PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
CIÊNCIA DA COMPUTAÇÃO

PRINCIPAIS TECNOLOGIAS DE SEGURANÇA DA *GOOGLE CLOUD PLATFORM*

ERIC SOUZA DANTAS

GOIÂNIA,
2023

ERIC SOUZA DANTAS

PRINCIPAIS TECNOLOGIAS DE SEGURANÇA DA *GOOGLE CLOUD*

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação.

Orientadora: Prof. Drª. Solange da Silva.

GOIÂNIA,

2023

ERIC SOUZA DANTAS

PRINCIPAIS TECNOLOGIAS DE SEGURAÇA DA *GOOLE CLOUD*

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Ciências da Computação, e aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, em ____/____/_____.

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Me. Fernando Goncalves Abadia

_____

Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA,

2023

AGRADECIMENTOS

A Deus por ter me dado sabedoria e resiliência para superar todas as dificuldades e obstáculos enfrentados.

A minha família, minha mãe Sueli, meu pai Celio, minha avó Aldenora, minha irmã Talita e minha sobrinha Cacau que sempre me apoiaram e me incentivaram nessa minha caminhada.

Em especial, gostaria de agradecer meus pais por sempre estarem ao meu lado e terem me proporcionado oportunidades de estudo.

A Professora Solange da Silva, pela paciência e por sempre ter me ajudado com conselhos e dicas na orientação e realização dessa monografia.

Agradeço a todos, de que uma forma ou de outra, contribuíram para a realização deste trabalho.

RESUMO

Este trabalho tem como objetivo identificar os principais serviços de segurança fornecidas pela *Google Cloud* e como são aplicadas, mostrando como cada um desses serviços funcionam e suas proteções de segurança. Quanto aos aspectos metodológicos, é uma pesquisa bibliográfica, documental e experimental. Os resultados mostraram que existem várias soluções de segurança oferecidas pela *Google Cloud* que tornam o ambiente mais seguro. Entretanto, se o cliente não tiver um domínio do funcionamento de cada serviço, ele dificilmente saberá como configurar sua infraestrutura em nuvem de forma segura. Além disso, saber quais são os principais tipos de vulnerabilidades e ataques são fatores para se ter uma boa configuração de segurança com a escolha dos serviços apropriados.

Palavras Chaves: Computação em nuvem, *Google Cloud*, Segurança em nuvem, Segurança de dados, Vulnerabilidade.

ABSTRACT

This work aims to identify the main security services provided by Google Cloud and how they are applied, showing how each of these services work and their security protections. As for the methodological aspects, it is a bibliographical, documental and experimental research. The results showed that there are several security solutions offered by Google Cloud that make the environment more secure. However, if the customer does not have a mastery of the functioning of each service, he will hardly know how to configure his cloud infrastructure in a secure way. In addition, knowing what the main types of vulnerabilities and attacks are factors to have a good security configuration with the choice of appropriate services.

Keywords: Cloud computing, Google Cloud, Cloud security, Data security, Vulnerabilities.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE SIGLAS

CA	*Certificate Authority* ou Autoridade de Certificação
C2	Comando e Controle
DDoS	*Distributed Denial of Services*
DLP	*Cloud Data Loss Prevention*
EKM	*External Key Management*
GCP	*Google Cloud Platform*
GKE	*Google Kubernetes Engine*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure ou* Protocolo de Segurança de Transporte de Hipertexto
IA	Inteligência Artificial
IaaS	*Infrastructure-as-a-Service* ou Infraestrutura como Serviço
IAM	*Identity and Access Management*
IAP	*Identity-Aware Proxy*
IP	*Internet Protocol* ou Protocolo de rede
KMS	*Cloud Key Management Service*
LAN	*Local Area Network* ou Rede local
MCC	*Mobile cloud computing* ou Computação em nuvens móvel
NIST	*National institute of standards and technology*
PaaS	*Platform-as-a-Service* ou Plataforma como Serviço
SaaS	*Software-as-a-Service* ou *Software* como Serviço
SEV	*Security Encripted Virtualization* ou Virtualização Criptografada Segura
SIEM	*Security Information and Event Management* ou Segurança de Informações e Gerenciamento de Eventos
SQL	*Structured Query Language* ou Linguagem de Consulta Estruturada
SOC	*Security Operations suite ou* Pacote de operações de segurança
TI	Tecnologia da Informação

UEFI	*Unified Extensible Firmware Interface* ou Interface Unificada de *Firmware* Extensível
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos
VM	*Virtual Machine* ou Máquina Virtual
vTPM	*Virtual Trusted Platform Module* ou Módulo de Plataforma Confiável
VPC	*Virtual Private Cloud* ou Nuvem Privada Virtual
VPN	*Virtual Private Network* ou Rede Privada Virtual
WWW	*World Wide Web*

SUMÁRIO

1. INTRODUÇÃO

Com o rápido desenvolvimento de tecnologias de sistemas distribuídos, um dos maiores desafios enfrentados pelo mundo está em garantir a segurança de dados sensíveis e confidenciais durante o transporte e armazenamento, que são considerados os desafios mais críticos enfrentados pela computação em nuvem (THABIT et al., 2021).

A computação em nuvem, ou *Cloud Computing,* é a entrega de recursos de tecnologia da informação (TI) sob demanda por meio da Internet com definição de preço de pagamento conforme o uso. Em vez de comprar, ter e manter data centers e servidores físicos, pode-se acessar serviços de tecnologia, como capacidade computacional, armazenamento e banco de dados, conforme a necessidade, usando um provedor de nuvem como a *Amazon Web Services* (AWS) (AMAZON, 2022).

Os clientes usam os recursos fornecidos pela nuvem e pagam de acordo com o uso. Por outro lado, os provedores do serviço em nuvem podem utilizar esses mesmos recursos assim que forem liberados por um usuário específico, resultando em uma melhor utilização de recursos (PRASAD et al., 2014).

A facilidade de uso é outra vantagem oferecida pela computação em nuvem, pois não exige que os clientes possuam conhecimento extraordinário relativo às tecnologias específicas da nuvem. O gerenciamento da tecnologia e dos serviços passou do usuário para o provedor de serviços em nuvem (DHAMOTHARAN et al., 2015).

A computação em nuvem fornece recursos virtualizados aos clientes usando várias tecnologias, por exemplo, serviços web, virtualização e multilocação (DUAN et al., 2012).

A computação em nuvem móvel tornou-se uma tecnologia viável devido ao crescimento acelerado de aplicações móveis. Ela incorpora a computação em nuvem nos dispositivos moveis, como no celular, abordando os desafios da computação na nuvem móvel como, capacidade de processamento, bateria, capacidade de armazenamento, privacidade e segurança (KHADHIM et al. 2021).

Segurança de nuvem é um termo amplo que engloba a tecnologia e as práticas recomendadas criadas para proteger os dados e as informações em uma arquitetura de

nuvem. Ela garante a privacidade, segurança e conformidade dos dados armazenados na nuvem (VMWARE, 2022).

A segurança dos dados é a proteção dos mesmo diante de ameaças, acidentes, roubo, destruição, entre outros. Segurança de dados refere-se à preservação das informações de uma organização, sendo uma preocupação não só do departamento de TI, mas de toda a empresa (LUCENA, 2017).

No início de 2022, um ataque que vale ser mencionado é o ocorrido nas lojas Americanas e seu grupo de lojas como Submarino e Shoptime, ocorrido no dia 19 de Fevereiro de 2022, nesta data foi identificado um acesso não autorizado aos servidores das lojas Americanas para evitar qualquer tipo de vazamento de dados as Americanas e Submarino seguiram os protocolos de segurança e desativaram seus serviços até que especialistas analisassem esse incidente. Estima-se que o grupo Americanas teve um prejuízo de quase R$3,3 bi devido aos sites ficarem fora do ar durante os dias 19 ao 21, além da desvalorização dos papéis da companhia 6,55% na Bolsa de valores. (SANTIAGO, 2022).

As normas ISO 27001, 27701, 27017, 27018 e 27032 constituem alguns dos principais padrões para proteger a cibersegurança e garantir a integridade da informação armazenada na nuvem, serviço oferecido por grandes empresas Data Centers como *Amazon Web Services* (AWS), *Google Cloud Platform* (GCP) ou *Microsoft Azure* (TORRES, 2022).

Justifica-se estudar esse tema pois, em todo o mundo, as organizações governamentais e grandes empresas têm modificado a infraestrutura computacional de serviços localmente mantidos para serviços ofertados por meio da computação em nuvem, de forma a reduzir o custo total com os investimentos em infraestrutura de TI e aproveitar os benefícios desse novo paradigma de computação (JONES et al., 2019). Além disso, a alta demanda de infraestrutura das empresas e das pessoas, principalmente com o agravamento da pandemia de 2019, causada pela COVID-19, que forçou e aumentou a demanda de tecnologia de serviços e micros serviços. Assim, é de suma importância analisar como é a segurança nestes serviços oferecidos na computação em nuvem.

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: **Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na Google e suas aplicações?**

O objetivo geral deste trabalho é identificar e descrever os serviços de segurança oferecidos pela *Google Cloud*, apresentando como são aplicadas na computação em nuvem.

Os objetivos específicos são:

- Mapear os serviços de segurança da ferramenta *Google Cloud*;
- Identificar as principais práticas de segurança aplicada em cada um destes serviço de segurança;

Esse trabalho faz parte de uma série de pesquisas envolvendo as plataformas que oferecem serviços de nuvem, e este trabalho tratará especificamente da plataforma *Google Cloud*.

Espera-se que os resultados deste trabalho possam contribuir:

- Informando a comunidade a identificar os principais riscos de segurança ao se utilizar estas tecnologias de computação em nuvem;
- Apresentando as principais tecnologias de computação em nuvem utilizadas;
- Mostrando a importância de se ter uma política de segurança;
- Apresentando as soluções e as normas de segurança oferecidas nas empresas que fornecem computação em nuvem.

Quantos aos aspectos metodológicos, a natureza desta pesquisa é um resumo de assunto. Quanto aos seus objetivos é uma pesquisa exploratória. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica, documental e experimental.

Esta monografia está estruturada da seguinte maneira: neste Capítulo é apresentado o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. O Capítulo 2 apresenta duas partes: uma de conceitos e definições da *Google Cloud Platform* (GCP) e outra dos serviços de segurança oferecidas pela GCP. No Capítulo 3 é descrito o método, mostrando como o trabalho foi desenvolvido e o que foi feito para atingir o objetivo geral. No Capítulo 4 estão descritos os serviços da Google relacionados com a segurança de dados. O capitulo 5 traz os experimentos para

comprovar a eficácia de alguns dos serviços descritos. O Capítulo 6 é apresentado a análise dos resultados obtidos. E por fim, o Capítulo 7 traz as considerações finais do TCC e sugestões para trabalhos futuros.

2. REFERENCIAL TEÓRICO

Neste capítulo é composto por duas partes: uma de conceitos e definições da *Google Cloud Platform* (GCP) e outra dos serviços de segurança oferecidas pela GCP.

2.1. GOOGLE CLOUD PLATFORM

Até meados da década de 1970, os computadores existentes eram apenas de grande porte (*Mainframes*) mantidos em ambientes controlados e acessados à distância. Ao final dos anos 70 e início dos anos 80 surgiram os microcomputadores, cuja adoção foi impulsionada pelo advento das redes ethernet e da transição da internet para uso civil. Ao final da década de 80, estavam colocados os elementos para o desenvolvimento de sistemas cliente/servidor. Diferentemente de um terminal com poder de processamento nulo ou exíguo da década de 70, o cliente em questão pode ser definido como um computador ou uma aplicação que executa certa quantidade de processamento de forma autônoma. Além disso, ele tem a capacidade de enviar requisições para um ou mais servidores para execução de processamentos ou solicitação de dados (RICCI, CARLINI, 2012).

A evolução da arquitetura cliente/servidor, no início dos anos 2000, foi marcada pela adoção de arcabouços para programação com objetivos distribuídos, uso de *Web Services* e a consolidação e o surgimento de arquiteturas como clusters e grades computacionais. Em especial, as grades destacam-se por formarem organizações virtuais que usam o poder de instituições ao redor do mundo para a colaboração entre pesquisadores e cálculo de aplicações científicas (DA ROSA et al., 2010).

A origem da ideia relacionada a computação em nuvem se deu por volta de meados de 1950. A ideia era "compartilhar o tempo" de um único computador central que permitia que vários usuários se comunicassem com este computador central de mainframe, onde todo o processamento era feito. Por volta da década de 1970, os dados e programas utilizavam-se principalmente de recursos locais e foi nesta época que se lançou a virtualização (ZAHARIA; RADU, 2017).

Além disso, na década de 60, a computação em *cluster* foi desenvolvida e substituiu as plataformas tradicionais baseadas em supercomputadores. *Clusters* são um

grupo de servidores paralelos ou distribuídos, que geralmente são interconectados por meio de uma *Local Area Network* (LAN), para formar um único computador virtual, permitindo uma computação de alto desempenho, alta disponibilidade e balanceamento de carga, e a computação em nuvem obteve vários benefícios desse tipo de computação em cluster (YEO et al. 2006).

Em 1991 a computação em nuvem teve um desenvolvimento significativo, já que foi nesse ano que a tecnologia *World Wide Web* (WWW) tornou-se disponível. Além disso, em 1997, o termo *Cloud Computing* ou Computação em nuvem foi finalmente definido, pelo Prof. Ramnath Chellappa, como um "paradigma onde os limites da computação serão determinados pela lógica econômica e não apenas pelos limites técnicos [...]"(CHELLAPPA, 1997).

A virtualização é uma tecnologia através da qual pode-se criar réplicas lógicas de recursos físicos acessíveis. Essas instâncias lógicas, máquina virtual ou em inglês *virtual machine* (VM), são isoladas, tem seus arquivos segregados e encapsulados que são correlacionados, mas independentes e podem se comportar como uma máquina completa (MUKHOPADHYAY et al., 2021).

As tecnologias de virtualização são consideradas um dos principais componentes da computação em nuvem, principalmente quanto aos serviços de infraestrutura. Esta tecnologia permite personalizar e criar um ambiente seguro e isolado quando criado para execução de processos de aplicativos, sem causar efeito em outros processos de usuários (PATEL, 2020).

Além disso, segundo Mukhopadhyay et al. (2021), as tecnologias de virtualização fornecem ambientes virtuais não apenas para execução de processos, mas também para memória, criação de redes e armazenamento.

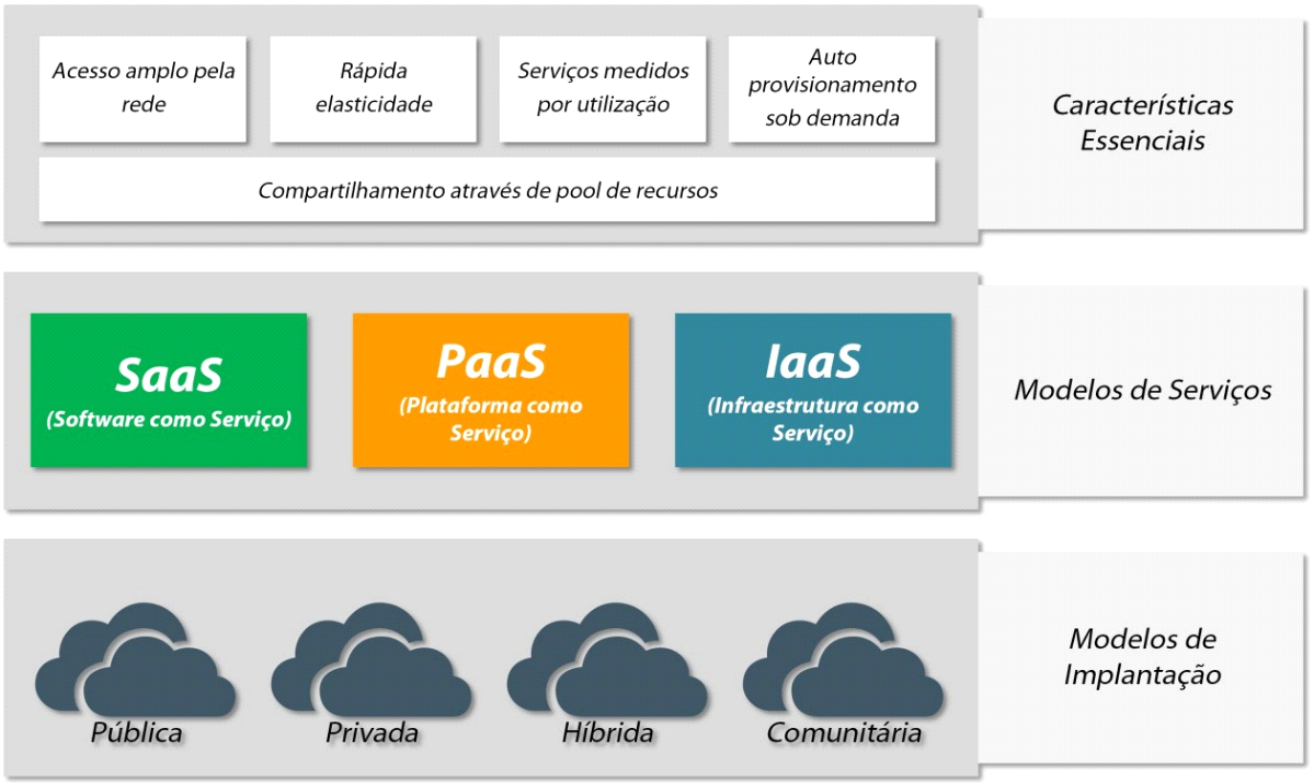
Os processos dos clientes são executados em um ambiente virtualizado que por outro lado utiliza recursos físicos. Múltiplos processos virtuais de vários usuários são alocados para uma mesma máquina física que são segregadas logicamente. Isso dá origem a um ambiente multilocatário na nuvem. Apesar das vantagens oferecidas, a computação em nuvem não é exclusiva de riscos, sendo a segurança o principal risco (LATIF et al. 2014).

A GCP foi disponibilizada ao público dia 7 de abril de 2008. Em 2012 ela lançou seu primeiro serviço de armazenamento chamado *Google Drive*. Esta seção baseia-se na referência documental da *Google* (2021).

Segundo o Gartner (2018), o mercado é dominado por cinco fornecedores que respondem por quase 80% do *market share* mundial da IaaS na nuvem em 2018. Esses fornecedores são *Amazon Web Service* (47,8%), *Microsoft Azure* (15,5%), Alibaba (7,7%), *Google Cloud* (4,0%) e IBM *Cloud* (1,8%).

No ano de 2022 o conceito de nuvem abrange cinco características essenciais, três modelos de serviço e quatro modelos de implantação, ilustrados na Figura 1.

Figura 1 – Forma visual dos conceitos de nuvem



Fonte: Adaptado da NIST, 2022.

O *National Institute of Standards and Technology* (NIST) descreve as cinco características essenciais de computação em nuvem da seguinte forma (MELL; GRANCE, 2011):

- Acesso amplo pela rede: os recursos da nuvem estão disponíveis para acesso pela rede por diferentes dispositivos através de mecanismos padrões;

- Rápida elasticidade: os recursos computacionais podem ser elasticamente provisionados e liberados e, em alguns casos, de maneira automática, adaptando-se à demanda;
- Serviços medidos por utilização: os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado, como armazenamento, processamento, largura de banda e contas de usuários ativas;
- Auto provisionamento sob demanda: o consumidor pode ter a iniciativa de provisionar recursos na nuvem e ajustá-los de acordo com as suas necessidades ao decorrer de serviços;
- Compartilhamento através de *pool* de recursos: os recursos computacionais do provedor são agrupados para servir a multiplos consumidores com recursos fisicos e virtuais, sendo alocados e realocados dinamicamente de acordo com a demanda dos seus consumidores.

Quanto aos três principais modelos de serviços de nuvem, eles são baseados numa arquitetura em camadas hierárquicas, na qual os serviços da camada superior são provisionados pela cama inferior subsequente (MELL; GRANCE, 2011):

- Infraestrutura como um serviço ou em inglês *Infrastructure-as-a-Service* (IaaS): é a capacidade oferecida ao consumidor de fornecer processamento, armazenamento, redes e outros recursos fundamentais de computação, nos quais se pode implementar e executar softwares arbitrários, podendo incluir sistemas operacionais e aplicativos. Exemplo de produto: *Google* Compute Engine.
- Plataforma como um serviço ou em inglês *Platform-as-a-Service* (PaaS): é a capacidade oferecida ao consumidor de implementar os aplicativos criados ou adquiridos na infraestrutura em nuvem. Exemplo: *Google* App Engine.
- Software como um serviço ou em inglês *Software-as-a-Service* (SaaS): é a possibilidade de usar os aplicativos do provedor em execução em uma infraestrutura de nuvem. Os aplicativos podem ser acessados de vários

tipos de dispositivos. Exemplos de empresas que usam o SaaS: NetFlix, Gmail.

Os modelos de implantação podem ser descritos da seguinte forma (MELL; GRANCE, 2011):

- Nuvem Privada: é quando a infraestrutura de nuvem está disponível para uso exclusivo de uma única organização;
- Nuvem Comunitária: é quando a infraestrutura de nuvem está disponível para uso exclusivo de uma comunidade específica;
- Nuvem Publica: a infraestrutura de nuvem pública está disponível para uso aberto do público em geral e fica nas instalações do provedor;
- Nuvem Hibrida: a infraestrutura é composta de duas ou mais infraestruturas de nuvem, podendo elas serem privada, comunitária ou pública.

A norma ISO 27017 define diretrizes para os controles de segurança da informação (SI), essa norma fornece controles e orientações de implementação para provedores de serviços de nuvem e para os clientes dessas empresas (GOOGLE, 2022).

As diretrizes, de acordo com a *Google* (2022), referentes à nuvem que a ISO 27017 proporciona são para 37 controles descritos na norma ISO 27002, além de sete novos controles relacionados aos serviços de nuvem que abordam:

- quem é responsável por qual ação entre o provedor de serviços de nuvem e o cliente;
- a remoção/devolução de recursos quando um contrato é rescindido;
- a proteção e separação do ambiente virtual do cliente;
- configuração da máquina virtual;
- os procedimentos e as operações administrativas associadas ao ambiente de nuvem;
- o monitoramento das atividades do cliente realizadas na nuvem;
- alinhamento do ambiente de rede de nuvem e virtual.

4. MÉTODO

Esta pesquisa segundo sua natureza é um resumo de assunto. Resumos de assunto buscam apenas sistematizar uma área de conhecimento, é necessário que o autor tenha conhecimento sólido da área e de seu desenvolvimento, bem como dos problemas em aberto (WAZLAWICK, 2014).

Segundo seus objetivos é uma pesquisa exploratória, ela pode ser considerada como o primeiro estágio de um processo de pesquisa mais longo. Neste tipo de pesquisa o autor busca examinar anomalias que não sejam ainda conhecidas e que possam ser a base para uma pesquisa mais elaborada (WAZLAWICK, 2014).

Quanto aos procedimentos técnicos, esta pesquisa é bibliográfica, documental e experimental. Pesquisa bibliográfica implica no estudo de artigos, teses, livros e outras publicações que podem ser citados no projeto (WAZLAWICK, 2014).

A pesquisa bibliográfica, será elaborada a partir de materiais já publicados, podendo incluir livros, teses, materiais disponibilizados na Internet, revistas, entre outros. A principal vantagem é permitir uma sucessão de fenômenos maior do que seria capaz de pesquisar diretamente (GIL, 2017).

De acordo com Gil (2017) a pesquisa bibliográfica deve seguir os seguintes passos:

a) Escolha do tema de pesquisa, que deve estar relacionado com o interesse do aluno, o tema escolhido foi: **Os principais serviços de segurança do *Google Cloud***;

b) Fazer o levantamento bibliográfico preliminar de periódicos e artigos relacionados ao assunto de pesquisa, no caso a computação em nuvem e seus serviços de segurança foram feitas na base de dados da CAPES, repositório da PUCGO, *Web of Science;*

c) Fazer a formulação do problema com base no levantamento bibliográfico, que será: **Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na *Google* e suas aplicações?**

d) Identificar as fontes capazes de fornecer as respostas adequadas ao problema proposto;

e) Se tido como suficiente, ler o material selecionado para responder o problema, periódicos, artigos, jornais e etc, de preferência materiais publicados a pelo menos cinco anos atrás;

f) Realizado o fichamento de todo o material lido, para facilitar e relembrar principalmente da referência bibliográfica;

g) Realizada redação do TCC de acordo com as normas da ABNT.

A pesquisa documental consiste na análise de documentos ou dados, sendo eles relatórios de empresas, banco de dados, correspondências etc. (WAZLAWICK, 2014). Segundo Gil (2017), uma pesquisa é considerada documental quando o material consultado é interno à organização.

De acordo com Gil (2017) a pesquisa documental, por apresentar muitos pontos de semelhança com a pesquisa bibliográfica, ela seguirá as mesmas etapas, diferenciando-se apenas por alguns documentos que serão tidos como fontes no desenvolvimento. O passo a passo foi idêntico ao da pesquisa bibliográfica.

A pesquisa experimental é caracterizada por ter uma ou mais variáveis experimentais que podem ser coordenadas pelo pesquisador (WAZLAWICK, 2014).

A pesquisa experimental consiste em estabelecer um objeto de estudo, escolher as variáveis que a influenciam e determinar as formas de controle e observar os efeitos que a variável gera no objeto. Realiza pelo menos um dos elementos que julga ser responsável pela circunstância que está sendo pesquisado (GIL, 2017).

A pesquisa experimental é composta das seguintes etapas, conforme Gil (2017):

a) Fazer a formulação do problema, que será: **Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na *Google* e suas aplicações?**

b) Definição do plano experimental: foi descrito como se configurar certos serviços de segurança da *Google Cloud*. Foi utilizado um site fictício, com intuito de explorar a vulnerabilidade de um ataque por injeção de código do tipo *Structured Query Language* (SQL);

c) Determinação do ambiente: foi realizado experimentos demonstrando um ataque de SQL Injection, para mostrar como se configurar e mitigar regras e políticas de segurança pelo *Cloud Armor*, além da utilização de uma VM confidencial. Para se configurar a VM confidencial, foi utilizado uma VM de segunda geração, da série N2D,

que inclui a tecnologia de CPU AMD EPYC. Ela é responsável pela virtualização criptografada segura (SEV), com 2vCPU, 8 GB de memória RAM, um espaço em disco de 10 GB e rodando um SO Ubuntu 20.04 LTS. Já para a publicação do site, usou-se uma máquina virtual de segunda geração, da série E2, o tipo da máquina selecionado foi um e2-micro com 2vCPU, 1 GB de memória RAM, um espaço em disco de 10 GB e rodando um SO Debian GNU/Linux11. A VM foi criada com uma imagem de um contêiner disponibilizado pelo OWASP para fazer testes de segurança, a imagem do contêiner usado foi o *OWASP Juice Shop*;

d) Análise e interpretação dos dados: foram monitorados e analisados os resultados obtidos de acordo com as configurações de regras, políticas de segurança e testes realizados na coleta de dados;

e) Realizada redação do TCC de acordo com as normas da ABNT.

5. SERVIÇOS E SEGURANÇA DA PLATAFORMA *GOOGLE CLOUD*

Este capítulo descreve os 30 serviços de segurança da GCP. Todo o material deste capítulo foi retirado da documentação oficial da *Google Cloud* (Google, 2022).

Os serviços de segurança da GCP estão divididos entre 30 serviços, a seguir:

- Transparência no acesso
- *Assured Workloads*
- Autorização binaria
- *Chronicle*
- Inventario de recursos do Cloud
- *Cloud Data Loss Prevention*
- *Cloud IDS*
- *Cloud Key Management*
- Computação confidencial
- *Firewalls*
- Gerenciador de secrets
- *Security Command Center*
- VMs protegidas
- *VPC Service Controls*
- *BeyondCorp Enterprise*
- *Certificate Authority Services*
- *Cloud Identidy*
- *Identity and Access Managment*
- *Identity-Aware Proxy*
- *Identity Platform*
- Serviço gerenciado para *Microsoft Active Directory*
- *Policy Intelligence*
- *Resource Manager*
- Chave de segurança Titan
- *ReCAPTCHA Enterprise*

- *Web Risk*
- *Software* de código aberto garantido
- *Software Delivery Shield*
- *Cloud Armor*
- Serviços de segurança da *Mandiant*

5.1. Serviço de Transparência no acesso

A transparência de acesso é um serviço que ajuda a expandir a visibilidade e o controle sobre o provedor de nuvem com registros de acesso de administrador e controles de aprovação.

Os registros de transparência no acesso registram as ações que a equipe do *Google* realiza ao acessar o conteúdo do cliente, elas incluem detalhes como a ação e os recursos afetados, a hora da ação, o motivo e as informações da pessoa que a acessou. Os dados dos clientes só são acessados pela equipe do *Google* exclusivamente para cumprir obrigações contratuais. Deve-se usar a transparência no acesso pelos seguintes motivos:

- Verificar se a equipe do *Google* está acessando o conteúdo somente por motivos comerciais válidos, como para corrigir uma interrupção ou atender às solicitações de suporte;
- Verificar se a equipe do *Google* não cometeu um erro ao seguir as instruções;
- Verificar e rastrear a conformidade com obrigações legais ou regulamentares;
- Coletar e analisar eventos de acesso rastreados por meio de uma ferramenta automatizada de informações de segurança e gerenciamento de eventos, ou no inglês, *Security Information and Event Management* (SIEM).

Um dos principais benefícios que esse serviço oferece é que há a possibilidade de auditar o acesso do provedor de nuvem, já que tudo fica guardado nesses registros, ter o controle para aprovar ou recusar as solicitações de acesso feitas pelos funcionários do *Google*.

Os principais recursos dentro da transparência no acesso são:

- *Access Approval,* também conhecido como Aprovação de acesso;
- Justificações de acesso: motivo de cada acesso;
- Identificação de recursos e métodos: identifica os recursos exatos que foram acessados por administradores e os métodos executados;
- Integração do *Cloud Logging*;
- Local de quem fez o acesso: mostra o país de onde o administrador realizou a ação;
- Controle de proteção de dados: controles de proteção de dados do *Google* que limita a capacidade das equipes de suporte de acessar os dados;
- Publicação quase em tempo real: acesse registro quase em tempo real.

A aprovação de acesso é um recurso que garante que o administrador aprove explicitamente o acesso aos dados ou configurações no *Google Cloud*. A ação de aprovação é verificada criptograficamente para garantir a integridade da Aprovação de acesso. A Aprovação de acesso ajuda na implementação do princípio de segurança de menor privilégio, que declara que ninguém precisa ter mais permissões e acesso do que o necessário.

O funcionamento da Aprovação de acesso se dá com o envio de um e-mail ou mensagem do Pub/Sub com uma solicitação de acesso, que pode ser aprovado ou recusada através do console do *Google Cloud* ou a *API* da Aprovação de acesso. Este recurso solicita seu consentimento apenas para solicitações de acesso ao conteúdo armazenado nos serviços selecionados pelo administrador.

Uma solicitação de aprovação de acesso deve conter os seguintes campos:

- Recurso: deve conter o local do recurso o qual o funcionário do *Google* está solicitando acesso;
- Tempo de solicitação: a hora que a aprovação de acesso enviou a solicitação de acesso;
- Acesso expira em: hora em que o acesso solicitado expira;
- Local do escritório: o local é um código do país, um identificador de continente ou *ANY,* ambos em inglês, para indicar que qualquer local é permitido;

- Localização física: o local é um código do país, um identificador de continente ou *ANY,* ambos em inglês, para indicar que qualquer local é permitido;
- Motivo: a razão do acesso.

A Figura 2 ilustra um exemplo de solicitação de Aprovação de acesso:

Figura 2 – Código de solicitação de aprovação de acesso


```
{
  "name": "projects/123456/approvalRequests/xyzabc123",
  "requestedResourceName": "projects/123456",
  "requestedReason": {
    "detail":  "Case number: bar123"
    "type":  "CUSTOMER_INITIATED_SUPPORT"
  },
  "requestedLocations": {
    "principalOfficeCountry": "US",
    "principalPhysicalLocationCountry": "US"
  },
  "requestTime": "2018-08-28T19:07:12.286Z",
  "requestedExpiration": "2018-09-02T19:07:11.877Z"
}
```


Fonte: *Google Cloud*, 2022.

A Aprovação de acesso usa uma chave criptográfica para assinar a solicitação de acesso, usada para verificar a integridade da aprovação do acesso. Você pode usar uma chave de assinatura através do *Cloud KMS* ou com o *Cloud EKM*.

5.2. *Assured Workloads*

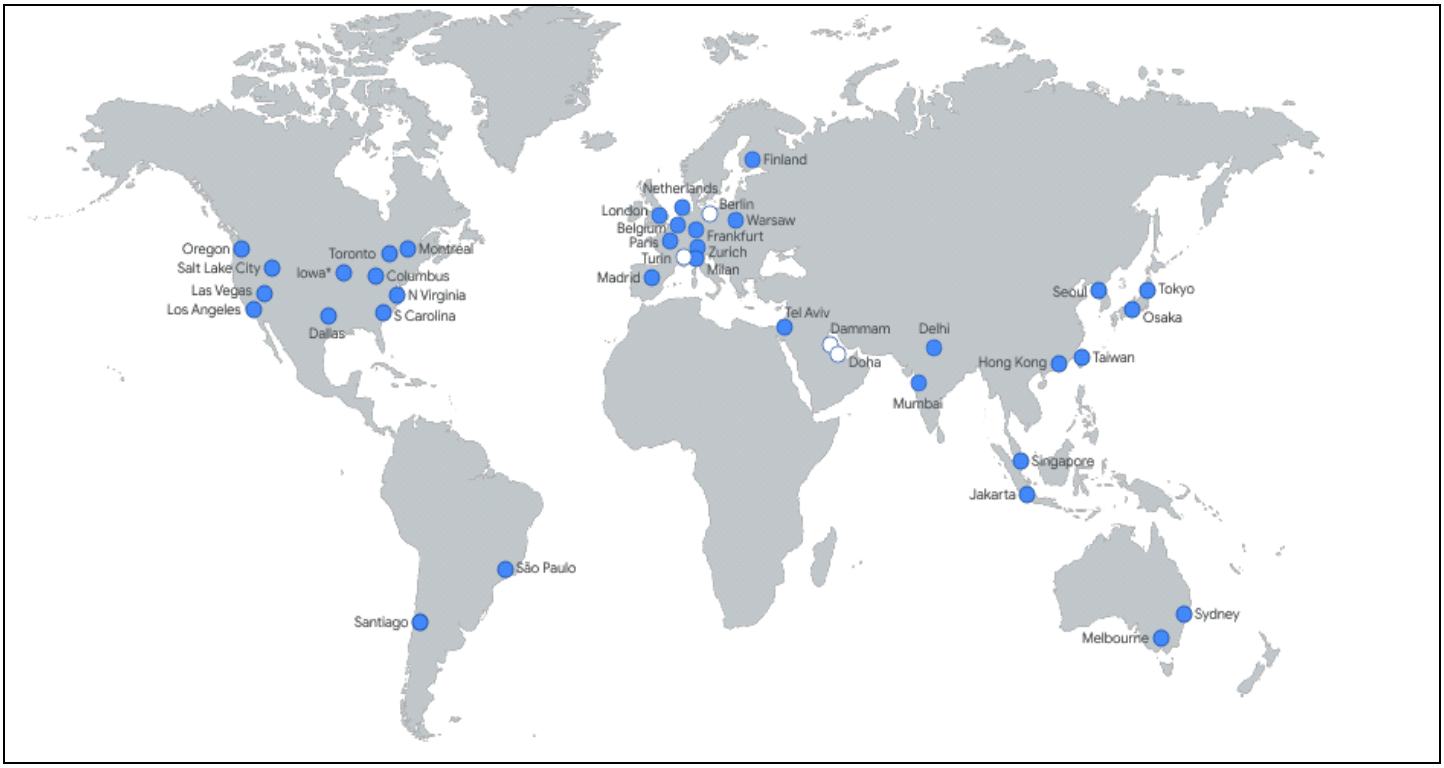
O *Assured Workloads* é uma ferramenta da *Google Cloud* que tem a capacidade de aplicar controles de segurança a um ambiente, em suporte aos requisitos de conformidade.

Este serviço é usado quando pretende-se atender aos seguintes requisitos de controle de segurança:

- Residência dos dados: garante que os dados do cliente sejam armazenados em uma região do GC selecionado pelo cliente. Esses dados só podem ser armazenados em uma única região ou várias regiões, de acordo com a região disponível na *Google* e selecionada pelo desenvolvedor. E caso o desenvolvedor de um cliente tentar armazenar dados em uma região fora da seleção, então a ação será bloqueada.

A Figura 3 mostra as 35 regiões em que a GC está presente e disponíveis em mais de 200 países e territórios.

Figura 3 – Regiões de atuação da *Google Cloud*



Fonte: *Google Cloud*, 2022.

- Controle de acesso a dados pessoal com base em atributos:
- Controle de propriedade do caso de suporte de pessoal com base nos atributos:
- Criptografia: as chaves de criptografia gerenciadas pelo *Google*, fornecidas por padrão, são compatíveis com o FIPS-140-2.

5.3. Autorização binária

A autorização binária é um controle de segurança de tempo de implantação que garante que apenas imagens de contêineres confiáveis sejam implantadas no *Google Kubernetes Engine* (GKE) ou no *Cloud Run*. Com a autorização binária, é possível solicitar que as imagens sejam assinadas por autoridades confiáveis durante o processo de desenvolvimento e, então, aplicar a validação da assinatura na implantação. Ao fazer isso, você consegue maior controle sobre o ambiente de contêiner, garantindo que apenas imagens verificadas sejam integradas ao processo de criação e lançamento.

5.4. *Chronicle*

O *Chronicle* é um pacote de operações de segurança, reúne toda a estrutura de escala da *Google* para aumentar a velocidade de detecção de ameaças, investigação e respostas as ameaças.

Esse serviço usa da escalabilidade da infraestrutura da *Google* para armazenar e analisar toda a telemetria de segurança, com pacotes de respostas para casos comuns de segurança.

O *Chronicle* possui dois principais recursos, o *Chronicle SIEM e o Chronicle SOAR.* O *Chronicle SIEM* utiliza das telemetrias de segurança, do contratante, para detectar possíveis pontos cegos na segurança, essa ferramenta está continuamente atualizada com novas regras e indicadores de ameaças feitas por pesquisadores do *Google*. Esta ferramenta de detecção inclui regras predefinidas mapeadas para ameaças específicas, atividades suspeitas e *frameworks* de segurança. Já o *Chronicle SOAR* é uma ferramenta de automação e resposta a ameaças. Ela usa uma combinação de automação de protocolos de segurança, gerenciamento de casos e inteligência integrada, fazendo com que a equipe de segurança consiga conter a ameaça em minutos.

O pacote de operações de segurança consegue reunir e apresentar informações sobre uma entidade de múltiplas fontes de dados relevantes, tais como VirusTotal e o *Google Cloud Threat Intelligence,* para ajudar na rápida tomada de decisão da equipe de segurança.

5.5. Inventário de recursos do *Cloud*

É um serviço de inventário, com base em um banco de dados, de metadados que permite visualizar, monitorar e analisar todos os recursos do GC e do *Anthos*. Com o inventário de recursos do *Cloud*, é possível:

- Pesquisar metadados do recurso usando uma linguagem de consulta personalizada;
- Exportar todos os metadados de recursos em um determinado carimbo de data/hora ou exportar o histórico de alterações de eventos durante um período especifico para um arquivo do *Cloud Storage* ou uma tabela do *BigQuery*;
- Monitorar alterações de recursos através de notificações em tempo real;
- Analisar a política de IAM para descobrir quem tem acesso a quê.

4.6. *Cloud Data Loss Prevention*

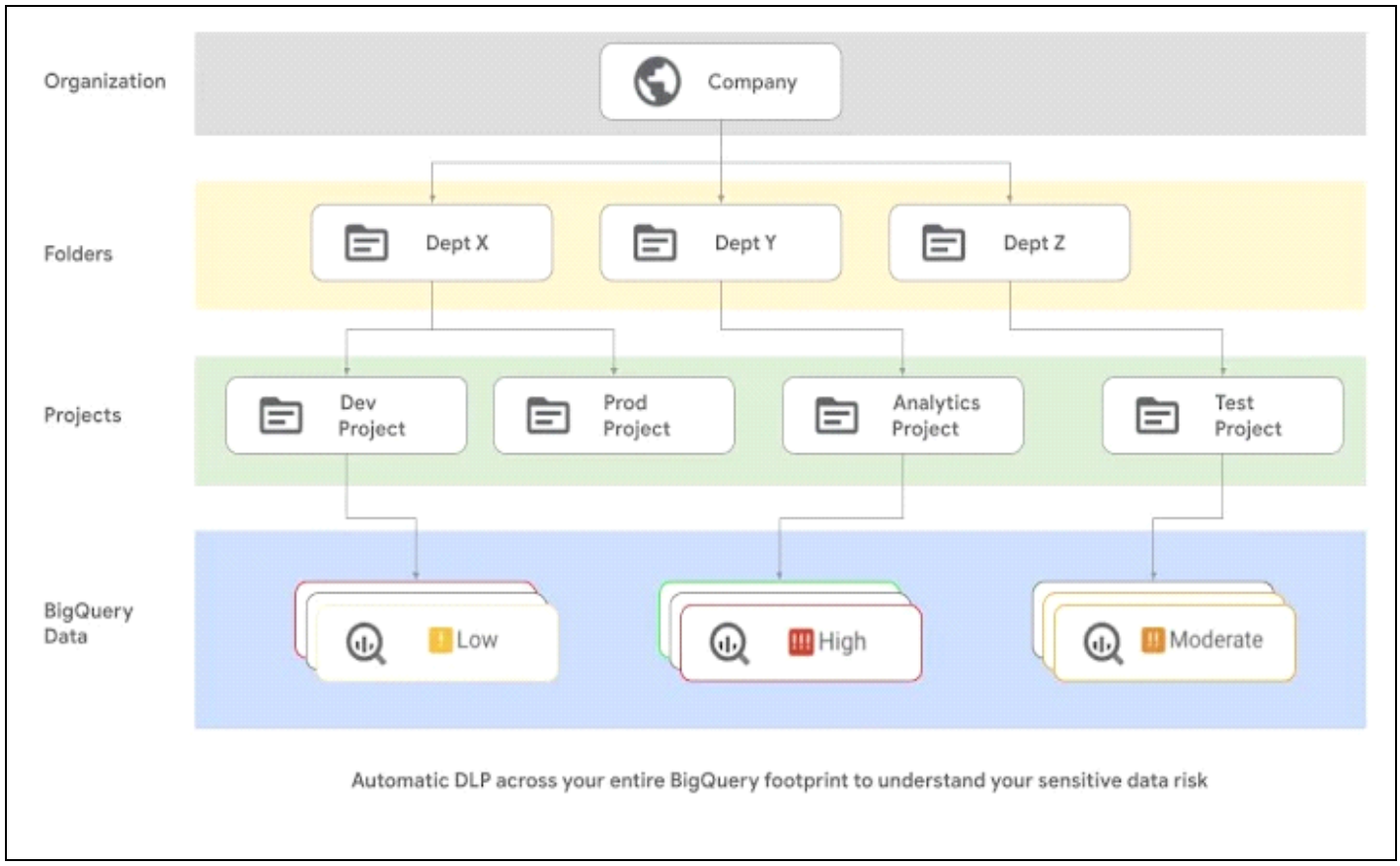
O *Cloud Data Loss Prevention* (*Cloud DLP*) é um serviço que possibilita o gerenciamento para ajudar a descobrir, classificar e proteger os dados mais confidenciais. Esse serviço oferece o controle de seus dados na nuvem ou fora dela, mostra maior visibilidade sobre os riscos de dados confidenciais em toda a organização. Um dos principais recursos oferecidos pelo *Cloud DLP* são:

- Descoberta automatizada de dados confidenciais: o DLP consegue identificar dados confidenciais através de analises das tabelas e colunas do *BigQuery* em toda a organização, podendo ser selecionado pastas ou projetos individuais da organização;
- Possibilidade de usar o *Cloud DLP* de praticamente qualquer lugar: o *Cloud DLP* tem suporte nativo para verificar e classificar dados confidenciais no *Cloud Storage*, no *BigQuery* e no *Datastore*, e por ser um *API* de conteúdo de streaming ela permite compatibilidade com outras fontes de dados, cargas de trabalho e aplicativos;
- Mascare automaticamente seus dados: o *Cloud DLP* fornece ferramentas para classificar, mascarar, tokenizar e transformar elementos confidenciais.

Fornece suporte para dados estruturados e não estruturados, ajuda a preservar a utilidade dos dados para mesclagem, análise e Inteligência Artificial (IA).

A Figura 4 mostra como a descoberta automática funciona, ao classificar o grau de risco quanto a dados confidenciais em projetos de uma organização.

Figura 4 – Descoberta automática de dados confidenciais



Fonte: *Google Cloud*, 2022.

4.7. *Cloud IDS*

O *Cloud IDS,* ou Sistema de detecção de intrusões do *Cloud*, é um serviço que oferece detecção de ameaças de rede nativa da nuvem, como *malware, spyware*, ataque de comando e controle na rede. O serviço funciona criando uma rede com *peering* gerenciada pelo *Google* com VMs espalhadas. O tráfego na rede com *peering* é espelhado pelas tecnologias de proteção contra ameaças da *Palo Alto Networks*. É possível espelhar todo o tráfego ou espelhar somente o tráfego filtrado com base no protocolo, no intervalo de endereços IP ou na entrada e na saída.

O *Cloud IDS* detecta e alerta sobre ameaças, mas não toma medidas para evitar ataques ou reparos.

O *Endpoint IDS* é um recurso zonal que pode inspecionar o tráfego de qualquer zona na região e cada *endpoint* do IDS recebe tráfego espelhado e executa análise de detecção de ameaças. O funcionamento desse recurso se dá através de uma conexão particular que conecta as VMs de uma organização às VMs com *peering* do *Google*, que cria uma cópia do tráfego de rede que é enviado a um único *endpoint* de IDS para inspeção.

O Cloud IDS oferece um conjunto de assinaturas de ameaças, que podem ser personalizadas de acordo com o nível de gravidade do alerta. As assinaturas são usadas para detectar vulnerabilidades e *spywares*.

As assinaturas de detecção de vulnerabilidades detectam tentativas de exploração de falhas do sistema ou de acesso não autorizado aos sistemas. As assinaturas *antispyware* ajudam a identificar os hosts infectados quando o tráfego sai da rede. Já as assinaturas de detecção de vulnerabilidade protegem contra ameaças que entram na rede. Por exemplo, as assinaturas de detecção de vulnerabilidades ajudam a proteger contra estouro de buffer, execução de código ilegal e outras tentativas de explorar vulnerabilidades do sistema. As assinaturas de detecção de vulnerabilidades padrão oferecem detecção para clientes e servidores de todas as ameaças críticas, de alta e média gravidade conhecidas.

As assinaturas *anti-spyware* são usadas para detectar *spywares* em hosts comprometidos. Esses spywares podem tentar entrar em contato com servidores externos de comando e controle (C2). Quando o *Cloud IDS* detecta tráfego malicioso que

deixa a rede dos hosts infectados, ele gera um alerta, que é salvo no registro de ameaças e também exibido no console do *Google Cloud*.

A gravidade de uma assinatura indica o risco do evento detectado, e o Cloud IDS gera alertas para o tráfego correspondente. O Quadro 1 apresenta um resumo dos níveis de gravidade das ameaças.

QUADRO 1 – Resumo dos níveis de gravidade das ameaças

Gravidade	Descrição
Crítica	Ameaças graves, como as que afetam a instalação padrão de software amplamente implantado, resultam em comprometimento raiz dos servidores e em que o código de exploração está amplamente disponível para os invasores. O invasor geralmente não precisa de credenciais de autenticação especiais nem de conhecimento sobre as vítimas individuais, e o alvo não precisa ser manipulado para executar funções especiais.
Alto	Ameaças que podem se tornar críticas, mas há fatores de mitigação. Por exemplo, elas podem ser difíceis de explorar, não resultar em privilégios elevados ou não têm um grande número de vítimas.
Média	Pequenas ameaças em que o impacto é minimizado, que não compromete o alvo ou explorações que exigem que um invasor resida na mesma rede local da vítima, afetam apenas configurações não padrão ou ocultam aplicativos ou oferecem acesso muito limitado.
Baixa	Ameaças no nível de alerta com pouco impacto na infraestrutura de uma organização. Eles geralmente precisam de acesso local ou físico ao sistema e podem resultar em problemas de privacidade da vítima e vazamento de informações.
Informativa	Eventos suspeitos que não representam uma ameaça imediata, mas que são chamados para chamar a atenção para problemas mais profundos que podem existir.

Fonte: *Google Cloud*, 2022.

4.8. *Cloud Key Management*

O *Cloud KMS é* um serviço de gerenciamento de chaves criptografadas (KMS) fornecido pela GC. Oferece o gerenciamento de chaves armazenadas na nuvem de criptografia simétricas e assimétricas, com ela é possível gerar, usar e destruir chaves criptográficas AES 256, RSA 2048, RSA 3072, RSA 4096, EC P256 e EC P384. Outros recursos oferecidos são:

- Segurança de chave de hardware com o módulo de segurança de hardware (HSM, na sigla em inglês): possibilita alternar entre chaves de criptografia protegidas por software e hardware com validação FIPS 140-2 de nível 3;
- Suporte para chaves externas: oferece suporte a sistemas de gerenciamento de chaves terceirizado que é implantado fora da infraestrutura do *Google* através do *External Key Management* (EKM).

4.9. Computação confidencial

A Computação confidencial é um serviço de proteção dos dados em uso com o Ambiente de execução confiável baseado em hardware. Os Ambiente de execução confiável baseado em hardware são ambientes seguros e isolados que impedem o acesso ou a modificação não autorizada de aplicativos e dados enquanto estão em uso.

Este serviço usa criptografia de ponta a ponta, ou seja, há a criptografia em repouso, quando os dados estão sendo armazenados, criptografia em trânsito, quando os dados estão sendo movidos entre dois pontos e a criptografia em uso, quando os dados estão sendo processados.

Um recurso fornecido pela Computação confidencial são as VMs confidenciais, que são um tipo de VM do *Compute Engine* que garante que os dados e aplicativos permaneçam particulares e criptografados mesmo durante o uso.

O serviço de Computação confidencial da *Google* tem parceria com a *AMD*, então suas VMs confidenciais são executadas em *hosts* com processadores *AMD EPYC* que apresentam virtualização criptografada segura (SEV, na sigla em inglês) AMD.

4.10. *Firewalls*

Um *firewall* é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança (CISCO, 2022).

O serviço de *Cloud Firewall* é totalmente distribuído e nativo na malha de rede da GC, ele é oferecido em dois níveis: *Cloud Firewall Essentials* e *Cloud Firewall Standard*.

O *Cloud Firewall Standard* oferece políticas expandidas usando objetos para regras de firewall que simplificam a configuração e a microssegmentação. O *Cloud Firewall Essentials* é o nível básico que inclui políticas de firewall de rede, tags gerenciadas pelo *Identity and Access Management* (IAM).

4.11. Gerenciador de *secrets*

O Gerenciador de *secrets* ou *Secret Manager* é um sistema de armazenamento para chaves de APIs, senhas, certificados e outros dados confidenciais. Ele proporciona um local central e uma fonte única para gerenciar, acessar e fazer auditoria de *secrets* no GC.

Um *secret* é um objeto global de um projeto que contém uma coleção de metadados, que podem incluir locais de replicação, rótulos, anotações e permissões. Seus principais recursos são:

- Políticas de replicação: é possível escolher regiões especificas para armazenar *secrets*;
- Controle de versões: os dados do *secret* não podem ser mudados, é possível fixar um *secret* em versões especificas;
- Integração com o *Cloud* IAM: controle de acesso aos *secrets,* somente os proprietários do projeto têm permissão de acesso;
- Criptografia por padrão: em trânsito, os dados são criptografados com TLS e, em repouso, com as chaves de criptografia AES de 256 bits.

4.12. *Security Command Center*

O *Security Command Center* é o serviço de gerenciamento de segurança e risco do GC, este serviço ajuda a avaliar a superfície de segurança identificando configurações incorretas, vulnerabilidades e ameaças, além de ajudar a mitigar e corrigir riscos. O *Security Command Center* é dividido em dois níveis: *Standard* e *Premium.*

O nível *Standard* oferece recursos como:

- *Security Health Analytics*: verificação de vulnerabilidade e detecção automática de configurações incorretas dos recursos da GC;
- *Web Security Scanner*: verificações personalizadas de aplicativos implantados com URLs e endereços IP públicos que não estão protegidos por firewall;
- Erros do *Security Command Center*: ele fornece orientações de detecção e remediação para erros de configuração que impedem o funcionamento correto do Security Command Center e dos serviços;
- Suporte para conceder aos usuários papéis do IAM no nível da organização.
- Acesso a serviços integrados do GC, incluindo os seguintes:
    - O *Cloud Data Loss Prevention* descobre, classifica e protege dados confidenciais;
    - O *Google Cloud Armor* protege as implantações do GC contra ameaças;
    - A detecção de anomalias identifica anomalias de segurança dos projetos e instâncias de VM, como possíveis credenciais vazadas e mineração de moedas.
- Integração com o *BigQuery*, que exporta descobertas para o *BigQuery* para análise;
- Integração com o *Forseti Security*, o kit de ferramentas de segurança de código aberto para o GC e aplicativos de gerenciamento de eventos e informações de segurança de terceiros.

O nível *Premium* inclui todos os recursos do nível *Standard* e adiciona os seguintes recursos:

- *Event Threat Detection* usa inteligência de ameaças, *machine learning* e outros métodos para monitorar o *Cloud Logging* e o *Google Workspace* da organização e detectar as seguintes ameaças:
    - Malware
    - Criptomineração
    - Ataques de força bruta contra SSH

    - DoS de saída
    - Concessão anômala de IAM
    - Exfiltração de dados
- O *Event Threat Detection* também identifica as seguintes ameaças no *Google Workspace*:
    - Vazamento de senhas
    - Tentativa de violação de contas
    - Mudanças nas configurações da verificação em duas etapas
    - Mudanças nas configurações de *Logon* único (SSO)
    - Ataques apoiados pelo governo
- O *Container Threat Detection* detecta os seguintes ataques ao ambiente de execução do contêiner:
    - Adição de binário executado
    - Adição de biblioteca carregada
    - Script malicioso executado
    - Shell reverso
- A *Virtual Machine Threat Detection* detecta aplicativos de mineração de criptomoedas executados em instâncias de VM.
- No nível Premium, o *Security Health Analytics* inclui monitoramento e geração de relatórios para os seguintes padrões e protocolos de segurança:
    - CIS 1.2
    - CIS 1.1
    - CIS 1.0
    - PCI DSS v3.2.1
    - NIST 800-53
    - ISO 27001
- O *Rapid Vulnerability Detection* verifica as redes e os aplicativos da *Web* para detectar credenciais fracas, instalações de software incompletas e outras vulnerabilidades críticas com alta probabilidade de serem exploradas.

4.13. VMs protegidas

As VMs protegidas são máquinas virtuais no GC que contam com um conjunto de controles de segurança contra *rootkits* e *bootkits*. Elas ajudam a proteger as cargas de trabalho da empresa contra ameaças como ataques remotos, escalonamento de privilégios e pessoas mal-intencionadas com informações privilegiadas. Essas VMs protegidas usam recursos avançados de segurança da plataforma, como Inicialização medida e segura, um módulo de plataforma confiável virtual, ou em inglês *virtual Trusted Platform Module* (vTPM), interface unificada de *firmware* extensível, ou no inglês *Unified Extensible Firmware Interface* (UEFI) e monitoramento de integridade.

A Iniciação segura garante que o sistema execute apenas um software autêntico por meio da verificação da assinatura digital de todos os componentes de inicialização e da interrupção do processo de inicialização se a verificação da assinatura falhar.

A UEFI gerencia com segurança os certificados que contêm as chaves usadas pelos fabricantes de software para assinar o firmware do sistema, o carregador de inicialização do sistema e todos os binários que eles carregam. Em cada inicialização, o *firmware* UEFI verifica a assinatura digital de cada componente de inicialização em relação às chaves aprovadas armazenadas com segurança.

O vTPM é um ícone de computador especializado que pode ser usado para proteger objetos, como chaves e certificados, utilizados para autenticar o acesso ao sistema.

4.14. *VPC Service Controls*

VPC Service Controls é um serviço que permite definir políticas de segurança que impedem o acesso a serviços gerenciados pelo *Google* fora de um perímetro confiável pré-determinado, bloquear o acesso a dados em locais não confiáveis e reduzir riscos de exfiltração de dados. É possível usar o *VPC Service Controls* para as seguintes aplicações:

- isolar recursos do *Google Cloud* e redes em nuvem privada virtual, em inglês *Virtual Private Cloud* (VPC) em perímetros de serviço;
- estender perímetros a redes locais para rede privada virtual, ou em inglês *Virtual Private Network* (VPN) autorizada ou *Cloud Interconnect*;
- controlar o acesso aos recursos do GC pela Internet;
- proteger a troca de dados em perímetros e organizações usando regras de entrada e saída;
- permitir acesso baseado no contexto a recursos com base nos atributos do cliente usando regras de entrada.

4.15. *BeyondCorp Enterprise*

O *BeyondCorp Enterprise* é um serviço do *Google* que possibilita as organizações que, ao reunir as informações de um usuário com o contexto do dispositivo e do local, uma empresa pode tomar decisões avançadas de acesso e aplicar a política de segurança. As principais características deste serviço são:

- A proteção de dados e contra ameaças traz segurança aos dispositivos da sua empresa ao trabalhar para proteger os usuários contra riscos de exfiltração, como copiar e colar, ampliar as proteções da DLP no navegador e ajudar a evitar que um malware entre em dispositivos gerenciados por corporações.
- Controles de acesso que protegem o acesso a sistemas seguros (aplicativos, máquinas virtuais, APIs e assim por diante) usando o contexto da solicitação de um usuário final para garantir que cada solicitação seja tão autenticada, autorizada e segura quanto possível.

Esse serviço se aplica muito bem no caso de uso de vários usuários finais trabalharem fora do escritório, *home office,* e a partir de vários tipos diferentes de dispositivos.

4.16. *Certificate Authority Services*

O *Certificate Authority Service* é um serviço altamente disponível e escalonável do GC. Com ele, você simplifica, automatiza e personaliza as implantações, o gerenciamento e a segurança de autoridades de certificação ou em inglês *Certificate Authority* (CA) privadas.

4.17. *Cloud Identidy*

É uma plataforma unificada de gerenciamento de identidades, acessos, APPs e *endpoints*.

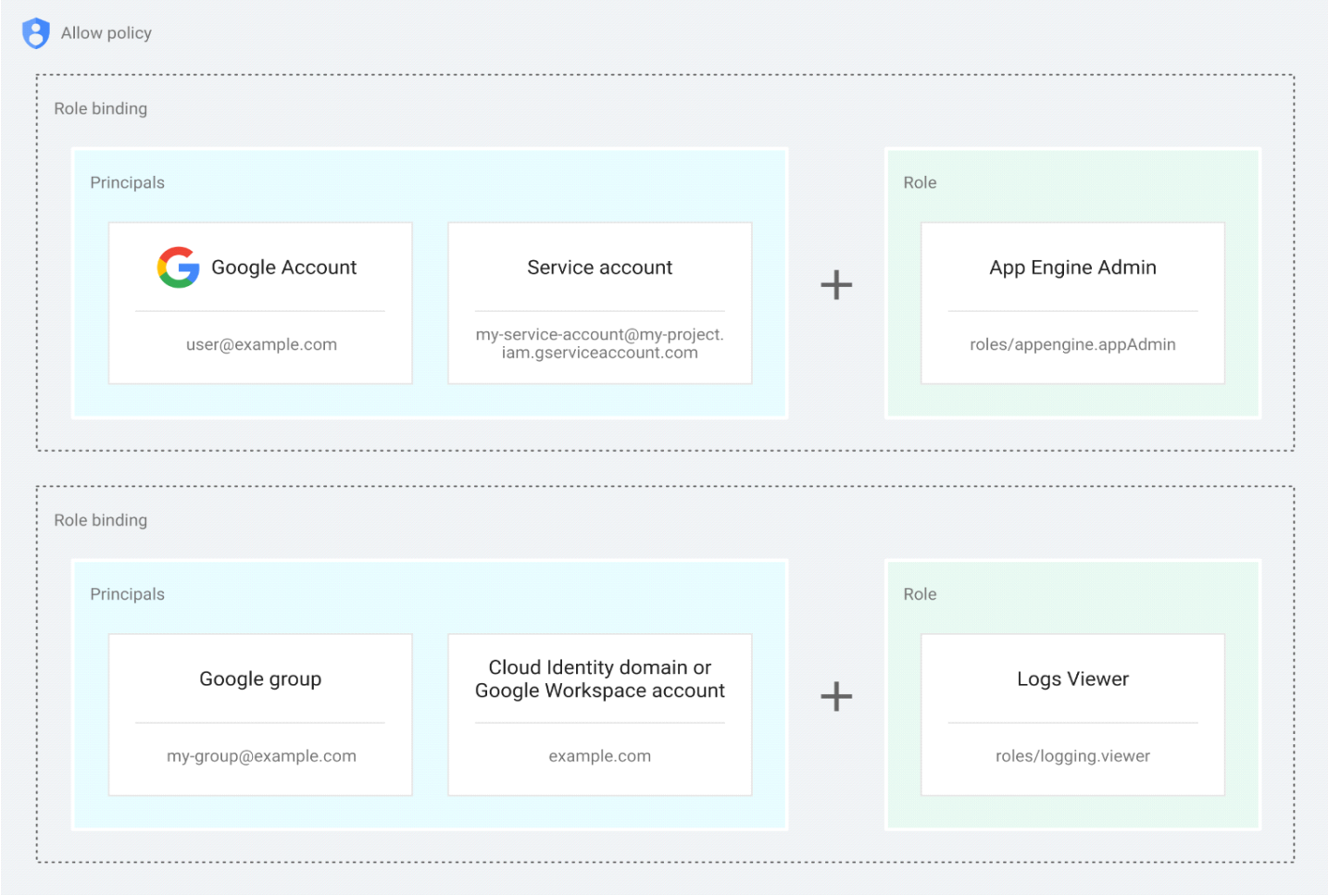
O *Cloud Identidy* possui recursos como a autenticação multifator, segurança de dispositivos com o gerenciamento de *endpoints* compativel com dispositivos Android, IOS e Windows.

4.18. *Identity and Access Managment*

O *Identity and Access Managment* (IAM) é um serviço de controle de acesso e visibilidade para o gerenciamento centralizado de recursos em nuvem, com ele os administradores autorizam quem pode realizar ações em determinados recursos. Dessa forma o administrador tem total controle e visibilidade para gerenciar os recursos do GC de maneira centralizada.

Com o IAM, o administrador gerencia o controle de acesso definindo quem (identidade) tem qual acesso (papel) a que recurso, por exemplo, as instancias de VM, os *clusters* do *Google Kubernetes Engine* (GKE). A Figura 6 ilustra o gerenciamento de permissões no IAM.

Figura 6 – Gerenciamento de permissões no IAM



Fonte: *Google Cloud*, 2022.

Este modelo de gerenciamento de acesso tem três partes principais:

- Principal: Um principal pode ser uma Conta do *Google* (para usuários finais), uma conta de serviço (para aplicativos e cargas de trabalho de computação), um Grupo do *Google* ou uma conta do *Google Workspace* ou um domínio do Cloud Identity, que pode acessar um recurso. Cada principal tem um identificador próprio, que normalmente é um endereço de e-mail.
- Papel: Um papel é um conjunto de permissões. Com as permissões, você determina quais operações são permitidas em um recurso. Ao conceder

um papel a um membro, são concedidas todas as permissões contidas nele.

- Política: A política de permissão é um conjunto de vinculações de papéis que associa um ou mais principais a papéis individuais. Quando o administrador quiser definir quem (principal) tem qual tipo de acesso (papel) em um recurso, crie uma política e anexe ela ao recurso.

4.19. *Identity-Aware Proxy*

O *Identity-Aware Proxy* (IAP) usa identidade e contexto para proteger o acesso a seus aplicativos e VMs. Com o IAP consegue-se estabelecer uma camada de autorização central para aplicativos acessados por protocolo de segurança de transferência de hipertexto, ou em inglês *Hyper Text Transfer Protocol Secure* (HTTPS), possibilitando adotar um modelo de controle de acesso no nível do aplicativo, em vez de confiar apenas nos firewalls da rede.

Quando um aplicativo ou recurso é protegido pelo IAP, ele só pode ser acessado pelo proxy por um usuário definido pelo IAM. Quando um usuário tenta acessar um recurso protegido pelo IAP, o IAP executa verificações de autenticação e autorização.

Este serviço funciona da seguinte forma, na parte da autenticação o código de infraestrutura verifica se o IAP está ativado para o app ou o serviço de back-end, caso esteja, as informações sobre o recurso protegido são enviadas ao servidor de autenticação do IAP. Em seguida, o IAP verifica as credenciais do navegador do usuário, se não houver nenhuma, o usuário será redirecionado para um fluxo de login da Conta do *Google* no *OAuth* 2.0, que armazena um *token* em um cookie do navegador para logins futuros.

Se as credenciais da solicitação forem válidas, o servidor de autenticação usará essas credenciais para conseguir a identidade do usuário (endereço de e-mail e ID do usuário). O servidor de autenticação usa a identidade para verificar o papel do IAM do usuário e verificar se ele está autorizado a acessar o recurso.

Após a autenticação, o IAP aplica a política do IAM pertinente para verificar se o usuário está autorizado a acessar o recurso solicitado. Se o usuário tiver o papel de usuário do app da *Web* protegido pelo IAP, ele terá autorização para acessar o aplicativo.

O IAP protege a autenticação e autorização de todas as solicitações ao *APP Engine*, ao *Cloud Load Balancing* (HTTPS) ou ao balanceamento de carga HTTP interno. O IAP não oferece proteção contra atividades no projeto, como outra VM.

4.20. *Identity Platform*

O *Identity Platform* é uma plataforma de gerenciamento de identidade e acesso do cliente. Com este serviço é possível adicionar autenticação aos aplicativos da Web e em dispositivos moveis. Ele fornece o recurso de autenticação multifator, além de ser compatível com vários métodos de autenticação, como SAML, OIDC, e-mail/senha, mídias sociais, smartphones e autenticação personalizadas.

4.21. Serviço gerenciado para *Microsoft Active Directory*

O Serviço Gerenciado para *Microsoft Active Directory* (M*anaged Microsoft AD*) oferece domínios do *Microsoft Active Directory* para ajudar a reduzir as tarefas administrativas confidenciais, necessárias para gerenciar o *Active Directory*.

O *Managed Microsoft AD* executa controladores de domínio reais do *Microsoft Active Directory* em máquinas virtuais Windows para garantir a compatibilidade de aplicativos.

O serviço cria e mantém os controladores de domínio, reduzindo as tarefas de manutenção necessárias para gerenciar.

4.22. *Policy Intelligence*

O *Policy Intelligence* é um serviço de controle de recursos e gerenciamento de acesso. Devido ao amplo conjunto de políticas do GC que uma organização pode ter,

esse serviço ajuda a entender e gerenciar as políticas para melhorar proativamente as configurações de segurança.

Há várias ferramentas do *Policy Intelligence* que ajudam a entender qual acesso as políticas permitem e como elas são usadas. Uma destas ferramentas é o *Cloud Asset Inventory* que fornece políticas de analisador, que permitem descobrir quais usuários têm acesso a quais recursos do GC com base nas suas políticas de permissão do IAM.

O *Policy Analyzer* ajuda a responder perguntas como as seguintes:

- "Quem tem acesso a esta conta de serviço do IAM?"
- "Quais papéis e permissões o usuário tem neste conjunto de dados do *BigQuery*?"
- "Quais conjuntos de dados do *BigQuery* esse usuário tem permissão para ler?"

4.23. *Resource Manager*

O GC oferece recursos de contêiner, como organizações e projetos, que permitem agrupar e organizar hierarquicamente outros recursos do GC. Com essa organização hierárquica é possível gerenciar aspectos comuns dos recursos, como controle de acesso e ajustes de configuração. Com a API do *Resource Manager*, é possível gerenciar esses recursos de contêiner.

Um dos recursos que o *Resource Manager* oferece é a possibilidade de criar, atualizar e excluir projetos da organização, usar as pastas do *Cloud* para organizar recursos e configurar políticas do IAM para todos os recursos filhos inseridos nessas pastas.

4.24. Chave de segurança *Titan*

O *Titan* é um serviço de autenticação de dois fatores para a proteção de contas de usuários. Seus principais recursos são:

- A autenticação de dois fatores resistente a *phishing:* as chaves de segurança *Titan* oferecem comprovação criptográfica de que os usuários

estão interagindo com o serviço legitimo no qual registraram a chave de segurança e de que ainda estão em posse;

- Hardware resistente a violações: um chip de *hardware* que inclui um *firmware* desenvolvido pelo *Google* que ajuda a verificar se as chaves não foram violadas. Os *chips* de *hardware* foram criados para resistir a ataques físicos que tentam extrair o *firmware* e o material da chave secreta;
- Vários formatos para garantir a compatibilidade com os dispositivos: as chaves de segurança *Titan* estão disponíveis em dois formatos *USB-A/NFC* e *USB-C/NFC*.

4.25. *reCAPTCHA Enterprise*

O *reCAPTCHA Enterprise* tem o propósito de proteger o site contra atividades fraudulentas, *spam* e abuso sem interrupções. Ele foi criado com base na API *reCAPTCHA* atual e usa técnicas de análise de risco para distinguir pessoas e *bots*. Essa ferramenta consegue detectar atividades fraudulentas como, preenchimento de credenciais, invasões de conta e criação automática de contas.

O *reCAPTCHA Enterprise* é útil quando se quer detectar ameaças ou ataques automatizados ao site. Essas ameaças normalmente vêm de *scripts*, emuladores de dispositivos móveis, *software bot* ou humanos. Quando o *reCAPTCHA Enterprise* é implantado no ambiente, ele interage com o *back-end*/servidor do cliente e as páginas da Web do cliente.

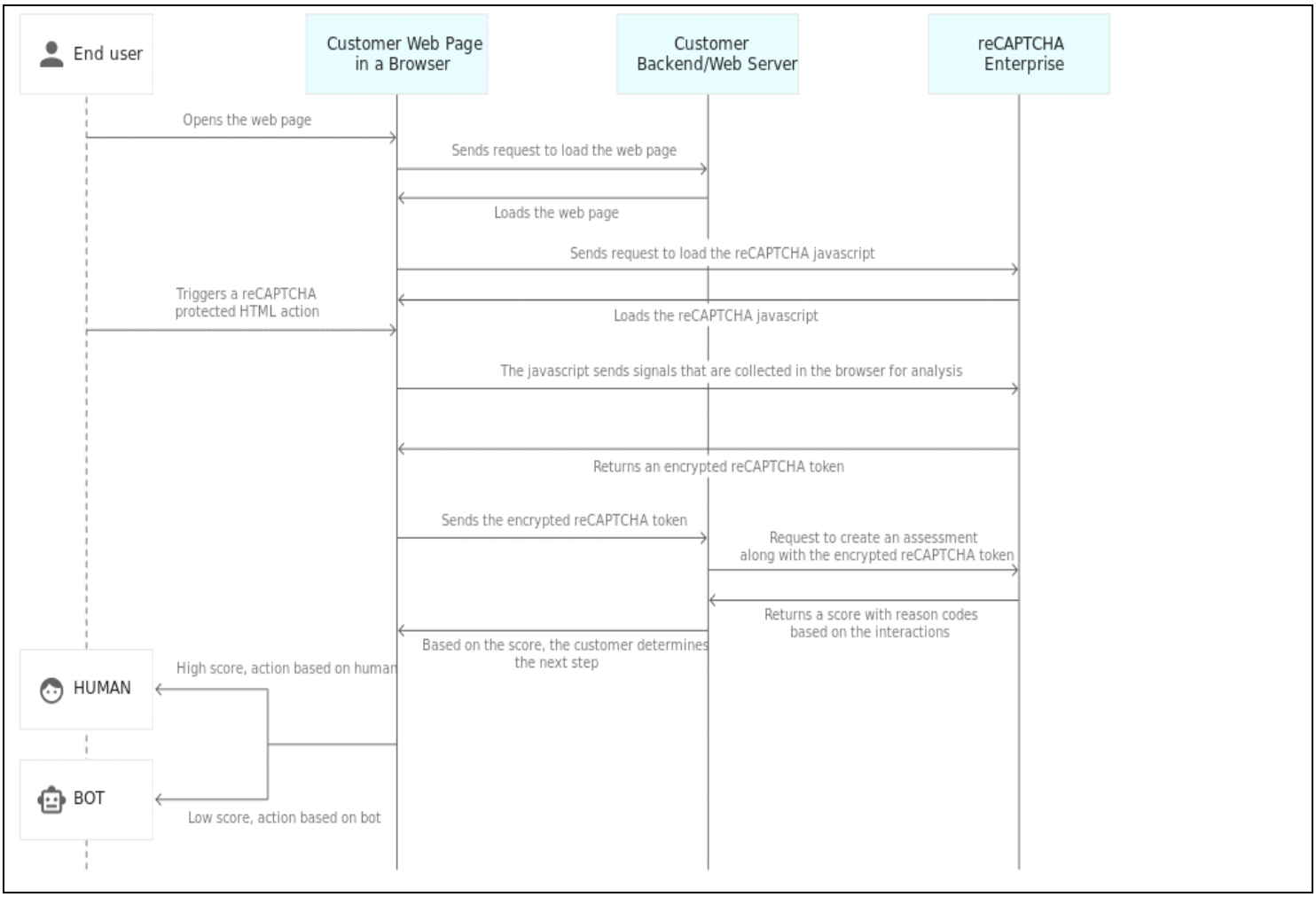
Quando um usuário final acesse a página da *Web*, os seguintes eventos são acionados em sequência:

- O navegador carrega a página da *Web* do cliente armazenada no servidor de *back-end*/web e, em seguida, carrega o *reCAPTCHA* JavaScript do *reCAPTCHA Enterprise;*
- Quando o usuário final aciona uma ação HTML protegida pelo *reCAPTCHA*, como o login, a página da Web envia os sinais coletados no navegador para o *reCAPTCHA Enterprise* para análise;

- O *reCAPTCHA Enterprise* envia um *token reCAPTCHA* criptografado à página da *Web* para uso posterior;
- A página da *Web* envia o *token reCAPTCHA* criptografado ao servidor de *back-end*/Web para avaliação;
- O servidor da *Web*/*back-end* envia a solicitação de criação da avaliação e o *token reCAPTCHA* criptografado para o *reCAPTCHA Enterprise;*
- Após a avaliação, o *reCAPTCHA Enterprise* retorna uma pontuação, de 0,0 a 1,0, e um código de motivo, com base nas interações, para o servidor da *Web*/*back-end;*
- Dependendo da pontuação, o desenvolvedor pode determinar as próximas etapas para realizar ações relacionadas ao usuário.

A Figura 7 do diagrama de sequência mostra a representação gráfica do fluxo de trabalho do *reCAPTCHA Enterprise*:

Figura 7 – Diagrama de sequência do fluxo de trabalho do *reCAPTCHA Enterprise*



Fonte: *Google Cloud*, 2022.

4.26. *Web Risk*

O *Web Risk* é um serviço do GC usado pelos aplicativos clientes para verificar URLs nas listas do *Google* de recursos inseguros da *Web*, que são constantemente atualizadas e incluem sites de engenharia social, como páginas enganosas e de *phishing*, além daquelas que hospedam malware ou software indesejado.

Com o *Web Risk*, é possível verificar rapidamente sites duvidosos conhecidos, avisar os usuários antes que eles cliquem em links infectados e impedir que eles publiquem links para páginas infectadas conhecidas do seu site. O *Web Risk* inclui dados

em mais de um milhão de URLs inseguros e mantêm-se atualizados examinando bilhões de URLs todos os dias.

4.27. *Software* de código aberto

O *Software* de código aberto é um serviço para melhorar a segurança da cadeia de suprimentos de *software,* incorporando os mesmos pacotes de *software* de código aberto confiáveis que o Google usa nos seus próprios fluxos de trabalho de desenvolvedores.

Um dos principais recursos disponíveis por esse serviço são:

- Leitura de código e teste de vulnerabilidade, que são pacotes criados nos próprios *pipelines* protegidos do Google e são verificados regularmente, analisados e testados no *fuzz* para encontrar vulnerabilidades;
- Metadados enriquecidos
- *Builds* em conformidade com a SLSA
- Procedência verificada e SBOMs automáticos

4.28. *Software Delivery Shield*

O *Software Delivery Shield* é um serviço de solução completa e de gerenciamento total que aprimora a segurança da cadeia de suprimentos de *software* em todo o ciclo de vida do desenvolvimento de *software*, desde o desenvolvimento, fornecimento e CI/CD. Este serviço consiste em:

- Produtos e recursos do GC que incorporam práticas recomendadas de segurança para desenvolvimento, criação, teste, verificação, implantação e aplicação de políticas;
- Painéis no console do GC que exibem informações de segurança sobre origem, versões, artefatos, implantações e ambiente de execução;

- Informações que identificam o nível de maturidade da segurança da cadeia de suprimentos de software usando o *framework* de níveis de cadeia de suprimentos para artefatos de *software* (SLSA, na sigla em inglês).

Existem recursos e produtos que fazem parte da solução do *Software Delivery Shield* para ajudar na proteção das etapas do ciclo de vida do desenvolvimento do *software.*

Os componentes que ajudam a proteger o desenvolvimento são:

- Estações de trabalho do Cloud, também conhecido como *Cloud Workstations*, que oferece ambientes de desenvolvimento totalmente gerenciados no GC, permitindo que administradores de TI e segurança provisionem, dimensionem, gerenciem e protejam os próprios ambientes de desenvolvimento. O *Cloud Workstations* possui recursos de segurança como o *VPC Service Controls*, políticas de acesso do IAM, dentre outras;
- Proteção de origem do *Cloud Code,* que oferece suporte ao ambiente de desenvolvimento integrado para criar, implantar e integrar aplicativos com o GC. A proteção de origem do *Cloud Code* fornece aos desenvolvedores *feedback* de segurança em tempo real, como identificação de dependências vulneráveis e relatórios de licença.

O uso generalizado de software de código aberto torna o processo de proteção a fonte do software bem desafiador, com isso outros componentes que ajudam a proteger artefatos de compilação e dependências de aplicativos são disponibilizados para o uso, sendo eles:

- *Assus* garantido, ou também conhecido como *Assured Open Source Software* (*Assured OSS),* que permite acessar e incorporar os pacotes OSS que foram verificados e testados pelo Google, esses pacotes são verificados, analisados e testados regularmente em busca de vulnerabilidades pela Google;
- *Artifact Registry* e análise de contêiner, ele permite armazenar, proteger e gerenciar os artefatos de versão, e a análise de contêiner detecta vulnerabilidades para artefatos no *Artifact Regisitry* de maneira proativa.

Tambem há componentes para proteger o pipeline de CI/CD, sendo eles:

- *Cloud Build,* que é responsável por executar seus *builds* na infraestrutura da GC. Ele oferece recursos de segurança, como permissões granulares do IAM, *VPC Service Controls* e ambientes de compilação isolados e efêmeros;
- *Google Cloud Deploy,* que automatiza a entrega de seus aplicativos para uma série de ambientes de destino em uma sequência definida, podendo suportar entregas diretamente no *Google Kubernetes Engine (GKE), Anthos* e *Cloud Run;*

E, por último, componentes que ajudam a proteger aplicativos em produção, ou seja, recursos de segurança para proteger os aplicativos no momento da execução, são eles:

- *GKE,* que é um recurso que ajuda a avaliar a segurança de contêineres e fornece orientações ativas sobre as configurações do cluster, da carga de trabalho e das vulnerabilidades;
- *Cloud Run,* que contém um painel de segurança que exibe *insights* de segurança da cadeia de suprimentos de software, procedência do *build* e vulnerabilidades encontradas nos serviços em execução.

4.29. *Cloud Armor*

O *Cloud Armor* é um serviço para proteção de aplicativos e sites contra ataques na Web e negação de serviços (DDoS, da sigla em inglês).

Um dos principais benefícios que esse serviço oferece é a proteção de nível empresarial contra DDoS, já que ele aproveita a experiencia de proteção da Google que são utilizados no Youtube, Gmail e na Pesquisa Google, fornecendo assim defesas contra ataques de DDoS de camadas 3 e 4.

Outro benefício é a redução dos 10 principais riscos do *Open Worldwide Application Security Project* (OWASP), através de normas predefinidas para ajudar na proteção contra ataques cibernéticos, como *scripting* em vários locais e injeção de SQL.

Esses benefícios são oferecidos através de diversos recursos, sendo um deles a Proteção adaptativa, regras de *WAF*, gerenciamento de *bots*, limitação de taxa.

A Proteção adaptativa fornece defesa contra DDoS, como sobrecarga de HTTP e outras camadas de alta frequência 7, a nível do aplicativo.

Ela cria modelos de *machine learning* (ML) que fazem o seguinte:

1. Detectar e alertar sobre atividades anômalas;
2. Gere uma assinatura descrevendo o possível ataque;
3. Gerar uma regra personalizada da *WAF* do Google *Cloud Armor* para bloquear a assinatura.

Os alertas sobre tráfegos anômalos, que podem ser ataques potenciais, aparecem no painel de eventos da Proteção adaptativa e seus registros de eventos são enviados para o *Cloud Logging*, onde podem ser analisados ou enviados para a equipe de monitoramento.

As regras de *WAF* são regras complexas do *firewall* de aplicativos da Web com dezenas de assinaturas compiladas a partir dos padrões do setor de código aberto OWASP. Cada assinatura corresponde a uma regra de detecção de ataque no conjunto de regras.

O gerenciamento de *bots* é uma proteção automatizada para os aplicativos contra *bots* e ajuda a impedir fraudes na fila e na borda por meio da integração nativa com o *reCAPTCHA Enterprise*. Como dito anteriormente o *reCAPTCHA Enterprise* usa técnicas avançadas de análise de risco para distinguir usuários humanos de clientes automatizados, após a avaliação do usuário ele emite um *token* criptografado. O *Google Armor* decodifica esse *token* e com base nos atributos deste *token* o *Google Cloud Armor* possibilita permitir, negar, limitar a taxa ou redirecionar as solicitações recebidas.

A limitação de taxa são regras baseadas em taxa que ajudam a proteger os aplicativos contra um grande volume de solicitações que sobrecarregam as instancias e bloqueiam o acesso de usuários legítimos.

A Limitação de taxa pode fazer o seguinte:

- Impedir que um determinado cliente esgote os recursos do aplicativo;
- Proteja as instancias de aplicativos contra picos erráticos e imprevisíveis na taxa de solicitações de clientes.

O *Google Cloud Armor* tem dois tipos de regras com base em taxas:

1. Limitação, onde é possível aplicar um limite máximo de solicitações por cliente ou um limite máximo em todos os clientes configurado pelo usuário;

2. Proibição baseada em taxa: é possível classificar solicitações de limite que correspondem a uma regra por cliente e, em seguida, proibir temporariamente esses clientes por um período configurado, se eles excederem um limite configurado pelo usuário.

Para se identificar clientes individuais para a limitação de taxa o *Cloud Armor* utiliza os seguintes tipos de chave para agregar solicitações e aplicar limites de taxa:

- ALL: uma única chave para todos os clientes com solicitações que atendem à condição de correspondência de regra;
- IP: uma única chave para cada endereço IP de origem do cliente cujas solicitações atendem à condição de correspondência da regra;
- HTTP-HEADER: uma única chave para cada valor de cabeçalho HTTP exclusivo com nome configurado. O valor da chave é truncado para os primeiros 128 bytes do valor do cabeçalho. O tipo de chave assume o padrão ALL se não houver nenhum cabeçalho presente ou se tentarem usar esse tipo de chave com um balanceador de carga de proxy TCP ou de proxy SSL externos;
- XFF-IP: uma chave exclusiva para cada endereço IP de origem original do cliente, ou seja, o primeiro endereço IP na lista de IPs especificados no cabeçalho HTTP X-Forwarded-For. O tipo de chave assume o padrão de endereço IP se nenhum cabeçalho estiver presente, se o valor não for um endereço IP válido ou se você tentar usar esse tipo de chave com um balanceador de carga de proxy TCP ou de proxy SSL externos;
- HTTP-COOKIE: uma chave exclusiva para cada valor de cookie HTTP com o nome configurado. O valor da chave é truncado para os primeiros 128 bytes do valor do cookie. O tipo de chave assume o padrão ALL se não houver nenhum cookie presente ou se você tentar usar esse tipo de chave com um balanceador de carga de proxy TCP ou de proxy SSL externos;
- HTTP-PATH: o caminho do URL da solicitação HTTP. O valor da chave é truncado nos primeiros 128 bytes;

- SNI: a indicação do nome do servidor na sessão TLS da solicitação HTTPS. O valor da chave é truncado nos primeiros 128 bytes. O tipo de chave é **ALL** por padrão em uma sessão HTTP;
- REGION-CODE: o país/região de origem da solicitação.

O *Cloud Armor* consegue limitar o tráfego através da ação *Throttle* em uma regra que permite que se aplique um limite de solicitação por cliente para proteger os serviços de *back-end.* O limite é configurado como um número especificado de solicitações em um intervalo de tempo especificado.

Por exemplo, é possível definir o limite de solicitações para 2.000 solicitações em 1.200 segundos (20 minutos). Se um cliente enviar 2.500 solicitações em um período de 1.200 segundos, aproximadamente 20% do tráfego dele será limitado até que o volume de solicitações permitido seja igual ou inferior ao limite configurado.

Pode-se também banir temporariamente clientes que excedem o limite de solicitações através da ação *rate_based_ban.*

4.30. Serviços de segurança da *Mandiant*

A *Mandiant* é empresa independente que faz parceria com a Google e outras. Ela é uma plataforma de segurança que usa o modelo SaaS para oferecer seus serviços de segurança. Seus serviços não estão presentes dentro da GCP, porém são multiplataformas e podem ter a integração direta do site da *Mandiant* para a *Google Cloud*.

Por ser uma empresa focada no mercado de segurança cibernética, ela fornece serviços mais especializados na parte de monitoramento e prevenção contra invasões. Com ela, mais uma camada de segurança pode ser integrada nas organizações e projetos dentro do *Google Cloud Plataform*.

5. Experimentos

Este capítulo mostra como configurar alguns dos principais serviços da plataforma Google Cloud. Além disso, será abordado o passo a passo para se configurar estes serviços de segurança, assim como monitoramento de permissões. Também é mostrado um exemplo de um ataque utilizando injeção por SQL e como evitar este tipo de ataque, através de configurações de regras.

5.1. Computação confidencial

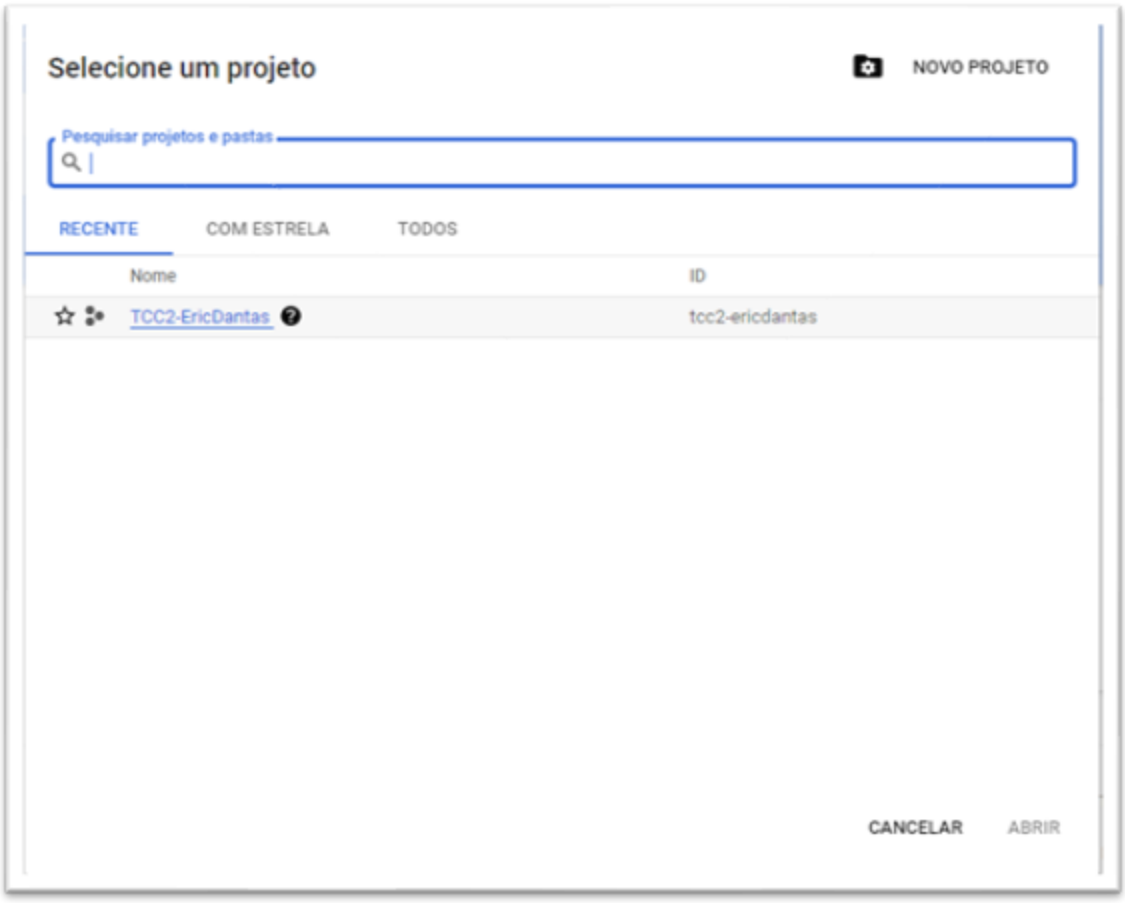
A importância de se ter VMs protegidas com criptografia de ponta a ponta é fundamental para se ter um ambiente seguro. A computação confidencial fornece serviços de VMs confidenciais que garantem que os dados e aplicativos permaneçam seguros e criptografados, mesmo durante o uso dos mesmos.

Só é possível ativar a computação confidencial quando se tem uma VM instanciada.

Como se configurar VMs confidenciais na plataforma Google Cloud:

Supondo que já tenha uma instancia de uma VM já criada, com a API *Compute Engine* ativada e o *Google Cloud CLI* instalado, caso queira executar linhas de comando via console. Com um projeto selecionado com as devidas permissões para poder criar e configurar a VM. No caso, neste experimento foi criado um projeto de nome “TCC2-EricDantas” com as permissões de proprietário, conforme mostrado na Figura 8.

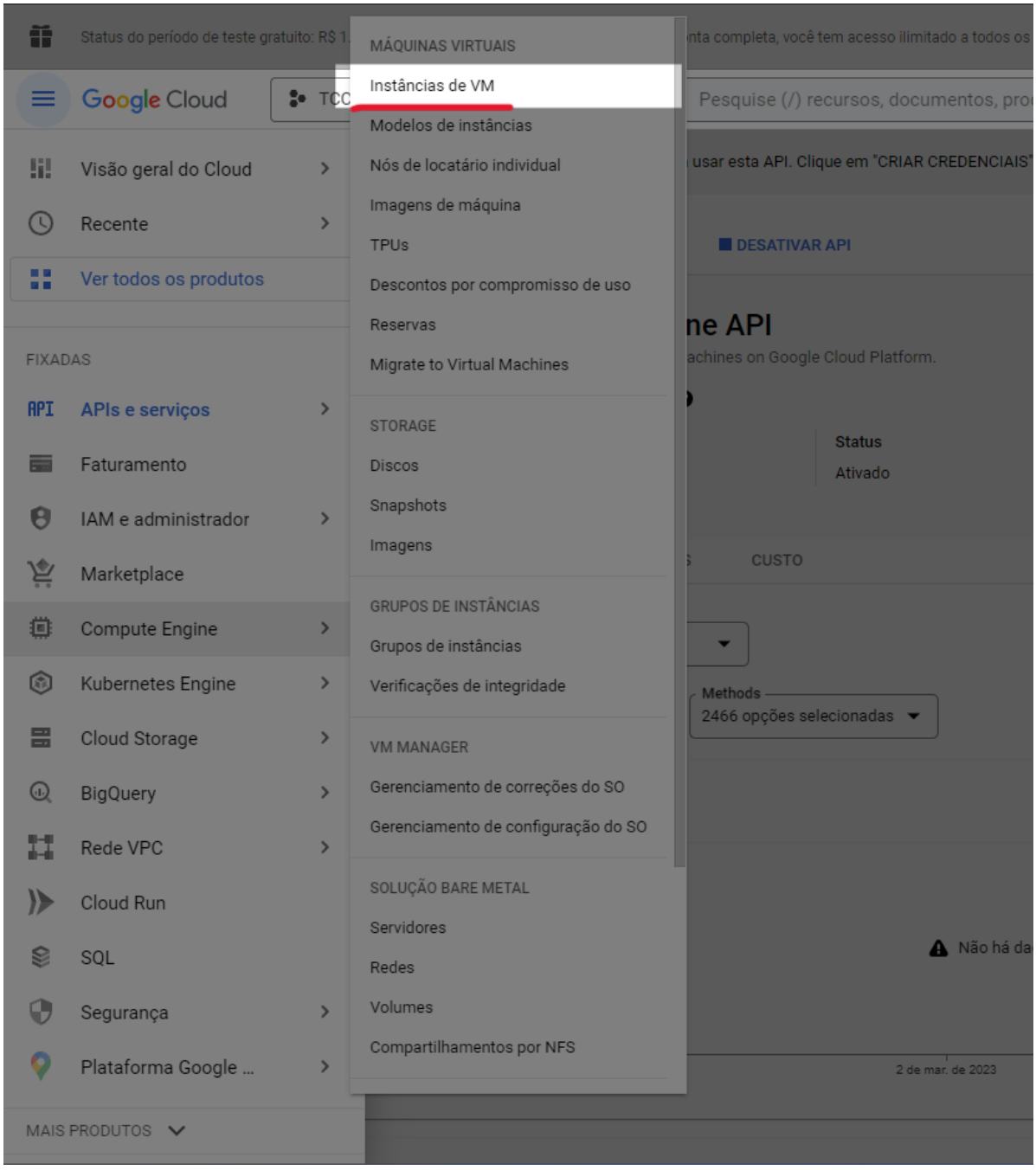
Figura 8 – Seleção do projeto



Fonte: Autoria própria, 2023.

No menu de navegação do Console do *Google Cloud*, clique em *Compute Engine* e selecione Instâncias de VM conforme apresentado na Figura 9:

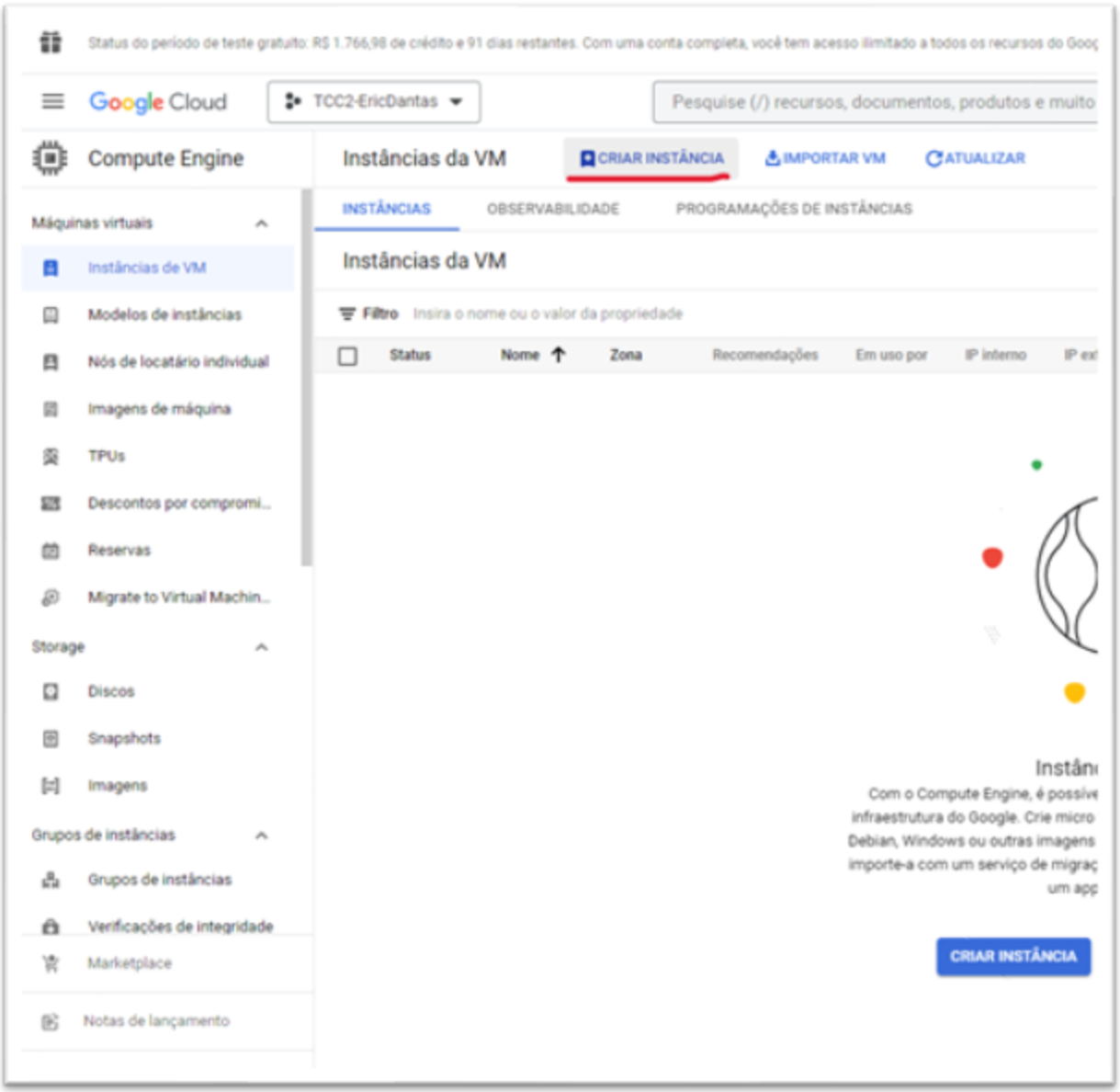
Figura 9 – Seleção da Instância de VM



Fonte: Autoria própria, 2023.

Depois clique em Criar Instancia, de acordo com as figuras 10 e 11:

Figura 10 – Criação de uma VM

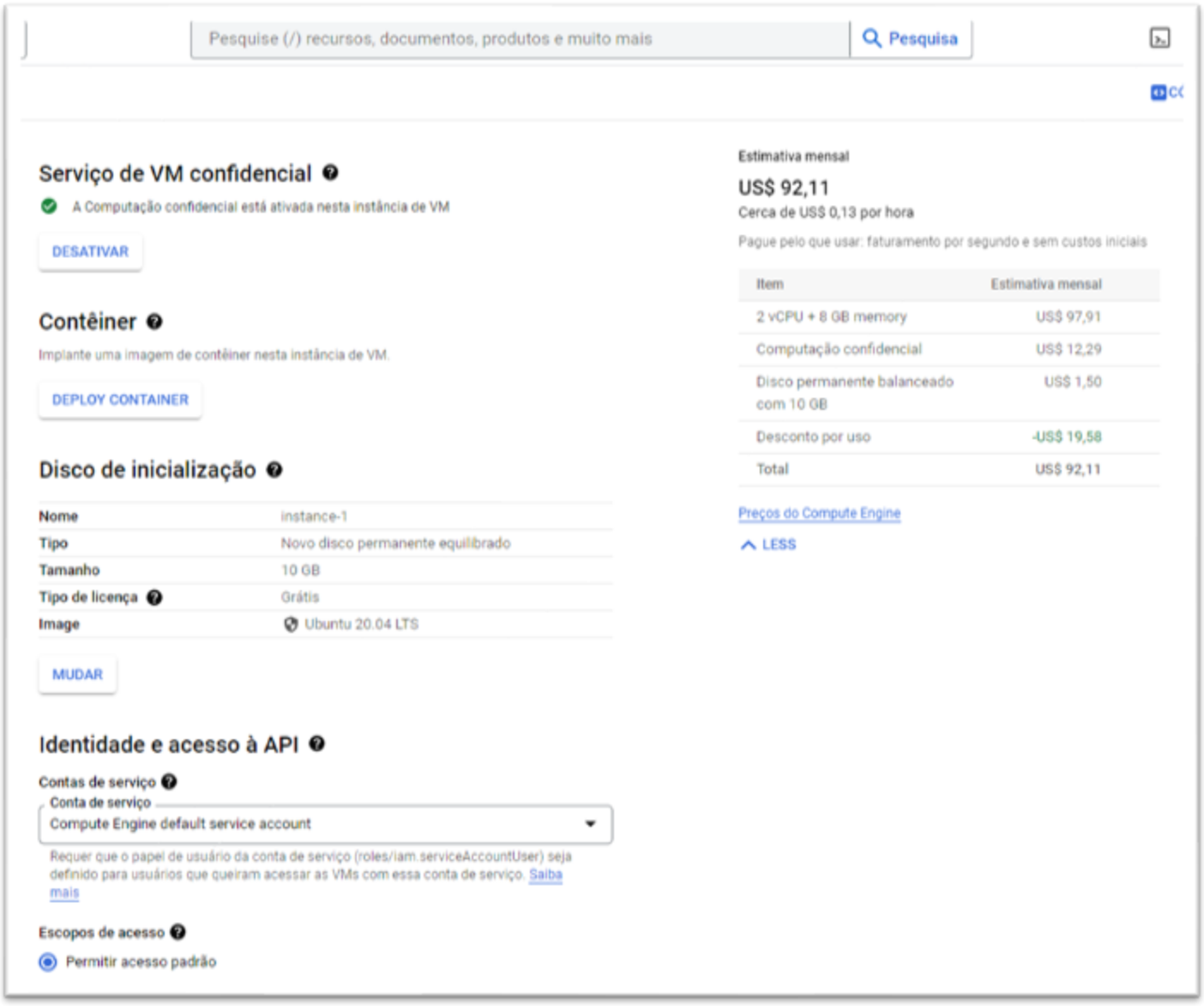


Fonte: Autoria própria, 2023.

A VM utilizada para se configurar o serviço de VM confidencial foi uma VM de segunda geração, da série N2D, que inclui a tecnologia de CPU AMD EPYC. Ela é responsável pela virtualização criptografada segura (SEV), com 2vCPU, 8 GB de memória RAM, um espaço em disco de 10 GB e rodando um SO Ubuntu 20.04 LTS.

Antes de instanciar a VM deve-se garantir que o Serviço de VM confidencial esteja ativado:

Figura 11 – Configuração da VM



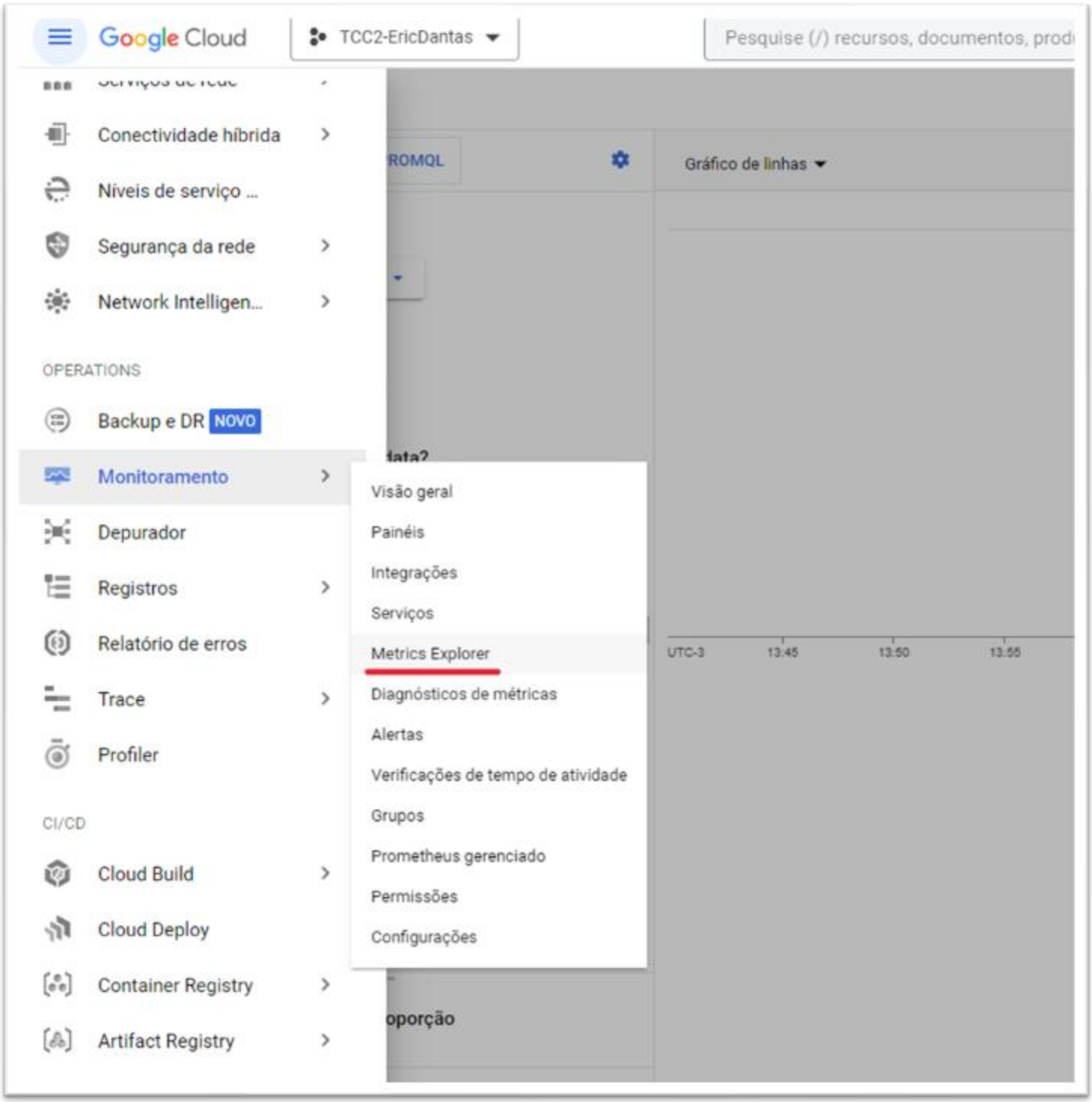
Fonte: Autoria própria, 2023.

Com a VM confidencial criada e ativada é possível se fazer o monitoramento da integridade das VMs, presentes nos serviços de VM protegida e da VM confidencial, que ajuda a entender e tomar decisões sobre o estado das instâncias de VM. O

monitoramento de integridade é ativado por padrão em novas instancias de VM confidencial.

O monitoramento pode ser visualizado através de relatórios de integridade no *Cloud Monitoring* e também pode-se analisar os detalhes dos resultados de monitoramento de integridade no *Cloud Logging,* conforme a Figura 12:

Figura 12 – Acesso ao monitoramento da VM



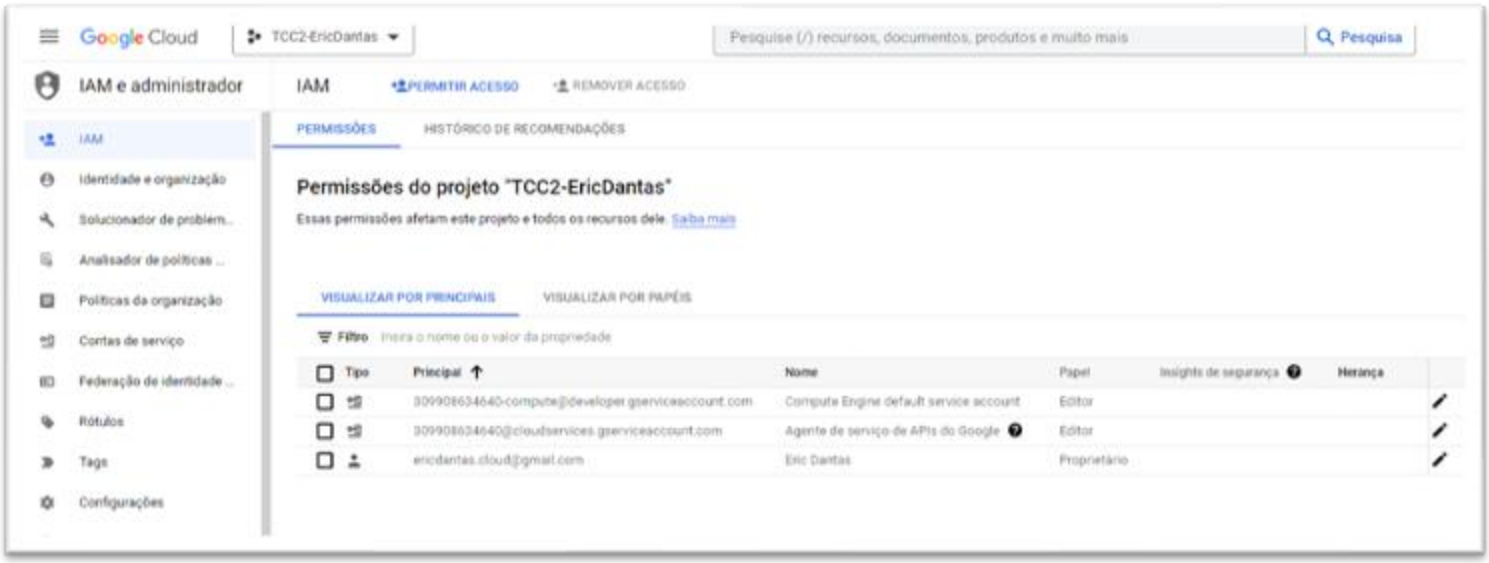
Fonte: Autoria própria, 2023.

5.2. *Identity and Access Managment*

O *Identity and Access Managment* (IAM) é um serviço de controle de acesso e visibilidade para o gerenciamento centralizado de recursos em nuvem. Com o IAM, o administrador gerencia o controle de acesso definindo quem (identidade) tem qual acesso (papel) a que recurso.

Quando se cria um novo projeto, o usuário que criou o projeto é definido com as permissões de proprietário. Ou seja, ele terá acesso total a maioria dos recursos do google cloud para aquele projeto. Na figura 13, é possível identificar três principais, que no caso são uma conta da google, identificada como ericdantas.cloud@gmail.com e ela possui o papel de Proprietário que em suas políticas possuem permissões de acesso total a maioria dos recursos do Google Cloud. Além de dois domínios do *Cloud Identity* que são as APIs ativadas na criação da VM com papel de Editor, que em sua política, possuem permissões de visualizar, criar, atualizar e excluir os recursos da VM criada.

Figura 13 – Usuários e conta de serviço no IAM



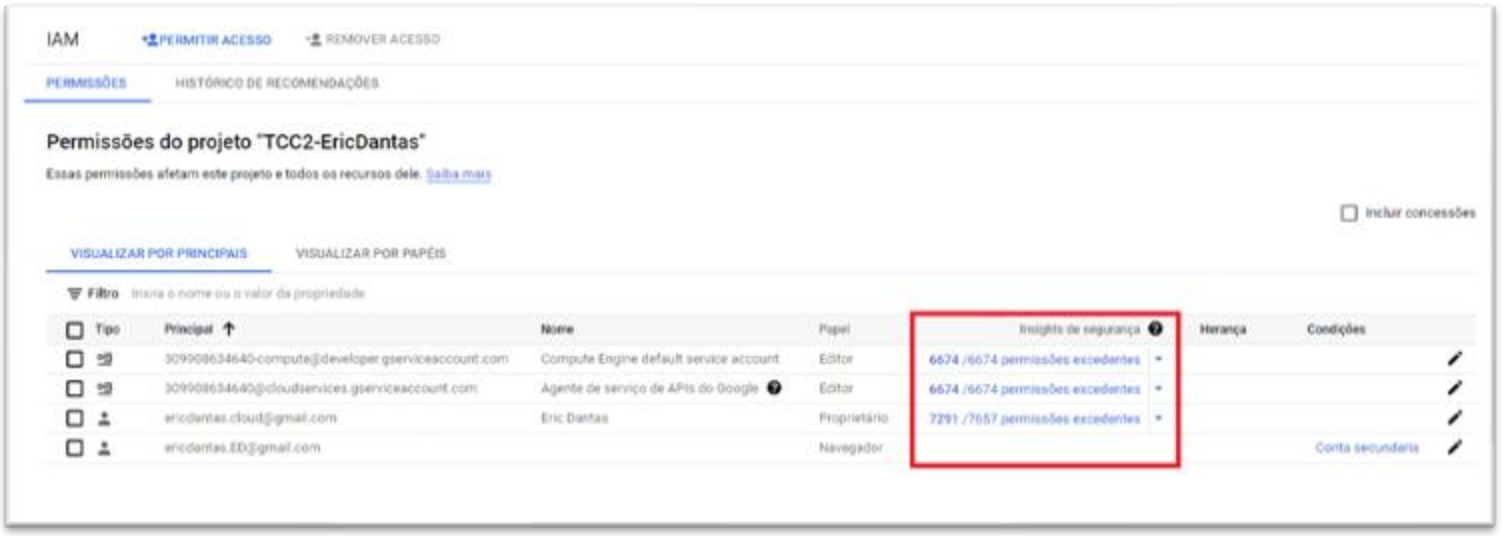
Fonte: Autoria própria, 2023.

O serviço de IAM também oferece sugestões sobre permissões dos *principals*, quando se há muitas permissões e geralmente o *principal* em questão não utiliza essas permissões. Assim, o próprio IAM sugere revogar as permissões que não estão sendo

usadas, a ponto de prevenir e limitar as ações do principal, deixando somente o necessário para se trabalhar no projeto atual.

A Figura 14 mostra as sugestões do IAM para revogar permissões de alguns *principals*.

Figura 14 – *Insights* de segurança do IAM

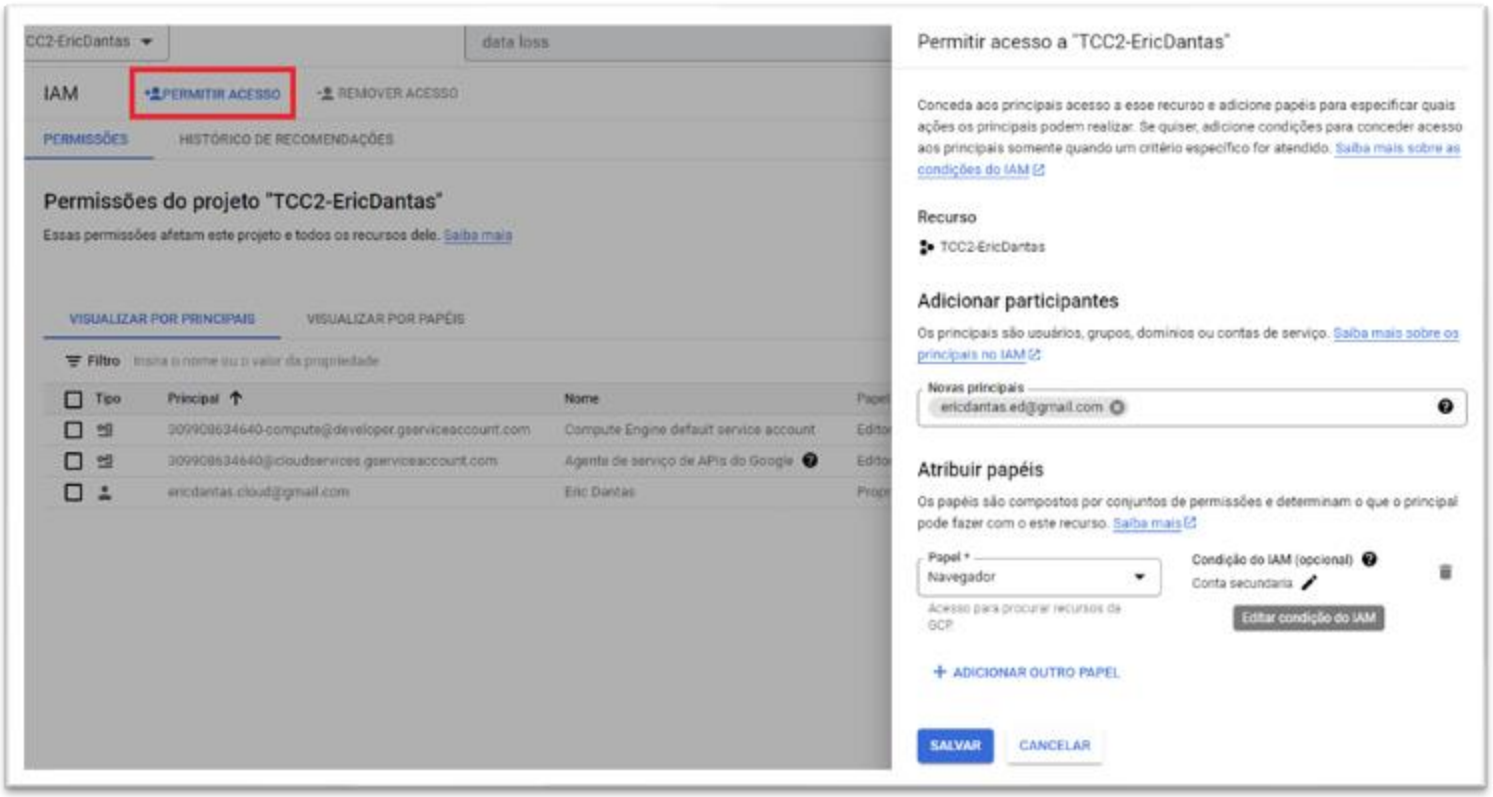


Fonte: Autoria própria, 2023.

Também há a possibilidade de se adicionar e permitir acesso a novos *principals*, definindo seus papeis e podendo até limitar o acesso a determinados dias, horas ou a expiração dessa permissão.

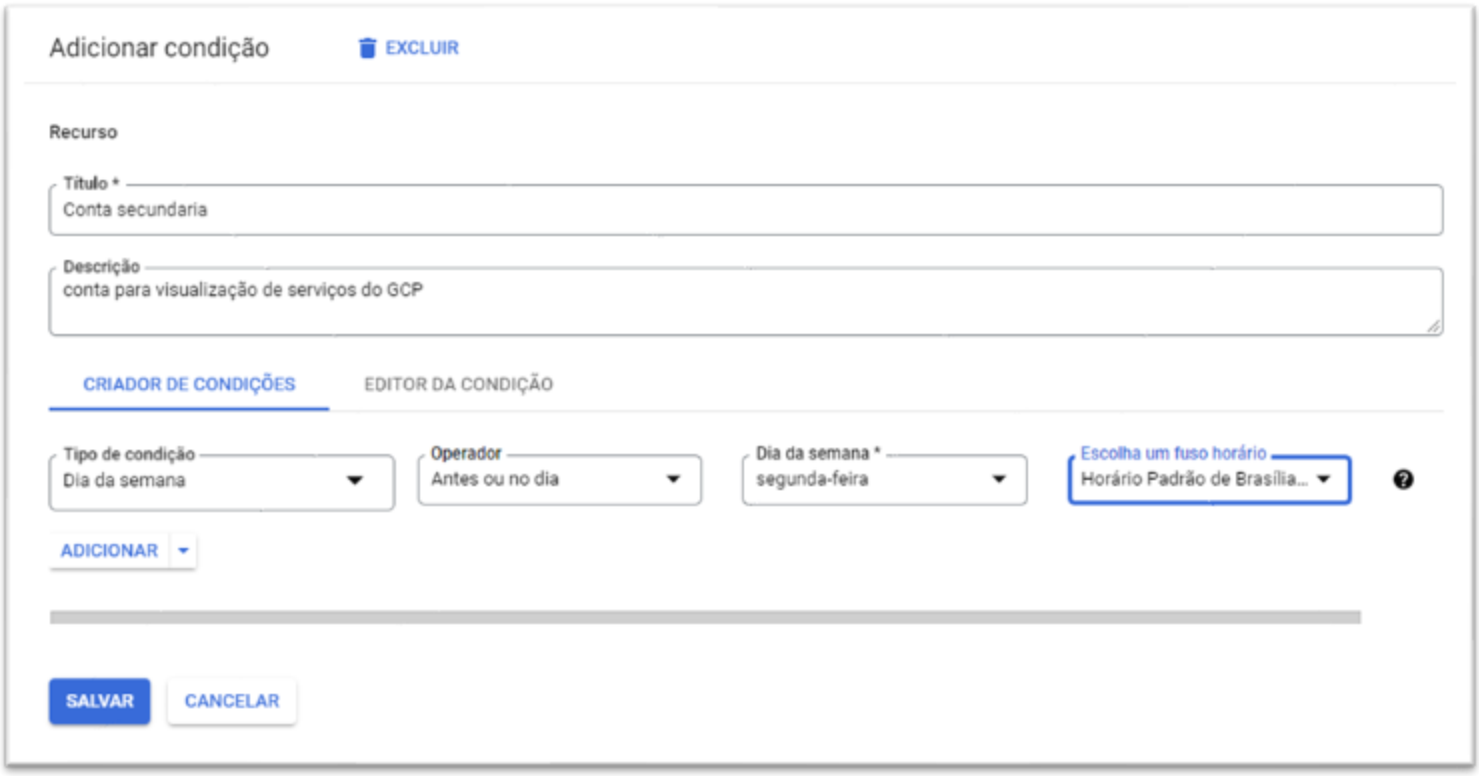
As Figuras 15 e 16 mostram o processo para se adicionar e permitir o acesso de um *principal*.

Figura 15 – Criação de acesso de um *principal*



Fonte: Autoria própria, 2023.

Figura 16 – Criação de acesso de um *principal*

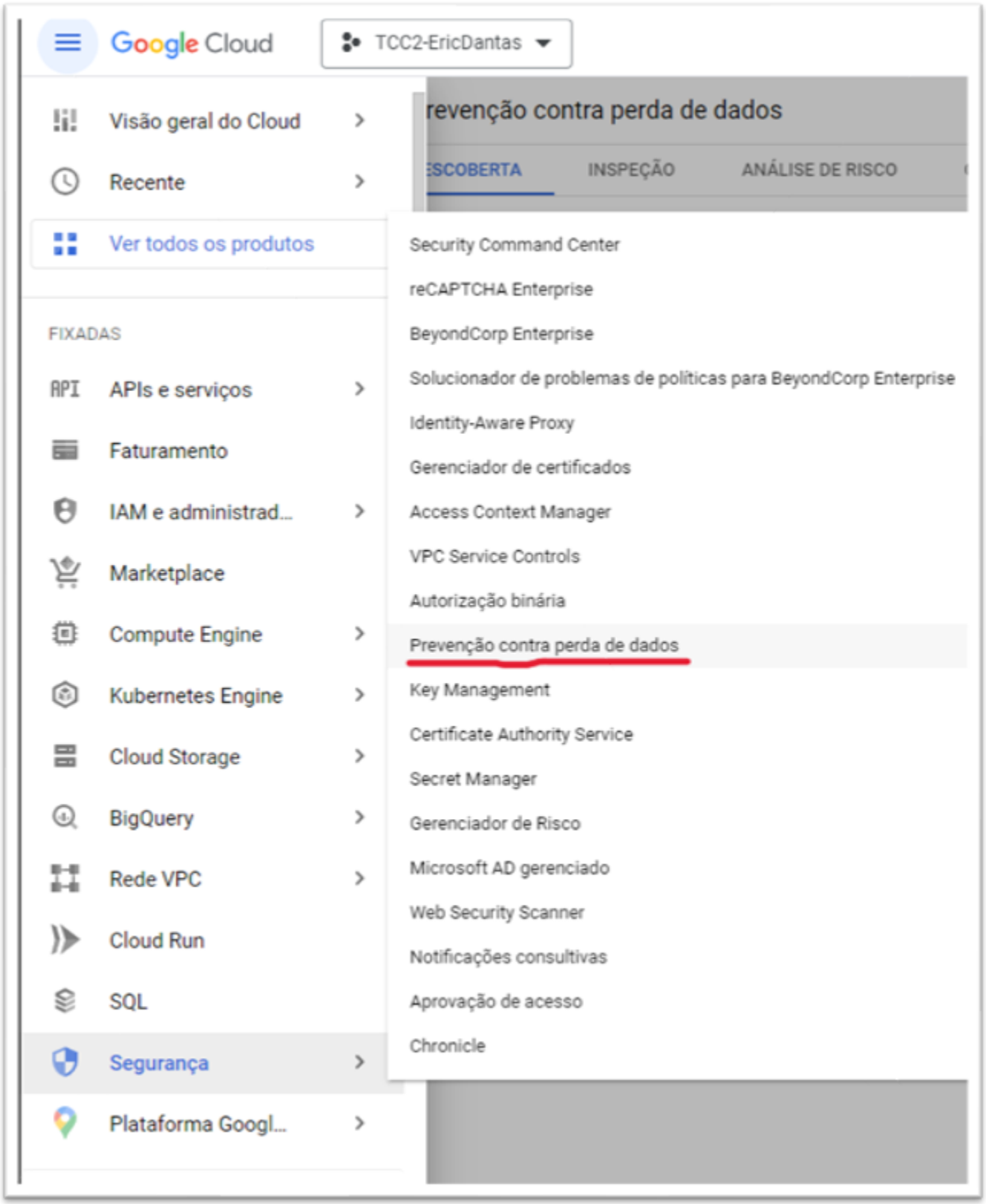


Fonte: Autoria própria, 2023.

5.3. *Cloud Data Loss Prevention*

O Cloud DLP verifica e analisa dados para verificar a segurança de dados sensíveis, isto pode ser feito através da configuração de gatilhos de verificações de inspeção do Cloud DLP. Esses gatilhos são eventos que automatizam a execução de tarefas do Cloud DLP para verificar os repositórios de armazenamento do Google Cloud (*Cloud Storage, BigQuery e Datastore*). É possível acessar o *Cloud DLP* conforme ilustrado na Figura 17:

Figura 17 – Acesso ao *Cloud DLP*



Fonte: Autoria própria, 2023.

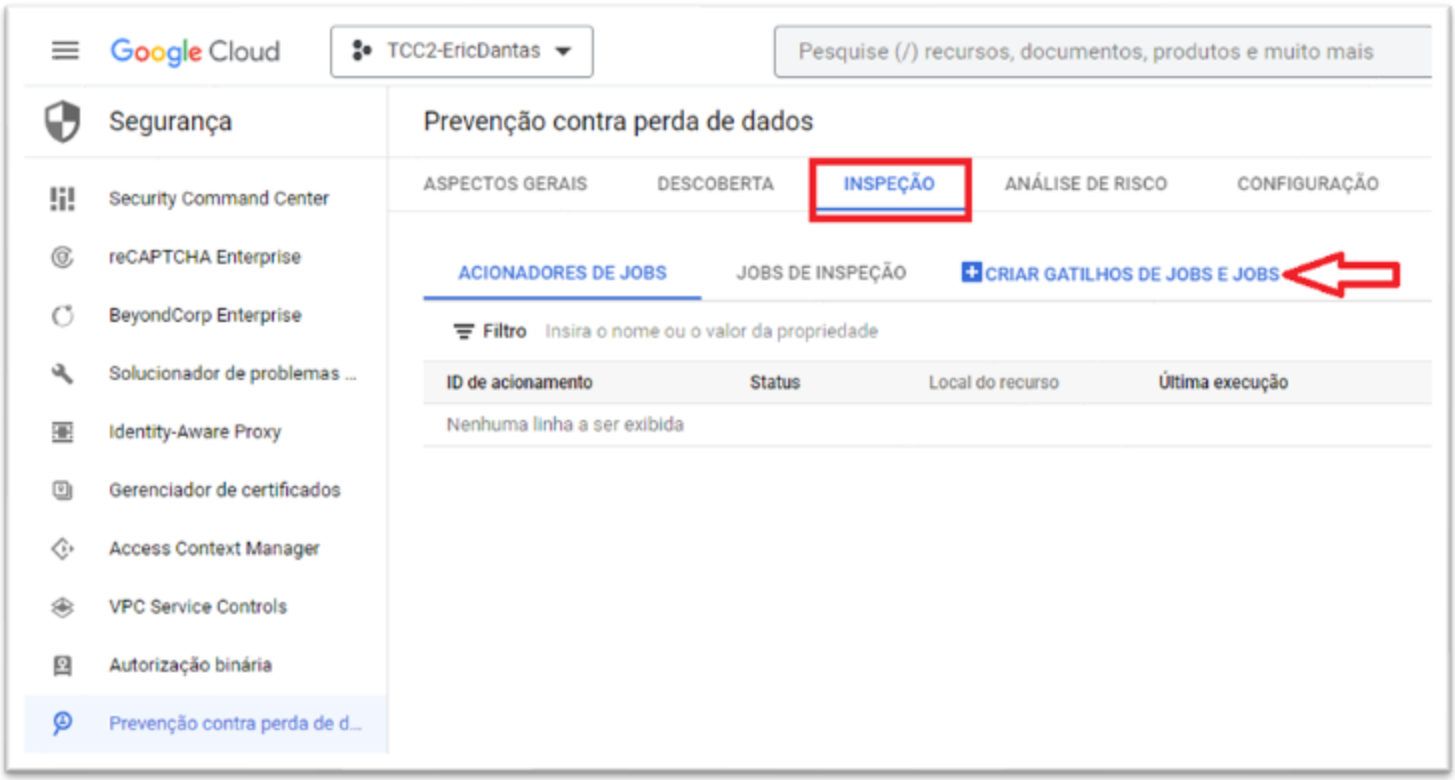
O *Cloud DLP* possui três ferramentas de análises:

- A Análise de risco, na qual se criam tarefas para se analisar dados e calcular métricas de privacidades, de acordo com propriedades pré-definidas pela Google;
- A Descoberta, que é a ferramenta que verifica os projetos de uma organização e que depois de 24 horas gera relatórios e recomendações sobre dados sensíveis;
- A Inspeção que será tratada no experimento, que é responsável por criar gatilhos de tarefas para verificação automática de dados armazenados no *Google Cloud*.

A seguir será mostrado como configurar um gatilho de tarefa para a verificação de dados armazenados, mostrado na Figura 18. Os dados usados foram um conjunto de dados públicos do *BigQuery* que possui endereços de estações de aluguel de bicicleta em uma cidade.

Com a API do *Cloud Data Loss Prevention* ativada, deve-se clicar na guia Inspeção para se criar os gatilhos de verificação.

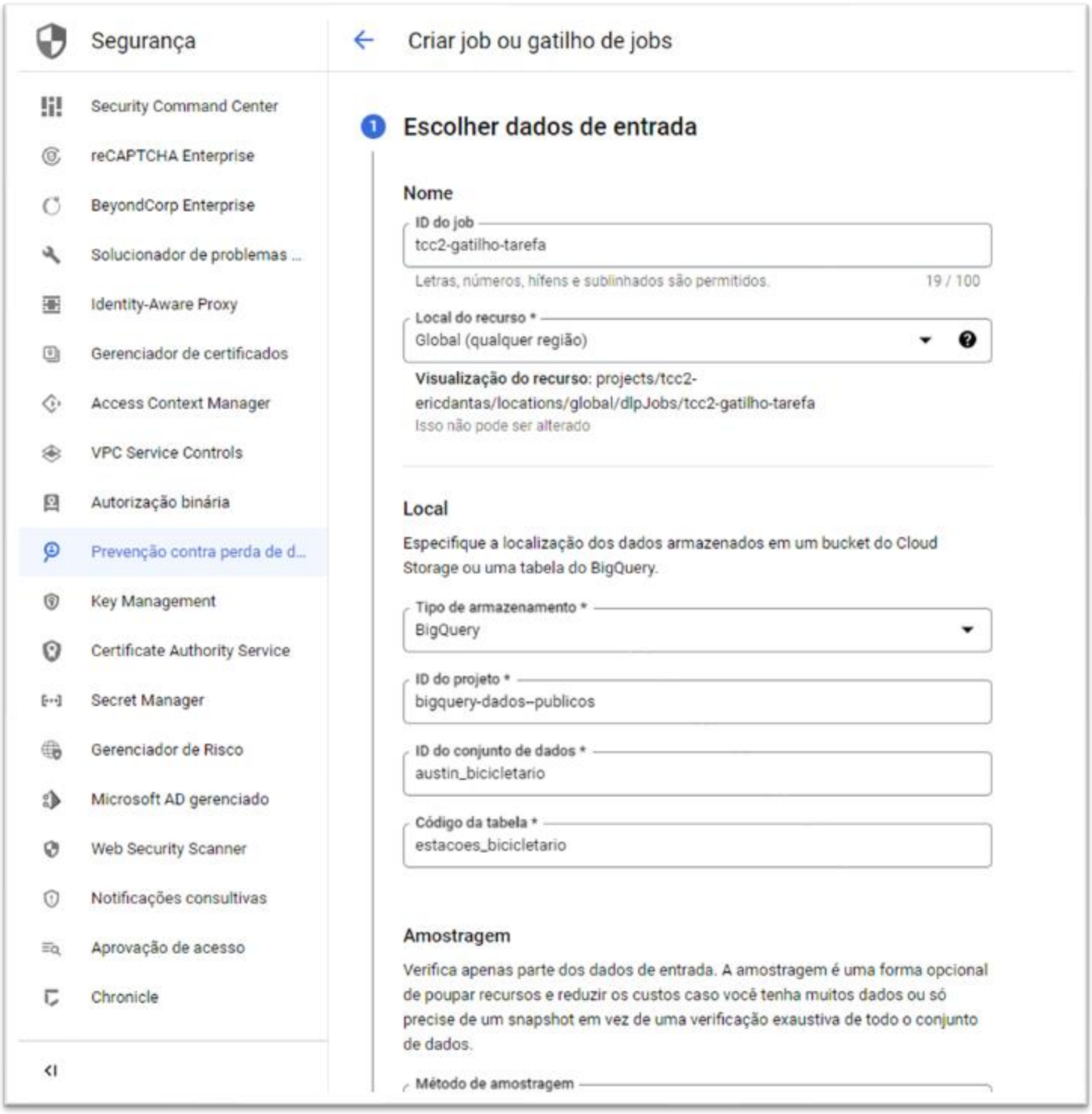
Figura 18 – Processo de criação de uma inspeção



Fonte: Autoria própria, 2023.

O ID do *job* usado foi “tcc2-gatilho-tarefa" e o local onde o Cloud DLP irá armazenar esse recurso do *job* será Global, conforme mostrado nas Figuras 19 e 20. O tipo de armazenamento será o *BigQuery* com as seguintes configurações: ID do projeto “bigquery-dados--publicos”, ID do conjunto de dados "austin_bicicletario", ID da tabela "estacoes_bicicletario" e no campo número máximo de linhas modifique para 10.

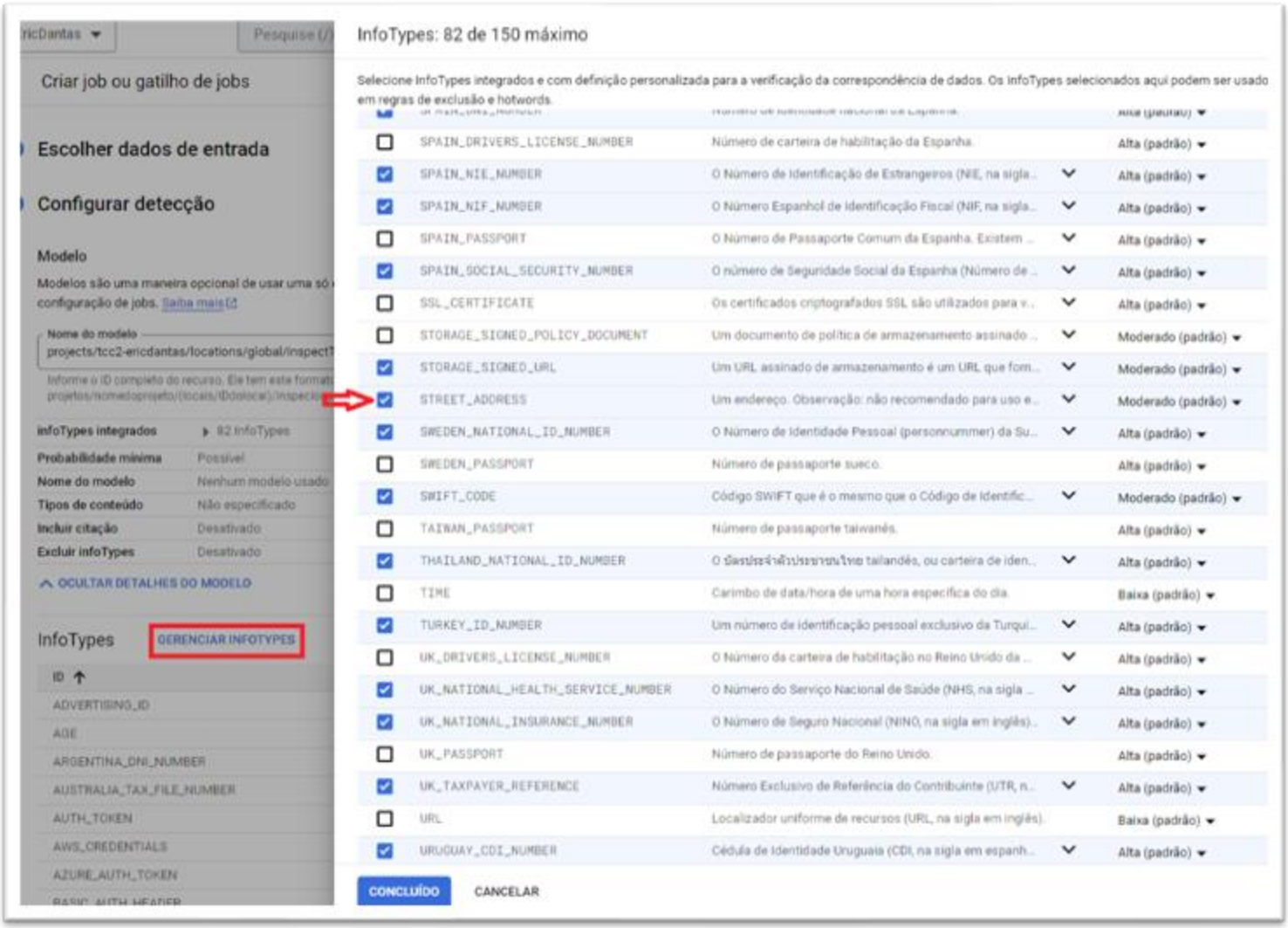
Figura 19 – Criação de um gatilho de *job*



Fonte: Autoria própria, 2023.

Na parte de configuração de detecção, clica-se em gerenciar *InfoTypes* e depois procure e selecione *STREE_ADDRESS.* E em Limite de confiança, seleciona-se na aba o item “Possível".

Figura 20 – Configuração do gatilho de *job*

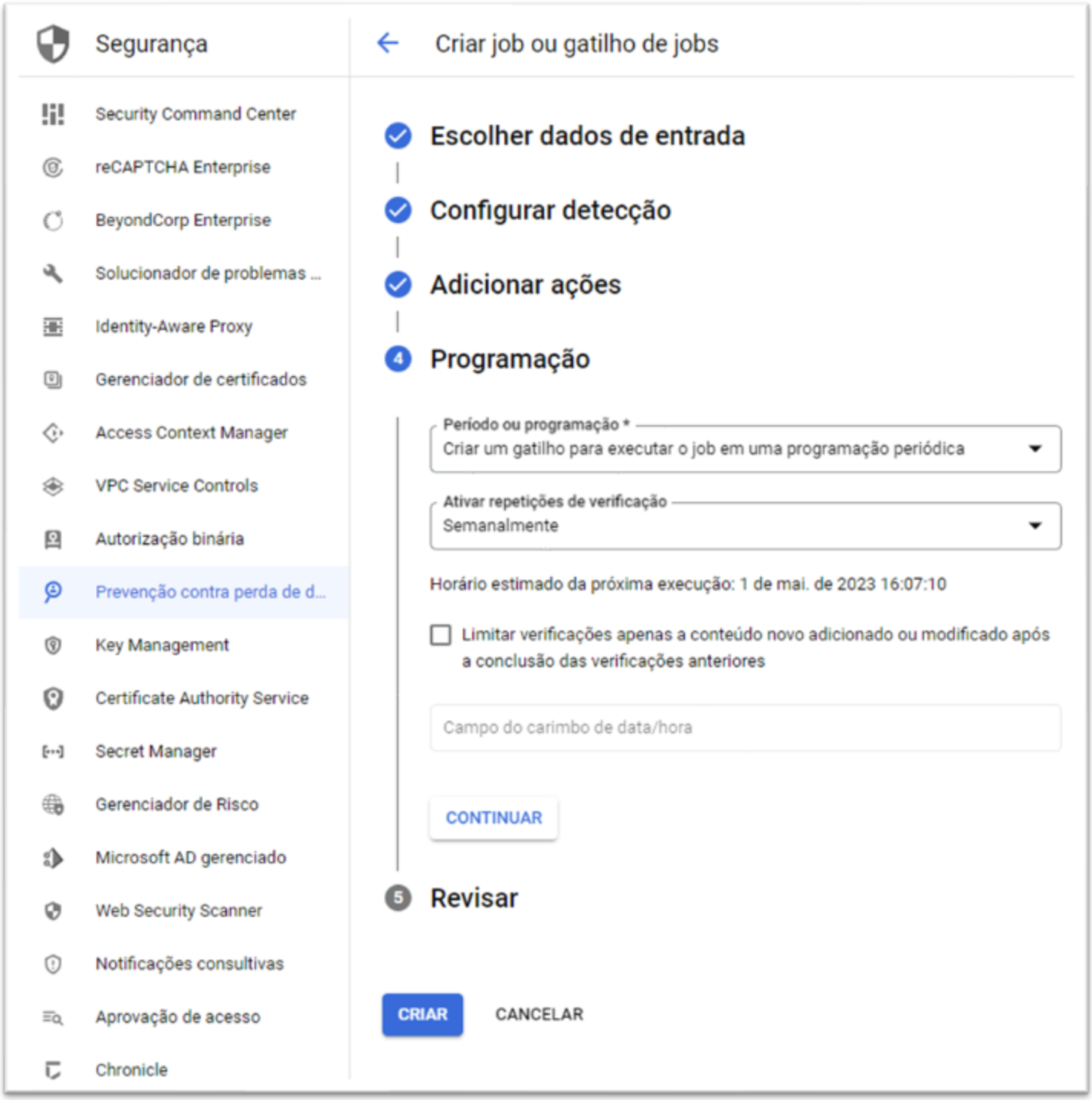


Fonte: Autoria própria, 2023.

Depois dos parâmetros pré-configurados, deve-se adicionar as ações de pós-verificação, que são ações de notificação e a programação periódica em que esse gatilho de tarefa será executado.

Na Figura 21 foi definido que as notificações serão enviadas para os proprietários de acordo com as permissões do IAM, e esta programação periódica será repetida semanalmente.

Figura 21 – Definições de notificação do gatilho de *job*



Fonte: Autoria própria, 2023.

Depois de revisar a configuração de toda tarefa em formato JSON, agora é só finalizar a criação da tarefa e executá-lo. Quando executado, a tarefa verifica os repositórios de armazenamento do *Google Cloud*, que neste caso, o usado foi o *BigQuery,* e o tipo de informação (*InfoTypes*) definido, que foi o endereço da rua (*STREET_ADDRESS*). Assim, a tarefa verifica e identifica se os dados são confidenciais.

Figura 22 – Revisão e execução do gatilho de *job*

Fonte: Autoria própria, 2023.

5.4. *Cloud Armor*

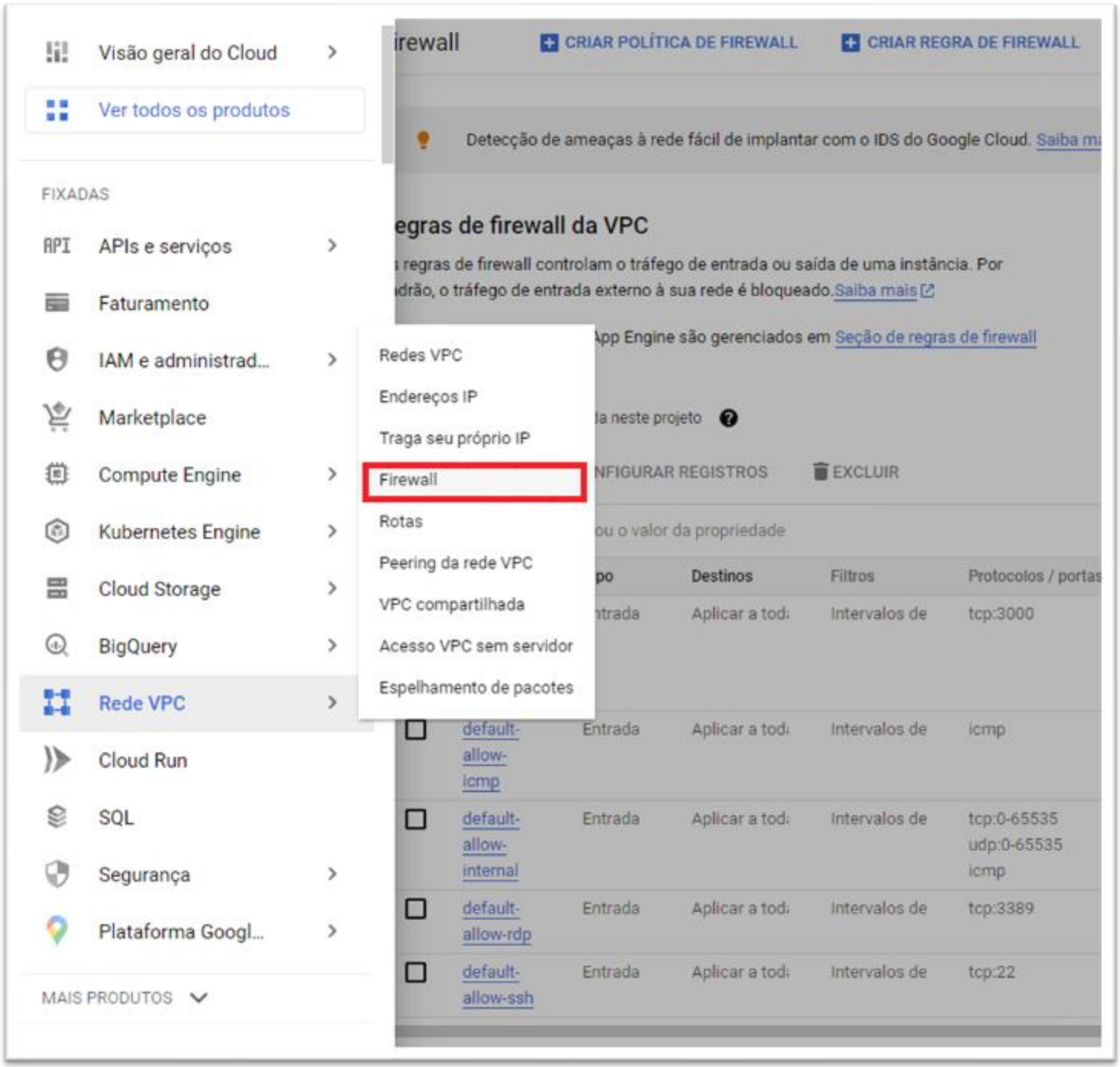
Como citado no item 4.29, no capítulo 4, o Google *Cloud Armor* é um serviço que ajuda a proteger aplicações dentro do Google Cloud contra vários tipos de ameaças. Neste experimento foi criado um ambiente de teste para mostrar como configurar o *Cloud Armor*, assim como suas políticas e regras para se evitar um ataque por SQL *Injection*.

O primeiro passo a se fazer é criar uma instancia de uma VM, no caso a instância usada foi uma VM de segunda geração, da série E2, o tipo da máquina selecionado foi um e2-micro com 2vCPU, 1 GB de memória RAM, um espaço em disco de 10 GB e rodando um SO Debian GNU/Linux11. A VM foi criada com uma imagem de um contêiner

disponibilizado pelo OWASP para fazer testes de segurança, a imagem do contêiner usado foi o *OWASP Juice Shop*.

O ambiente de teste criado foi o “aplicacao-owasp-juice-shop" e quando iniciado ele fornece IPs interno e externo para se poder conectar a aplicação, porém é necessário se configurar a parte de regras do *firewall* para se conectar a aplicação. Para acessar a parte de configuração do *firewall* basta procurar o serviço de Rede VPC no menu de navegação da plataforma do Google Cloud e depois clicar em *Firewall,* como mostrado na Figura 23.

Figura 23 – Acesso ao *Firewall*

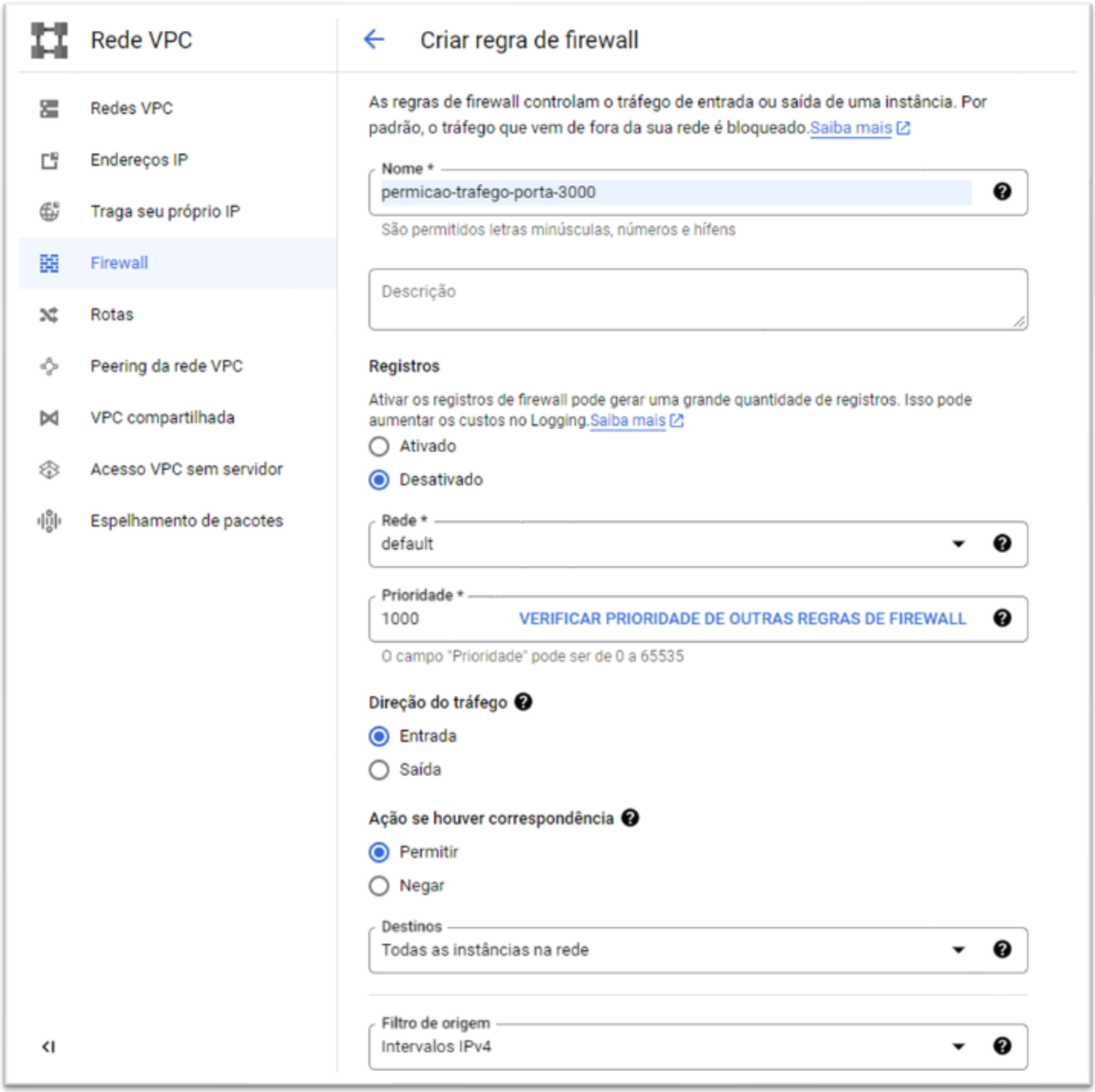


Fonte: Autoria própria, 2023.

Após entrar na página de configuração do *Firewall*, deve-se clicar em Criar Regra de Firewall, para que a porta 3000 seja liberada e o protocolo de comunicação TCP seja

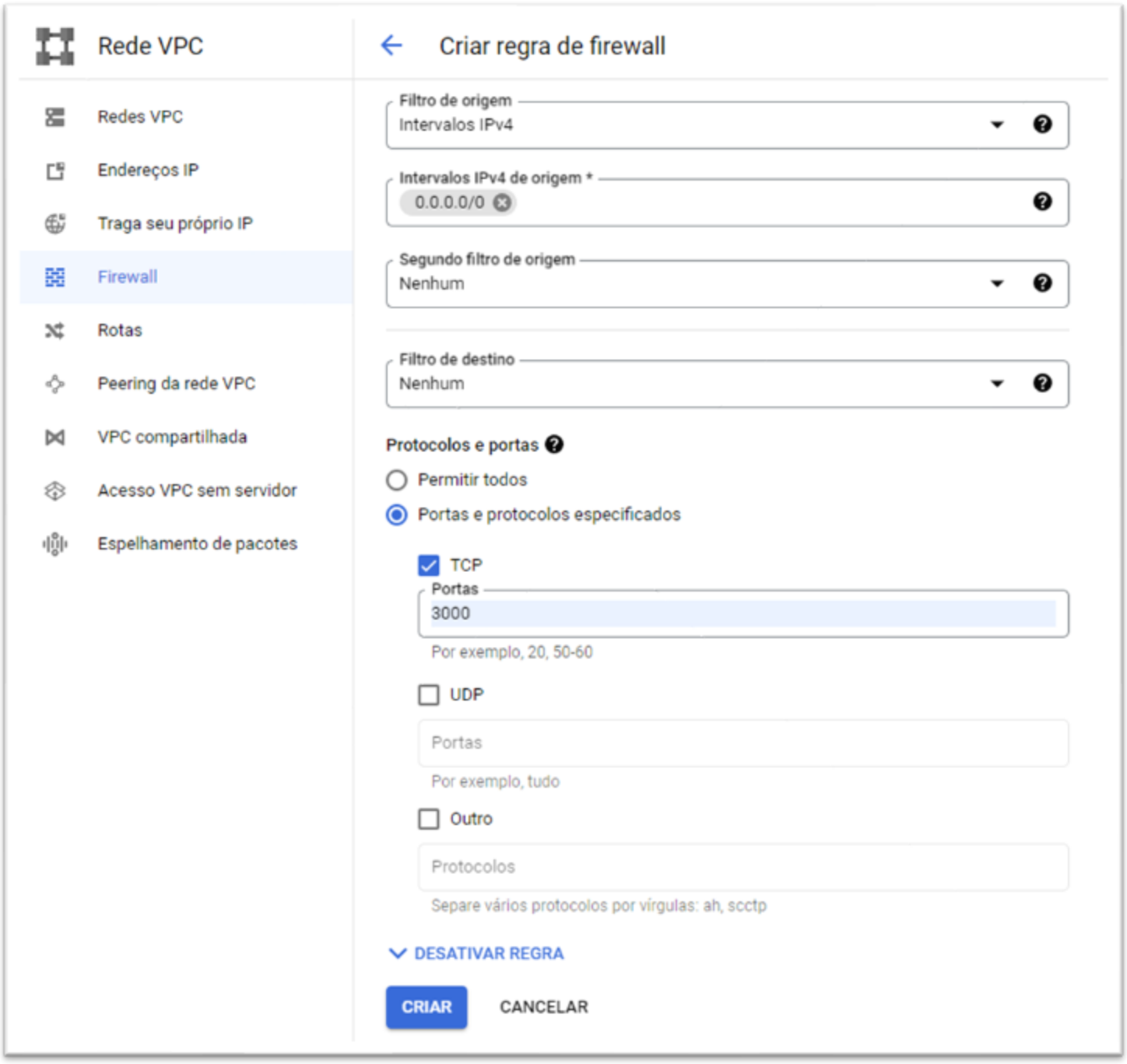
configurado corretamente. Nas Figuras 24 e 25 são mostrados a parte de configurações de regras do *firewall* para a liberação da porta 3000, onde será feito o tráfego da aplicação via IP externo.

Figura 24 – Configuração da porta 3000 no *firewall*



Fonte: Autoria própria, 2023.

Figura 25 – Configuração da porta 3000 no *firewall*



Fonte: Autoria própria, 2023.

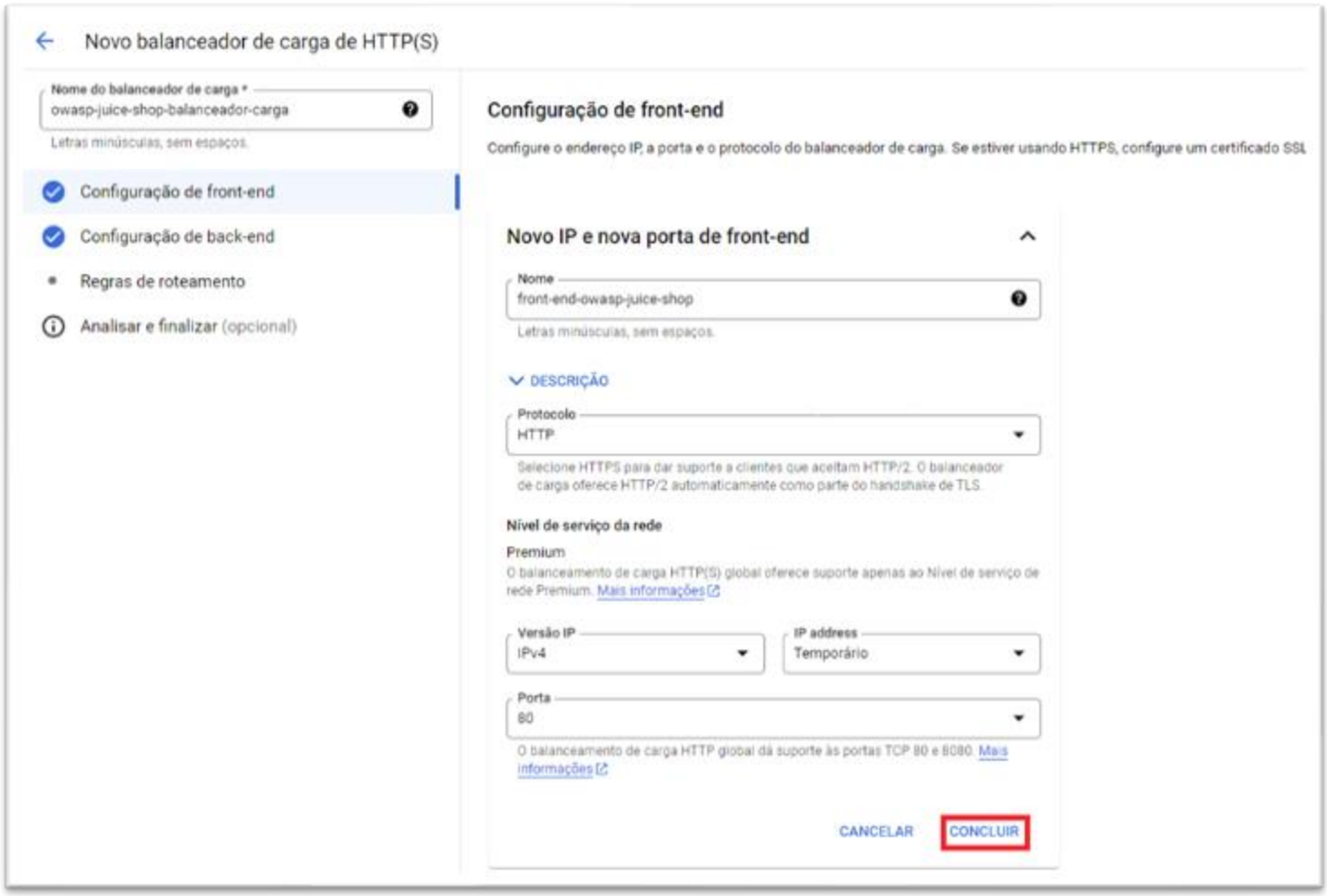
Na Figura 24 foi definido qual seria o nome da regra, que no caso foi nomeada como “permissao-trafego-porta-3000”, e foi mudado somente o “Destinos”, que será para todas as instancias na rede. Ou seja, essa regra foi aplicada em todas as instancias VMs

dentro da rede virtual do projeto TCC2-EricDantas. Já na Figura 25 o intervalo IPv4 de origem foi definido como 0.0.0.0/0 para que a aplicação seja acessada de qualquer endereço IP, já que a aplicação é feita para ser acessada de qualquer lugar do mundo. Depois é definido qual protocolo será usado, que no caso será o TCP na porta 3000.

Depois da regra *firewall* criada, já é possível ter acesso à aplicação através do IP externo na porta 3000, que foram gerados quando a VM com a aplicação foi iniciada. Porém, em ambientes de produção é necessário se usar o serviço de Balanceamento de Carga, ou *Cloud Load Balancing,* que é responsável por equilibrar o tráfego HTTP e HTTPS entre as instancias de *back-end*.

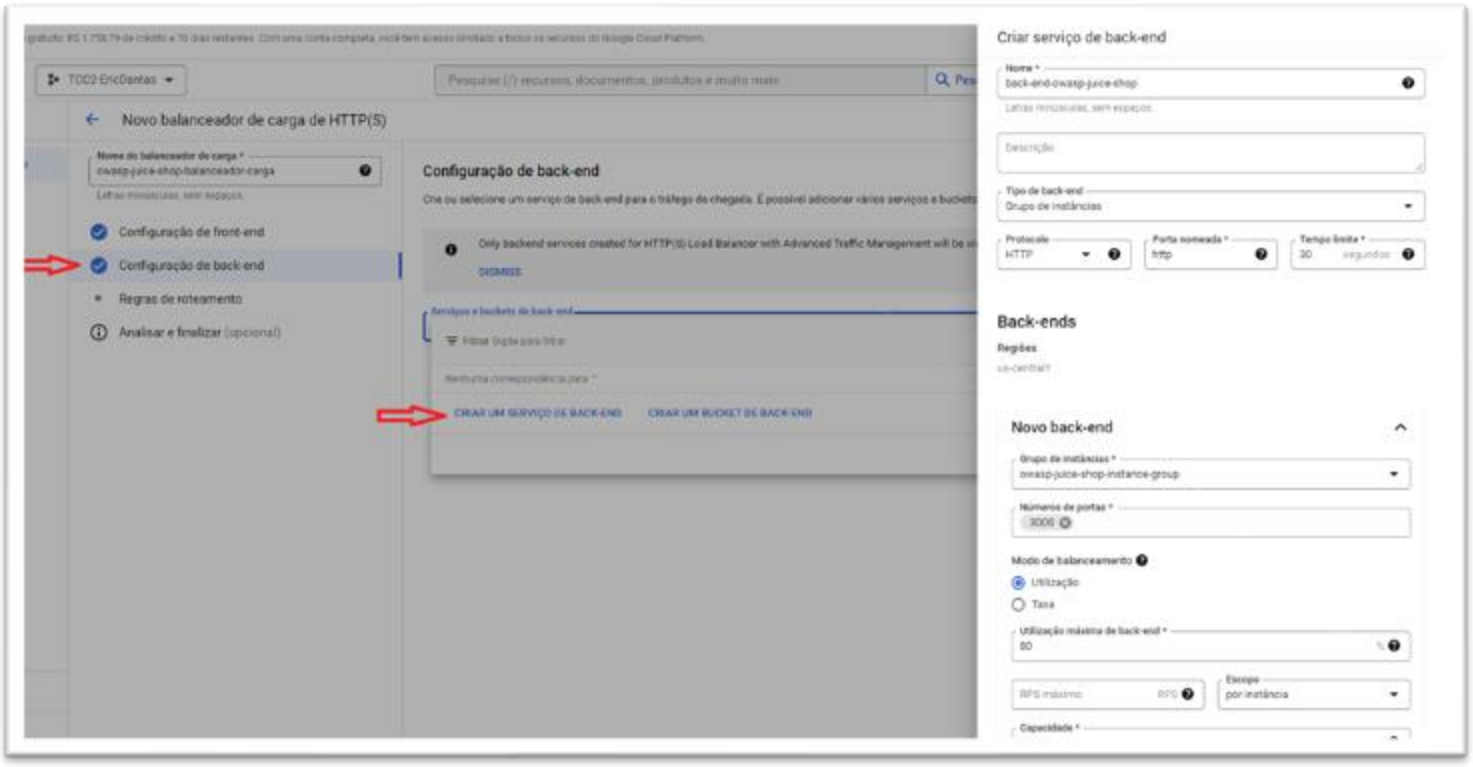
Nas Figuras 26 e 27 são mostradas as configurações usadas no balanceador de carga de HTTP(S) na parte de *front-end* e *back-end.*

Figura 26 – Configuração do balanceador de carga de HTTP(S), *front-end*



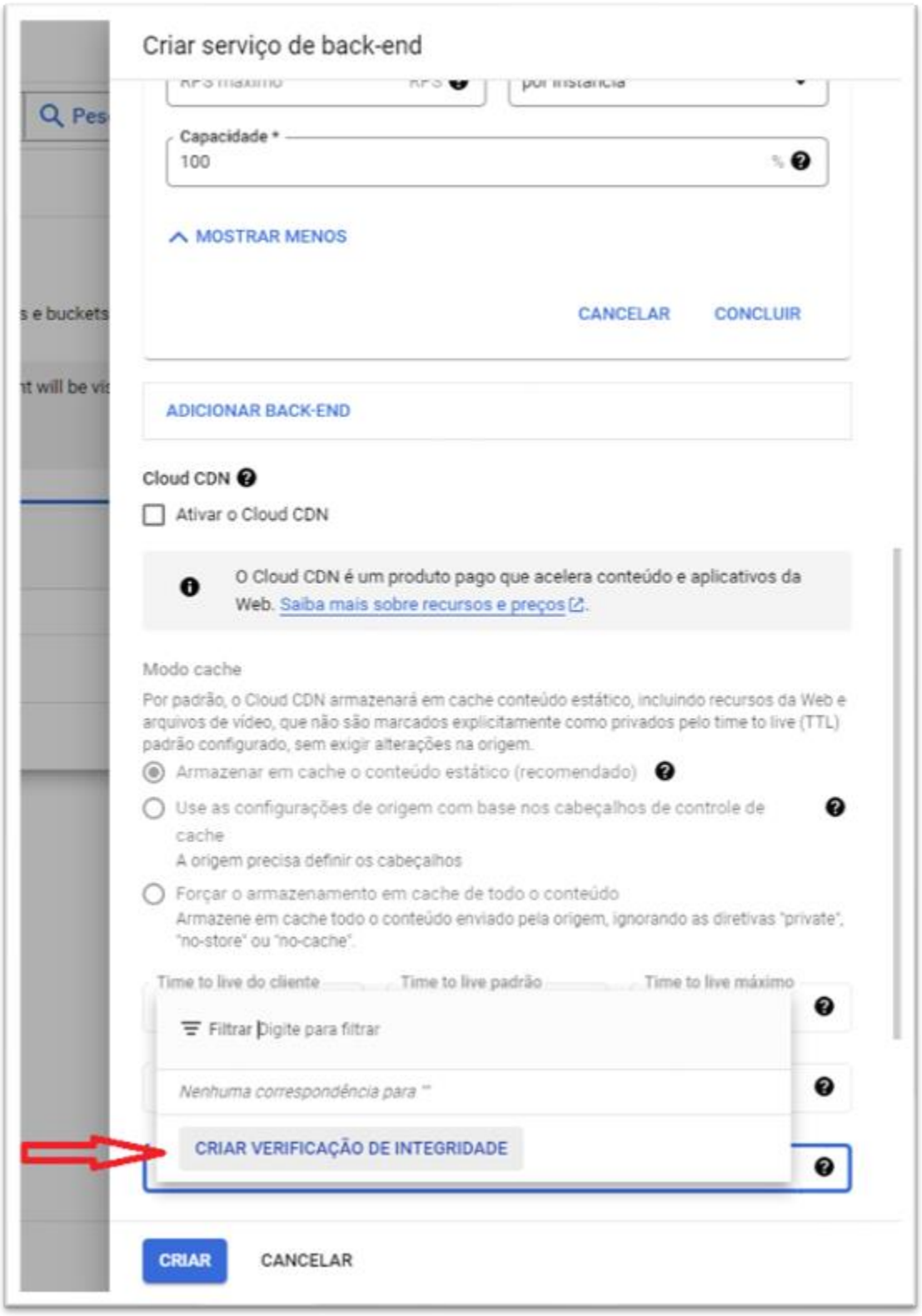
Fonte: Autoria própria, 2023.

Figura 27 – Configuração do balanceador de carga de HTTP(S), *back-end*



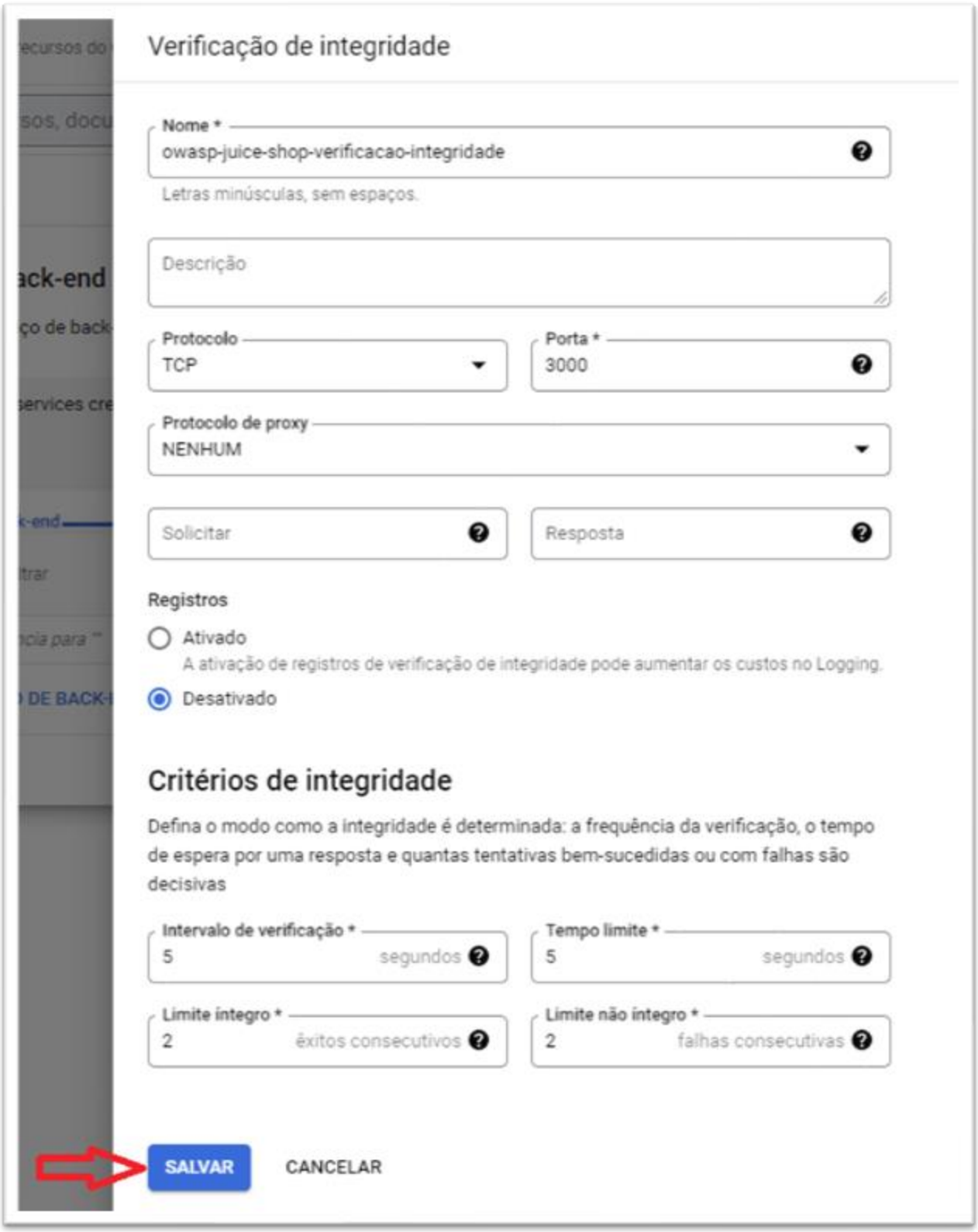
Fonte: Autoria própria, 2023.

Figura 28 – Configuração do balanceador de carga de HTTP(S), *back-end*



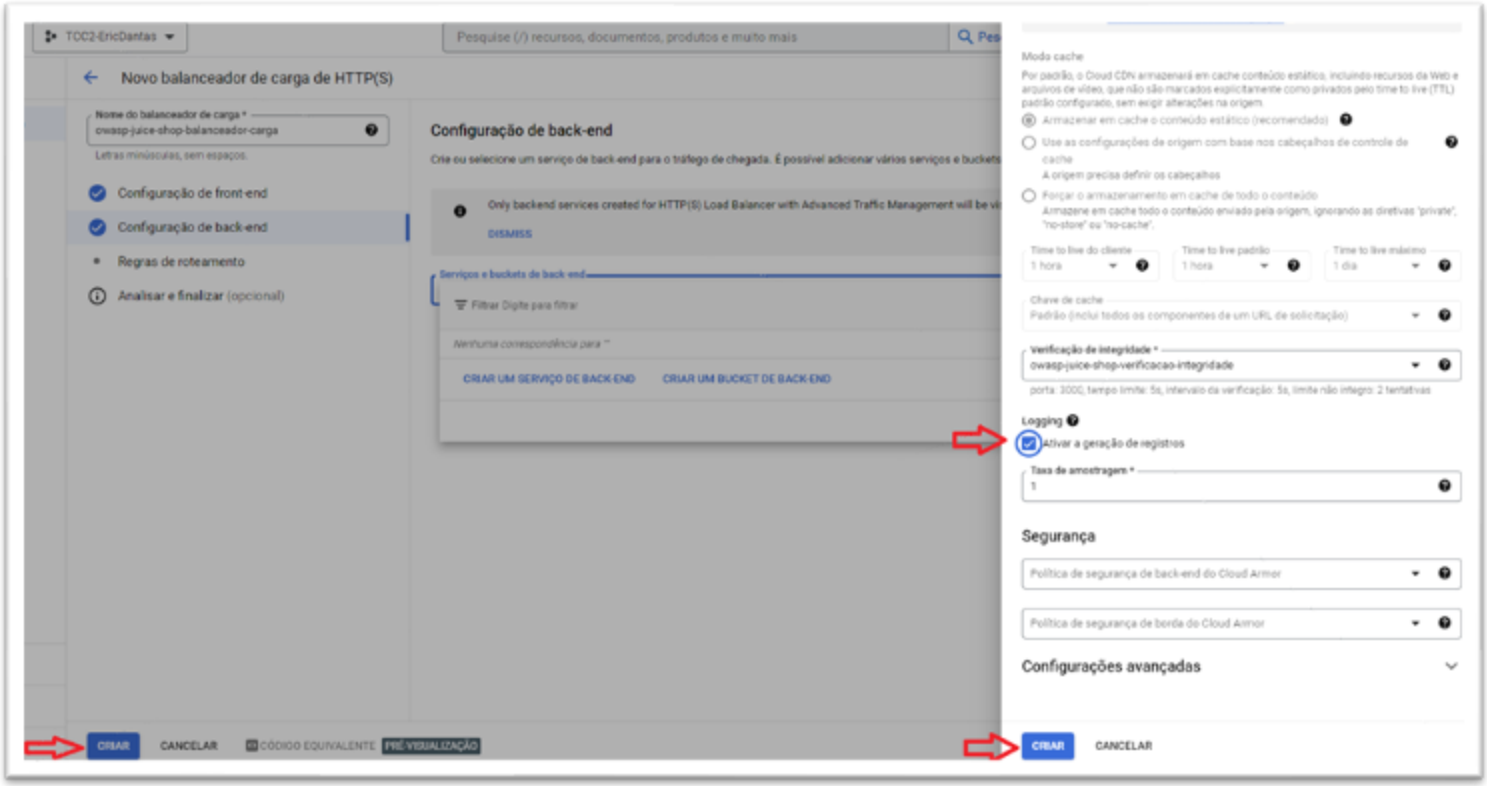
Fonte: Autoria própria, 2023.

Figura 29 – Configuração do balanceador de carga de HTTP(S), *back-end*



Fonte: Autoria própria, 2023.

Figura 30 – Configuração do balanceador de carga de HTTP(S), *back-end*



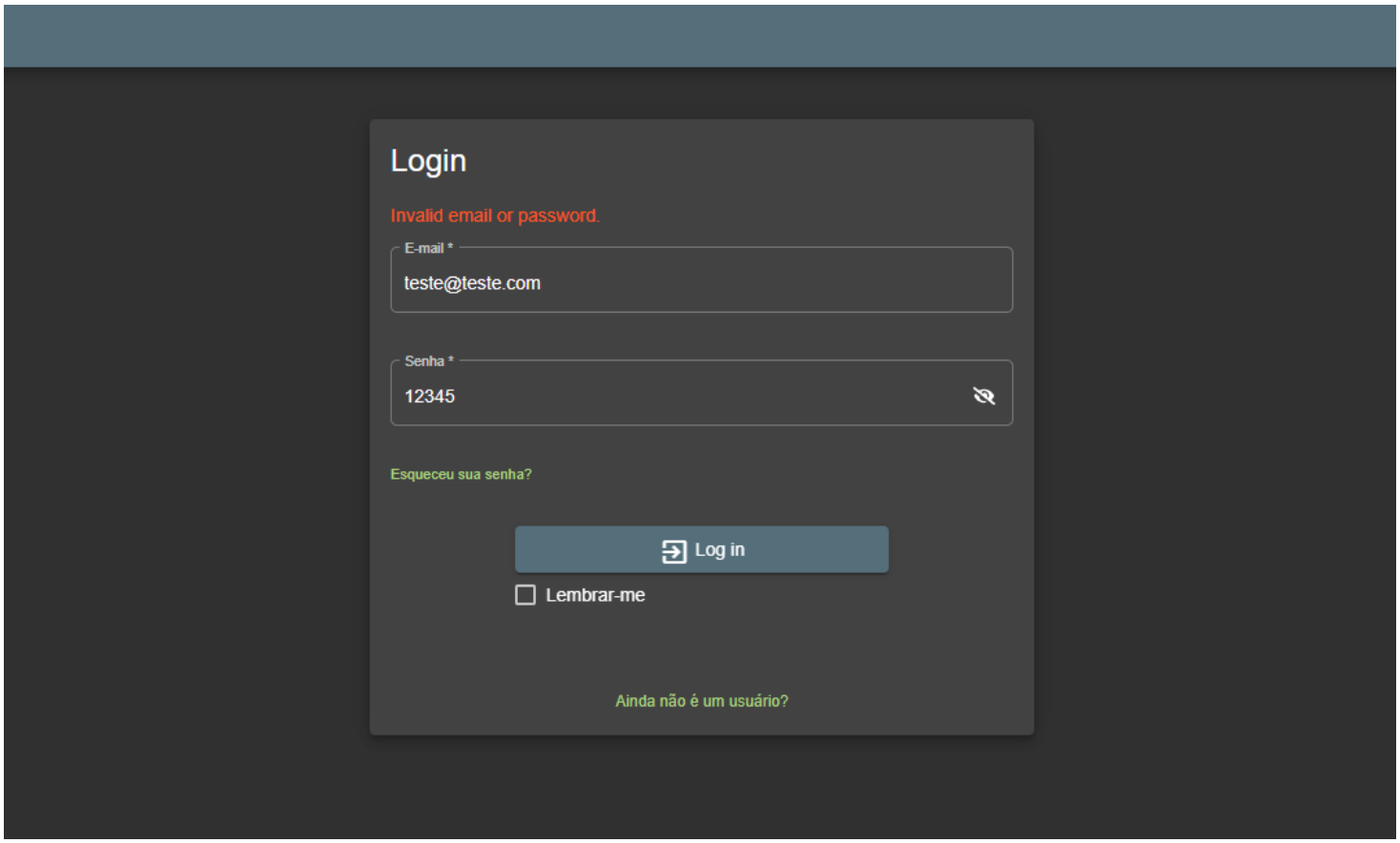
Fonte: Autoria própria, 2023.

Com o *Cloud Load Balance* configurado, agora a aplicação será acessada pelo IP do próprio balanceador de carga e não mais pelo IP da máquina virtual, que usa o protocolo HTTP e porta 80.

Com todo ambiente configurado foi realizado um ataque de injeção de SQL simples para mostrar como o *Cloud Armor* funciona com esse tipo de ataque.

Para demonstrar o ataque, foi utilizado um simples código de SQL que explora uma falha no código da aplicação, com isso foi possível fazer o login em uma conta do tipo admin. A Figura 31 mostra que ao se utilizar uma conta de e-mail “teste@teste.com” e senha “12345” recebe-se um aviso de e-mail e senha invalida.

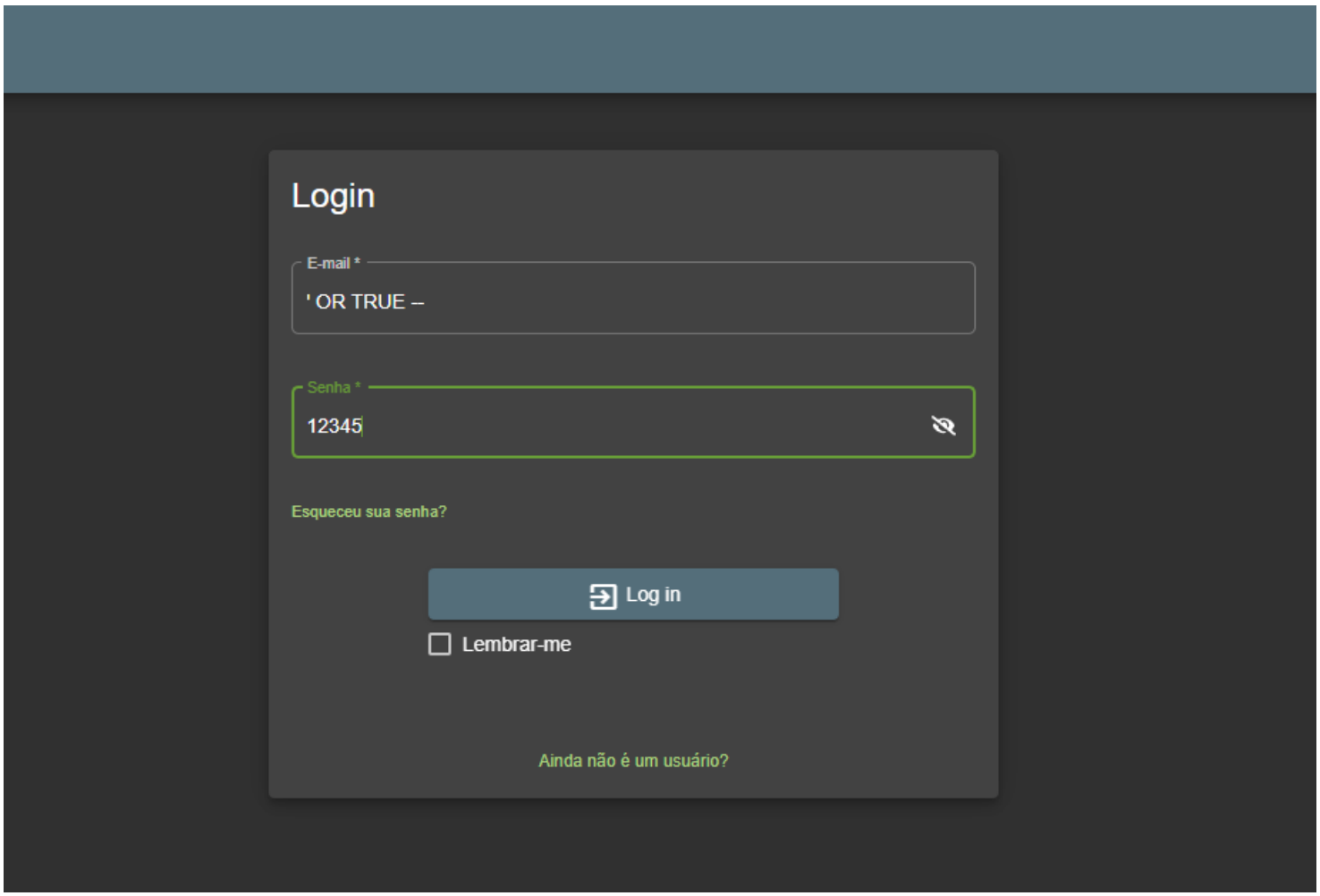
Figura 31 – Teste de acesso por login



Fonte: Adaptado da OWASP, 2023.

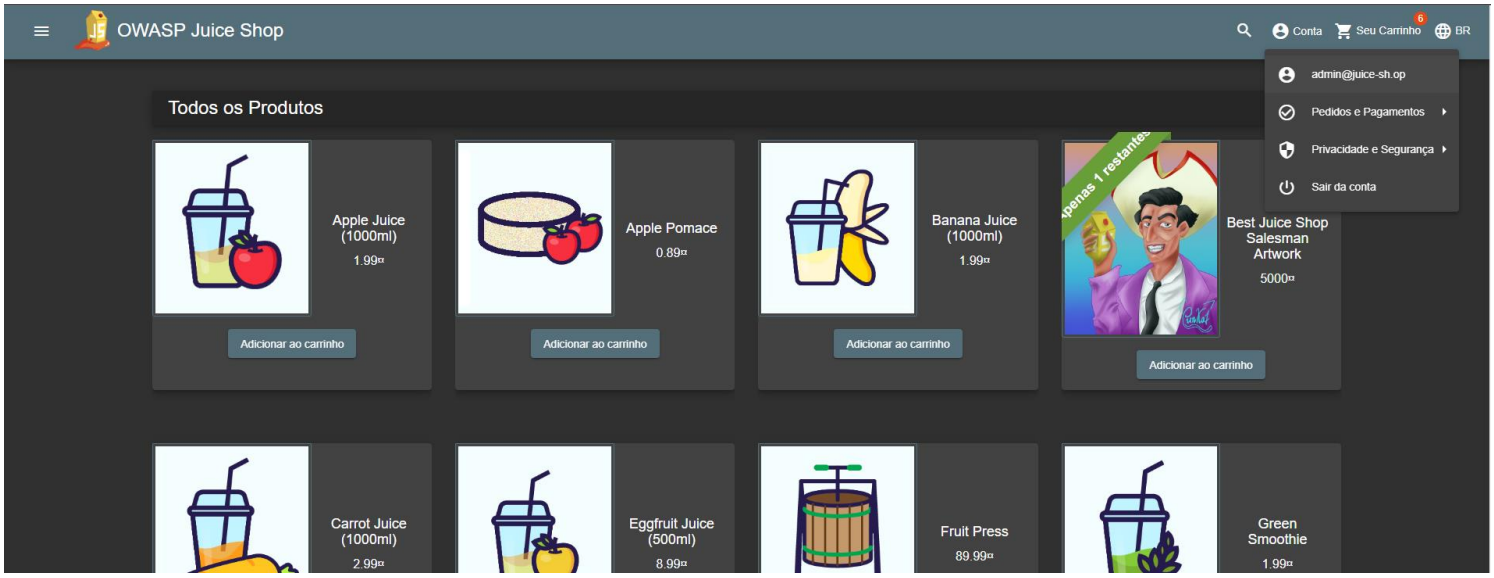
Porém ao se utilizar o código de injeção SQL “ ‘ OR TRUE – ”no campo de E-mail e usar a mesma senha “12345”, o login é feito com sucesso e em uma conta do tipo admin. Como mostrado nas figuras 32 e 33:

Figura 32 – Injeção de SQL no login



Fonte: Adaptado da OWASP, 2023.

Figura 33 – Acesso a conta *admin* por injeção de SQL



Fonte: Adaptado da OWASP, 2023.

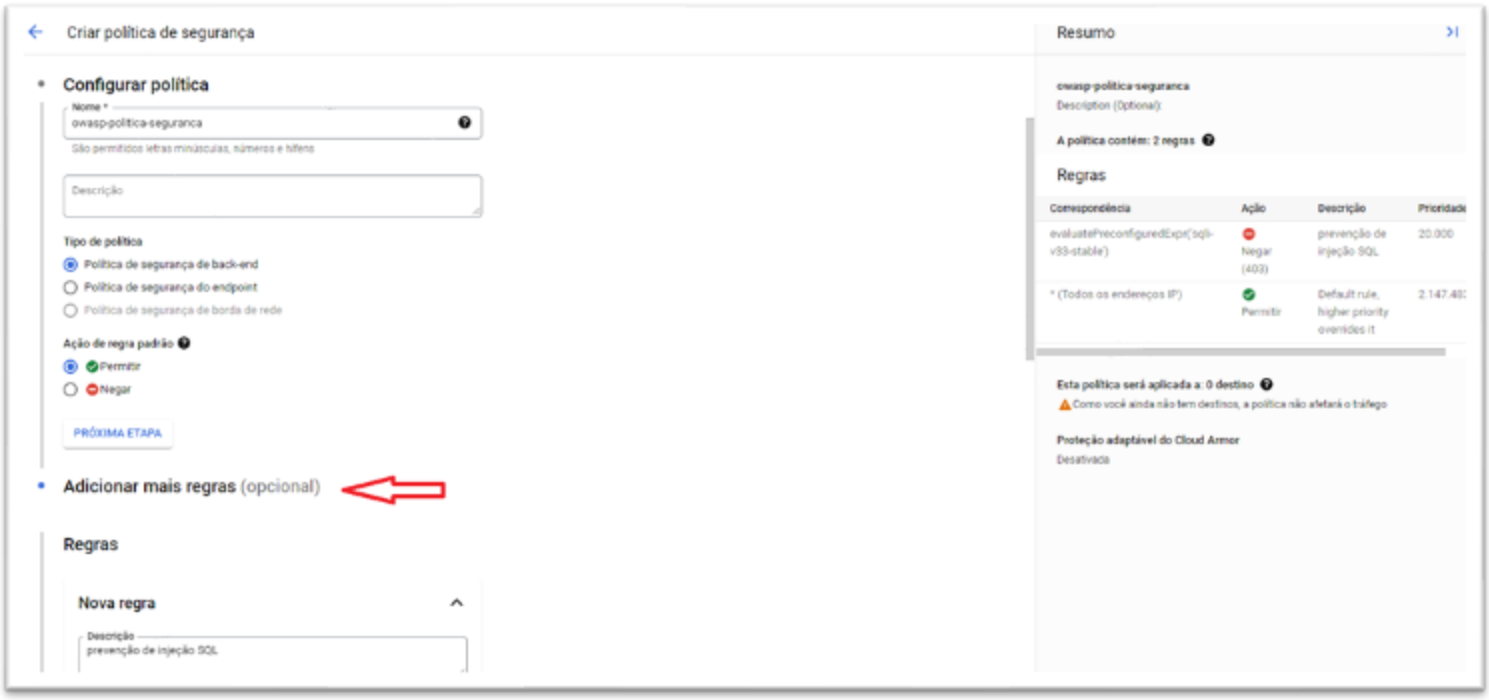
Uma solução para se resolver essa vulnerabilidade sem a necessidade de se modificar o código da aplicação é usar o *Cloud Armor*.

O *Cloud Armor* possibilita criar políticas e regras que podem ajudar a proteger contra injeção de SQL, *scripting* em vários locais, inclusão de arquivo local, ataque de injeção PHP, dentre outras.

Ao entrar na página do *Cloud Armor* deve-se criar políticas de segurança para evitar esses tipos de vulnerabilidades.

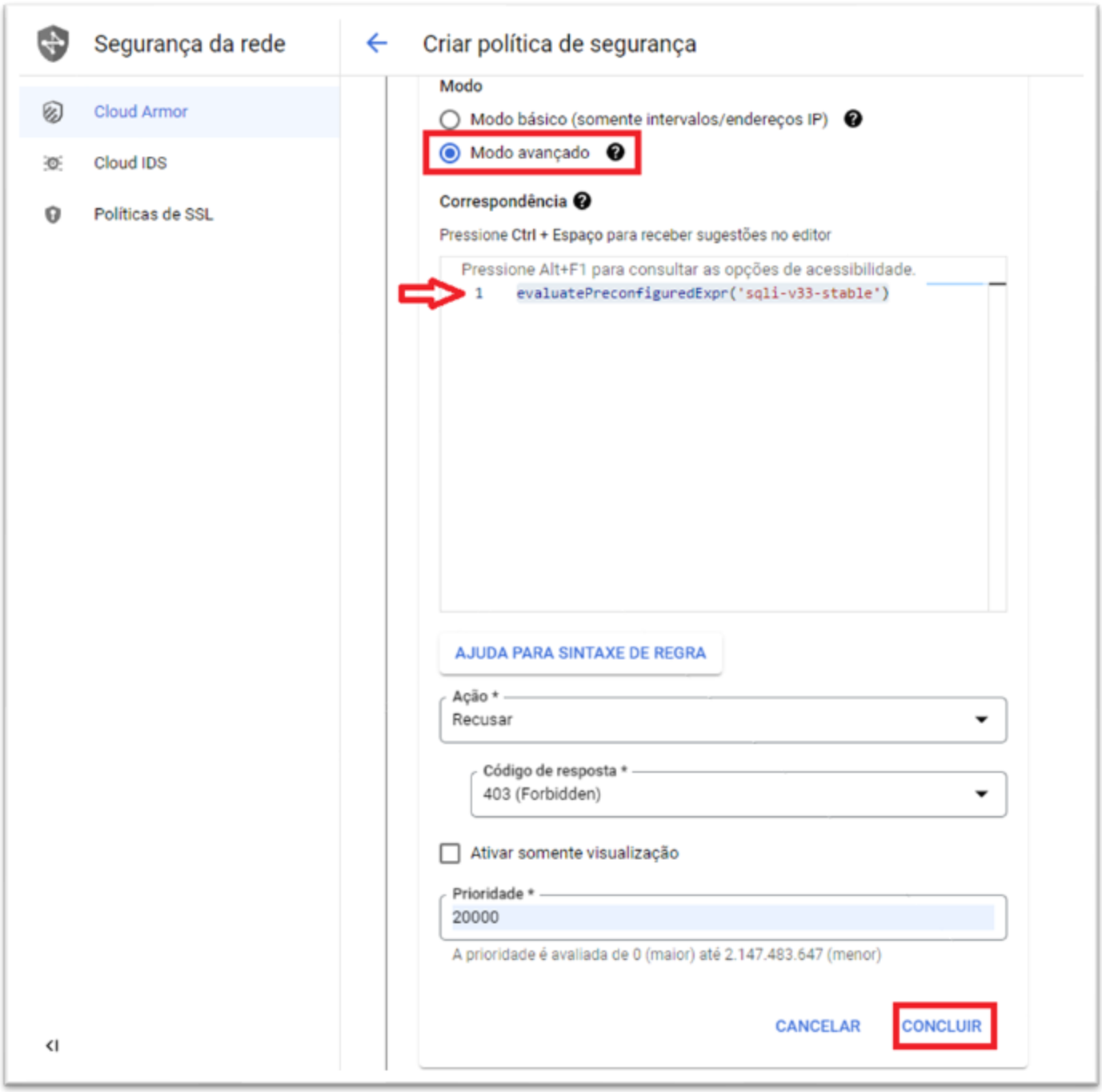
As Figuras 34, 35 e 36 mostram como foi configurado a política de segurança para barrar a injeção de SQL.

Figura 34 – Configuração de políticas de segurança no *Cloud Armor*



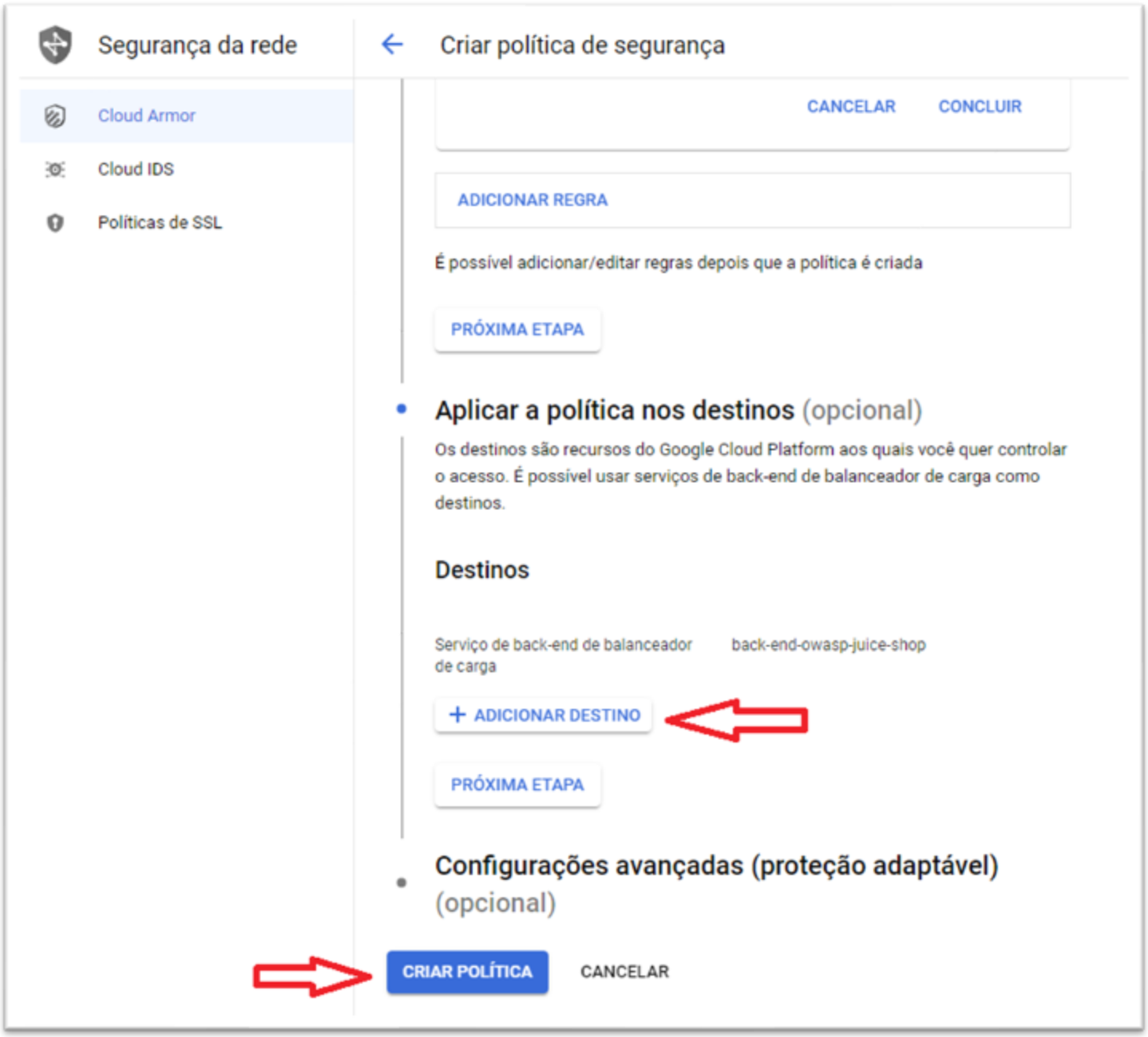
Fonte: Autoria própria, 2023.

Figura 35 – Configuração de políticas de segurança no *Cloud Armor*



Fonte: Autoria própria, 2023.

Figura 36 – Configuração de políticas de segurança no *Cloud Armor*



Fonte: Autoria própria, 2023.

A regra foi definida como política de segurança de *back-end.* Com base na documentação do próprio *Cloud Armor* foi adicionado uma nova regra. Ao selecionar o modo avançado, foi definida qual regra pré-configurada de WAF seria usada.

De acordo com a sintaxe da documentação foi utilizado o código “evaluatePreconfiguredExpr('sqli-v33-stable')”. Esse código significa que foi utilizado regras pré-configuradas do WAF de nome “sqli-v33-stable”, que se refere a proteção contra injeção de SQL. Essa regra vai ter a ação de recusar qualquer conexão feita com a aplicação mostrando o código de erro 403. Com a regra definida, deve-se adicionar o destino, que no caso será o serviço de *back-end* do balanceador de carga.

Com a utilização de regras pré-configuradas, a ocorrência de problemas de acesso a aplicação é muito comum, e caso ocorra algum problema de acesso deve-se usar o serviço *Cloud Logging* para analisar os registros e identificar qual o problema.

Neste caso duas regras dentro desse conjunto de regras pré-configurada, estão impedindo o acesso a aplicação e para identificar qual o id dessas duas regras deve-se acessar o *Cloud Logging.*

6. ANÁLISE DOS RESULTADOS OBTIDOS

Este capítulo apresenta uma discussão da parte teórica e uma parte pratica, mostrando a importância de se configurar os serviços de segurança de forma correta e como evitar um ataque do tipo injeção de código SQL.

6.1. Discussão (Parte teórica)

Devido aos *lockdowns* causado pelo agravamento da pandemia do COVID-19, a procura por infraestrutura em nuvem aumentou muito e, com isso, o aumento de crimes cibernéticos também acompanhou esse aumento, já que muitas das empresas e pessoas tinham pouco conhecimento de como se criar uma arquitetura em nuvem.

A urgência de se criar ambientes de trabalho remoto, também trouxe varias falhas de segurança, pois a falta de profissionais com experiencia causavam uma má configuração da infraestrutura em nuvem.

De acordo com a OWASP, a maioria dos ataques busca encontrar falhas em aplicações WEB, e mesmo com diversos serviços de segurança que a Google Cloud oferece, na maioria dos casos uma invasão ocorre devido ao sequestro de credenciais de algum funcionário. E os possíveis transtornos que uma invasão pode ocasionar, pode levar a uma grande perda tanto financeira como judicial, caso vaze dados sensíveis.

6.2. Como configurar os serviços (Parte prática)

O desenvolvimento da parte pratica da configuração dos serviços de segurança, foi criado utilizando a plataforma da *Google Cloud*. Em um dos serviços, foi se utilizado um site fictício de uma loja online para simular um ataque por injeção de SQL.

A injeção de um código SQL foi feita com o objetivo de:

- Efetuar o login no site com as credenciais de administrador;
- Gerar registros que serão monitorados e analisados;
- Criar regras e políticas de segurança baseadas nos registros analisados;

Os registros gerados pela injeção de código SQL, permitiu que fossem analisados quais regras e politicas de seguranças deviam ser aplicadas, possibilitando a modificação de regras já pré-definidas para melhor se adaptar a situação e as necessidades do site ou projetos.

Os responsáveis pela segurança dessas infraestruturas em nuvem devem ser treinados e alertados quanto as questões de segurança, para que possam configurar de forma correta e segura os serviços.

Desta forma, ao demonstrar como se configura alguns serviços do GCP, verificou-se que, mesmo configurando da forma correta, o próprio serviço dá sugestões de modificações nas configurações para limitar possíveis falhas de segurança. Pois, em casos de regras e permissões mal configuradas, o invasor poderia ter privilégios que poderia ocasionar em uma possível perda para a empresa.

Portanto, para prevenir que a empresa ou organização sofra uma invasão, é importante dominar o funcionamento dos serviços de segurança fornecidos pela Google Cloud e de se fazer o uso das boas práticas de segurança.

7. CONCLUSÃO

Esta monografia teve o intuito de responder a seguinte questão de pesquisa: **Quais são os serviços de segurança oferecidos pela tecnologia de *cloud computing* na *Google* e suas aplicações?**

Este estudo permitiu observar que conhecer os serviços e ferramentas de segurança oferecidas pela *Google Cloud* é essencial para se ter uma infraestrutura bem configurada e segura de ataques e vazamentos de dados. Pois a utilização de serviços como o *Google Firewall* e IAM, vão auxiliar como uma barreira para deixar o ambiente mais seguro.

Além disso, esta pesquisa possibilitou concluir que:

- Na empresa é necessário conhecer os serviços de segurança e as formas corretas de se configurar um ambiente seguro é uma maneira de se prevenir que as empresas e organizações sofram ataques. O conhecimento de protocolos e a utilização de boas práticas de segurança, ajudam a prevenir e a mitigar possíveis problemas na criação de ambientes de trabalho em nuvem;
- Os funcionários também são o elo mais fraco quando se trava de invasão, e mesmo a GCP tendo serviços de proteção contra ataques de tipo *phising* e por *bots,* o treinamento de funcionários é uma ferramenta e uma alternativa mais barata para se prevenir invasões;
- Com a migração da infraestrutura das grandes e pequenas empresas para o ambiente em nuvem, grande parte causada pela pandemia da COVID-19, os crimes cibernéticos aumentaram bastante, o que tornou a segurança dos dados ainda mais importante. O conhecimento dos serviços de segurança fornecidos pela plataforma do Google Cloud assim como as principais vulnerabilidades que uma infraestrutura em nuvem pode ter é fundamental para prevenir a invasão e o roubo de dados, diminuindo assim possíveis prejuízos e consequências para a empresa;
- E devido a grande quantidade de serviços de segurança, existem diversas soluções que podem ser adotadas para resolver e mitigar os problemas de segurança em uma infraestrutura em nuvem. Então saber como cada serviço funciona e pra qual funcionalidade ele serve ajudará a empresa a ter um ambiente

seguro e minimizar os gastos com segurança se forem usados os serviços corretos.

Dessa forma, respondendo à questão de pesquisa deste trabalho, existem várias soluções de segurança oferecidas pela *Google Cloud* que tornam o ambiente mais seguro. Entretanto, se o cliente não tiver um domínio do funcionamento de cada serviço, ele dificilmente saberá como configurar sua infraestrutura em nuvem de forma segura. Além disso, saber quais são os principais tipos de vulnerabilidades e ataques são fatores para se ter uma boa configuração de segurança com a escolha de serviços apropriados.

Para continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:

- Criar possíveis ataques para testar outros serviços de segurança;
- Criar ambientes de teste para se monitorar e analisar os logs dos ataques;

REFERÊNCIAS

AMAZON. **O que é AWS?.** Disponível em: <https://aws.amazon.com/pt/what-is-aws/>. Acesso em: 8 set. 2022, 11:24:16.

_____ . **Amazon Web Services: Visão geral dos processos de segurança.** Disponível em: <https://d1.awsstatic.com/whitepapers/pt_BR/aws-security-whitepaper.pdf?did=wp_card&trk=wp_card> . Acesso em: 11 set. 2022, 13:38:10.

CISCO. **O que é um *firewall*?.** Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html. Acessado em: 20 nov. 2022.

DA ROSA RIGHI, R.; PILLA, L. L.; CARISSIMI, A.; NAVAUX, P. A.; HEISS, H.-U. ***Parallel Processing Letters***, v. 20, n. 2, p. 123–144, 2010.

DHAMOTHARAN, Revathi, ALI, Mazhar, KHAN, Eraj, KHAN, Samee U., VASILAKOS, Athanasios V., LI, Keqin, ZOMAYA, Albert Y. ***SeDaSC: Secure data sharing in clouds*.** IEEE Syst. J. 2015.

DUAN, Qiang, YAN, Yuhong, VASILAKOS, Athanasios V.. *A survey on service-oriented network virtualization toward convergence of networking and cloud computing.* ***IEEE Transactions on Network and Service Management***, vol. 9, no. 4, p. 373 - 392, 2012.

Gartner (2018). ***The Edge Completes the Cloud: A Gartner Trend Insight Report***. 14th September 2018.

_____ . ***Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018.*** Stamford, 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018>. Acesso em 16 nov. 2022.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017.

GOOGLE CLOUD. **ISO/IEC 27017.** Disponível em: <https://cloud.google.com/security/compliance/iso-27017>. Acesso em 13 set. 2022, 08:52:22.

LATIF, Rabia, ABBAS, Haider, ASSAR, Saïd, ALI, Qasim. *Cloud Computing risk assessment: A systematic literature review.* ***Future Information Technology***, Springer, p. 285-295, Berlin, Heidelberg, 2014.

LUCENA, Felipe. **Segurança de Dados: tudo que você precisa saber.** Diferencial TI. 2017. Disponível em: <https://blog.diferencialti.com.br/seguranca-de-dados/>. Acesso em: 3 set. 2022.

MELL, P. M; GRACE, T. ***The NIST definition of cloud computing Lecture Notes in Electrical Engineering***. Gaithersbur, MD, 2011. Disponivel em: <https://doi.org/10.6028/NIST.SP.800-145>. Acesso em: 16 nov. 2022.

MUKHOPADHYAY, Nirmalya, DE, Tushar Kanti, CHATTERJEE, Dipankar. *A Novel Virtualization Enabled Cloud Infrastructural Framework for Enhancing Private Cloud Communication Security*. ***International Journal of Information Security Science***, vol. 10, no. 1, 2021.

PATEL, Nimisha, PATEL, Hiren. *Energy efficient strategy for placement of virtual machines selected from underloaded servers in compute Cloud.* ***Journal of King Saud University - Computer and Information Sciences***, vol. 32, no. 6, p. 700-708, 2020.

PRASAD, A. , RAO, S. ***A mechanism design approach to resource procurement in cloud computing.*** *IEEE Transactions on Computers*. Vol. 63, Issue 1, p. 17-30. Janeiro 2014.

RICCI, L.; CARLINI, E. *Distributed virtual environments: From client server to cloud and p2p architectures*. ***International Conference on High Performance Computing & Simulation.*** p. 8-17, 2012.

SANTIAGO, Abinoan. **Colaboração para Tilt.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2022/02/23/por-que-site-americanas-saiu-do-ar.htm>. Acesso em: 3 set. 2022.

THABIT, Fursan, ALHOMDY, Sharaf, JAGTAP, Sudhir. *A new data security algorithm for cloud computing based on genetics techniques and logical-mathematical functions.* ***International Journal of Intelligent Networks*****.** KeAi, Vol. 2, p. 18-33, 2021.

TORRES, Cesar. **Normas ISO de segurança: 27001, 27701, 27017, 27018 e 27032.** Disponível em: <https://www.webdoxclm.com/pt/blog/normas-iso-de-ciberseguranca-27001-27701-27017-27018-27032>. Acesso em: 11 set. 2022, 13:55:23.

VMWARE. **Segurança de nuvem.** Disponível em: < https://www.vmware.com/br/topics/glossary/content/cloud-security.html >. Acesso em: 10 out. 2022, 18:56:16.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação.** 2ª ed. Rio de Janeiro - RJ, 2014. cap. 4, p. 21-24.

YEO C. S., BUYYA R., POURREZA H., ESKICIOGLU R., GRAHAM P., Sommers *Cluster Computing: high-performance, high-availability, and high-throughput processing on a network of computers,* ***Springer Science+Business Media Inc.***, Vol. 29, Issue 6, p. 521–551, New York, USA, 2006.

ZAHARIA-Rădulescu A.M., RADU I. *Cloud computing and public administration: approaches in several European countries.* ***Proceedings of the International Conference on Business Excellence.*** Vol. 11, Issue 1, p. 739-749, 2017.