sejam estes virtuais ou físicos. Uma definição simples pode então ser “um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na Internet”. O resultado é que a nuvem pode ser vista como o estágio mais evoluído do conceito de virtualização, a virtualização do próprio data center.

Com isso em mente, pode-se entender a escolha pela computação em nuvem. Um serviço de telefonia necessita de um alto grau de disponibilidade, tornando-se um ambiente perfeito para sua hospedagem.

2.2 Google Cloud Platform (GCP)

Ao olhar o mercado de computação em nuvem, é notável a enorme gama de soluções oferecidas para este tipo de serviço. Para o desenvolvimento deste trabalho, foi optada pela utilização do Google Cloud Platform, onde, no *website* da própria plataforma encontra-se a seguinte afirmação:

> ”O Google Cloud consiste em um conjunto de recursos físicos (computadores e unidades de disco rígido e recrusos virtuais, como máquinas virtuais (VMs), localizados nos data centers do Google por todo o mundo. Cada local do data center está em uma região. As regiões incluem Ásia, Austrália, Europa, América do Norte e América do Sul. Cada região é uma coleção de zonas, isoladas entre si dentro da região. Cada zona é identificada por um nome que combina um identificador de letra com o nome da região. Por exemplo, a zonan **a** na região da Ásia Oriental é denominada **asia-east1-a**.
>
> Essa distribuição de recursos oferece diversas vantagens, inclusive redundância em caso de falha e latência reduzida localizando recursos mais próximos dos clientes. Essa distribuição também introduz regras sobre como recursos podem ser usados juntos.”
> (*https://cloud.google.com/docs/overview?hl=pt-br*, 09/06/22 – 23:05)

A infraestrutura que suporta a GCP é muito robusta e resiliente, contando com rotas de tráfego exclusivas para seus serviços, o que, no final do processo, torna-se um grande diferencial em relação aos seus concorrentes.

2.3 VoIP

Sobre VoIP (***Voice over Internet Protocol***), Wallingford (2005, p. xv) afirma:

> Voice over IP é a família de tecnologias que possuem implicações abrangentes para todos que usam telefones, a Internet, máquinas de fax, email, e a Web. VoIP toma emprestado e melhora, várias disciplinas da tecnologias das comunicações; promete revolucionar a mais familiar desses tecnologias, o telefone. O Internet Protocol, telefone analógico, telefone digital e circuitos T1, processamento de sinal de áudio digital, rede de alta disponibilidade, e uma série de outras preocupações são tocadas pelas crescentes bordas do vasto, ambicioso reino da VoIP.

Ou seja, a tecnologia VoIP se baseia em uma infraestrutura já existente e com um grupo de protocolos de redes para possibilitar a comunicação por voz.

2.4 Issabel

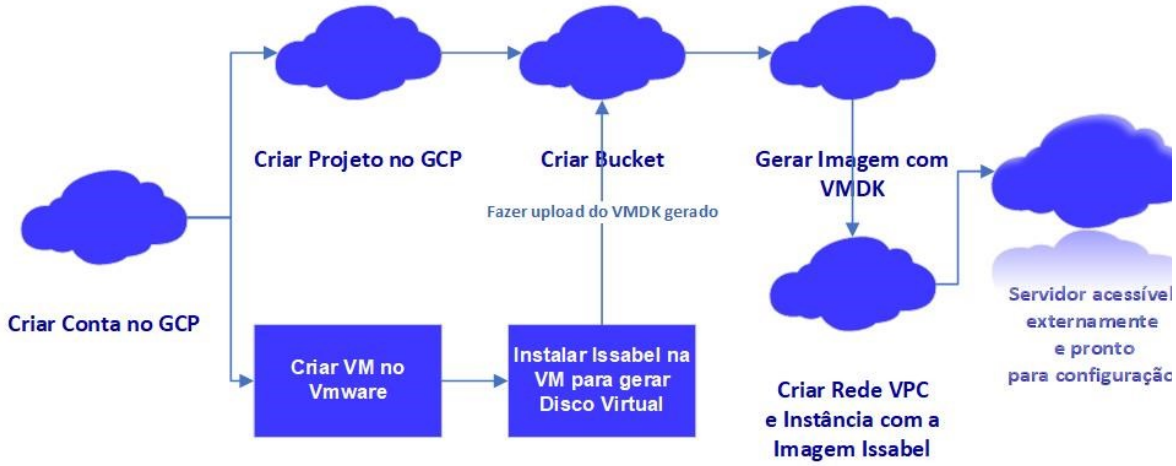
Sobre o Issabel, no próprio site da marca pode-se encontrar

> “Issabel é um Software Open Source Gratuito que unifica suas comunicações em uma única plataforma, baseado no Asterisk (Digium the Asterisk Company) integrando PBX, email e tarefas colaborativas, também um servidor de banco de dados”
> (*https://www.issabel.org/about-us*, 09/06/22)

3 Fluxo de desenvolvimento do projeto

Na figura 1 é apresentada uma visão do fluxo seguido para a criação do servidor na Google Cloud Platform, o qual irá hospedar a plataforma Issabel.

Figura 1 – Fluxo de criação do servidor no GCP



Fonte: Autor

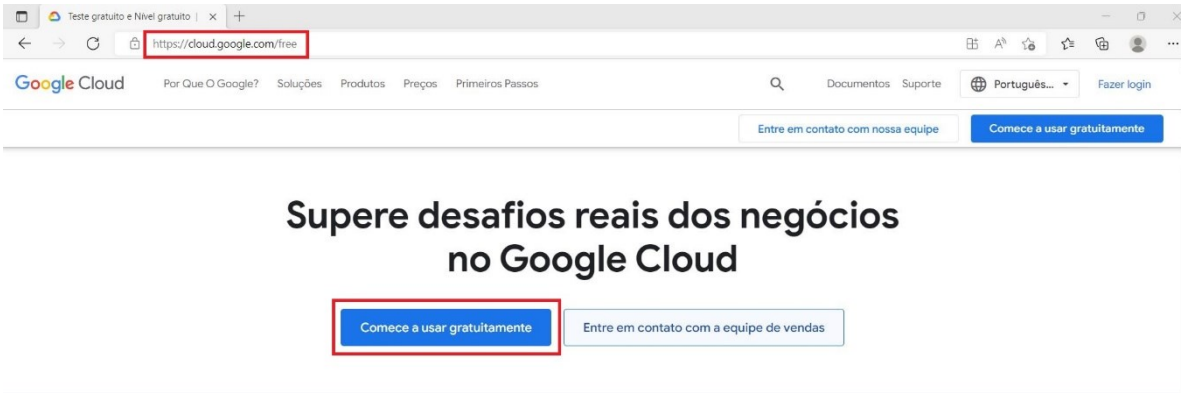
4 Criação de Conta e Projeto no GCP

Para a utilização do GCP, é necessária uma conta Google, sendo possível a criação de uma gratuitamente para utilização na plataforma.

4.1 Acesso ao GCP com conta Google

O Google fornece um período de degustação durante noventa dias para sua plataforma de computação em nuvem. Para o desenvolvimento deste projeto, foi utilizada essa modalidade de uso. Para isto, basta acessar o *link https://cloud.google.com/free* e cadastrar-se para a utilização, como mostrado na figura 2.

Figura 2 – Acesso ao GCP



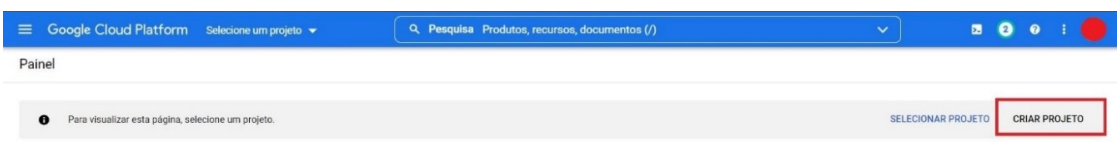
Fonte: Autor

4.2 Criação do Projeto

Após a criação da conta e acesso ao painel principal da plataforma, é necessária a criação de um projeto, o qual será o ambiente onde tudo o que for pertinente a ele será centralizado.

Para isso, como demonstrado na figura 3, acessa-se o “Criar Projeto” no painel principal.

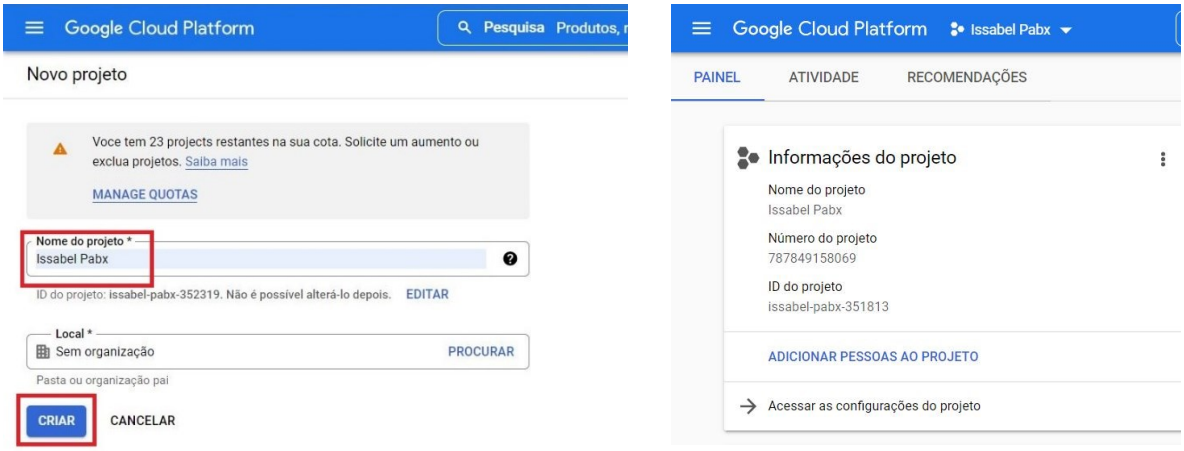
Figura 3 – Criar projeto



Fonte: Autor

Após realizar o acesso, irá ser fornecida a interface para criação do novo projeto, para isso, basta dar um nome a ele e, caso exista a necessidade, segmenta-lo por local. Como o uso apresentado não possui essa exigência, deixa-se com a configuração padrão neste campo, assim como indicado na figura 4.

Figura 4 – Informações do projeto



Fonte: Autor

5 Prepararação do Disco Virtual

O Google Cloud Platform fornece uma gama limitada de sistemas operacionais. Não existindo em sua biblioteca o sistema Issabel, para existir um servidor hospedando o software desejado, faz-se necessário o envio por parte do usuário da GCP, existindo várias maneiras de obter-se este resultado. Foi optado pelo autor deste relatório, o método em que consiste de criar-se um disco virtual através de uma máquina virtual local e envia-lo para um *bucket* no projeto e, desta maneira, ser possível a importação para criar uma imagem utilizável em uma instância.

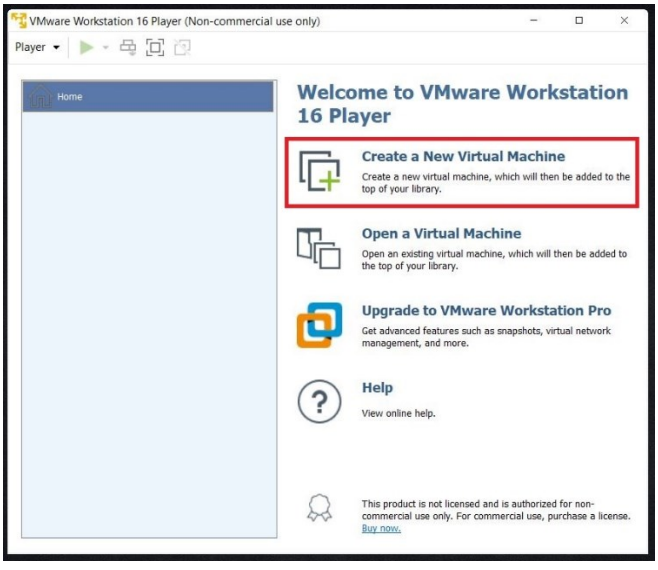
O *software* utilizado para criação da VM (***Virtual Machine***) foi o *VMware Workstation 16 Player*, versão gratuita para uso pessoal, e a imagem do disco para instalação do sistema Issabel foi baixado diretamente do *link www.issabel.org/get-issabel/*.

5.1 Criação da máquina virtual no VMware Workstation 16 Player

Para gerar o disco virtual, é necessário criar uma máquina virtual, onde será instalado a posteriori, o sistema para o serviço VoIP.

No software *VMware Workstation 16 Player*, assim como demonstrado na figura 5, seleciona-se a opção para criar uma nova máquina virtual.

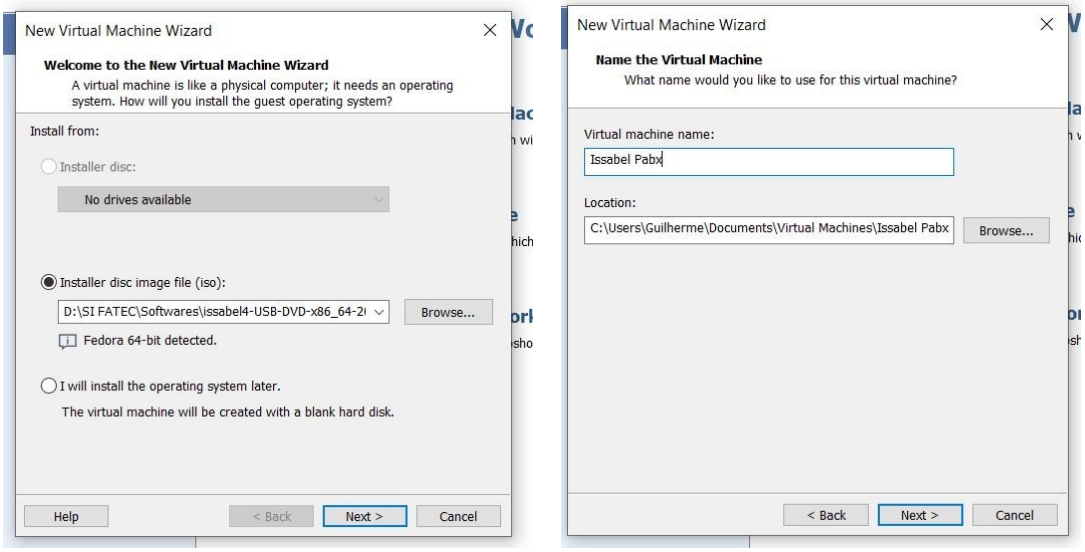
Figura 5 – Criar máquina virtual



Fonte: Autor

Nas opções para a criação de uma máquina virtual, pode-se selecionar, logo nessa etapa, a imagem do disco de instalação e logo após, é pedido o nome e o destino da máquina virtual, assim como indicado na figura 6.

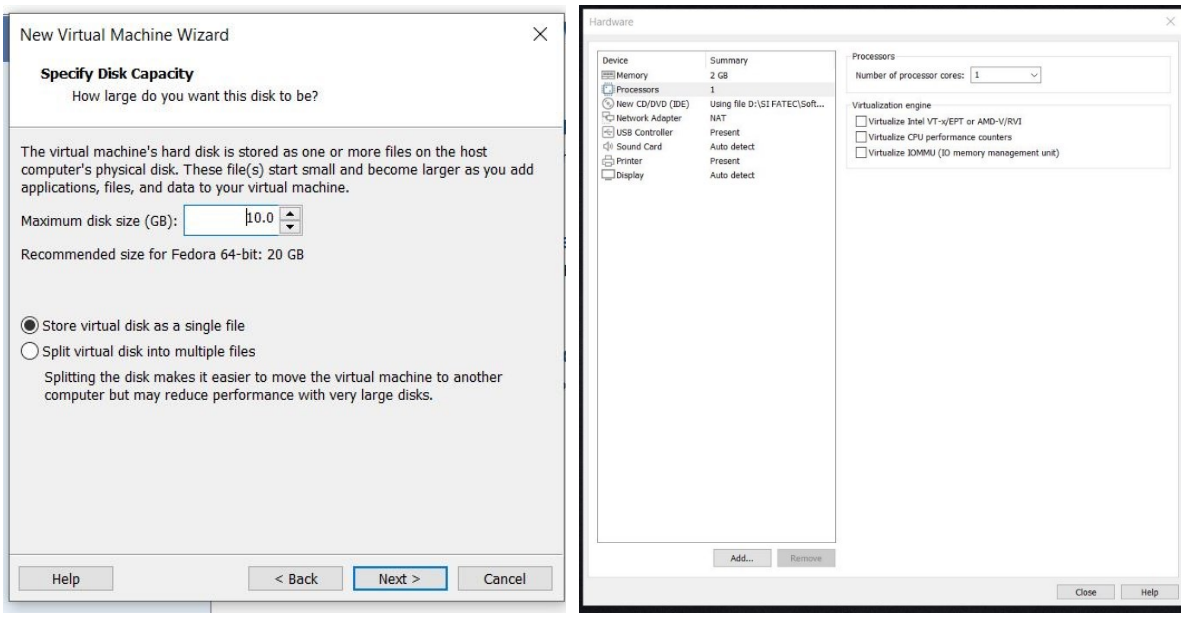
Figura 6 – Diretórios da máquina virtual



Fonte: Autor

Após essa etapa, serão solicitadas informações sobre o disco e *hardware* da VM, sendo necessária uma configuração mínima somente para o sistema ser instalado (figura 7).

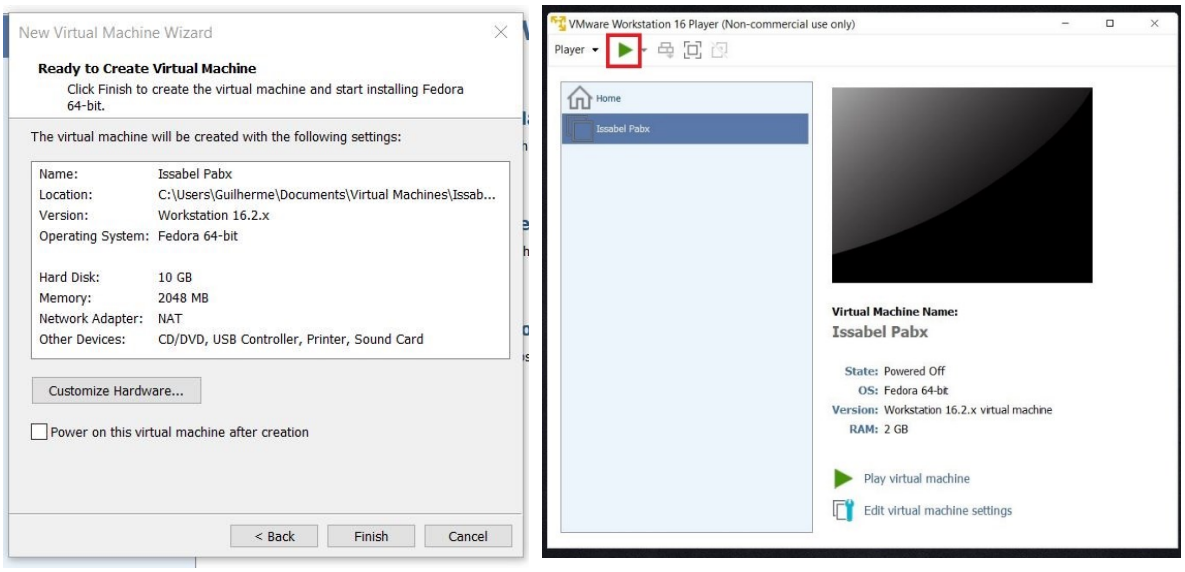
Figura 7 – *Hardware* da VM



Fonte: Autor

Em seguida, será fornecido um *overview* sobre a máquina configurada e já sendo possível sua inicialização, para, deste modo, realizar-se a instalação do sistema (figura 8).

Figura 8 – Finalização da criação da VM

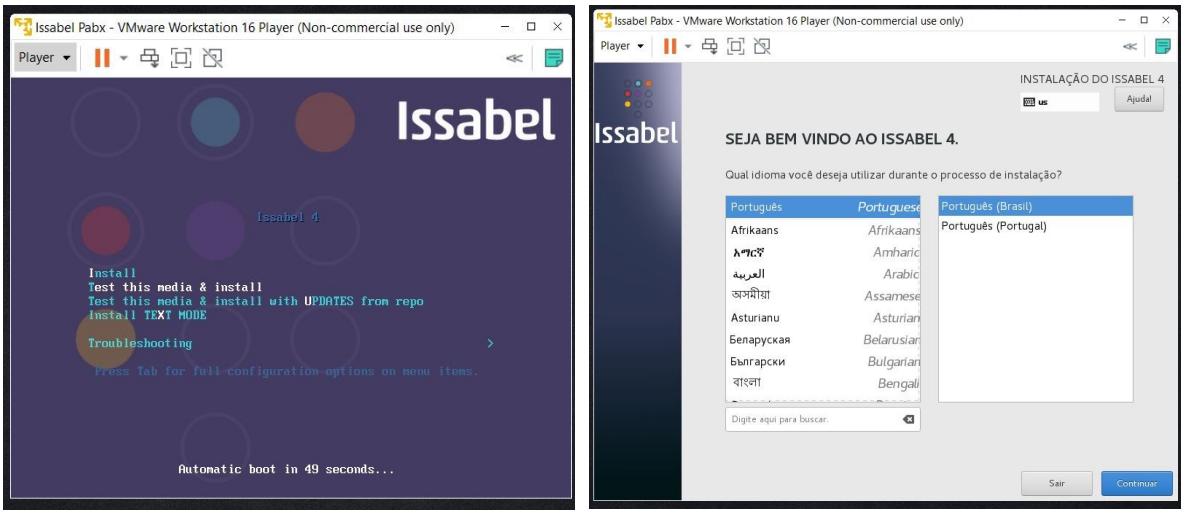


Fonte: Autor

5.2 Instalação do Issabel na máquina virtual

Ao inicializar a máquina, a imagem do sistema operacional já irá ser executada, possibilitando-se a instalação do sistema. Para prosseguir, será escolhida a opção "*Install*", sendo solicitadas informações básicas sobre o idioma a ser utilizado (figura 9).

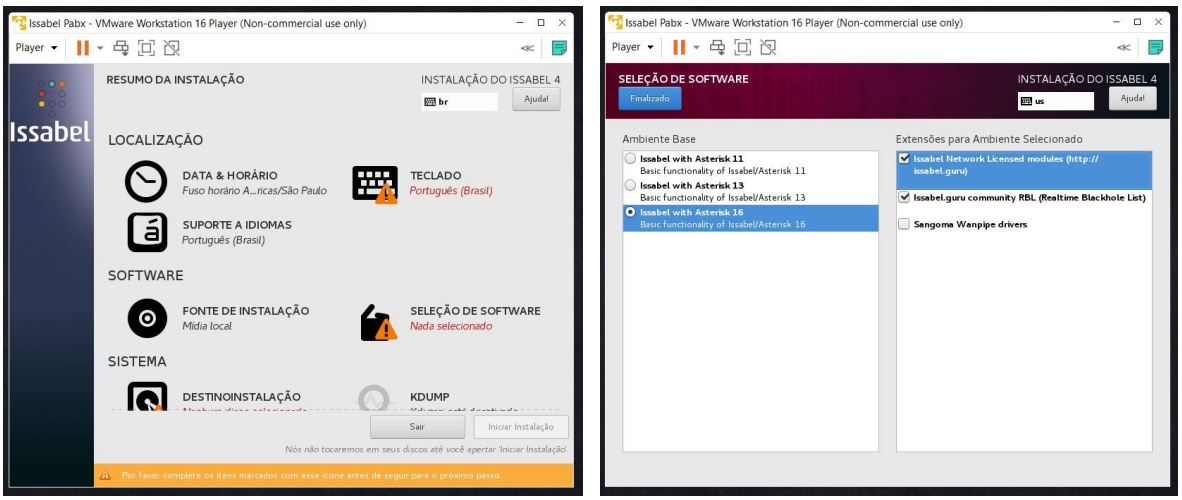
Figura 9 – Início da instalação



Fonte: Autor

Realizando a etapa anterior, é fornecido um resumo da instalação, onde é necessário configurar a interface do teclado, *softwares* a ser instalados e o destino da instalação.

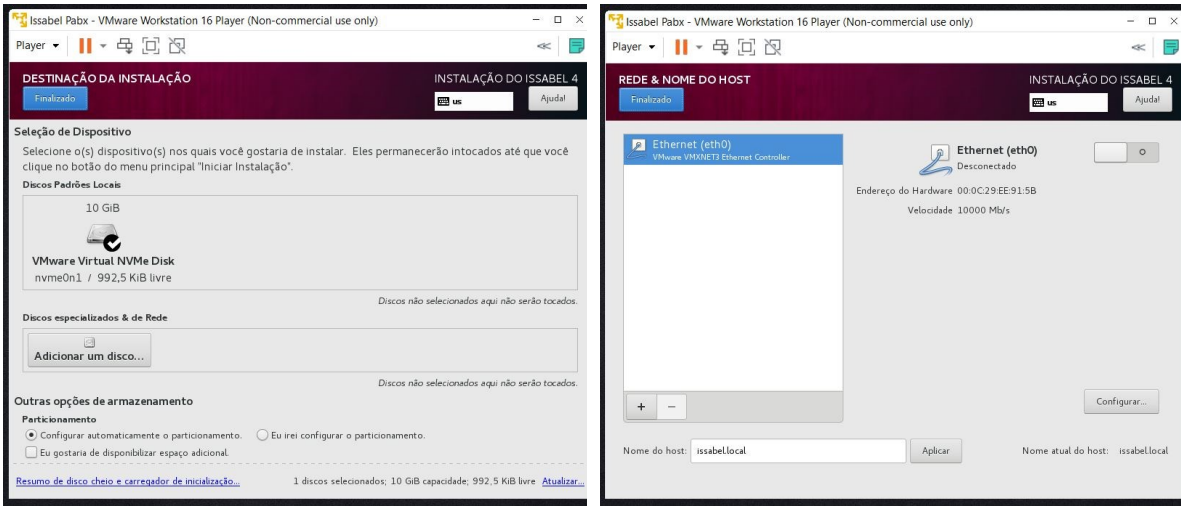
Figura 10 – Seleção de *software*



Fonte: Autor

Como mostrado na figura 10, foi selecionado o Issabel com o Asterisk mais atual, o 16, os módulos de rede licenciados e o *Realtime Blackhole List*.

Figura 11 – Destino de instalação e configuração de rede

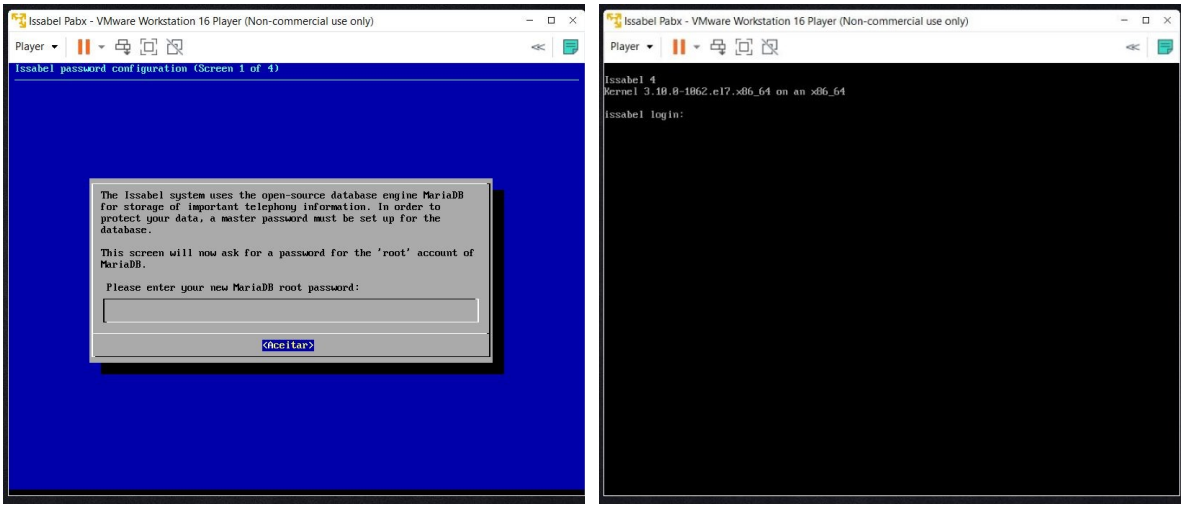


Fonte: Autor

Prosseguindo (figura 11), foi selecionado o disco de destino da instalação e optou-se pela configuração automática de particionamento.

Quanto as configurações de rede, foi optado pelo desligamento da interface *Ethernet*, procurando gerar o mínimo de possibilidades possível de incompatibilidades com a instância na GCP. Após configurado as exigências, foi habilitado o prosseguimento da instalação.

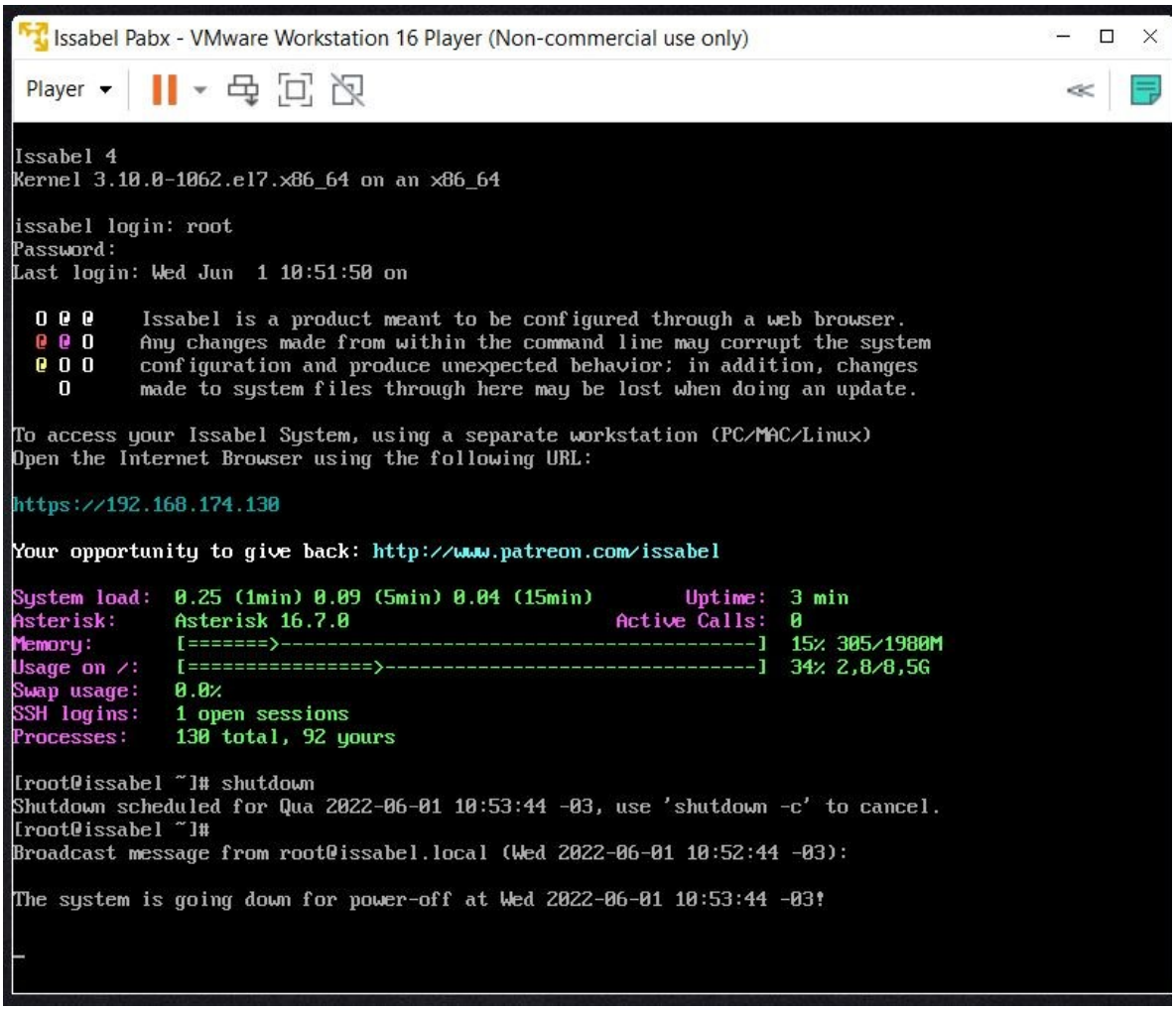
Figura 12 – MariaDB e *login*



Fonte: Autor

Durante a instalação, foi solicitada a criação de uma senha para o *root* e a criação de um novo usuário. Prosseguindo, foi instalado o SGBD (**Sistema de Gerenciamento de Banco de Dados**) MariaDB e solicitada a criação de uma senha para ele Logo em seguida a instalação foi finalizada e após a reinicialização da máquina, foi possível o seu acesso, como visto na figura 12.

Figura 13 – *Shutdown* na máquina



Fonte: Autor

Foi realizado o acesso ao sistema utilizando o *root*, para desta forma, validar-se a instalação e realizar um "*shutdown*" via *prompt* de comando para encerrar a atividade da máquina e diminuir as possibilidades de qualquer problema durante a criação da imagem no *Google Cloud Platform*, assim como exemplificado na figura 13.

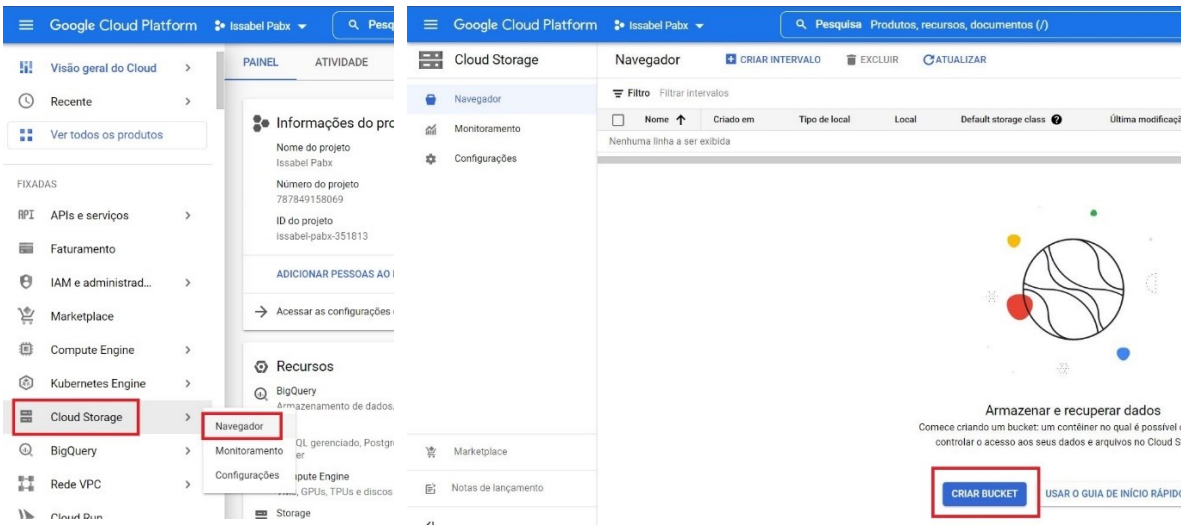
6 Criação do *Bucket*

Para ser possível a criação de uma imagem a partir de um disco virtual, será necessário criar um *bucket* no *Google Cloud Platform* para o envio do arquivo VMDK (***Virtual Machine Disk***) que se encontra no computador local.

Os *buckets* são os recipientes básicos que armazenam dados na *Cloud Storage*, sendo possível o controle de acesso a eles. O nome do *bucket* é exclusivo globalmente.

Para começar a criação do *bucket*, é necessário abrir o painel de funções no GCP, *Cloud Storage* e Navegador, como exemplificado na figura 14. Abrindo a interface de Navegador do *Cloud Storage*, bastar acessar a opção de “Criar Bucket” para começar a criação do repositório que será utilizado.

Figura 14 – Criar *Bucket*



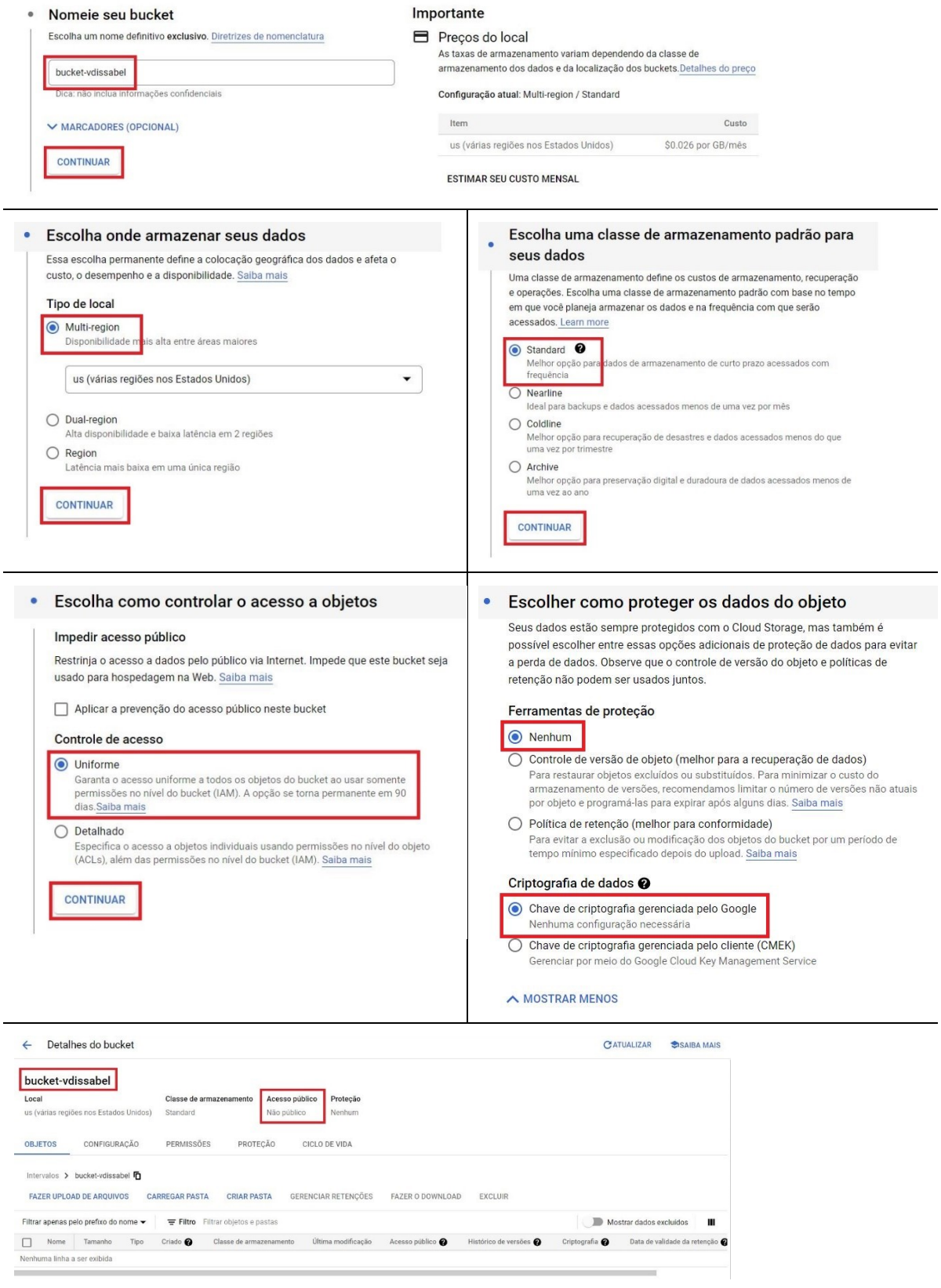
Fonte: Autor

Acessando a interface de criação do *bucket*, uma janela será aberta onde serão solicitadas as informações para o novo repositório, como mostrado na figura 15.

O repositório foi nomeado de ***bucket-vdissabel***, e o tipo de local foi optado pelo padrão de multi-região nos Estados Unidos, que será o local onde a instância será hospedada. Para a classe de armazenamento também optou-se pela padrão e a forma de controlar o acesso uniforme, tendo em vista que o autor é o proprietário do projeto e possui os acessos de administrador a ele.

Para finalizar, a proteção de dados do objeto será a forma padrão fornecida pelo GCP. Realizando as etapas anteriores, o *bucket* já terá sido criado, sendo possível observar informações sobre o repositório ao término.

Figura 15 – Criação do *Bucket*

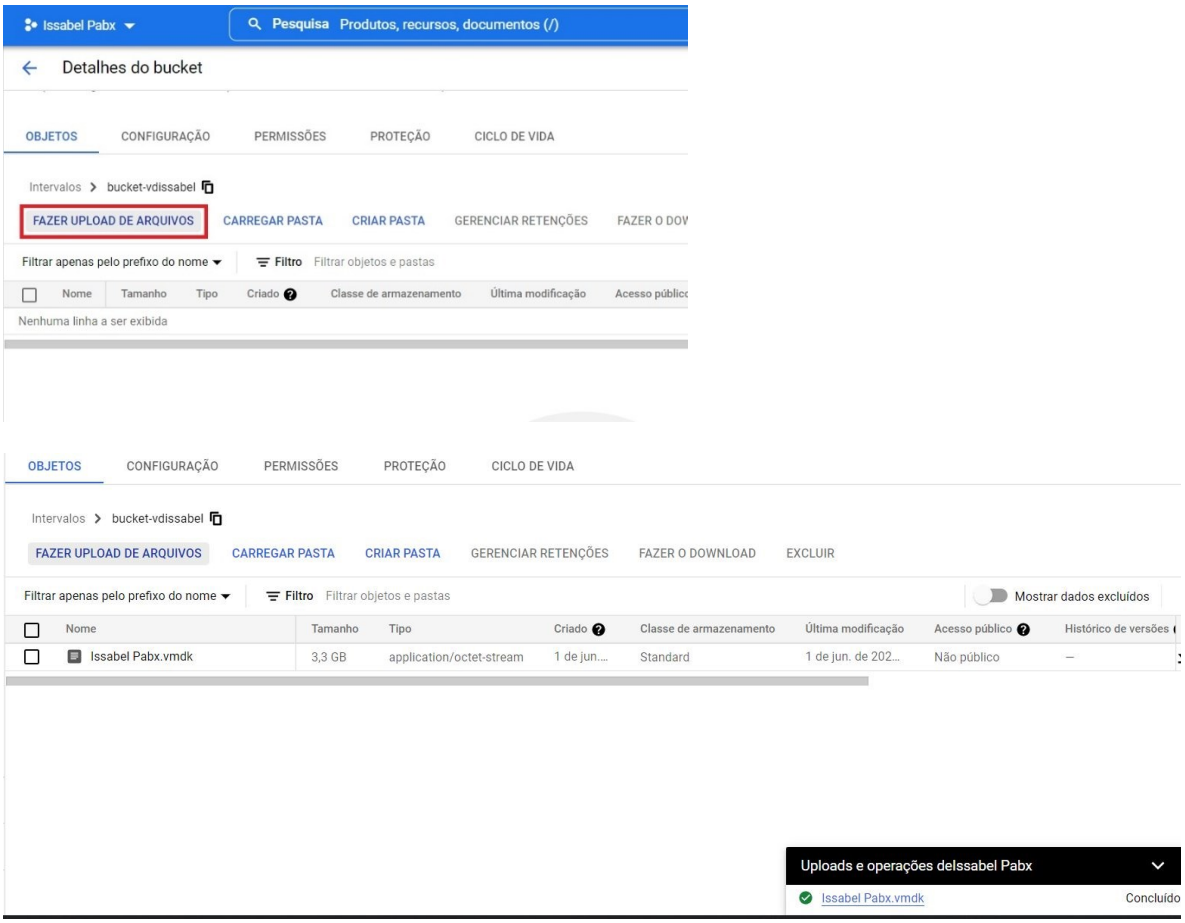


Fonte: Autor

7 *Upload* do disco virtual

Criado o repositório que irá ser utilizado, já é possível realizar o envio do arquivo VMDK, que será utilizado para a criação da imagem para o sistema Issabel.

Figura 16 – Envio do disco virtual para o *bucket*



Fonte: Autor

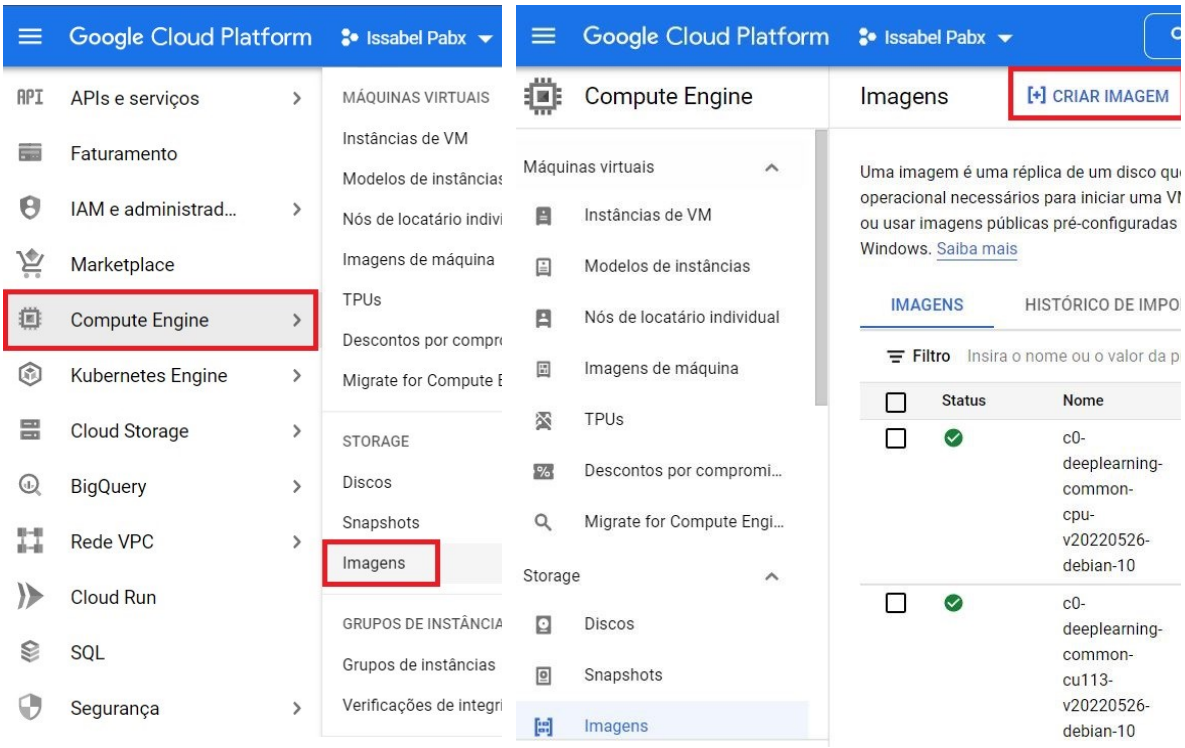
Na interface do próprio *bucket* seleciona-se a opção “Fazer *Upload* de Arquivos”. Após isso, basta ir até o diretório no qual se encontra os arquivos da máquina virtual criada e selecionar o disco virtual com extensão VMDK e transferi-lo (figura 16).

Após a conclusão deste processo, já é possível visualizar o arquivo no repositório. Deste modo, a próxima etapa pode ser inicializada.

8 Criação da imagem

Com o disco virtual disponível no *bucket* do projeto, será dado início na etapa de criação da imagem. Para isso, como mostrado na figura 17, acessa-se o *Compute Engine*.

Figura 17 – Criar Imagem

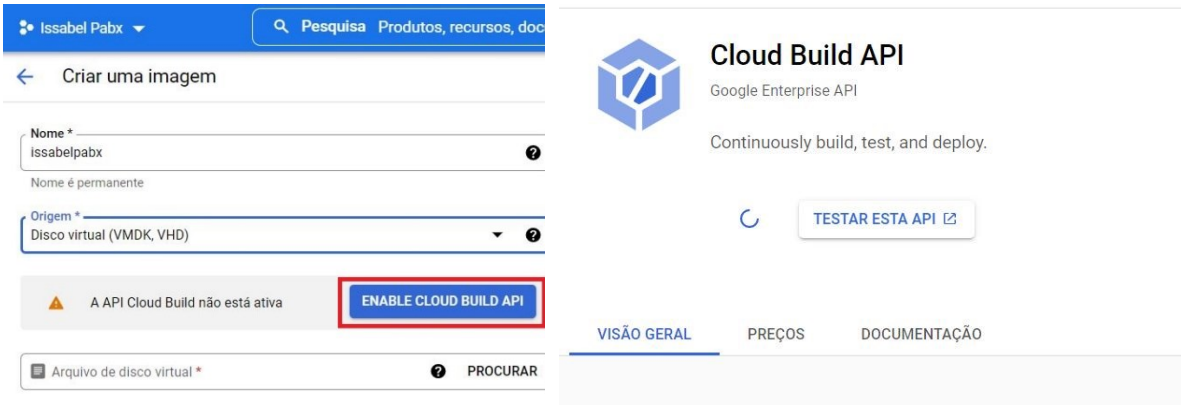


Fonte: Autor

Acessando a opção “Criar Imagem”, será necessário informar a origem do disco utilizado, que, para essa situação será utilizado o disco virtual com extensão VMDK.

Será informada a necessidade de ativar a API (***Application Programming Interface***) “*Cloud Build*” para essa função, a qual é responsável por criar e administrar *builds* no GCP.

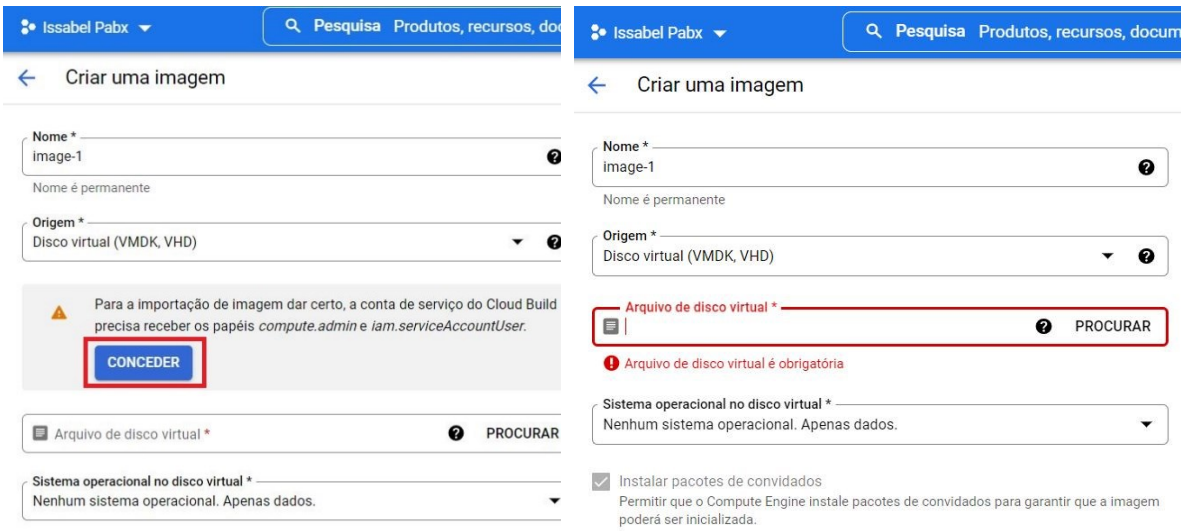
Figura 18 – Habilitar API *Cloud Build*



Fonte: Autor

Acessando o botão "*Enable Cloud Build* API", é direcionado para a interface de habilitação, sendo necessário apenas selecionar o botão para habilitar a aplicação, como demonstrado na figura 18.

Figura 19 – Conceder Papéis



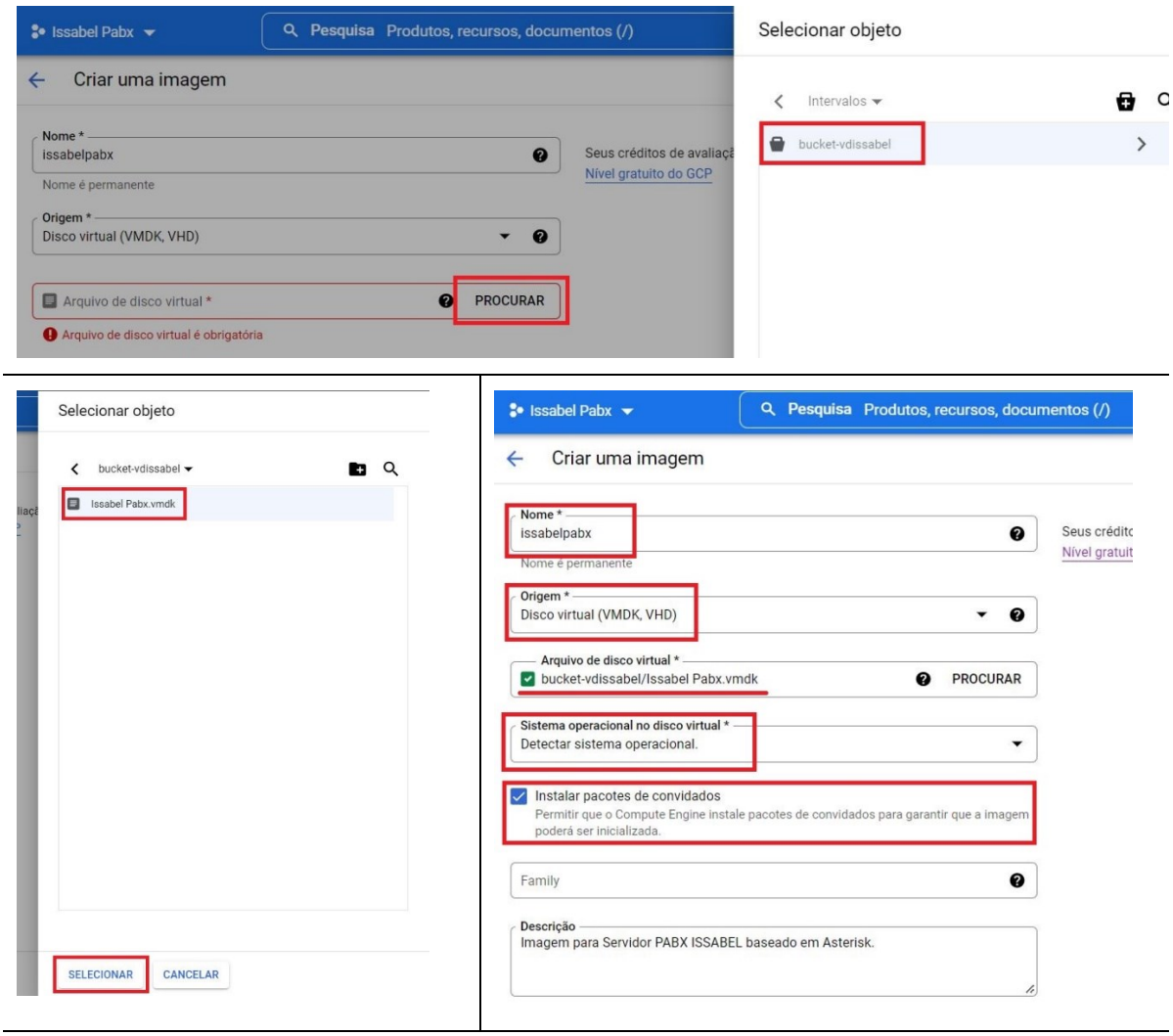
Fonte: Autor

Após habilitar a aplicação, o utilitário irá solicitar a concessão de papéis para a conta utilizada no *Cloud Build*, como mostrado na figura 19. Concedendo os papéis através da opção "Conceder", basta atualizar a página inteira para que as permissões entrem em vigor, sendo necessário recomeçar a criação da imagem no *Compute Engine*.

Realizando as etapas anteriores de habilitação da API e concessão de papéis para a conta utilizada, já é possível acessar o *bucket* e listar os arquivos contidos no mesmo. Para isso, após inserir um nome para a imagem e escolher a origem como disco virtual, no campo "Procurar" será relacionado o repositório onde se encontra o disco virtual (***bucket-vdissabel***). Para isso, basta selecioná-lo e logo em seguida selecionar também o arquivo VMDK, de acordo como representado na figura 20.

Será selecionada a detecção automática do Sistema Operacional contido no disco virtual e permitir a instalação de pacote de convidados para possibilitar a iniciação da imagem.

Figura 20 – Criação da Imagem

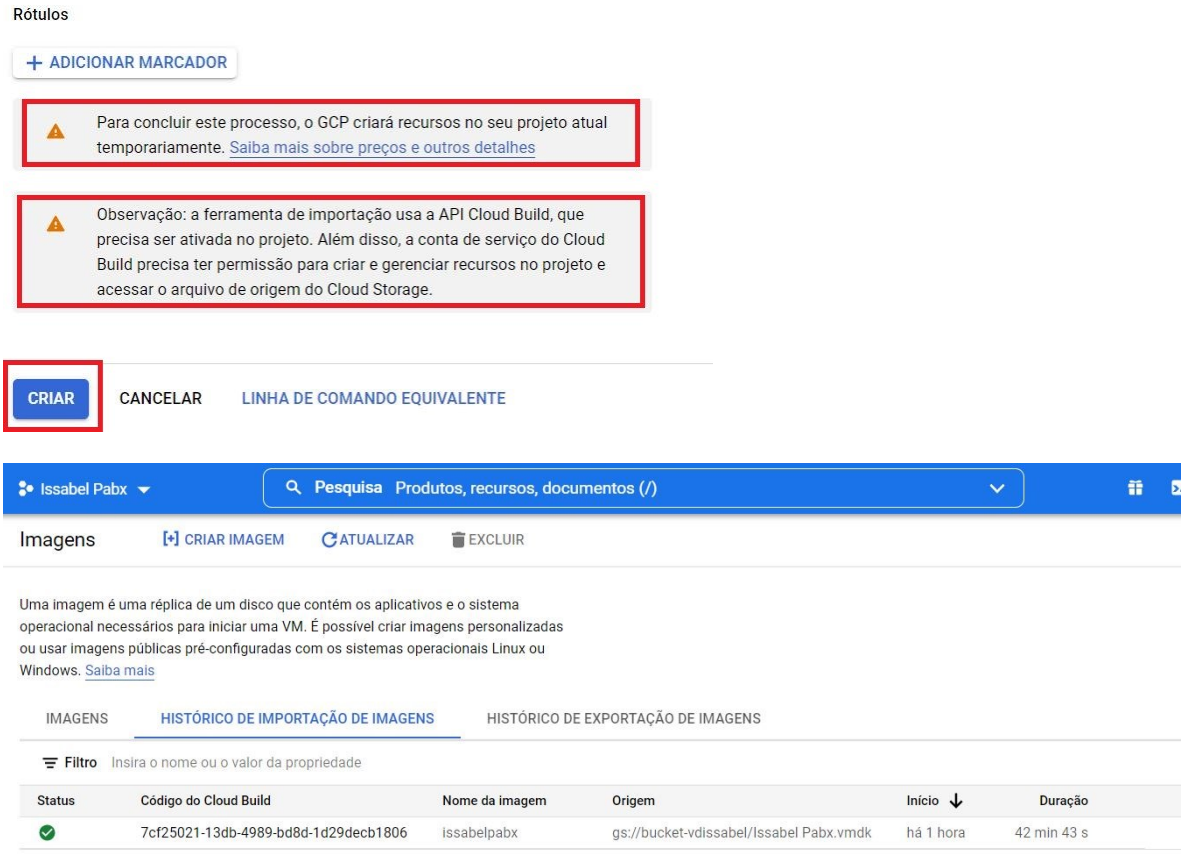


Fonte: Autor

É informado pela utilitário a criação de recursos temporários no projeto atual e as necessidades (previamente concedidas) para dar prosseguimento à criação, bastando selecionar a opção de “Criar” para inicializar o procedimento.

Como pode-se ver na figura 21, o processo de criação demorou aproximadamente quarenta minutos e foi concluído com êxito.

Figura 21 – Finalização da criação da Imagem



Fonte: Autor

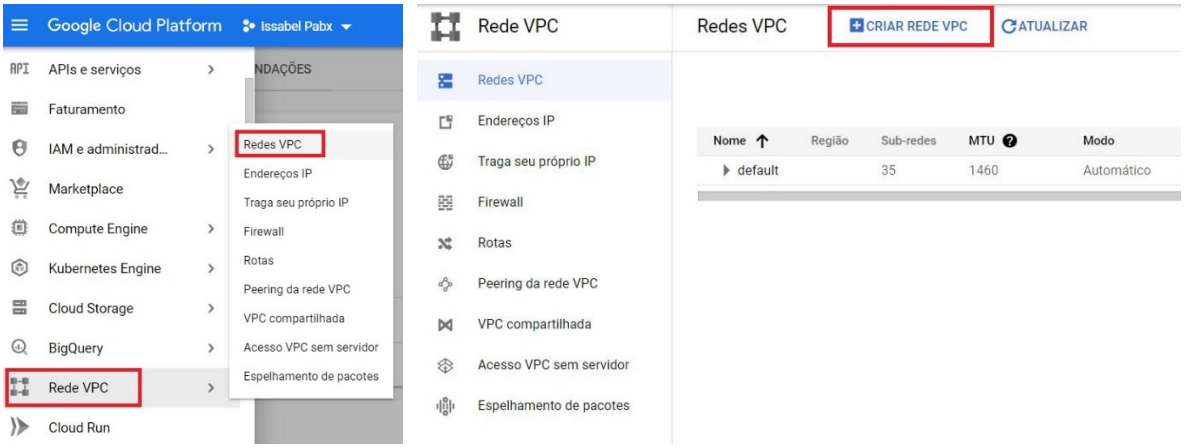
9 Criação da Rede VPC e Sub-Rede

A última etapa antes da montagem da instância é a de criação de uma rede VPC (***Virtual Private Cloud***) e em seguida, criar uma Sub-Rede.

9.1 Rede VPC

As redes VPC são basicamente uma versão virtual de uma rede física, que fornece conectividade para instâncias no *Compute Engine*. Para começar a criação, no painel do projeto é necessário acessar o “Rede VPC” e selecionar “Criar Rede VPC” de acordo como o mostrado pela figura 22.

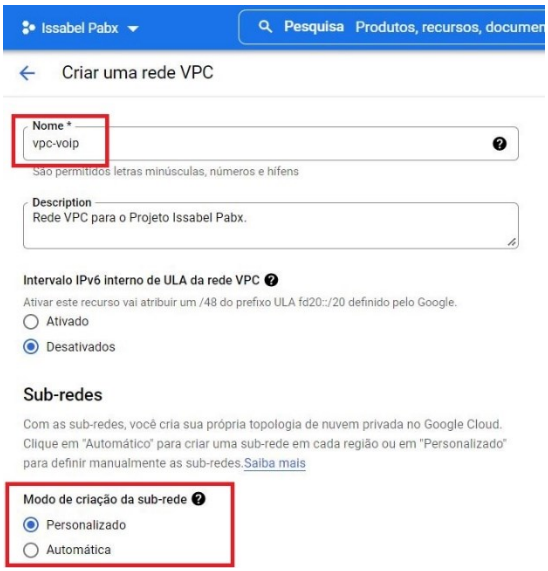
Figura 22 – Criar Rede VPC



Fonte: Autor

Será aberta a interface para a criação da rede, onde será solicitado o nome da rede e se é desejada a utilização de IPv6 (***Internet Protocol v6***) internamente, sendo neste caso preferida a sua não utilização, como mostrado na figura 23.

Figura 23 – Configuração VPC



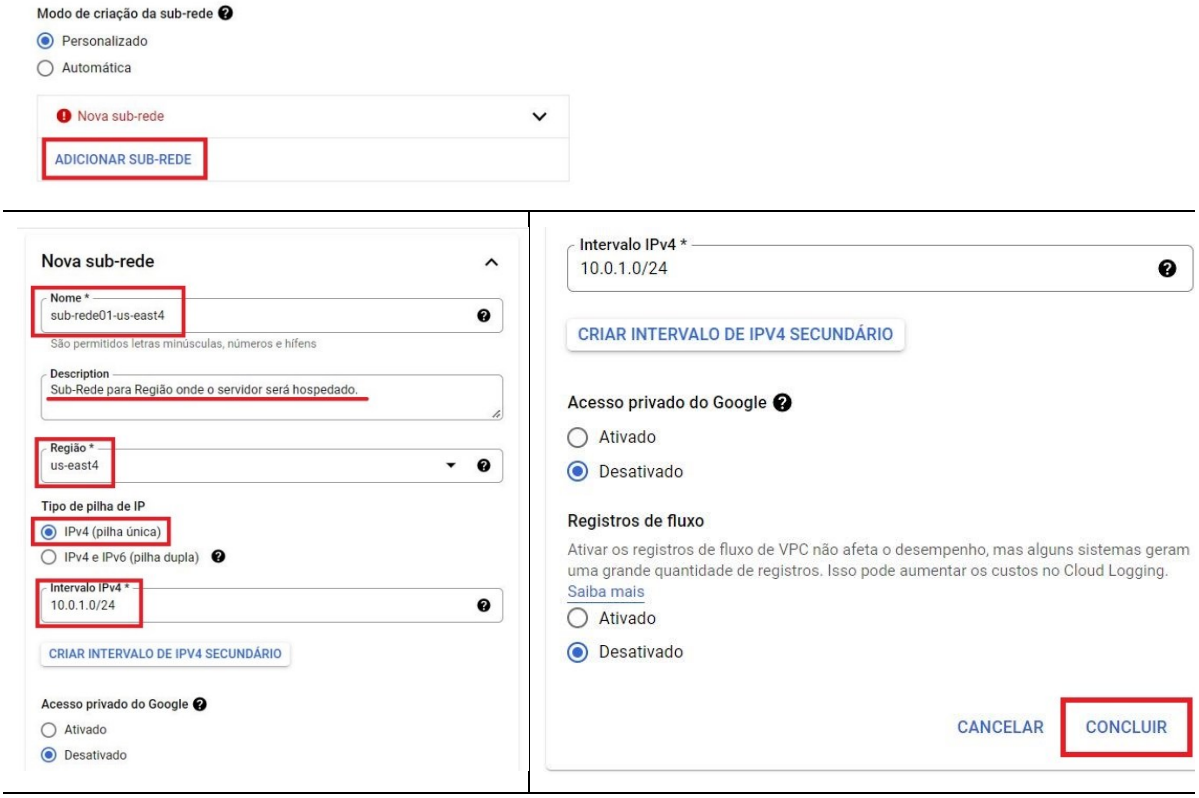
Fonte: Autor

O modo de criação da sub-rede irá ser escolhido como personalizado, sendo pedida a inserção das informações manualmente. Apartir deste ponto, será iniciada a configuração da sub-rede, e logo em seguida, será retornada a configuração geral da VPC.

9.2 Sub-Rede

As redes VPC são recursos globais, deste modo, toda rede de nuvem privada necessita de sub-redes, as quais consistem em um ou mais intervalos de endereços IP, sendo, desta maneira, recursos regionais.

Figura 24 – Criação de Sub-Rede



Fonte: Autor

Ao selecionar para a adição de uma sub-rede, faz-se necessária a inserção de um nome para ela, a seleção da região desejada, a qual deve ser a mesma que desejada para a instância de máquina virtual, de acordo com a figura 24.

O tipo de pilha de IP desejado é apenas o IPv4 e logo em seguida, definir o seu intervalo na sub-rede que está sendo criada, sendo possível, caso se deseje, a criação de um outro intervalo IP.

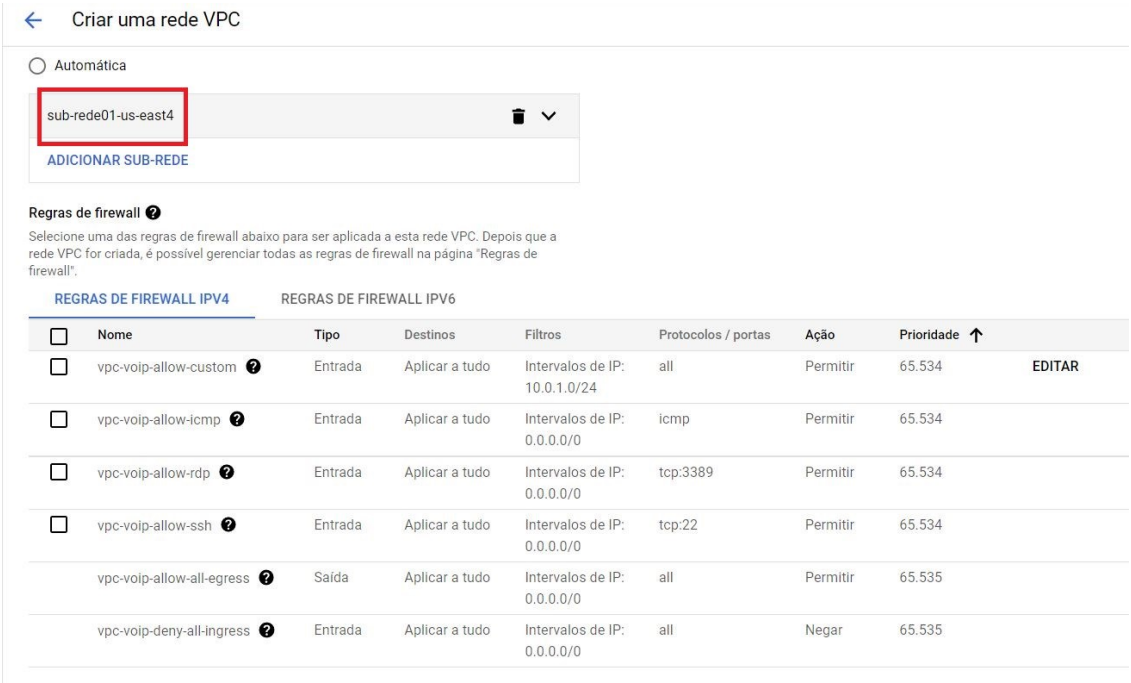
O campo “Acesso privado do Google” permite as VMs desta sub-rede de acessar os serviços do Google sem a atribuição de um IP externo, para o caso apresentado, esse recurso não se faz necessário, deixando-o desabilitado.

Os registros de fluxo serão desativados, caso haja necessidade, podem ser habilitados a posteriori. Após isso, basta clicar em “Concluir” para finalizar a criação da sub-rede.

9.3 Finalização da criação da VPC

Após a criação da sub-rede, pode-se dar prosseguimento na configuração da nuvem virtual privada, sendo necessário configurações básicas de regras de *firewall* e modo de roteamento dinâmico desejado.

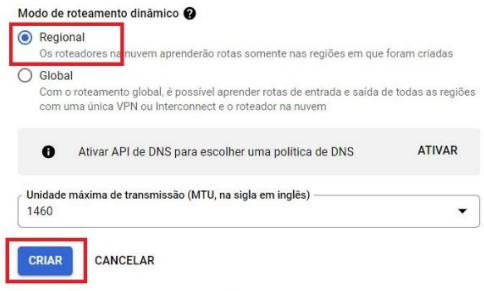
Figura 25 – Regras de *Firewall*



Fonte: Autor

As regras de *firewall* que serão utilizadas são apenas as padrão que não podem ser removidas, como mostrado na figura 25. Conforme as necessidades de *firewall* forem surgindo, as regras serão habilitadas. O modo do roteamento será apenas o Regional (figura 26).

Figura 26 – Modo de Roteamento Dinâmico



Fonte: Autor

Finalizando o processo de criação, será possível visualizar no painel de “Rede VPC” a rede criada e consequentemente a sub-rede, vide figura 27.

Figura 27 – Listagem da Rede

Nome	Região	Sub-redes	MTU	Modo	Intervalos de IPs internos	Intervalos de IPs externos	Intervalos de IPv4s secundários	Gateways
default		35	1460	Automático	Nenhum			
vpc-voip		1	1460	Personalizado	Nenhum			
	us-east4	sub-rede01-us-east4			10.0.1.0/24	Nenhum	Nenhum	10.0.1.1

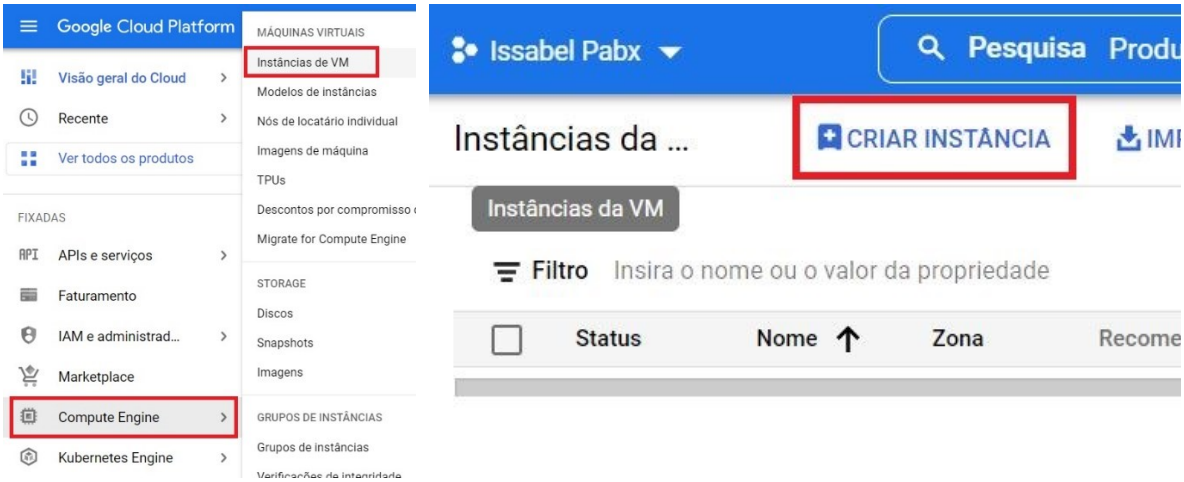
Fonte: Autor

10 Criação e configuração da Instância

Observando a figura 1 e analisando a trilha seguida com a finalidade de criar-se uma Instância de VM na GCP, a última etapa necessária para alcançar esse objetivo é a de criar a máquina virtual e fazer as configurações no *firewall da* VPC para permitir o acesso remoto ao servidor.

Para dar início a ela, no painel do projeto, "*Compute Engine*" e selecionar "Instância de VM", logo em seguida, clicar em "Criar Instância", como demonstrado na figura 28.

Figura 28 – Criar Instância



Fonte: Autor

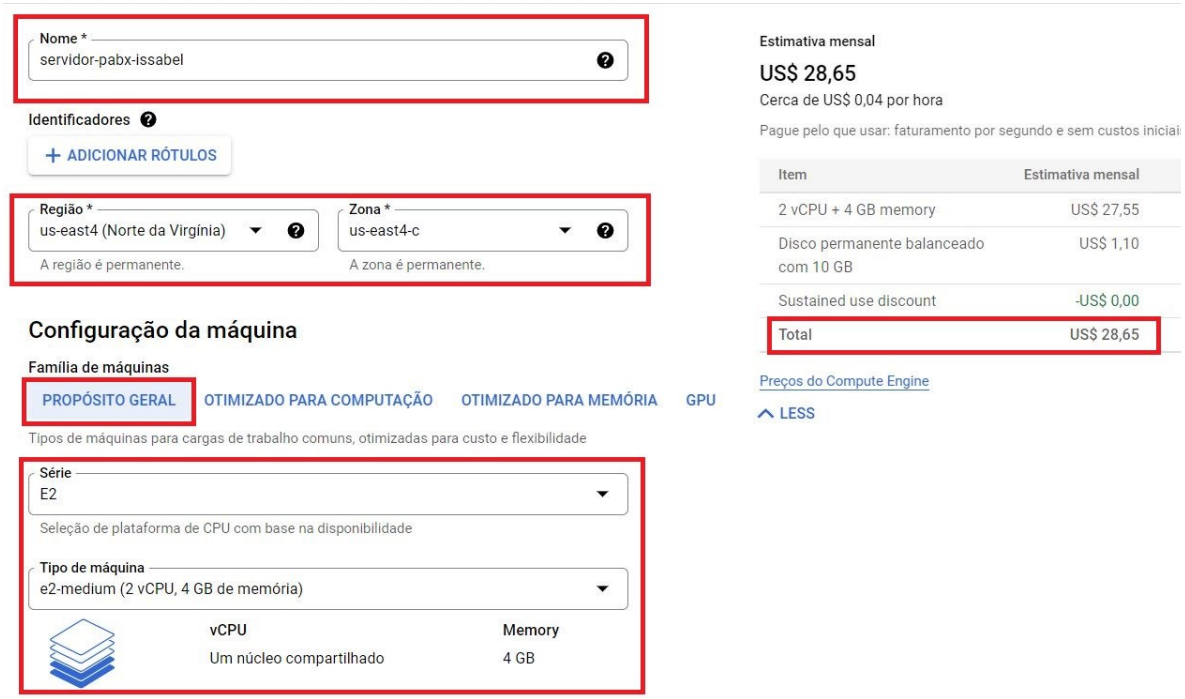
Após isso, será aberta a interface para criação da instância de máquina virtual e suas respectivas configurações.

10.1 Criação da Instância para o servidor com Issabel

Na figura 29, pode-se observar os campos necessário para serem configurados, como o nome da instância, região e zona, configuração da máquina, e ao lado, os valores estimados mensalmente da operação da máquina.

Foi optada a seleção da região **us-east4** pelo custo de operação da instância.

Figura 29 – Nome e Região da Instância



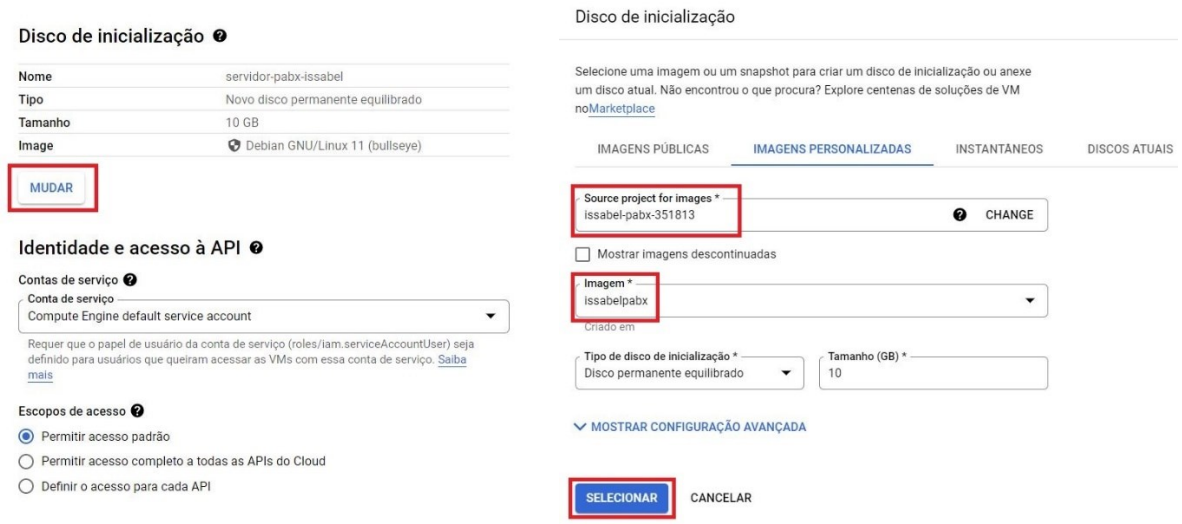
Fonte: Autor

Continuando a configuração da instância de máquina virtual, será necessária a seleção do disco de inicialização. Ao selecionar a opção de “Mudar”, será aberta a interface para fazer a navegação no projeto, sendo necessária sua seleção, para então no campo “Imagem” ser listada a imagem criada anteriormente utilizando o disco virtual criado em uma VM em um computador local.

Nesta etapa é possível alterar o tamanho do disco, porém foi optado por manter o tamanho original do gerado durante a configuração da máquina virtual no VMware.

Após selecionado o projeto fonte e a imagem, basta confirmar as configurações através do botão “Selecionar” e voltar para a configuração da instância, como mostrado na figura 30.

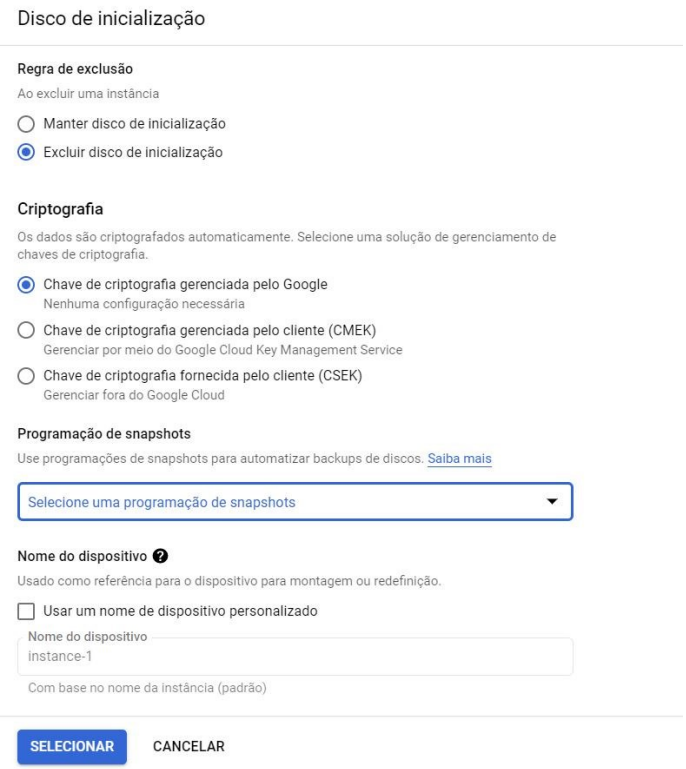
Figura 30 – Configuração de Disco



Fonte: Autor

No campo de Configuração Avançada (figura 31), será optada pela padrão.

Figura 31 – Configurações Avançadas



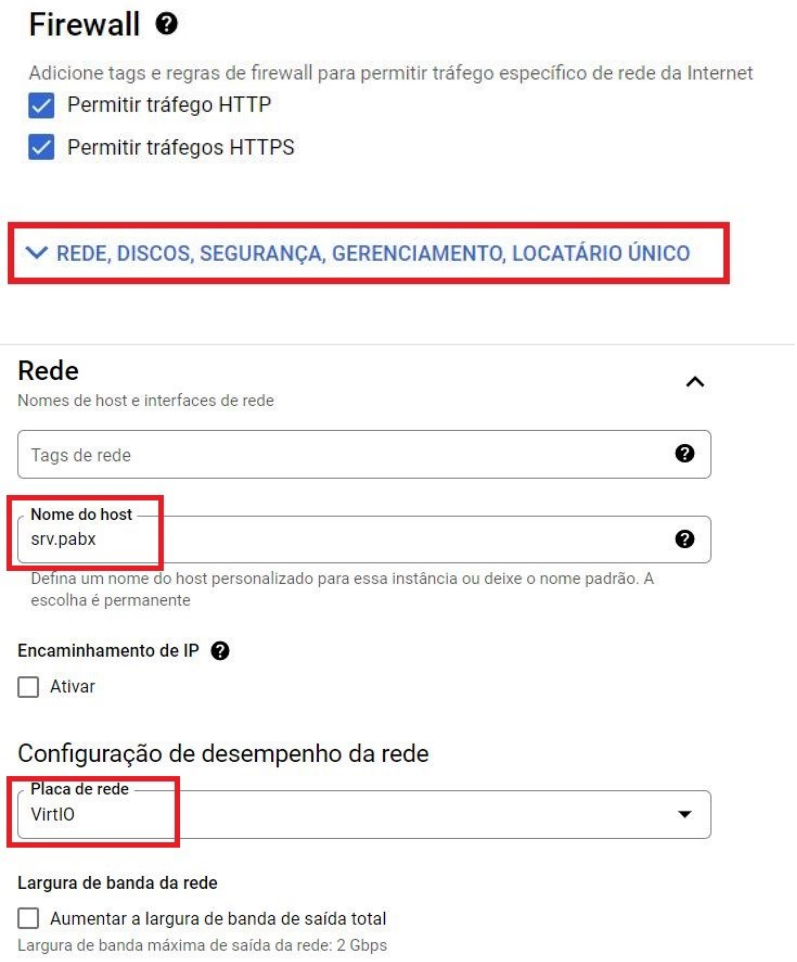
Fonte: Autor

As próximas configurações serão as de *firewall* e rede. A figura 32 mostra os arranjos básicos de segurança, deste modo, foram assinaladas as opções para a permissão de tráfego HTTP e HTTPS da máquina, sendo realizada automaticamente a liberação no *firewall* da VPC (mais para a frente será exemplificado como são realizadas as adições de regra no *firewall* e como elas são ativadas).

Seguindo o fluxo, agora, serão inseridas as configurações de rede. Para isso, é preciso selecionar “Rede, Discos, Segurança, Gerenciamento, Locatário Único” para ter acesso a elas.

Foi informado o nome do *host* e a seleção da placa de rede utilizada pela VM.

Figura 32 – *Firewall* e Rede

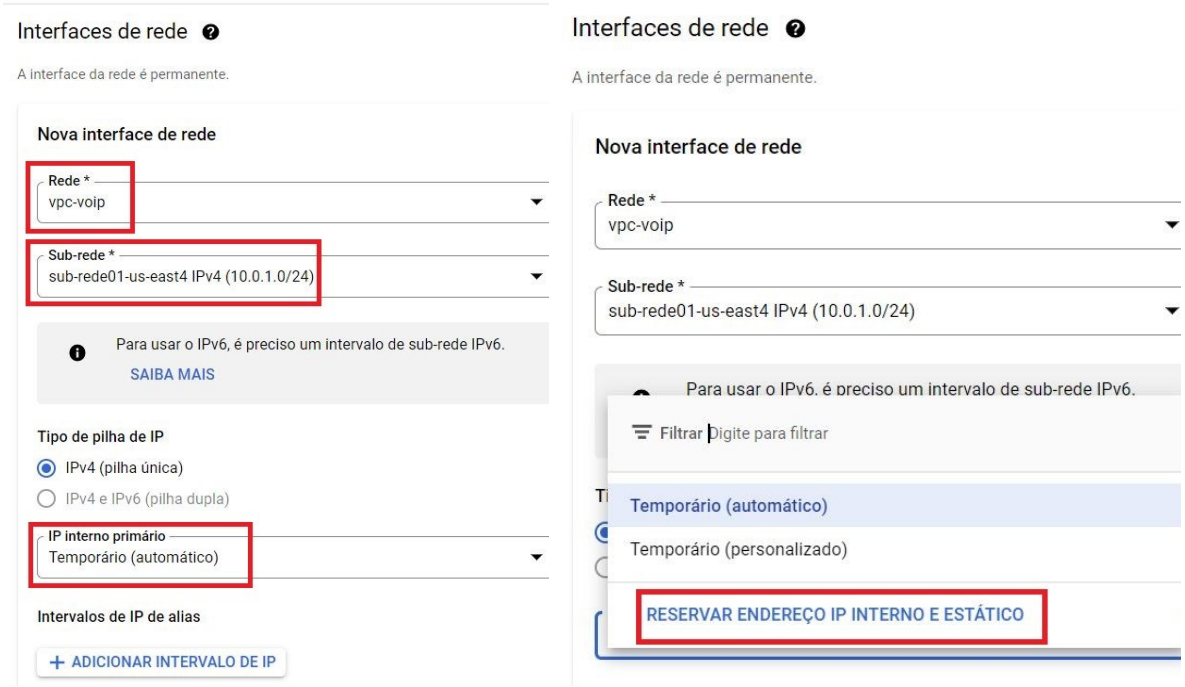


Fonte: Autor

Definido o tipo de placa de rede, pode-se realizar a configuração da mesma. Na figura 33 são mostradas as informações necessárias para a interface. A rede utilizada será a VPC criada anteriormente e, de mesma maneira, a sub-rede.

No campo “IP interno primário” será realizada a reserva de IP para o tornar estático.

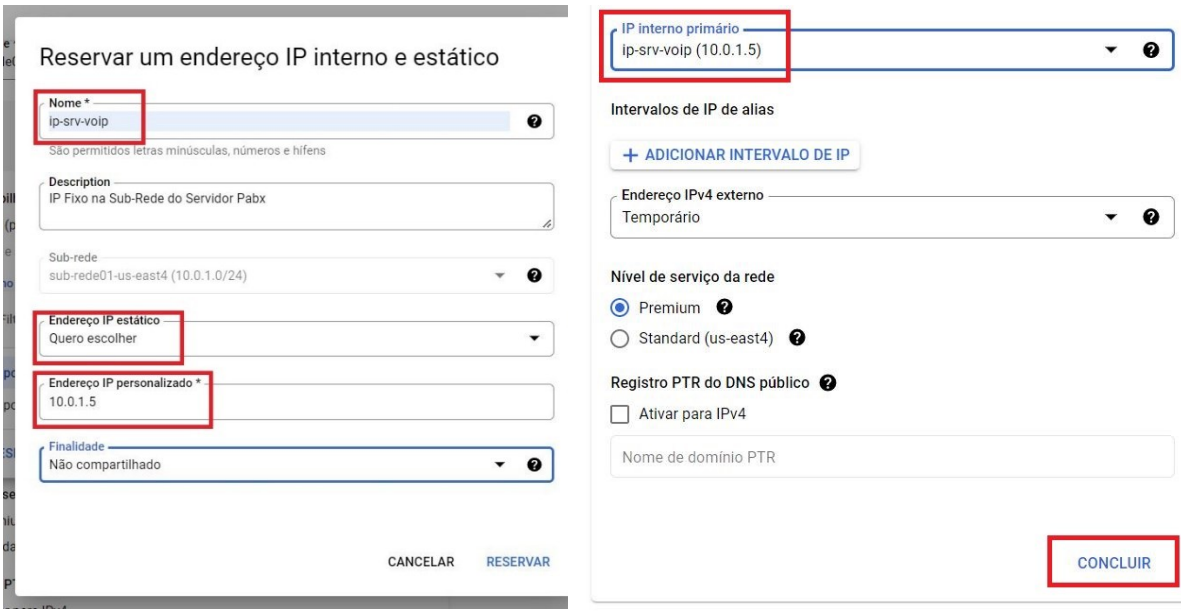
Figura 33 – Interface de Rede



Fonte: Autor

A figura 34 demonstra o processo para a fixação do IP até a sua conclusão.

Figura 34 – IP Estático

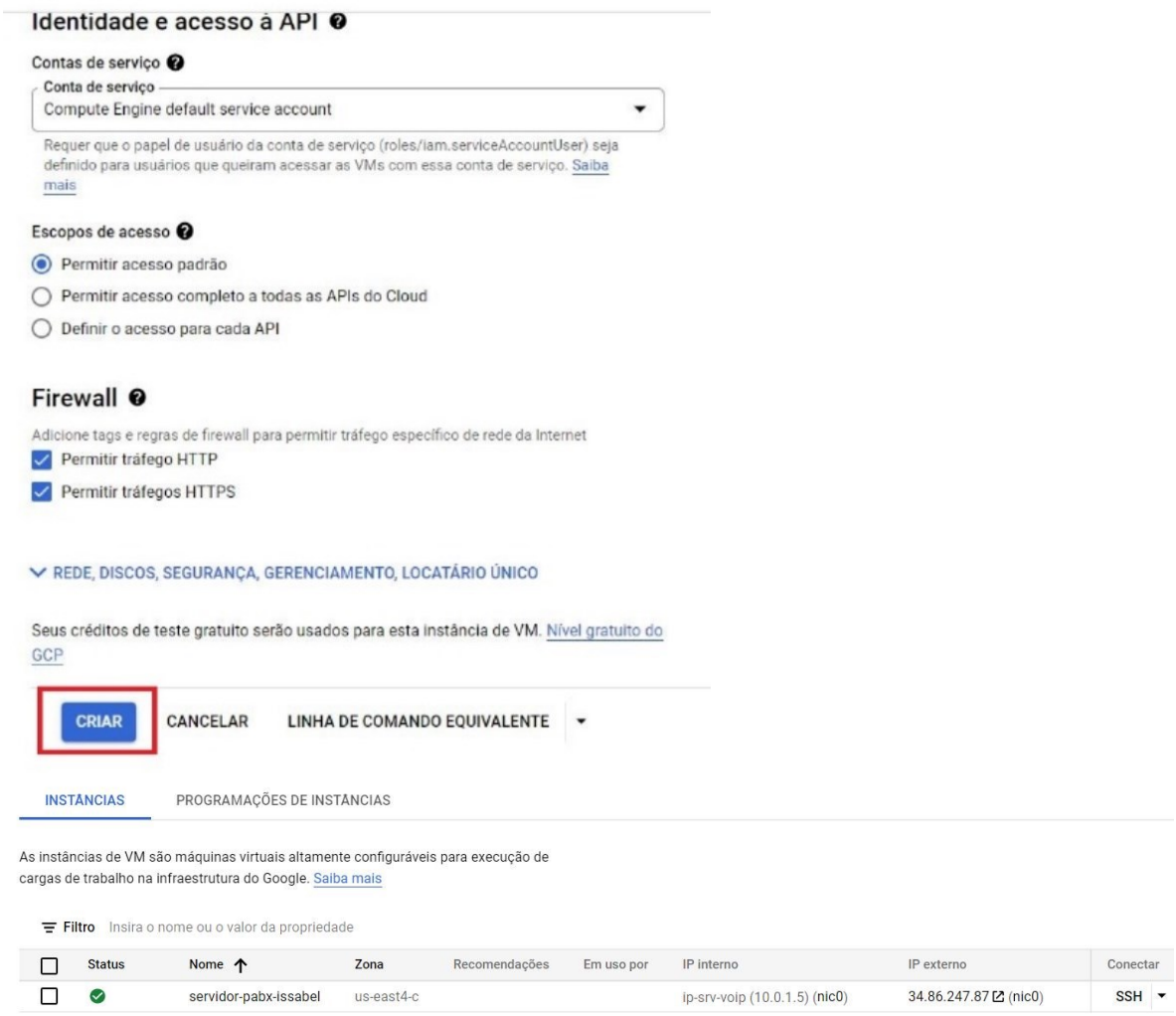


Fonte: Autor

Neste ponto, todas as configurações necessárias foram realizadas para a criação da instância, sendo possível a finalização deste processo ao clicar no botão “Criar” na parte inferior da interface, como mostrado na figura 35.

Após isso, na listagem de instâncias no *Compute Engine* será observada a instância já em pleno funcionamento após alguns segundos.

Figura 35 – Finalização de criação da instância

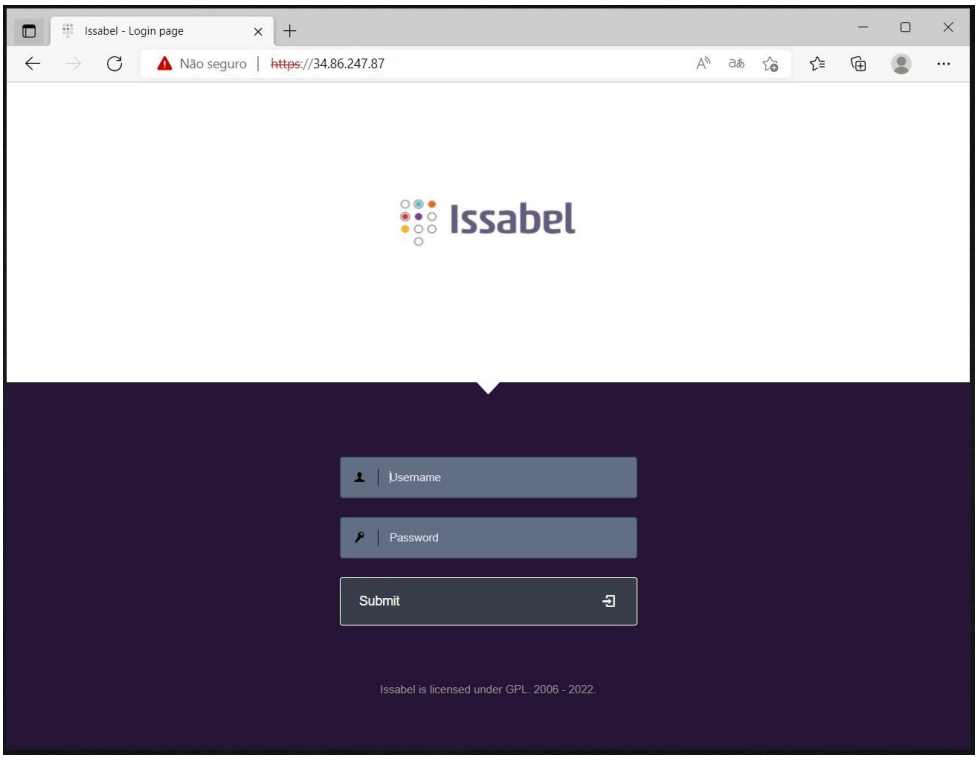


Fonte: Autor

Com a instância de VM em operação, um IP externo atribuído e as permissões de *firewall* possibilitando acesso HTTPS, será realizado um teste para validar se o servidor com o sistema Issabel está funcional.

Na figura 36 pode-se observar que o processo foi bem sucedido, sendo possível o acesso ao console *web* da aplicação.

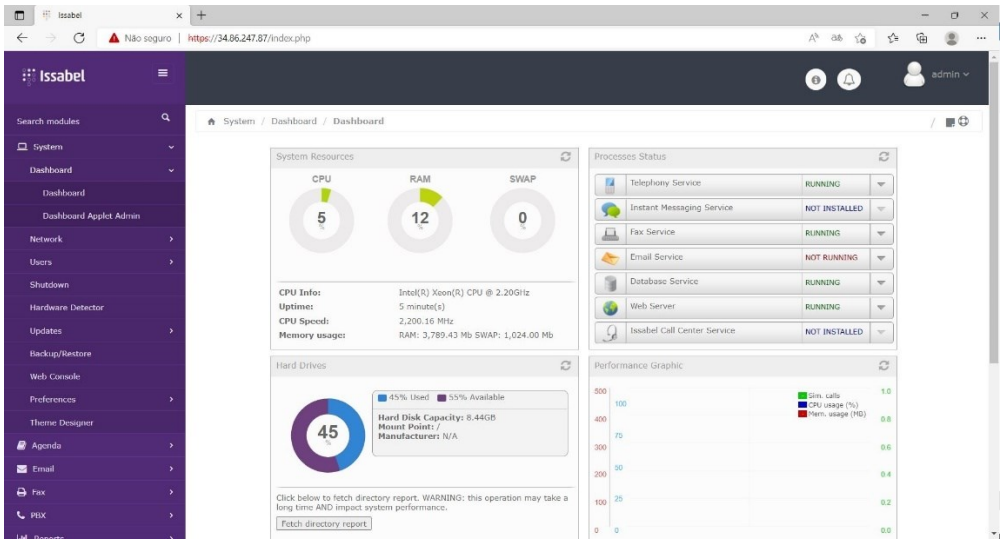
Figura 36 – Acesso à interface *WEB*



Fonte: Autor

Foi possível fazer *login* com as credenciais de administrador configuradas durante a instalação do sistema operacional na máquina virtual local (figura 37).

Figura 37 – *Login* no console



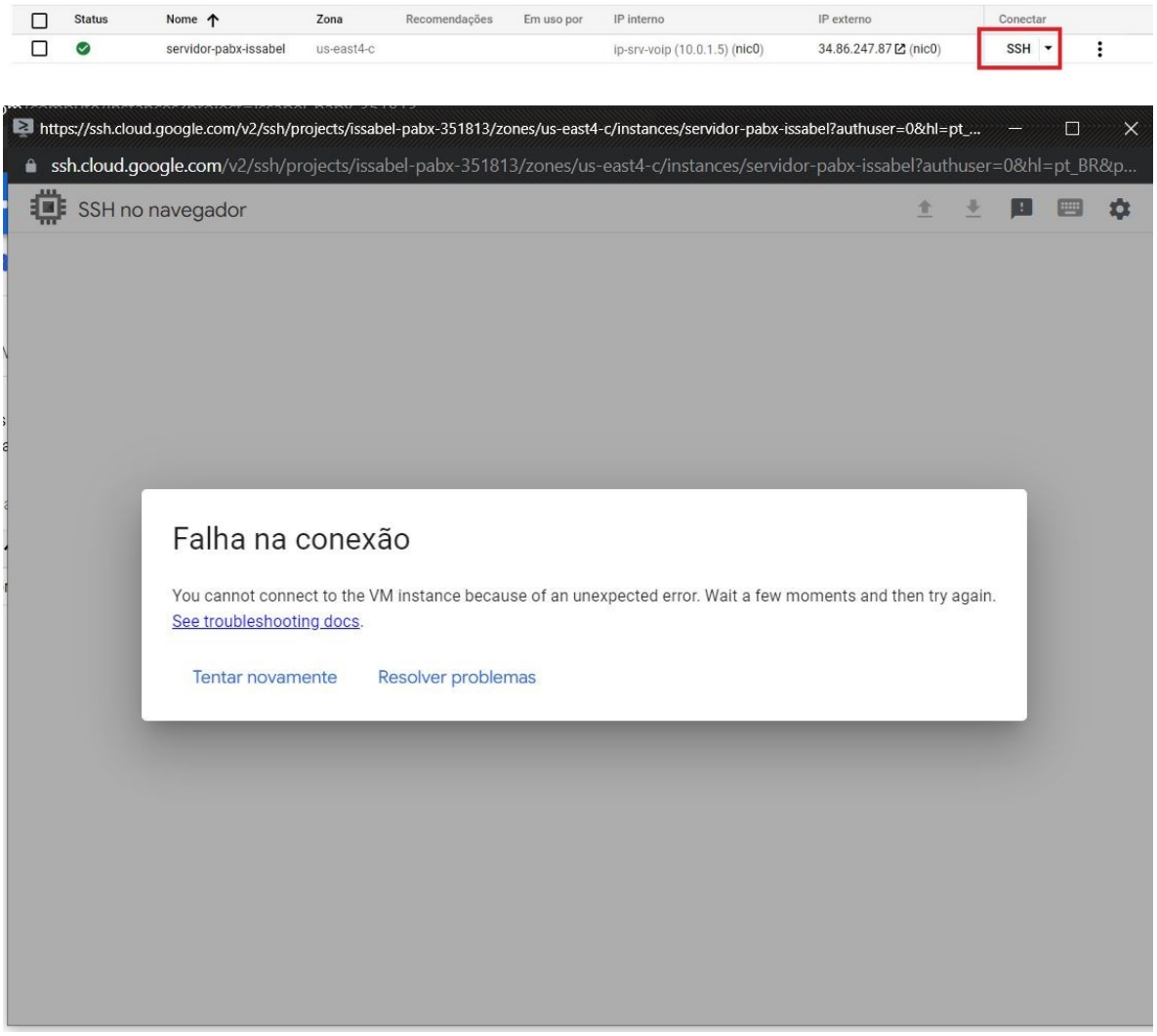
Fonte: Autor

10.2 Regra de *Firewall* para SSH e ICMP

Na figura 38 é demonstrada a tentativa de acesso via SSH (***Secure Shell***) através do utilitário fornecido pelo próprio GCP.

As regras de *firewall* ainda não foram liberadas para esse protocolo, por esse motivo, ocorre a falha na conexão.

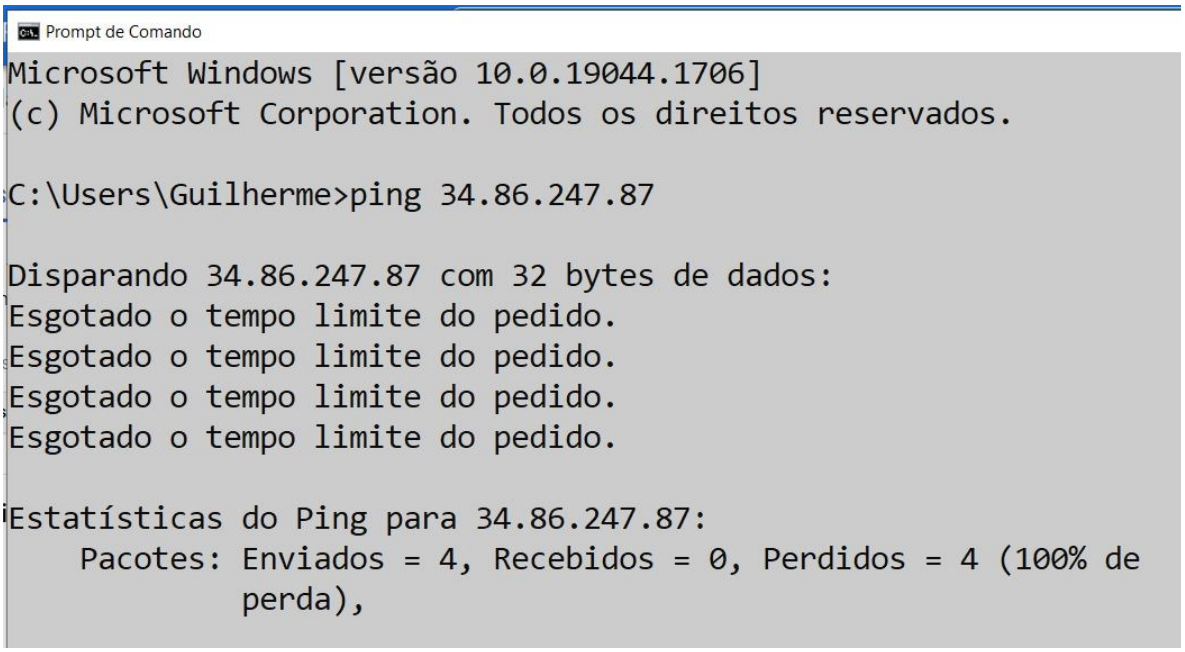
Figura 38 – Tentativa de acesso via SSH



Fonte: Autor

De mesma maneira, ocorre na tentativa de se fazer um ICMP (***Internet Control Message Protocol***) ao servidor, como exemplificado na figura 39.

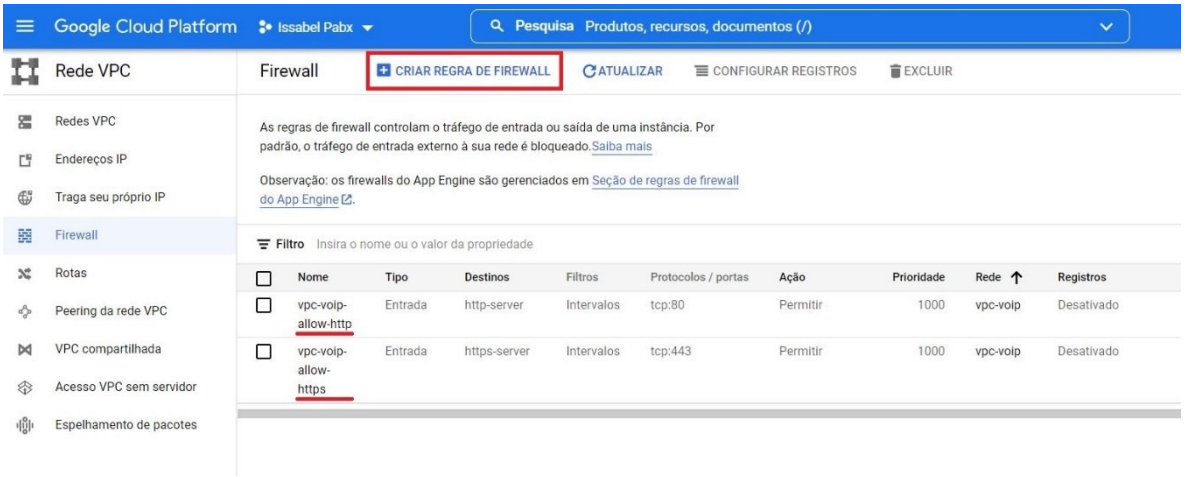
Figura 39 – Tentativa de ICMP



Fonte: Autor

Para utilizar estes protocolos (SSH e ICMP), necessita-se fazer a liberação através de regras no *firewall* da rede VPC. Através da figura 40 pode-se visualizar a existência de duas regras que foram criadas durante a criação da instância. Para criar novas regras, basta clicar no botão “Criar Regra de *Firewall*”.

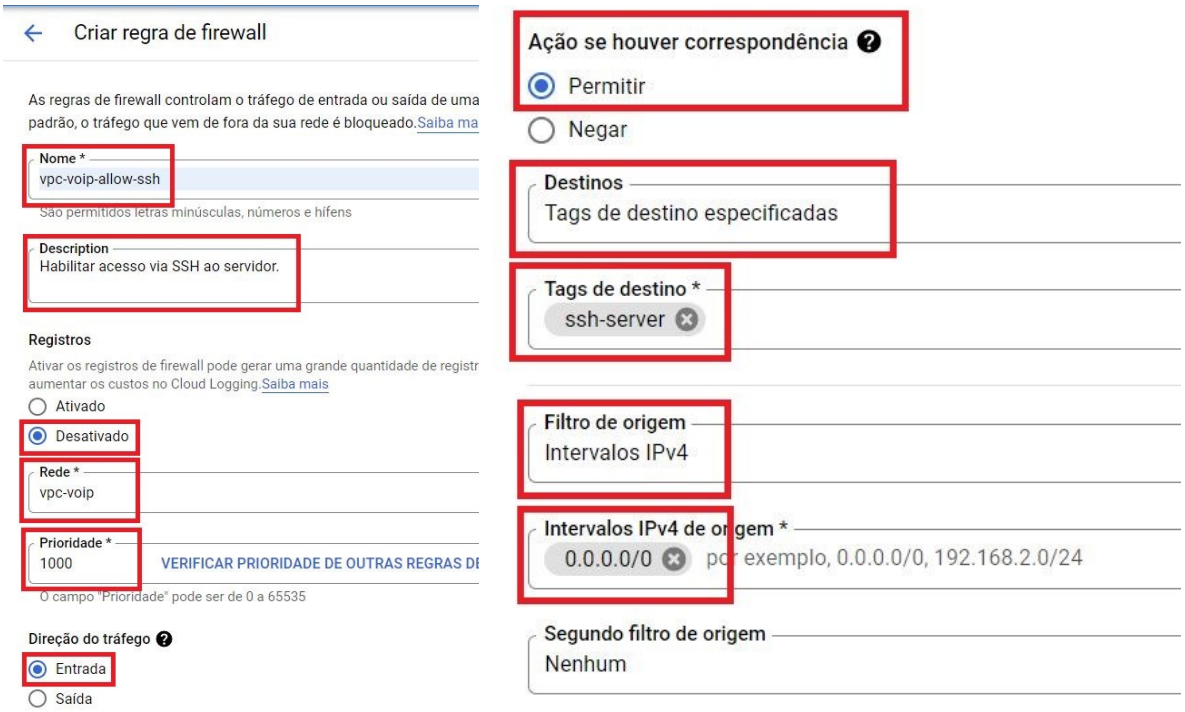
Figura 40 – Criar Regra de *Firewall*



Fonte: Autor

Automaticamente será aberta a interface para a inserção do novo registro (figura 41).

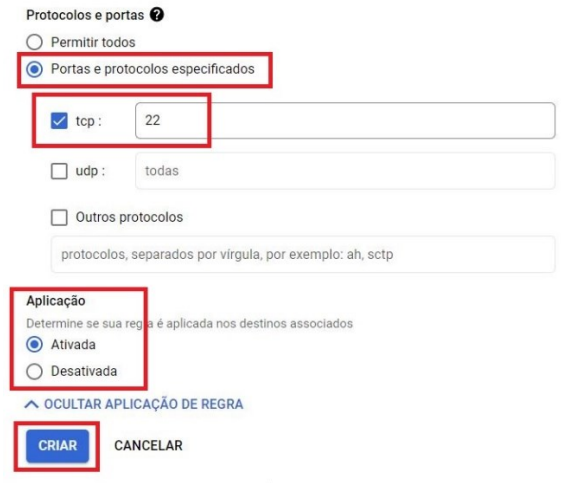
Figura 41 – Criar regra para SSH 01



Fonte: Autor

No mesmo painel será apresentado o restante das configurações (figura 42).

Figura 42 – Criar regra para SSH 02



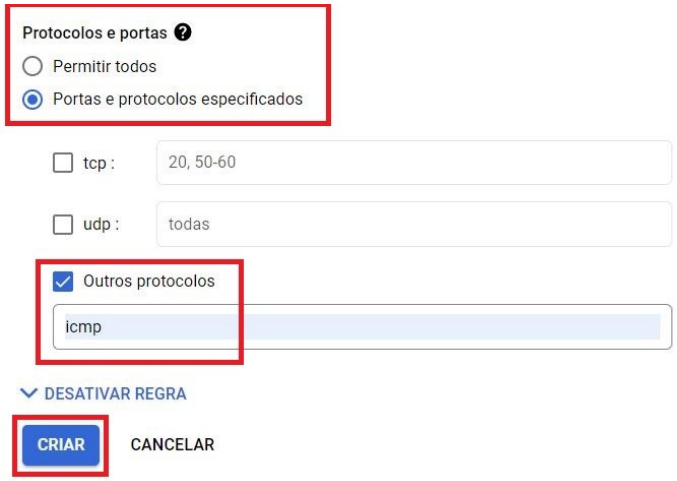
Fonte: Autor

Para a criação da regra ser realizada, é necessário o preenchimento de algumas informações sobre sua finalidade, como mostrado nas figuras 41 e 42.

- **Nome:** nome para a identificação da regra em específico;
- ***Description*:** descrição sobre a regra e qual sua finalidade;
- **Registros:** caso haja o desejo de que seja armazenado registros de atividade da regra, basta selecionado o *role* “Ativado”;
- **Rede:** escolha da rede à qual a regra se destina, neste caso é a VPC criada para o projeto;
- **Prioridade:** definir um valor de prioridade de acordo com sua importância dentro da tabela de regras do *firewall*;
- **Direção do tráfego:** definir se a regra é vale de dentro para fora ou de fora para dentro da rede;
- **Ação se houver correspondência:** caso a regra possa ser aplicada na requisição, o que se deve fazer com o pacote;
- **Destinos:** escolha do alvo da regra, para o caso deste projeto, foi decidido utilizar “Tags de destino especificadas”, o qual irá solicitar o nome de uma *tag* para atribuir a regra a um alvo específico, neste caso, a instância de VM criada para ser o servidor;
- ***Tags* de destino:** nome da *tag* para ser atribuída à instância;
- **Filtro de origem:** define o tipo da origem da solicitação, neste caso, como o IPv6 foi desabilitado, iremos utilizar apenas para o IPv4;
- **Intervalos de IPv4 de origem:** no caso desta regra, ela se destina para conexões externas, e pelo fato de não ter-se o conhecimento dos IPs de origem, foi habilitado para qualquer um;
- **Protocolos e portas:** como o intuito desta regra é o de habilitar o SSH via TCP (***Transmission Control Protocol***), seleciona-se ca porta “22” no “TCP”;
- **Aplicação:** se a regra será aplicada ou não nos destinos associados.

Após criada a regra para SSH, o mesmo, será feito para o ICMP, alterando apenas a identificação e a última etapa, como é possível ver na figura 43. Pelo fato do ICMP funcionar na camada de rede, ele deve ser habilitado através do campo “Outros protocolos”.

Figura 43 – Criar regra para ICMP



Fonte: Autor

Finalizando a criação das duas regras, agora já é possível vê-las listada no *firewall*, como mostrado na figura 44.

Figura 44 – Regras do *Firewall*

Fonte: Autor

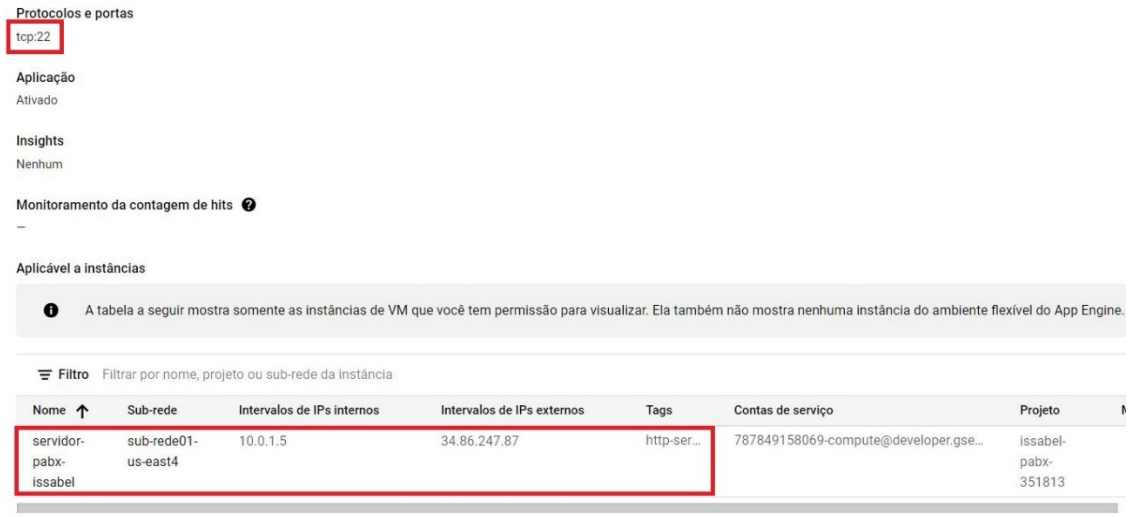
Como os destinos das regras foram definidos por *tags*, é necessário atribui-las à instância. Para isso é necessário ir até o "*Compute Engine*" e editá-la, de acordo com a imagem 45.

Figura 45 – Atribuir *tags* à instância

Fonte: Autor

No *firewall*, para validação, pode-se abrir a regra criada (no exemplo da figura 46 a SSH) e notar que a regra está sendo aplicada na instância **servidor-pabx-issabel**.

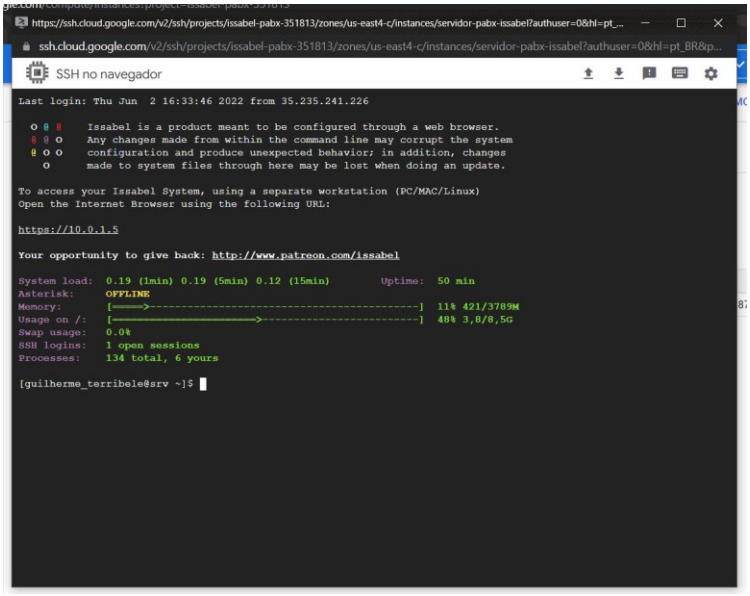
Figura 46 – Regra para SSH em vigor na instância



Fonte: Autor

A título de curiosidade, será realizada a tentativa de conexão via SSH através do utilitário do GCP (figura 47).

Figura 47 – Acesso SSH



Fonte: Autor

O mesmo será feito para o ICMP, enviando-se um *ping* ao servidor (figura 48).

Figura 48 – Teste de ICMP

```
C:\Users\Guilherme>ping 34.86.247.87

Disparando 34.86.247.87 com 32 bytes de dados:
Resposta de 34.86.247.87: bytes=32 tempo=121ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=120ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=120ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=119ms TTL=58

Estatísticas do Ping para 34.86.247.87:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 119ms, Máximo = 121ms, Média = 120ms
```

Fonte: Autor

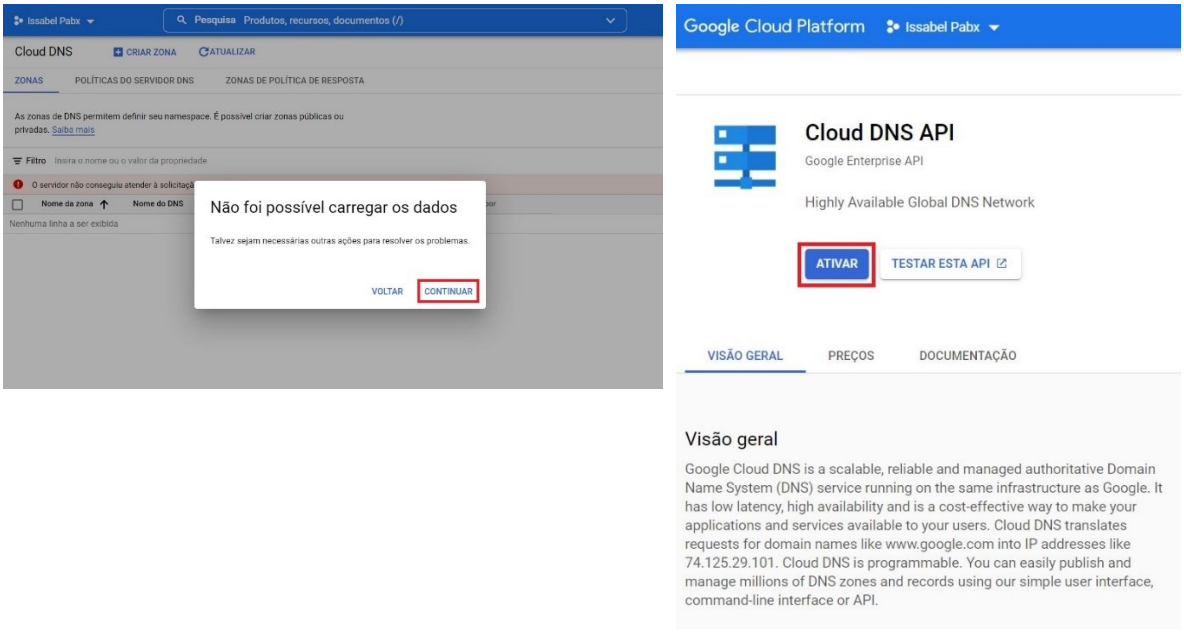
Como pode-se observar nas figuras 47 e 48, obteve-se êxito nos testes, sendo validado o funcionamento das regras no *firewall*, neste ponto, a máquina já esta habilitada para conexões via SSH, HTTP, HTTPS e a possibilidade de testes utilizando-se o ICMP.

11 Configuração do DNS

Através da plataforma de nuvem do Google, é possível realizar o registro de um domínio e configuração de DNS (***Domain Name System***), deste modo, essa função será explorada neste trabalho, possibilitando a utilização futura de um DDNS (***Dynamic Domain Name System***).

Para isso, é necessário acessar através do “Serviços de rede” a “Cloud DNS”, que não possibilita sua utilização no momento, como mostra a 49, sendo necessária a ativação da API responsável por este serviço.

Figura 49 – Habilitar API *Cloud* DNS

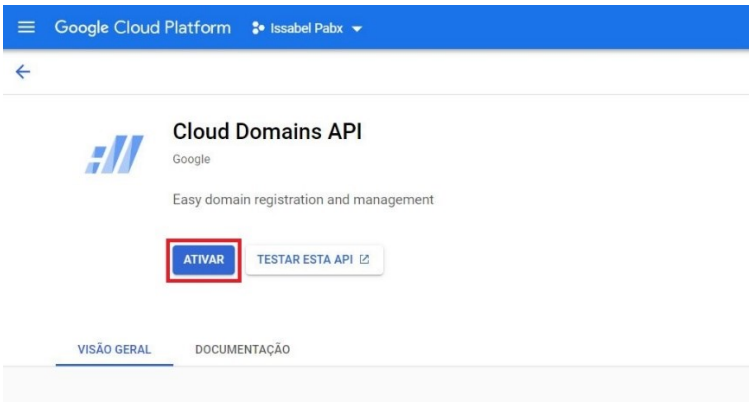


Fonte: Autor

11.1 Registro de Domínio através do *Cloud Domains*

Para utilizar o DNS em um domínio próprio, será realizado o registro de um para o autor. Deste modo, é necessário também realizar a ativação do *Cloud Domains* API. Para isso, basta acessar “*Cloud Domains*” em “Serviços de rede no painel principal, assim como exemplificado na figura 50.

Figura 50 – Habilitar API *Cloud Domains*



Fonte: Autor

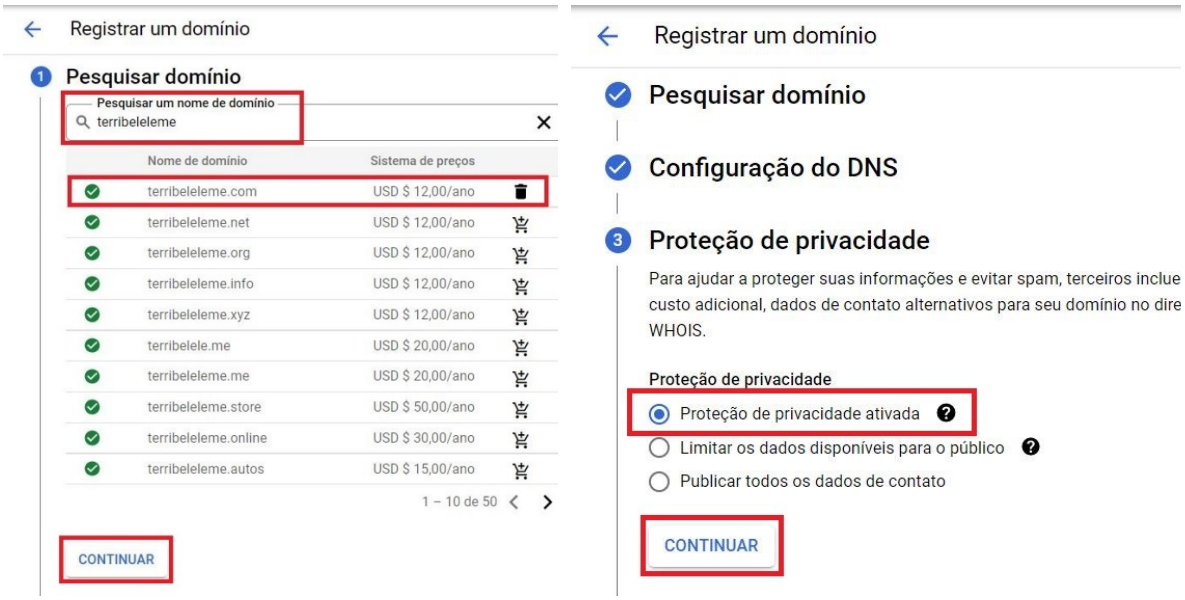
Ao ativar a API necessária, será possível acessar o painel *Cloud Domains*. Nesse ponto, para registrar um domínio, basta selecionar a opção de “Registrar Domínio”, como mostrado na figura 51, e seguir as etapas subsequentes, sendo necessário a escolha de um nome e algumas configurações básicas que foram optadas pelas padrões fornecidas pela plataforma.

Figura 51 – Registrar Domínio

Fonte: Autor

A figura 52 exemplifica a escolha do nome de domínio e a opção de privacidade desejada. Lembrando que para o registro de domínio existe um custo anual.

Figura 52 – Informações do Domínio



Fonte: Autor

Na figura 53 pode-se ver o domínio registrado com sucesso.

Figura 53 – Domínio criado

Fonte: Autor

11.2 Configuração do DNS

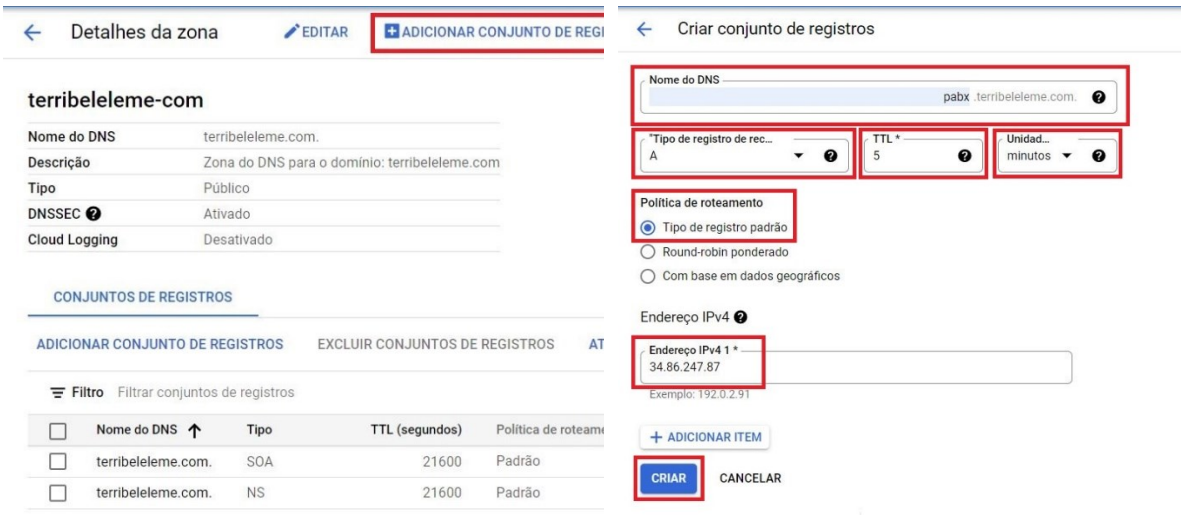
Após o domínio ser registrado, no *Cloud* DNS já é possível visualizar a zona contendo-o (figura 54), sendo necessária apenas a adição de um novo conjunto de registros contendo as informações do DNS.

Figura 54 – Zonas

Fonte: Autor

Na figura 55, as informações inseridas no registro da zona, basta clicar em “Criar” para finalizar sua adição.

Figura 55 – Domínio criado



Fonte: Autor

11.3 Teste do DNS

Existindo o DNS, será realizado um teste utilizando o ICMP para validar o funcionamento. Na figura 56, nota-se a resolução do nome bem sucedida.

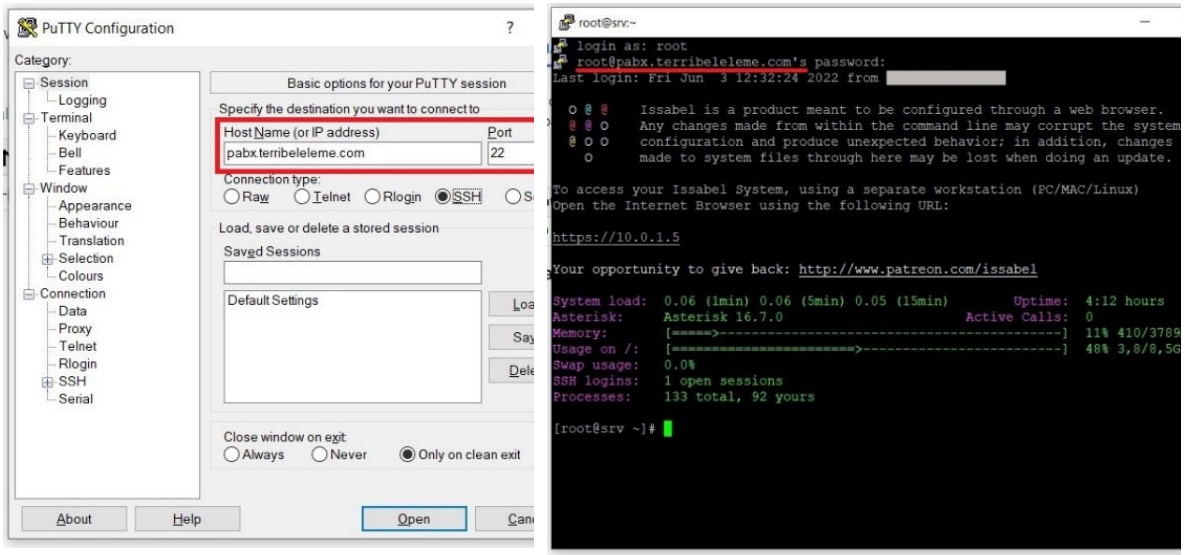
Figura 56 – Teste de *ping* utilizando DNS

```
C:\Users\Guilherme>ping pabx.terribeleleme.com

Disparando pabx.terribeleleme.com [34.86.247.87] com 32 bytes de dados:
Resposta de 34.86.247.87: bytes=32 tempo=121ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=121ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=121ms TTL=58
Resposta de 34.86.247.87: bytes=32 tempo=121ms TTL=58

Estatísticas do Ping para 34.86.247.87:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 121ms, Máximo = 121ms, Média = 121ms
```

Fonte: Autor

Será realizado um teste para acesso via SSH utilizando o PuTTY e através do endereço configurado no DNS, pode-se observar, na figura 57, o seu funcionamento, validando-se as configurações feitas previamente.

Figura 57 – Teste de acesso SSH utilizando DNS



Fonte: Autor

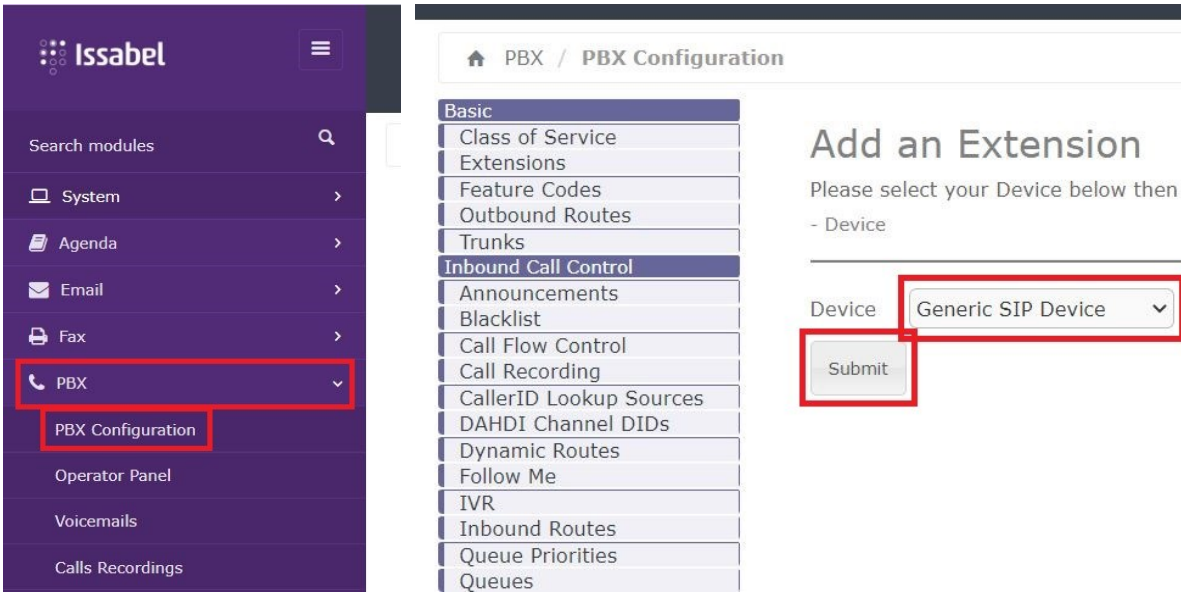
12 Configuração do PABX para ligações

Para configurar o PABX (***Private Automatic Branch Exchange***) de modo a possibilitar as ligações entre ramais (e caso desejado, entroncamentos para ligações externas), é necessário realizar a configuração de ramais, os quais serão configurados em *softphones* para que consigam comunicar entre si.

12.1 Criação de ramais

A palavra “ramal” tem como origem a palavra “ramo”, e é exatamente isso o que ela significa, pois será um dos ramos de toda uma estrutura telefônica local, que chegará até o usuário final. Deste modo, para validar o funcionamento do servidor PABX, é necessário que exista comunicação entre dois ramais, para o que, no Issabel serão criadas três contas de ramal.

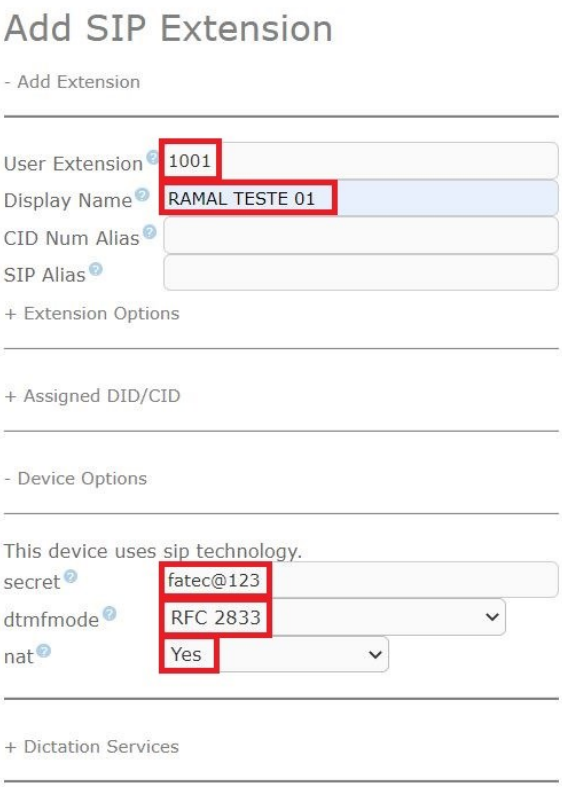
Figura 58 – Criar Ramais



Fonte: Autor

Como pode-se notar na figura 58, em “PBX” e, logo em seguida, em “PBX *Configuration*”, será possível a seleção do tipo de dispositivo que irá ser configurado. No caso deste projeto, foi optado por um dispositivo SIP (***Session Initiation Protocol***) padrão.

Figura 59 – Informação dos Ramais



Fonte: Autor

Após a página para iniciar a configuração dos ramais abrir, as informações pertinentes no momento para este projeto são apenas as listadas a seguir, sendo mantido o padrão para o restante:

- ***User Extension*:** será definido o ramal utilizado pelo usuário;
- ***Display Name*:** o nome do ramal que está sendo configurado, que serve para organização do PABX e será o nome exibido quando houver solicitação de ligação;
- ***secret*:** senha para a configuração do ramal no *softphone*;
- ***dtmfmode*:** é o tipo de discagem utilizada pelo dispositivo;
- **nat:** permitir autenticação de fora da rede.

Após devidamente configurado o ramal (figura 59), ao final da página será apresentado um botão "*Submit*" o qual irá provisionar as informações dos ramais e irá aguardar sua aplicação. De mesmo modo, serão criados mais dois ramais para teste. Logo em seguida, basta aplicar as configurações feitas da criação dos ramais e será apresentada a listagem dos já existentes (figura 60), que podem ser editados ou excluídos posteriormente.

Figura 60 – Ramais Criados

Fonte: Autor

12.2 Liberação de portas no *Firewall* da VPC

A próxima etapa é a necessidade de realizar a configuração do *firewall* para os protocolos SIP e RTP (***Real-time Transporte Protocol***), que serão responsáveis respectivamente pela autenticação dos ramais e o tráfego dos pacotes.

Para isso, como feito anteriormente, é necessário ir até as configurações de *firewall* da rede VPC e criar as regras necessárias. Como pode-se ver na figura 61, as portas necessárias para serem liberadas são as 5060 e a 10000 até 20000 utilizando o protocolo UDP (***User Datagram Protocol***). Notam-se as prioridades definidas diferente das padrões utilizadas anteriormente.

Figura 61 – Regras para SIP e RTP

	Nome	Tipo	Destinos	Filtros	Protocolos / portas	Ação	Prioridade	Rede
☐	vpc-voip-allow-sip	Entrada	sip-server	Intervalos	udp:5060	Permitir	100	vpc-voip
☐	vpc-voip-allow-rtp	Entrada	rtp-server	Intervalos	udp:10000-20000	Permitir	101	vpc-voip

Fonte: Autor

12.3 Configuração do SIP

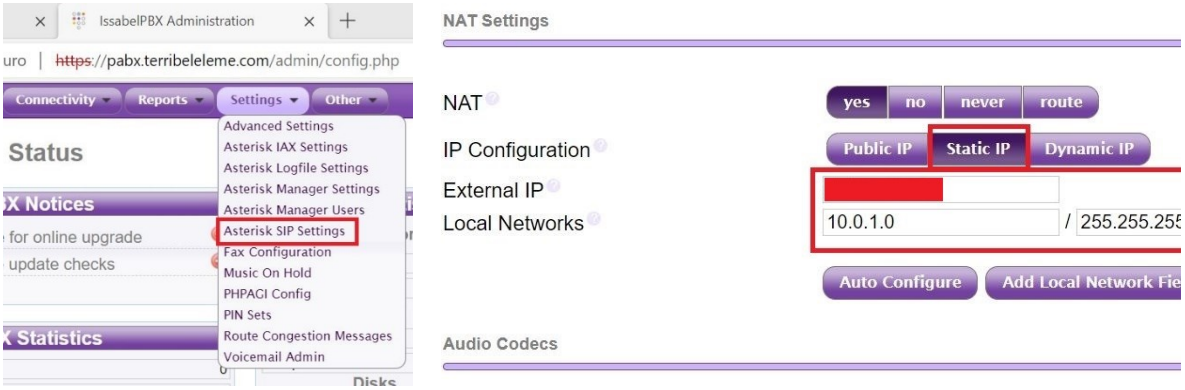
Com as portas necessárias habilitadas e os ramais criados, se faz necessária a configuração dos apontamentos do SIP. Para isso necessita-se habilitar as configurações em "*Advanced Settings*" da seção "*Security*" (figura 62).

Figura 62 – *Unembedded* IssabelPBX

Fonte: Autor

A figura 63 apresenta a interface para configurar o SIP Asterisk. O IP externo será definido pelo da instância de VM, e o IP da rede local é o da sub-rede na VPC. Após configurado, no final da página basta clicar no botão "Submit Changes" e desativar a permissão de acesso mostrada na figura 62.

Figura 63 – Configuração do SIP Asterisk



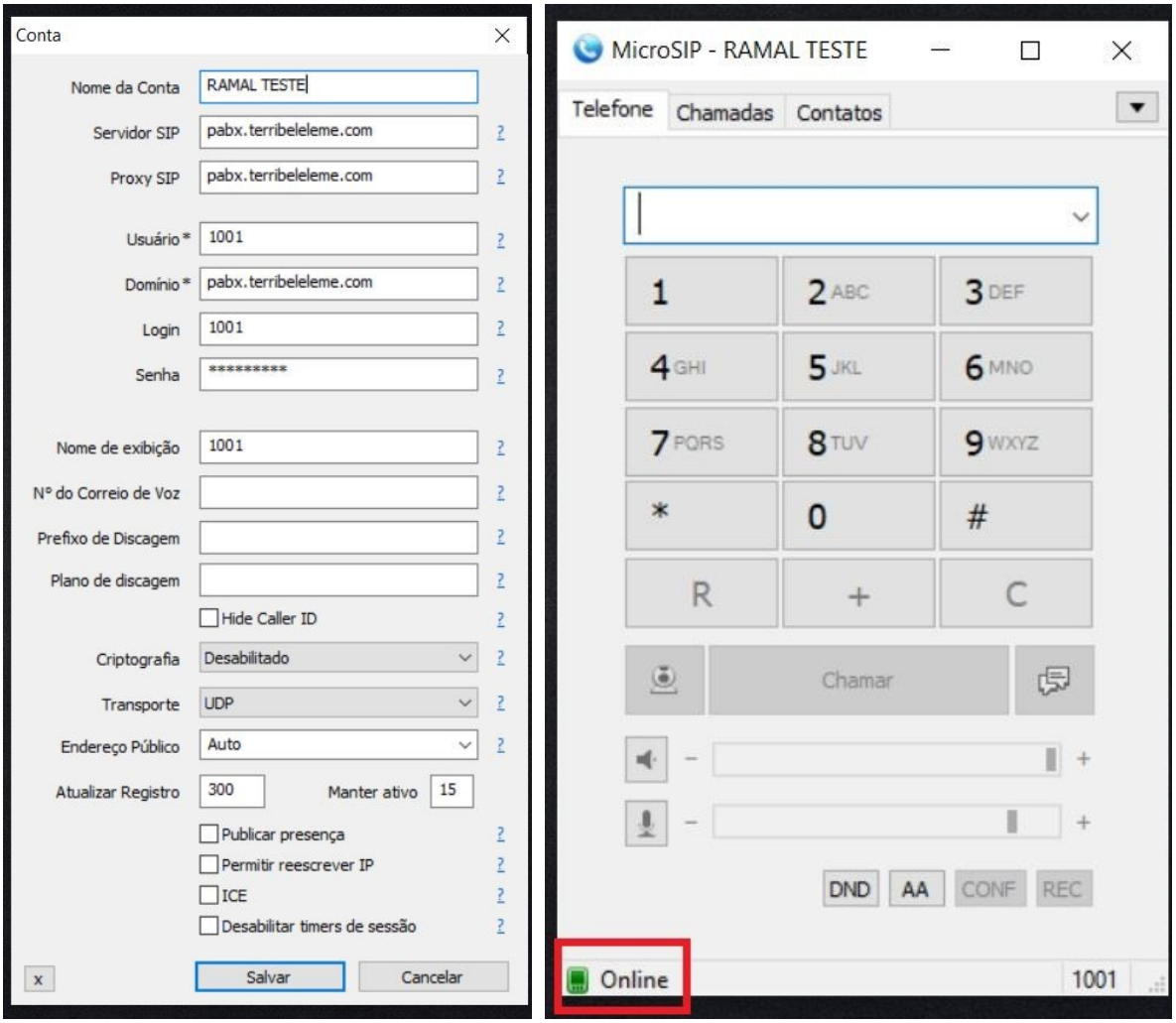
Fonte: Autor

Realizadas essas etapas, a máquina deve ser reiniciada, tanto pelo "*System*" e "*Shutdown*", quanto pelo painel da instância de VM no GCP.

12.4 Configuração do *Softphone*

Para realizar a validação da autenticação via SIP, será utilizado o *software* de softphone MicroSIP. Nas configurações da conta, é necessário preencher com as informações do servidor PABX e do ramal que se deseja configurar, como exemplificado na figura 64.

Figura 64 – Configuração do *Softphone*



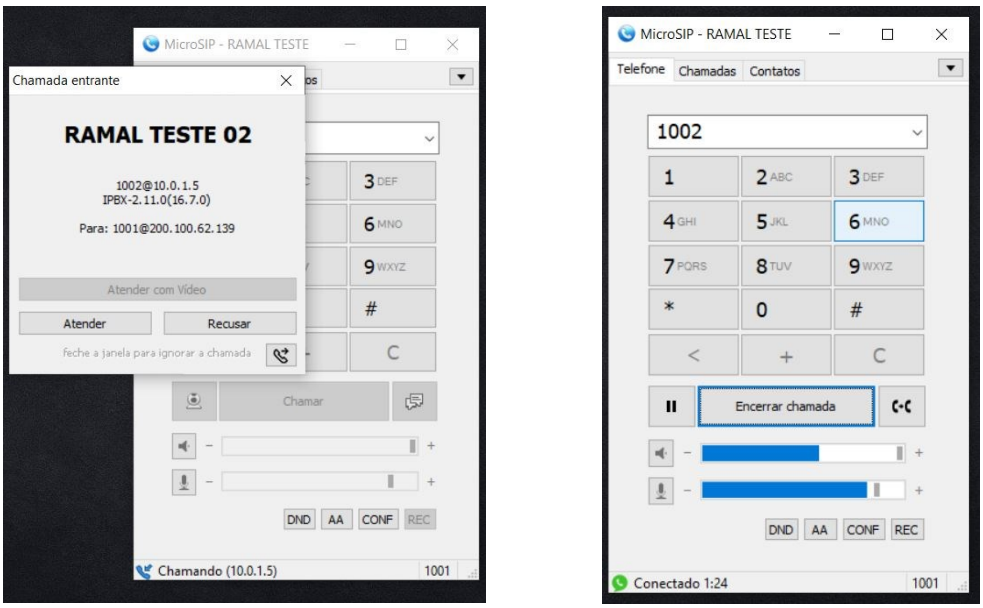
Fonte: Autor

12.5 Validação do serviço

Para validar o funcionamento do serviço instalado e configurado, é necessário configurar outro *softphone* e executar o teste de funcionamento, realizando uma chamada de um ramal para o outro e testando se os canais de comunicação funcionam, a qualidade, se a latência existente permite uma boa comunicação e afins.

Naa figuras 65 é possível observar a ligação sendo solicitada pelo “RAMAL TESTE 02” e logo atendida, com 1 minuto e 24 segundos de duração.

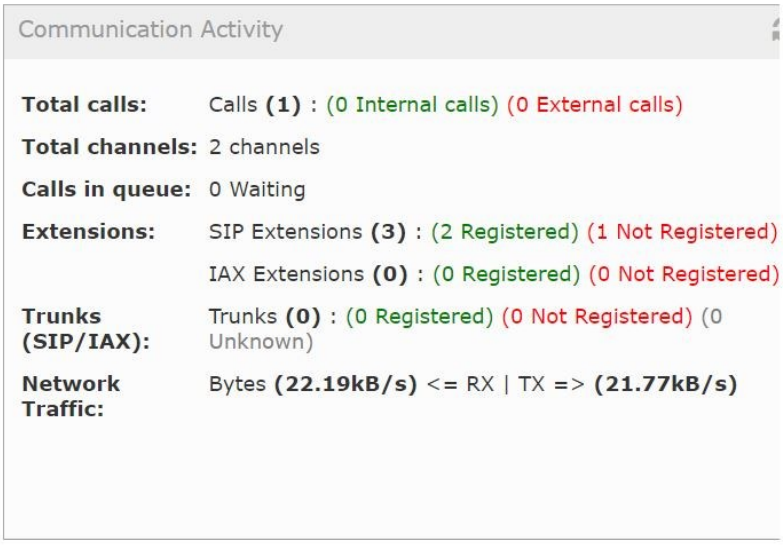
Figura 65 – Recebimento de Chamada



Fonte: Autor

Na figura 66, observa-se os ramais registrados e uma ligação ativa.

Figura 66 – Chamada ativa no PABX



Fonte: Autor

13 Considerações finais

Tendo em vista o objetivo do projeto, que foi o de hospedar um serviço VoIP no *Google Cloud Platform*, pôde-se observar todas as etapas seguidas para atingir esta finalidade, percorrendo o trajeto desde a criação e configuração de uma máquina virtual local com o Issabel PBX, elaboração do ambiente em *cloud* para receber a o disco virtual e a instância de VM até a sua plena operabilidade. Para isto, aplicam-se muitos conceitos e teorias estudadas durante a graduação, como, por exemplo, sistemas operacionais, redes de computadores, arquitetura de computadores, criação e administração de *firewall*, e muitas outras.

Considerando os resultados finais obtidos com a conclusão do projeto, é notável a qualidade do produto entregue, o qual, facilmente pode ser comercializado no mercado como uma solução de telefonia, visando alcançar os mais variados tipos de clientes, desde os mais simples até corporações maiores, devido à grande gama de recursos que o GCP tráz, facilmente paremetrizável com o ambiente desejado, podendo ser facilmente modulado a ele. Aliado com tecnologias de *snapshots* e fácil recuperação, torna-se fácil a recuperação do serviço em caso de alguma indisponibilidade, sem a necessidade de depender de um servidor local para o seu funcionamento.

Analisando a relação custo-benefício do projeto, a sua utilização é fortemente recomendada, pois a plataforma é de fácil utilização do profissional que irá a administrar e conta com uma vasta documentação publicada, tornando-se muito competitiva a solução.

14 Referências

Issabel Powered By Asterisk. Disponível em: <https://www.issabel.org/about-us/>. Acesso em: 30 Mai. 2022.

TAURION, Cezar. **Cloud Computing:** computação em nuvem: transformando o mundo da tecnologia da informação**.** 1 ª Edição. Rio de Janeiro: Brasport, 2009.

Visão Geral do Google Cloud. Disponível em: <https://cloud.google.com/docs/overview?hl=pt-br>. Acesso em: 09 Jun. 2022.

Wallingford, Ted. **Switching to VoIP.** 1ª Edição. Estados Unidos da América: O'Reilly, 2005.