 Universidad de los Andes	Universidad de los Andes Maestría en Seguridad de la Información - MESI	Abril 2025
---	--	------------

PROYECTO No. 2
Controles de seguridad para una aplicación en la nube

ESTUDIANTES:
Diana María Andica Bueno - 202413738
Johanna Alexandra Villamil Salinas - 202513858
Diego Felipe Sánchez Medina – 202322998

Profesor: Jonatan Legro
Bogotá D.C
2025



 Universidad de los Andes	Universidad de los Andes Maestría en Seguridad de la Información - MESI	Abril 2025
---	--	------------

Tabla de contenido

Objetivos	3
Desarrollo de actividades	4

 Universidad de los Andes	Universidad de los Andes Maestría en Seguridad de la Información - MESI	Abril 2025
---	--	------------

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.

Desarrollo de actividades

Se realizaron las siguientes configuraciones para mejorar la postura de seguridad de la aplicación BlogueandoAndo:

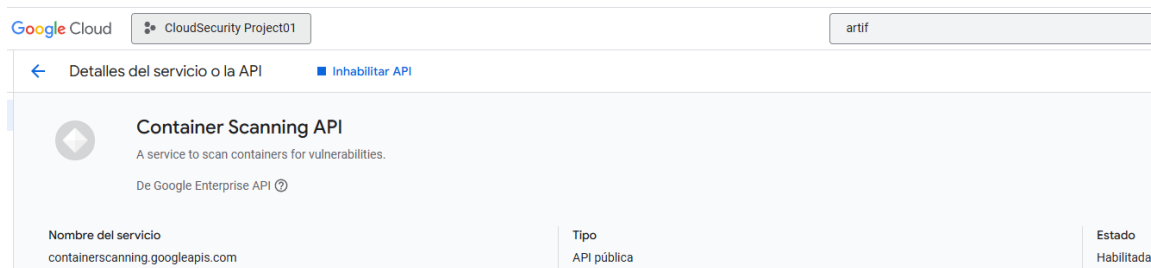
1. Análisis de Seguridad con Web Security Scanner y Artifact Analysis:

- Ejecutar análisis detallado sobre el contenedor [Artifact Analysis]

Para realizar el análisis respectivo, se deben habilitar las APIs: Artifact registry y Container Scanning API.



Se habilitó la API llamada “Container Scanning API”, el cual es un servicio para escanear contenedores en busca de vulnerabilidades.



Como nunca se ejecutó un análisis de vulnerabilidades sobre la imagen de los contenedores, es necesario volver a enviarla al registro, como se indica en la imagen.


us-central1-docker.pkg.dev > cloudsecurity-project01-202510 > my-repository > myfrontend

VERSIONES		ARCHIVOS				
<input checked="" type="checkbox"/> Ocultar artefactos alternativos de OCI		<input type="text"/> Filtro Ingresar el nombre o el valor de la propiedad				
<input type="checkbox"/>	Nombre	Descripción	Etiquetas ?	Fecha de creación ↑	Actualizado	Vulnerabilidades
<input type="checkbox"/>	3d3de730d2a0			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ? ⋮
<input type="checkbox"/>	60bcb3f9ad4a			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ? ⋮
<input type="checkbox"/>	529e21064494		v1	2 mar 2025	2 mar 2025	Nunca se realizó un análisis ? ⋮

Esta imagen nunca se analizó en busca de vulnerabilidades. Para analizar esta imagen, vuelve a enviarla al registro.

[MÁS INFORMACIÓN](#)

Para obtener los permisos que se requieren para enviar imágenes, se deben otorgar los siguientes 2 roles de IAM en el repositorio: lector de Artifact registry y escritor de artifact registry

<input type="checkbox"/> 	dianillab@gmail.com	Diana María Andica Bueno	Escritor de Artifact Registry
			Lector de Artifact Registry
			Propietario
			Usuario de instancia de Cloud SQL

Se cargan de nuevo las imágenes de los contenedores del back y del frontend en el repositorio

```
(blogueando) PS C:\Users\cesar\PycharmProjects> docker tag my-app us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myapp:v6
(blogueando) PS C:\Users\cesar\PycharmProjects> docker push us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myapp:v6
The push refers to repository [us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myapp]
5dbb3b698b72: Layer already exists
7cf63256a31a: Layer already exists
1c821c839187: Already exists
99bad17cdde1: Layer already exists
183f0922284a: Layer already exists
0c5ce2cb4ecc: Layer already exists
9ab846f2238c: Layer already exists
v6: digest: sha256:ad00c629a3e36a437ef8afbd6f9d8db3b88095ee4251919ebc486fa11880aa09 size: 856
```

```
(blogueando) PS C:\Users\cesar\PycharmProjects> docker tag my-frontend us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myfrontend:v2
(blogueando) PS C:\Users\cesar\PycharmProjects> docker push us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myfrontend:v2
The push refers to repository [us-central1-docker.pkg.dev/cloudsecurity-project01-202510/my-repository/myfrontend]
f18232174bc9: Layer already exists
0c7e4c092ab7: Layer already exists
984583bcf083: Layer already exists
8d27c072a58f: Layer already exists
24aae0483464: Already exists
5c6f71462175: Layer already exists
ccc35e35d420: Layer already exists
43f2ec460bdf: Layer already exists
ab3286a73463: Layer already exists
6d79cc6084d4: Layer already exists
v2: digest: sha256:529e21064494c98b0e29a844e0a4300b4e03a7a6abde84ae149433bc3ca8d2f9 size: 856
```

Como ya se tenía activado el análisis de vulnerabilidades, inmediatamente se ejecuta sobre el contenedor, en este caso se encontraron 6 vulnerabilidades en el contendor del frontend

Google Cloud CloudSecurity Project01 art

← Resúmenes de myfrontend BORRAR INSTRUCCIONES DE CONFIGURACIÓN

us-central1-docker.pkg.dev > cloudsecurity-project01-202510 > my-repository > myfrontend

VERSIONES

ARCHIVOS

☒ Ocultar artefactos alternativos de OCI Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre	Descripción	Etiquetas ?	Fecha de creación ↑	Actualizado	Vulnerabilidades	
<input type="checkbox"/>	3d3de730d2a0			2 mar 2025	Hace unos instantes	Nunca se realizó un análisis ?	⋮
<input type="checkbox"/>	60bcb3f9ad4a			2 mar 2025	Hace unos instantes	⚠ 6	⋮
<input type="checkbox"/>	529e21064494		v1 v2	2 mar 2025	Hace unos instantes	⚠ 6	⋮



















Se observa que hay dos vulnerabilidades de gravedad alta y 4 sin especificar

Filtro Filtrar vulnerabilidades

















Nombre	Gravedad efectiva ? ↓	CVSS ?	Corrección disponible	Estado de VEX ?	Paquete	Tipo de paquete	
CVE-2024-8176	Alto	7.5	Si	Sin especificar	expat	OS	VER CORRECCIÓN
CVE-2025-27113	Alto	7.5	Si	Sin especificar	libxml2	OS	VER CORRECCIÓN
CVE-2025-24928	Sin especificar	0	Si	Sin especificar	libxml2	OS	VER CORRECCIÓN
CVE-2025-24855	Sin especificar	0	Si	Sin especificar	libxslt	OS	VER CORRECCIÓN
CVE-2024-55549	Sin especificar	0	Si	Sin especificar	libxslt	OS	VER CORRECCIÓN
CVE-2024-56171	Sin especificar	0	Si	Sin especificar	libxml2	OS	VER CORRECCIÓN

En la última imagen del backend se encuentran 47 vulnerabilidades

us-central1-docker.pkg.dev > cloudsecurity-project01-202510 > my-repository > myapp

VERSIONES		ARCHIVOS					
<input checked="" type="checkbox"/> Ocultar artefactos alternativos de OCI		 Filtro Ingresar el nombre o el valor de la propiedad					
<input type="checkbox"/>	Nombre	Descripción	Etiquetas ?	Fecha de creación ↑	Actualizado	Vulnerabilidades	
<input type="checkbox"/>	 af21ca062f0a			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 830914b39483			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 1bf0536fa9e5		v1	2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 a74b49db7a33			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 b0850a93f2c4			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 127baa415695		v2	2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 ef7a5e71d512			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 03b5fffc1176			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 6eeb3a9cd486		v3	2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 7e17b992d513			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 bef243256aed			2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 4db0adb18335		v4	2 mar 2025	2 mar 2025	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 5d95e49d991c			2 mar 2025	hace 9 minutos	 47	
<input type="checkbox"/>	 4888e37b4c46			2 mar 2025	hace 9 minutos	Nunca se realizó un análisis ?	
<input type="checkbox"/>	 ad00c629a3e3		v5 v6	2 mar 2025	hace 9 minutos	 47	

Se observa que hay una vulnerabilidad crítica, 2 vulnerabilidades medias, 43 de gravedad baja y 1 sin especificar

 Filtro Filtrar vulnerabilidades							
Nombre	Gravedad efectiva ? ↓	CVSS ?	Corrección disponible	Estado de VEX ?	Paquete	Tipo de paquete	
CVE-2023-45853 	 Crítico	9.8	No	Sin especificar	zlib	OS	
CVE-2024-6345 	 Alto	0	Sí	Sin especificar	setuptools	Python	
CVE-2025-27516 	 Medio	0	Sí	Sin especificar	jinja2	Python	
CVE-2023-5752 	 Medio	3.3	Sí	Sin especificar	pip	Python	
CVE-2025-30258 	 Bajo	0	No	Sin especificar	gnupg2	OS	
CVE-2019-1010022 	 Bajo	9.8	No	Sin especificar	glibc	OS	
CVE-2023-50495 	 Bajo	6.5	No	Sin especificar	ncurses	OS	
CVE-2007-5686 	 Bajo	4.9	No	Sin especificar	shadow	OS	
CVE-2016-2781 	 Bajo	6.5	No	Sin especificar	coreutils	OS	
CVE-2019-1010025 	 Bajo	5.3	No	Sin especificar	glibc	OS	
CVE-2024-2236 	 Bajo	0	No	Sin especificar	libcrypt20	OS	
CVE-2010-4756 	 Bajo	4	No	Sin especificar	glibc	OS	



- Ejecutar análisis detallado sobre la aplicación web en ejecución.

Nuestra aplicación web está desplegada en Cloud Run, aunque Web Security Scanner no es compatible directamente con Cloud Run, se realizaron los siguientes pasos para hacerlo posible ya que la app es pública:

Antes que nada, debemos asegurar que la app de Cloud Run permita tráfico no autenticado:

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ gcloud run services add-iam-policy-binding myfrontend --member="allUsers" --role="roles/run.invoker" --region="us-central1"
Updated IAM policy for service [myfrontend].
bindings:
- members:
  - allUsers
  role: roles/run.invoker
etag: BwYx_HVteyg=
version: 1
```

Se habilita la API “Web Security Scanner” y se selecciona la opción Crear análisis

Cloud Web Security Scanner

Análisis de seguridad

Con Cloud Web Security Scanner puedes encontrar problemas de seguridad en tu app y evitar posibles ataques. Crea tu primer análisis para comenzar a ejecutar pruebas en tu app. [Más información](#)

[CREAR ANÁLISIS](#)

Se crea el nuevo análisis y se indica la URL pública de la aplicación

Google Cloud CloudSecurity Project01

Seguridad / Comenzar

← Crear un nuevo análisis

Nombre *

dianillab

Un nombre de usuario único para tu configuración de análisis

URL de inicio ?

Iniciando URL 1 *

https://myfrontend-613756850426.us-central1.run.app

Sin embargo, nos indica que se debe indicar una dirección IP estática, por lo tanto, se procede a asignarle una dirección estática externa para que se pueda ejecutar el análisis, para este caso, se asignó la dirección <https://35.209.172.83/>

Direcciones IP

RESERVAR DIRECCIÓN IP EXTERNA ESTÁTICA

RESERVA UNA DIRECCIÓN IP INTERNA ESTÁTICA

ACTUALIZAR

LIBERAR DIRECCIÓN ESTÁTICA

MOSTRAR PANEL DE IP

TODOS

DIRECCIONES IP INTERNAS

DIRECCIONES IP EXTERNAS

DIRECCIONES IPV4

DIRECCIONES IPV6

Filtro

Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre	Dirección IP	Tipo de acceso	Región	Tipo ↓	Versión	En uso por	Subred	Red de VPC	Nivel de red ?	Etiquetas	Acciones
<input type="checkbox"/>	bloqueando-ando	34.107.181.133	Externo		Estática	IPv4	<div>⚠ Ninguno</div>			Premium		<div></div>

Adicionalmente, se debe agregar roles para Administrador de seguridad de Compute y Administrador de red de Compute

Condición de IAM (opcional) ⓘ

+ Agregar condición de IAM

Rol
Administrador de seguridad d... ▼

Control completo de los recursos de almacenamiento de Compute Engine.

Condición de IAM (opcional) ⓘ

+ Agregar condición de IAM

Rol
Administrador de red de Com... ▼

Control completo de los recursos de red de Compute Engine.

Se debe generar un certificado ssl autoadministrado, para hacer uso de dicha IP estática, por lo tanto, se procede crear una clave privada RSA-2048

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ openssl genrsa -out 2048
```

Se puede observar la clave privada generada

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ cat 2048
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQFAASCBrkwgSlAgEAAoIBAQCuPoeissLjyFdg
H0a/tPYc2xyQot29xtzI2C7Enaj6ok3zs6lAbaKHur70ix0ON16/Jo9VogRveek
214u+1q0jVlVvKkYrYH9ceJ0MHdB2Ru48d8CZPnJPNcy138go0hzgkYkbLhPtF0I
a2OhknRnfJfvLr5iDknvV9yZL8fWgTOHlnf+KnVhKkPHgluGAnzitY2iLr49uBe8
HDERNncXvojKGLeQFnesQsDRcN5acXnEdfBxjMq6wCqR+h8bOGbI51gJKFtH9VHc
rLEPiasd2bnCV02ObEjAjuag4UMMGJOSgHTk22f41pnsuzEwALYHYW482J0mFByt
4g+kVjg/AgMBAAGCggEAAANRz55H1w/Cockk+jzoNeeCwBLqigcuylG51bFD57fe
goG2xdJyahsvHEMoYu00VkiFP5CWgtjzA6/UIjEvqsvrSyek4FICblb+97gaQOmI
7nn+q6GyWK2FmECkoqTD52LX1vR57CzScZCRbf+LlbpLENN6c9toGrXXoOpawK9N
RVFEgVnWpetF8p66e78a294QwqxNWI0CtnN1j3x8r+3iFN7H7C4PaFw4LwqEFGx
B21+MnwBTmRP32HBTJdgM05/XdHuTBcqkf13g/nGnP7qufEJv3zu8MERa71rjTU
IVpfd-rjy0WJ14D1AbTXawKGTfzmgF2CseyAu2gRRXQKBQDX6a15nfdP0UW47NixP
cm+3C/3/Vd4cqb5jceNjgwSE46PU2KpDRmzfgyIUv1/4JJ703+qliwyeHT2QVw7N
NxebSdmgtE1wJUPf3mQ1RG24PtELmL08JL1RBWoge/gg+mSzs12cfXJ2b42mkc
17vUoTtGTFNFqV3MnNgbjCjyDQKBgQD0mF0ad+ra4+90xfLYGYPrVagpmgs7C12
FmXFPc91zsdHx9JaFw9rO/AHweHdoEXKMw0x2qzq20aG1TagizfFkgROFv557
18OH0Gf21qSjzDB0CLatIR3Lbe2mEsC/Kmg0QWpuKk60jPsjwmmwlrqAQ1PvRhM
bj9hFWAI+wKBgQDPjfc0yf2r50i5VDiUxtVnWGPysmx1BtJTXnhdlkoxgv/2CgU
c+bFFKWOe1OWHt4FWBEhAgInHMTJtGauL3+p79wmlRj1lHfWg1L2P3m/6Saffff0
TjEXGKTLtdjb6K0h1sBNKoVI9QGj2A7DRblYNNW3GKGUFzPaMhuNA7E5IQKBgQCR
VFE6S10kue8gBNag3GIWS1/UBvuFjmagPugsy8CvKs0dpY8Gv8kY8TqkhBzVx/JH
2zr2H8ng3B7vH2DoqtCQ1k2BuzTc9BjyOWfM5Ggd4126ea8kEPUGjH5ZagKyp2
D+X2zJ4Vb1Fw2e/Yy1GGuo/9aNwKNCUOWUOwctONFKQBQDSuBRd9T/phG50utj0
Bbt7nRQMNViekiMyg2dVHN/En0yDdoz1ebWX0VUV/or662fcdx2N2XJ00tKcjntp
8s/1/E/ARE1E1Cm2Rsyjy1zBuqsVwAs8yb0Hdo1doUlxajfBDiFR1who0cqSH8Ezr
EC/z8Fot5/srugg+9p8bks016Q==
-----END PRIVATE KEY-----
```



También, se debe crear una clave privada ECDSA P-256

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ openssl genrsa -out 2048 2048  
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ openssl ecparam -name prime256v1 -genkey -noout -out 2048
```

A continuación, se genera el archivo de configuración de OpenSSL

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ cat <<'EOF' >certificado  
[req]  
default_bits = 2048  
req_extensions = extension_requirements  
distinguished_name = dn_requirements  
prompt = no  
  
[extension_requirements]  
basicConstraints = CA:FALSE  
keyUsage = nonRepudiation, digitalSignature, keyEncipherment  
subjectAltName = @sans_list  
  
[dn_requirements]  
countryName = Country Name (2 letter code)  
stateOrProvinceName = State or Province Name (full name)  
localityName = Locality Name (eg, city)  
o.organizationName = Organization Name (eg, company)  
organizationalUnitName = Organizational Unit Name (eg, section)  
commonName = Common Name (e.g. server FQDN or YOUR name)  
emailAddress = Email Address  
  
[sans_list]  
DNS.1 = www.blogueandoando9092.com  
DNS.2 = www.blogueandoando90.com  
  
EOF
```

Ejecuta el siguiente comando de OpenSSL para compilar un archivo de solicitud de firma de certificado (CSR)

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ openssl req -new -key 2048 \\  
-out CSR_FILE \1:~ (cloudsecurity-project01-202510) $ openssl req -new -key 2048 \\  
-config configuracion
```

Como se está creando un certificado autofirmado, se usó el siguiente comando de OpenSSL

```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ openssl x509 -req \  
-signkey 2048 \  
-in CSR_FILE \  
-out CERTIFICATE_FILE \  
-extfile configuracion \  
-extensions extension_requirements \  
-days 90  
Certificate request self-signature ok  
subject=C = CO, ST = Bogota, L = Bogota, O = Cloud, OU = Project, CN = Diana, emailAddress = d.andica@uniandes.edu.co
```

Se procede a subir y crear el certificado, que para este caso llamamos “certblogueando”, se copia el certificado y la clave privada en los campos en que se solicitan, los cuales fueron generados anteriormente



Google Cloud CloudSecurity Project01

Seguridad / Administrador de certificados / Certificados SSL / Crear certificado SSL

← Crea un certificado

Nombre *
certblogueando

Minúsculas, sin espacios.

Descripción

Información adicional

Nombres de host de DNS	www.blogueandoando9092.com, www.blogueandoando9092col.com
Vencimiento	3 jul 2025 21:05:23
Número de serie	23:97:26:42:4B:D3:B0:78:53:97: 27:54:C0:69:68:1E:8D:D1:98:5C
Emisor de certificados	Diana

Crear modo

☒ Subir certificado
Usa tus propios certificados de clave pública, cadenas de certificados y claves privadas

☐ Crear certificado administrado por Google
Google aprovisionará automáticamente un certificado SSL una vez que finalices la configuración de LB y dirijas el DNS de todos los dominios especificados a la IP asociada con el balanceador de cargas

Certificado * ②

HZzai1504V4CIQColg53FwrzrME5zATx9ScEKfVIFaeA9
EmAA/RVRxFvBA==
-----END CERTIFICATE-----

Subir

Clave privada *

Gjar3cOE07JSIEnGGhS
r2V94Q7WXIZPTV8X6TubBhV1PJQfNK/ngc==
-----END EC PRIVATE KEY-----

Subir

Crear Cancel Línea de comandos equivalente REST equivalente

Después de realizar la configuración correspondiente, se cuenta con el certificado certblogueando, para asignarlo a nuestro proyecto

Google Cloud CloudSecurity Project01

Seguridad / Administrador de certificados / Certificados SSL

Administrador de certificados [Crear certificado SSL](#) [Actualizar](#) [Borrar](#)

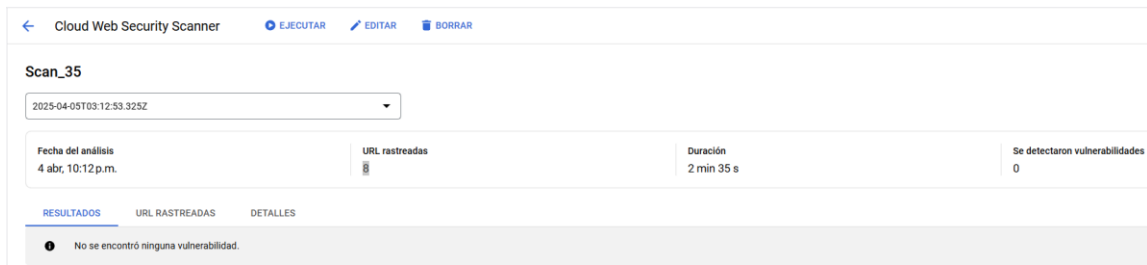
Certificados Mapas de certificados Certificados clásicos Configuración de confianza Configuración de emisión

Lista de certificados aprovisionados por Cloud Load Balancing.
[Haz clic aquí para volver a la vista de balanceadores de cargas.](#)

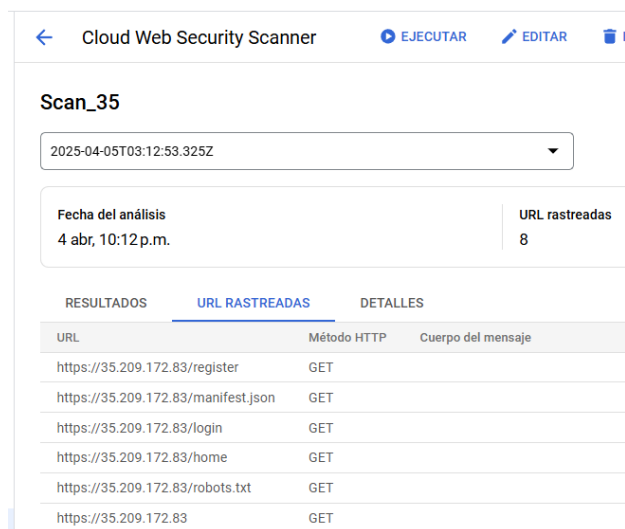
Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre ↑	Dominio	Vencimiento	Tipo	Alcance
<input type="checkbox"/>	certblogueando	www.blogueandoando9092.com, www.blogueandoando9092col.com	3 jul 2025 21:05:23	Autoadministrado	Global

Como ya se cuenta con la dirección IP estática y con el certificado SSL respectivo, ya se puede realizar el escaneo de la aplicación web, donde se puede observar que se tienen cero (0) vulnerabilidades



Se ingresa a la opción URL rastreadas y se muestra cuáles fueron evaluadas durante el escaneo



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

No se detectaron vulnerabilidades de inyección SQL o XSS, a través del escaneo que ya se realizó con Web Security Scanner.

En esta actividad se va a hacer uso de Security Health Analytics a través de Security Command Center, para detectar configuraciones inseguras o subóptimas en nuestro proyecto de GCP.

Antes de iniciar, se configuró la organización, ya que si el proyecto no pertenece a una organización no permite el uso de dicha API.

Se asignó el proyecto a la organización “blogueandoandocom.com”

blogueandoandocom.com

Buscar en proyectos y carpetas

🔍 |

Recientes
Destacados
Todos

	Nombre	ID
✓ ☆	CloudSecurity Project01 ⓘ	cloudsecurity-project01-202510
📁	blogueandoandocom.com ⓘ	696512074533

Se procede a habilitar Security Command Center y a habilitar los servicios que queremos utilizar, en este caso Security Health Analytics y Web Security Scanner

Security Health Analytics

Identifica una configuración incorrecta común de tu entorno, como firewalls abiertos, buckets públicos y, también, infracciones de CIS.

[Más información sobre Security Health Analytics](#)

✔ Habilitar

Web Security Scanner


Disponible para Premium o Enterprise

Descubre vulnerabilidades comunes, como secuencias de comandos entre sitios (XSS) y bibliotecas desactualizadas, que ponen en riesgo tus aplicaciones web.

[Más información sobre Web Security Scanner](#)

✔ Habilitar

Después de realizar las configuraciones respectivas, se cuenta con la herramienta activa


Seguridad

📌

Security Command Ce...

☰

Resumen de riesgos

🕒

Amenazas

⬇️

Vulnerabilidades

📊

Cumplimiento

📁

Recursos

🔍

Resultados

Obtén Security Command Center

✔

Seleccionar un nivel

|

✔

Seleccionar servicios

|

✔

Otorgar roles


|

4

Completar la configuración

✔

Listo para completar la configuración



En la opción resultados, se puede observar que se generaron 47 resultados para Security Health Analytics

state="ACTIVE" AND NOT mute="MUTED" AND parent_display_name="Security Health Analytics"
[EDITAR CONSULTA](#)
Intervalo de tiempo
Últimos 7 días

Filtros rápidos

[BORRAR TODO](#)

- subnetwork
 - ☐ Google Cloud resourceanemanager project 2
 - ☐ Google Cloud KMS cryptokey 1
- Gravedad
 - ☐ Low 44
 - ☐ Medium 2
 - ☐ High 1
 - ☐ Critical 0
 - ☐ Severity unspecified 0
- Nombre visible de la fuente
 - ☒ Security Health Analytics 47
- Proveedor de servicios en la nube
 - ☐ Google Cloud platform 47

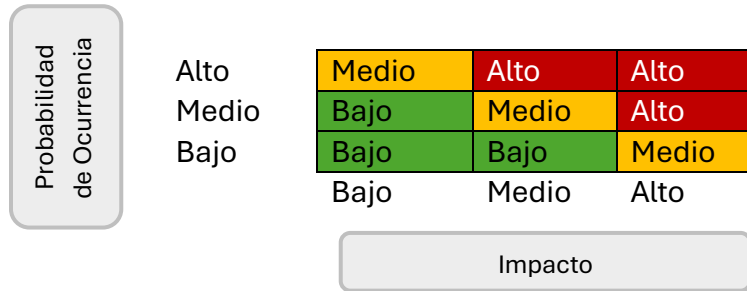
Resultados de la búsqueda

<input type="checkbox"/>	Categoría	ora del evento	Fecha de creación	Clase del resultado	Nombre visible del recurso
<input type="checkbox"/>	Private Google access disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:22	Misconfiguration	mynetwork
<input type="checkbox"/>	Flow logs disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:29	Misconfiguration	mynetwork
<input type="checkbox"/>	Flow logs disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:12	Misconfiguration	default
<input type="checkbox"/>	Flow logs disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:26	Misconfiguration	default
<input type="checkbox"/>	Flow logs disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:28	Misconfiguration	mynetwork
<input type="checkbox"/>	Private Google access disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:30	Misconfiguration	default
<input type="checkbox"/>	Flow logs disabled	6 abr 2025 8:11:21	16 abr 2025 18:17:29	Misconfiguration	default
<input type="checkbox"/>	KMS key not rotated	6 abr 2025 8:11:21	16 abr 2025 18:17:30	Misconfiguration	projects/cloudsecurity-project01-202510/locations/us-central1/keyRings/cloud-sql-keyring/cryptKeys/cloud-sql-key

Dónde se indican configuraciones inseguras sobre los recursos del proyecto, por ejemplo:

- Flow logs disabled, indica que los VPC Flow Logs están desactivados en la red mencionada (default, mynetwork) y esto impide que se registren detalles sobre el tráfico de red (fuente, destino, puerto, protocolo, etc.).
 - Private Google access disabled, lo cual nos indica que las subredes indicadas no tienen habilitado el acceso privado a servicios de Google.
 - KMS key not rotated, lo que indica que la clave KMS (en tu caso cloud-sql-key) no ha sido rotada dentro del período recomendado.
- Establecer una priorización de las vulnerabilidades para una posterior remediación.

Se estableció la correspondiente priorización de vulnerabilidades de acuerdo con la probabilidad e impacto de la vulnerabilidad, obteniendo como resultado la criticidad, utilizando el siguiente mapa de calor y el puntaje obtenido en los resultados del escaneo



Para una posterior remediación, se priorizaron las vulnerabilidades de criticidad alta y media, ya que requieren ser solucionadas con mayor urgencia debido a su alta probabilidad de ocurrencia y/o impacto.

Las vulnerabilidades de criticidad baja también deben ser atendidas, aunque pueden ser abordadas una vez se hayan resuelto aquellas de mayor criticidad

ID	Vulnerabilidad	Componente afectado	CVSS Score	Probabilidad	Impacto	Criticidad	Solución
1	MiniZip en zlib a través de 1.3 tiene un desbordamiento de enteros y desbordamiento de búfer resultante basado en heap en zipOpenNewFileInZip4_64 a través de un nombre de archivo largo, comentario o campo extra.	Backend	9.8	Alta	Alta	Alta	Actualizar componente
2	Existe una vulnerabilidad de desbordamiento de pila en la biblioteca libexpat debido a la forma en que maneja la expansión recursiva de entidades en documentos XML	Frontend	7.5	Media	Alto	Alta	Actualizar componente
3	libxml2 antes de 2.12.10 y 2.13.x antes de 2.13.6 tiene una desviación de puntero NULL en xmlPatMatch en pattern.c.	Frontend	7.5	Media	Alto	Alta	Actualizar componente
4	Una vulnerabilidad en el módulo package_index de las versiones de pypa/setuptools hasta la 69.1.1 permite la ejecución remota de código a través de sus funciones de descarga.	Backend	7.5	Media	Alto	Alta	Actualizar componente
5	Un descuido en la forma en que el entorno sandbox de Jinja interactúa con el filtro attr permite a un atacante que controle el contenido de una plantilla ejecutar código Python arbitrario.	Backend	6	Baja	Medio	Media	Actualizar componente
6	Al instalar un paquete desde una URL Mercurial VCS (es decir, «pip install hg+...») con pip antes de la v23.3, la revisión Mercurial especificada podía utilizarse para inyectar opciones de configuración arbitrarias a la llamada «hg clone» (es decir, «--config»)	Backend	6	Baja	Medio	Media	Actualizar componente

2. Revisión de Configuraciones IAM existentes:

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

Para esto, se revisaron los permisos desde la consola y se pudo observar que existen permisos excedidos para todos los usuarios



```
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ gcloud projects get-iam-policy cloudsecurity-project01-202510 \
--format=json > iam-policy.json
dianillab@cloudshell:~ (cloudsecurity-project01-202510) $ cat iam-policy.json
{
  "bindings": [
    {
      "members": [
        "user:dianillab@gmail.com"
      ],
      "role": "roles/artifactregistry.reader"
    },
    {
      "members": [
        "serviceAccount:service-613756850426@gcp-sa-artifactregistry.iam.gserviceaccount.com"
      ],
      "role": "roles/artifactregistry.serviceAgent"
    },
    {
      "members": [
        "user:dianillab@gmail.com"
      ],
      "role": "roles/artifactregistry.writer"
    }
  ]
}
```

Se puede observar con mayor detalle en la interfaz de usuario, donde se observa que los usuarios cuentan con permisos excedidos

IAM

[Más inform...](#)

Permitir	Rechazada	Historial de recomendaciones			Estadísticas
<input type="checkbox"/> Tipo	Principal	Nombre	Rol		
<input type="checkbox"/>	613756850426-compute@developer.gserviceaccount.com	Default compute service account	Propietario		10929/10937 permisos
<input type="checkbox"/>	alexa555.JV@gmail.com		Administrador de Secret Manager		9222/9625 permisos
			Editor		10512/10933 permisos
			Propietario		10846/10933 permisos
<input type="checkbox"/>	dfsanchezme@gmail.com		Propietario		
			Usuario con acceso a secretos de Secret Manager		
<input type="checkbox"/>	dianillab@gmail.com	Diana María Andica Bueno	Administrador de gestión de Cloud Security Command Center		
			Administrador de Secret Manager		
			Administrador de seguridad de Compute		
			Escritor de Artifact Registry		

- 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. Documentar pruebas y resultados.

Como ya se cuenta con una lista de usuarios como se mostró en el punto anterior, se van a tomar las recomendaciones de la plataforma para usar solamente los permisos que se requieren y que se han utilizado en los últimos días

Por ejemplo, para el usuario 613756850426-compute@developer.gserviceaccount.com, se van a dejar configurados sólo los permisos que se han utilizado y se van a desactivar los demás permisos que nunca se han utilizado.

Permisos para 613756850426-compute@developer.gserviceaccount.com

Proyecto: CloudSecurity Project0

Permisos actuales para la función Propietario	
Último análisis 4/4/25	1 cloudsql.instances.connect 2 cloudsql.instances.get 3 logging.logEntries.create 4 monitoring.timeSeries.create
Permisos no utilizados	5 accessapproval.requests.approve 6 accessapproval.requests.dismiss 7 accessapproval.requests.get 8 accessapproval.requests.invalidate 9 accessapproval.requests.list 10 accessapproval.serviceAccounts.get 11 accessapproval.settings.delete 12 accessapproval.settings.get 13 accessapproval.settings.update 14 accesscontextmanager.accessLevels.create 15 accesscontextmanager.accessLevels.delete

Se realizaron dichas acciones para todos los usuarios, obtenido como resultado que cada uno cuenta con los permisos necesarios y de menor privilegio sobre el proyecto, como se observa ya no se tiene el mensaje de “permisos excedidos” en los usuarios IAM

Permitir	Rechazada	Historial de recomendaciones	
<input type="checkbox"/>		613756850426-compute@developer.gserviceaccount.com	Default compute service account Cliente de Cloud SQL Lector de Cloud SQL Monitoring Snooze Editor Visualizador de registros
<input type="checkbox"/>		alexa555.JV@gmail.com	Administrador de Secret Manager
<input type="checkbox"/>		cuenta-m-nima-para-mi-app@cloudsecurity-project01-202510.iam.gserviceaccount.com	Cuenta mínima para mi-app Creador de objetos de Storage Usuario con acceso a secretos de Secret Manager Usuario de instancia de Cloud SQL Visualizador de objetos de Storage
<input type="checkbox"/>		d.andica@blogueandoandocom.com	Administrador de cuenta de servicio Administrador del centro de seguridad Propietario
<input type="checkbox"/>		dfsanchezme@gmail.com	Usuario con acceso a secretos de Secret Manager
<input type="checkbox"/>		dianillab@gmail.com	Diana María Andica Bueno Administrador de gestión de Cloud Security Command Center Administrador de Secret Manager Administrador de seguridad de Compute Escritor de Artifact Registry Lector de Artifact Registry



3. Load Balancing y Controles de red:

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

Se creó el balanceador “serverless-lb”

Google Cloud CloudSecurity Project01

Balaneo de cargas [+ CREAR BALANCEADOR DE CARGAS](#) [ACTUALIZAR](#) [BORRAR](#)

BALANCEADORES DE CARGAS BACKENDS FRONTENDS POLÍTICAS DE LB DE SERVICIOS

Rendimiento web más rápido y mayor protección web con Cloud CDN y Cloud Armor. [Más información](#)

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre	Tipo de balanceador de cargas	Tipo de acceso	Protocolos	Región	Backends
<input type="checkbox"/>	serverless-lb	Aplicación (clásico)	Externo	HTTPS	us-central1	✓ 1 servicio de backend (0 grupos de instancias, 1 grupo de extremos de red)

serverless-lb

Balanceador de cargas de aplicaciones clásico

Rendimiento web más rápido y mayor protección web con Cloud CDN y Cloud Armor. [Más información](#)

DETALLES MONITORING ALMACENAMIENTO EN CACHE MIGRACIÓN

Frontend

Protocolo	IP:Puerto	Certificado	Mapa de certificados	Política de SSL	Nivel de red
HTTPS	35.209.172.83:443	certblogueando		Predeterminada de GCP	Estándar

Reglas de host y ruta

Hosts	Rutas	Backend
Todos los que no coincidan (predeterminado)	Todos los que no coincidan (predeterminado)	blog-backend-lb

- 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.

Se crearon 3 reglas para permitir el tráfico necesario de internet al frontend, del frontend al backend y del backend a la base de datos.



[Actualizar](#) [Configurar registros](#) [Borrar](#)

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre	Tipo	Destinos	Filtros	Protocolos/puertos	Acción	Prioridad	Red ↑	Registros
<input type="checkbox"/>	allow-ingress-from-lap	Entrada	Aplicar a	Intervalos de IP:	tcp:22, 3389	Permitir	1000	default	Desactivado
<input checked="" type="checkbox"/>	allow-internet-to-frontend	Entrada	frontend	Intervalos de IP:	tcp:443	Permitir	1000	default	Desactivado
<input type="checkbox"/>	allow-port-4000	Entrada	Aplicar a	Intervalos de IP:	tcp:4000	Permitir	1000	default	Desactivado
<input checked="" type="checkbox"/>	allow-traffic-frontend-to-backend	Entrada	backend	Etiquetas:	tcp:8080	Permitir	1000	default	Desactivado
<input type="checkbox"/>	fw-allow-health-check	Entrada	allow-health-	Intervalos de IP:	tcp:80	Permitir	1000	default	Desactivado
<input type="checkbox"/>	www-firewall-network-lb	Entrada	network-lb-	Intervalos de IP:	tcp:80	Permitir	1000	default	Desactivado
<input checked="" type="checkbox"/>	allow-backend-to-cloudsql	Salida	bd-cloud-sql	Intervalos de IP:	tcp:3306	Permitir	1000	default	Desactivado

- Bastion host para acceder a los recursos.

Se crea el bastion host

Instancias de VM

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Estado	Nombre ↑	Zona	Recomendaciones	En uso por	IP interna	IP externa	Conectar
<input type="checkbox"/>		bastion-host	us-central1-a			10.128.0.2 (nic0)	34.45.185.0 ↗ (nic0)	SSH ▼

Se crea una regla de firewall para permitir solo acceso SSH (puerto 22) desde IPs seguras

<input type="checkbox"/>	allow-ssh-to-bastion	Entrada	bastion	Intervalos de IP:	tcp:22	Permitir	1000	mynetwork	Desactivado
--------------------------	--------------------------------------	---------	---------	-------------------	--------	----------	------	---------------------------	-------------

4. Google Secret Manager:

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

Para configurar Secret Manager, es necesario habilitar las APIs y los servicios correspondientes en la consola de Google Cloud. Esto permitirá que el sistema acceda a las funcionalidades de gestión de secretos y garantice su correcta integración con otras aplicaciones o servicios.



Google Cloud CloudSecurity Project01

Detalles del producto

Secret Manager API

Google Enterprise API

Stores sensitive data such as API keys, passwords, and certificates.
Provides convenience while...

ADMINISTRAR PROBAR ESTA API API habilitada

DESCRIPCIÓN GENERAL PRECIOS DOCUMENTACIÓN PRODUCTOS RELACIONADOS

Descripción general

Stores sensitive data such as API keys, passwords, and certificates.
Provides convenience while improving security.

Detalles adicionales

Tipo: [SaaS & APIs](#)

En Secret Manager, se puede acceder al administrador de secretos, una herramienta centralizada que permite gestionar y almacenar de manera segura los secretos del proyecto. A través de esta interfaz, es posible crear, actualizar y controlar el acceso a nuevos secretos, garantizando así su protección y disponibilidad para las aplicaciones y servicios del proyecto.

Google Cloud CloudSecurity Project01

Seguridad / Secret Manager

Administrador de secretos

El administrador de secretos te permite almacenar, administrar y proteger el acceso a los secretos de tu aplicación. [Más información](#)

Elige Secrets regionales si tus datos secretos están sujetos a estrictos requisitos reglamentarios o de cumplimiento, como FedRAMP High o Impact Level 4 (IL4).

+ CREAR SECRETO + CREAR SECRET REGIONAL

Presentamos el administrador de parámetros

El administrador de parámetros asiste en la administración de parámetros de configuración, almacenamiento, acceso y ciclo de vida relacionados con la implementación de carga de trabajo. [Más información](#)

IR AL ADMINISTRADOR DE PARÁMETROS

Al crear un nuevo secreto en Secret Manager, es necesario proporcionar un nombre único y asignar un valor al secreto, que representará la información sensible a almacenar. Estos detalles son fundamentales para poder identificar y gestionar correctamente el secreto en el futuro. Además, es recomendable definir etiquetas y permisos de acceso apropiados para asegurar que solo los usuarios o servicios autorizados puedan consultar o modificar dicho secreto.

la página superior

Detalles del secreto

Esta acción creará un Secret con el valor del Secret de la primera versión. [Más información](#)

Nombre *
password

El nombre debe poder identificarse y ser único en este proyecto.

Valor secreto

Ingresa tu valor secreto o impórtalo directamente desde un archivo.

Subir archivo EXPLORAR

Tamaño máximo: 64 KiB ?

Valor secreto
xyzpdq

1

Suma de verificación CRC-32C: 0xE5DFEC7F ?

Dentro de las etiquetas, es crucial añadir tanto la clave como el valor correspondientes, ya que estos elementos son esenciales para clasificar y gestionar correctamente el secreto. Una vez completada esta información, se podrá proceder a guardar el secreto de manera segura. En el contexto de la aplicación desarrollada, se almacenaron claves API y credenciales de bases de datos como secretos, garantizando su protección y permitiendo un acceso controlado solo a los servicios o usuarios autorizados.



/ Secret: password / Editar Secret

← Editar Secret

Retrasar la destrucción de la versión del secreto

De forma predeterminada, las versiones del secreto se destruyen inmediatamente luego de solicitarlo. Para demorar la destrucción de las versiones del secreto, selecciona **Establecer** la demora en la destrucción que está debajo. Si especificas la duración de la demora en la destrucción, la destrucción de una versión del secreto inhabilitará inmediatamente la versión y programará la destrucción después de la duración especificada. [Más información](#)

☐ Definir la duración de la destrucción demorada

Etiquetas ?

Utiliza etiquetas para organizar y categorizar tus secretos.

Clave 1
team

Valor 1
acme

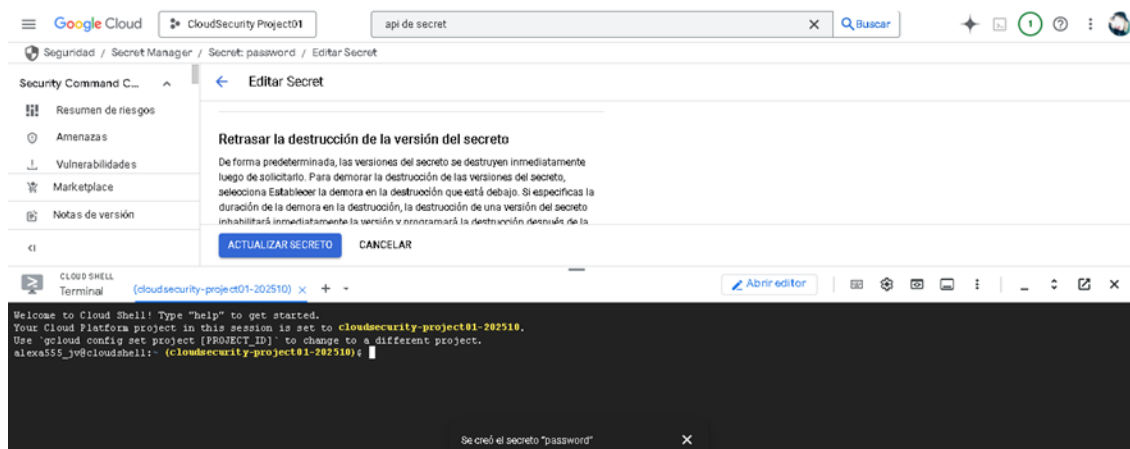
+ AGREGAR UNA ETIQUETA

ACTUALIZAR SECRETO CANCELAR

Se creó el secreto "password" X

- [Habilitar el versionado de secretos para facilitar la gestión de cambios.](#)

Para habilitar el versionado de secretos en Secret Manager, se debe ejecutar el siguiente comando: `gcloud secrets versions access 2 --secret="password"`. Este comando permite acceder a una versión específica del secreto, en este caso, la versión 2 del secreto denominado 'password'. Utilizar el versionado facilita el control de cambios y la recuperación de versiones anteriores de los secretos, asegurando así una gestión más eficiente y segura de la información sensible.



Al ejecutar el comando anterior, se logrará la activación exitosa de la versión solicitada del secreto. Este proceso confirma que el acceso al secreto y su versión específica se ha realizado correctamente, lo que garantiza que la información sensible esté disponible para su uso conforme a las políticas de seguridad establecidas. Si el comando se ejecuta correctamente, se mostrará un mensaje de confirmación que indica que la operación fue exitosa.

Seguridad / Secret Manager / Secret: password / Editar Secret

← Editar Secret

Retrasar la destrucción de la versión del secreto

De forma predeterminada, las versiones del secreto se destruyen inmediatamente luego de solicitarlo. Para demorar la destrucción de las versiones del secreto.

ACTUALIZAR SECRETO CANCELAR

(cloudsecurity-project01-202510) x + - Editor

```

Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to cloudsecurity-project01-202510.
Use 'gcloud config set project [PROJECT_ID]' to change to a different project.
alexa555_jv@cloudshell:~ (cloudsecurity-project01-202510) $ gcloud secrets versions access
l --secret="password"
xyzpdqalexa555_jv@cloudshell:~ (cloudsecurity-project01-202510) $ ||
  
```

Se creó el secreto "password" X

La activación del versionado de secretos podrá ser visualizada directamente en Secret Manager, donde se mostrará una lista de todas las versiones disponibles para cada secreto. Esta interfaz permite realizar un seguimiento detallado de los cambios y gestionar fácilmente las versiones activas, lo que facilita la administración de secretos y asegura un acceso controlado a la información sensible en todo momento.

Google Cloud CloudSecurity Project01 api de secret Buscar

Seguridad / Secret Manager / Secret: password / Versiones

← Secret: "password" EDITAR SECRET BORRAR

projects/613756850425/secrets/password

DESCRIPCIÓN GENERAL VERSIONES PERMISOS REGISTROS

Versiones + VERSIÓN NUEVA HABILITAR INHABILITAR DESTRUIR

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Versión	Alias	Estado	Destrucción programada para el	Encriptación	Fecha de creación	Acciones
<input type="checkbox"/>	1	-	Habilitada	-	Administrada por Google	6/4/25, 00:24	

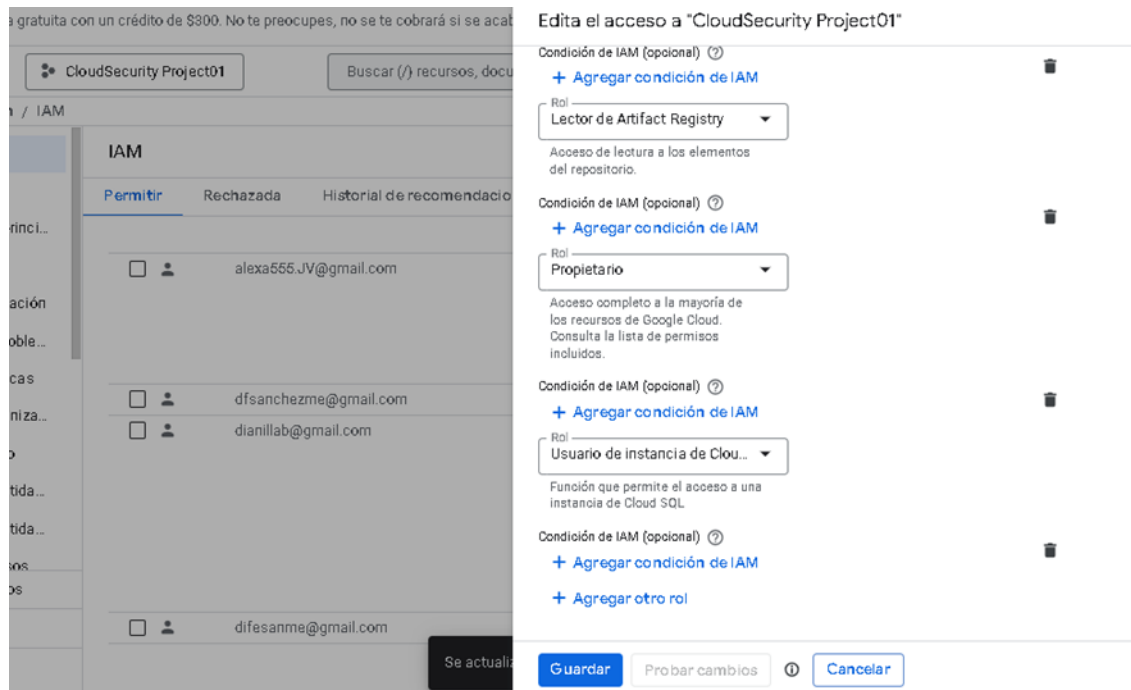
No se seleccionaron versiones



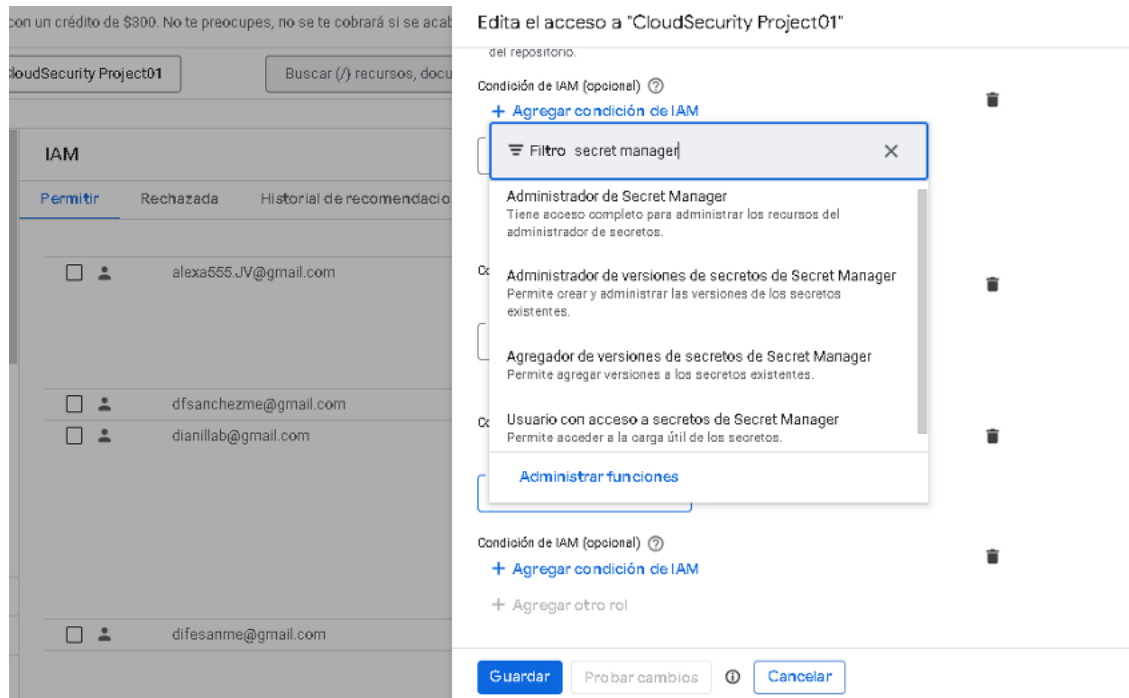
5. Roles y Permisos:

- Establecer roles específicos en IAM para limitar el acceso a secretos según las responsabilidades del equipo:
 - roles/secretmanager.admin para administradores.

A través de la gestión de IAM (Identity and Access Management) y en la sección correspondiente, se pueden visualizar los diferentes usuarios, junto con los roles y permisos asignados a cada uno. Esta herramienta permite administrar de manera eficiente los accesos y garantizar que los usuarios tengan los privilegios adecuados según sus funciones y necesidades dentro de la plataforma.



En la sección 'Seleccionar rol', se debe buscar y asignar el rol correspondiente. En el caso de los administradores, se debe seleccionar el rol 'roles/secretmanager.admin', el cual otorga los permisos necesarios para gestionar los secretos en la plataforma de manera segura y eficiente."



De esta manera, se asignará al usuario **dianillab@gmail.com** el rol de administrador de **Secret Manager**, otorgándole los permisos necesarios para gestionar y administrar los secretos dentro de la plataforma, garantizando un control adecuado sobre los recursos y la seguridad.



- roles/secretmanager.secretAccessor para servicios y usuarios que necesitan acceso a secretos.

El usuario **dfsanchez@gmail.com** será utilizado para aquellos usuarios que no desempeñan funciones de administración, pero que requieren acceso a **Secret Manager**. A

este usuario se le asignarán permisos específicos que le permitan acceder a los secretos necesarios para su trabajo, sin otorgarle privilegios administrativos adicionales."

<input type="checkbox"/>	alex555 JV@gmail.com	Johanna Villamil	Administrador de Secret Manager		
			Editor	9185/9582 permisos excedidos	▼
			Propietario	10474/10889 permisos excedidos	▼
			Usuario de instancia de Cloud SQL		
<input type="checkbox"/>	dfsanchezme@gmail.com		Propietario	10802/10889 permisos excedidos	▼
			Usuario con acceso a secretos de Secret Manager		
<input type="checkbox"/>	dianillab@gmail.com		Administrador de red de Compute		
			Administrador de Secret Manager		
			Administrador de seguridad de Compute		
			Escritor de Artifact Registry		
			Lector de Artifact Registry		
			Propietario	10490/10892 permisos excedidos	▼
			Usuario de instancia de Cloud SQL		

6. Rotación de Claves:

- Implementar políticas de rotación automática de claves cada 90 días utilizando funciones de rotación en Secret Manager.

Para implementar políticas de rotación automática de claves, se comienza con la creación de un 'llavero de claves' denominado **projectkeys**, el cual debe configurarse adecuadamente. Esta configuración permitirá gestionar de forma segura las claves, asegurando que su rotación se realice de manera periódica y automática, mejorando así la seguridad de las aplicaciones al evitar el uso prolongado de las mismas claves.



Grupos de Claves / Llaveros de Claves / Crear llavero de claves

← Crear un llavero de claves

Los llaveros de claves sirven para agrupar claves y mantenerlas organizadas. En el siguiente paso, crearás claves que se agrupan en este llavero. [Más información](#)

Nombre del proyecto

cloudsecurity-project01-202510

Nombre del llavero de claves *

projectkeys

Tipo de ubicación ?

☒ Región

Latencia más baja dentro de una sola región

☐ Multirregional

Disponibilidad máxima en el área más amplia

Región *

us-east1 (Carolina del Sur)

CREAR

CANCELAR

Una vez creado el llavero de claves, se procederá a generar las claves correspondientes, configurándolas según el uso específico que se les dará.

CloudSecurity Project01

Buscar (/) recursos, documentos, productos y más

tración de claves / Llaveros de claves / Llavero de claves: projectkeys / Claves / Crear clave

^

← Crear clave

Una clave criptográfica es un recurso que se utiliza para cifrar y descifrar datos o para producir y verificar firmas digitales. Puede tener varias combinaciones.[Más información](#)

• **Nombre y nivel de protección**

Nombre de la clave *

my-key-rotate

Nivel de protección

☒ Software

Las operaciones criptográficas se realizan en software

☐ HSM

Las operaciones criptográficas se realizan en un módulo de seguridad de hardware (HSM)

☐ Usuarios externos

Las operaciones criptográficas se realizan con una clave almacenada en un administrador de claves externo. [Más información](#)

CONTINUAR

CREAR CANCELAR

Se creó el llavero de claves projectkeys

Detalle

Nombre de proyecto

Ubicación

Llavero de

En la sección de **Versiones**, se ajustará el campo correspondiente al **período de rotación** a **90 días**, comenzando desde la fecha vigente. Una vez realizados los ajustes, se deberá hacer clic en **Guardar** para que los cambios sean aplicados y se inicie la rotación automática de las claves según el nuevo intervalo establecido.

CloudSecurity Project01
Buscar (/) recursos, documentos, productos y más
Buscar

stración de claves / Llaveros de claves / Llavero de claves: projectkeys / Claves / Crear clave

Crear clave

CONTINUAR

- Material de clave**

Key material	Generada
--------------	----------
- Propósito y algoritmo**

Propósito	Encriptación/desencriptación simétrica
Algoritmo	Clave Simétrica de Google
- Versiones**

Período de rotación de claves	90 días
A partir del	5/7/25
- Configuración adicional (opcional)**

Duración del estado de "destrucción programada"	30 días (configuración predeterminada)
---	--

CREAR CANCELAR

Se creó el llavero de claves projectkeys

En la sección de **Claves**, se podrá visualizar el listado completo de las claves creadas, incluyendo detalles como el nombre, estado, fecha de creación y la configuración de rotación asignada a cada una. Esta vista proporciona una manera centralizada de gestionar y supervisar las claves, facilitando su seguimiento y administración."

CloudSecurity Project01
Buscar (/) recursos, documentos, productos y más
Buscar

stración de claves / Llaveros de claves / Llavero de claves: projectkeys / Claves

Detalles del llavero de claves

+ CREAR CLAVE + CREAR TRABAJO DE IMPORTACIÓN ACTUALIZAR MOSTRAR PANEL DE INFORM

CLAVES TRABAJOS DE IMPORTACIÓN

Claves del llavero "projectkeys"

Una clave criptográfica es un recurso que se utiliza para encriptar y desencriptar datos o para producir y verificar firmas digitales. Para realizar operaciones en los datos con una clave, usa la API de Cloud KMS [Más información](#)

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	Nombre	Estado	Nivel de protección	Propósito	Próxima rotación	Acciones
<input type="checkbox"/>	my-key-rotate	Disponible	Software	Encriptación/desencriptación simétrica	5 jul 2025	

No se seleccionaron claves



Al hacer clic en el nombre de una clave, se podrán visualizar las distintas versiones de dicha clave, junto con su estado actual, fecha de creación y la configuración de rotación aplicada. Esta funcionalidad permite un seguimiento detallado de cada versión, facilitando la gestión y auditoría de las claves a lo largo del tiempo.

CloudSecurity Project01

Buscar (/) recursos, documentos, productos y más

Buscar

4

stración de claves / Llaveros de claves / Llavero de claves: projectkeys / Claves / Clave: my-key-rotate

← Clave: "my-key-rotate" ROTAR CLAVE EDITAR PERÍODO DE ROTACIÓN IMPORTAR VERSIÓN DE CLAVE MOSTRAR PANEL D

Una clave contiene versiones que tienen material de clave asociado con esta. Una clave debe tener al menos una versión de clave para operar en datos. [Más información](#)

Estado: Disponible Ubicación: us-east1 Nivel de protección: Software Objetivo: Encriptación/descriptación simétrica Rotación: Cada 90 días

DESCRIPCIÓN GENERAL VERSIONES SEGUIMIENTO DE USO PERMISOS

Versiones HABILITAR INHABILITAR RESTABLECER DESTRUIR

Filtro Ingresar el nombre o el valor de la propiedad

<input type="checkbox"/>	↓ Versión	Estado	Algoritmo	Fecha de creación	Creado a partir de	Acciones
<input type="checkbox"/>	1	Habilitada y principal	Clave Simétrica de Google	6/4/25, 12:45	Generada	⋮

No se seleccionaron versiones.

Se creó la clave my-key-rotate.


7. 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.

Actualmente, la instancia de base de datos db-blogueando-ando-2025 está desplegada en Cloud SQL for PostgreSQL, un servicio administrado de bases de datos en Google Cloud Platform (GCP). Esta instancia utiliza cifrado en reposo por defecto, mediante claves administradas por Google (Google-managed encryption keys, GMEK).

GCP cifra automáticamente todos los datos almacenados en Cloud SQL utilizando el sistema de cifrado en múltiples capas (multi-layered encryption). Este sistema emplea Advanced Encryption Standard (AES-256) para proteger los datos, incluyendo:

- Archivos de datos de la base de datos
- Backups automáticos

 Universidad de los Andes	Universidad de los Andes Maestría en Seguridad de la Información - MESI	Abril 2025
---	--	------------

- Registros de transacciones
- Snapshots y configuraciones

Además, GCP gestiona de forma segura el ciclo de vida de las claves de cifrado, la rotación periódica, y el control de acceso mediante Cloud Key Management Service (KMS) y Identity and Access Management (IAM).

Aunque en este caso no se ha habilitado cifrado con Customer-Managed Encryption Keys (CMEK), la base de datos sigue cumpliendo con los principios de cifrado por defecto, protección de datos en reposo, y control de acceso basado en roles (RBAC).

Por tanto, se concluye que la solución desplegada ya cuenta con cifrado activo y eficaz, brindando confidencialidad, integridad y cumplimiento normativo para la información almacenada.


8. 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.

Estrategia de Backups:

Es fundamental establecer criterios claros y efectivos para la estrategia de respaldos, con el objetivo de garantizar la disponibilidad y protección de los datos. Los siguientes puntos deben ser considerados:

- **Realización de respaldos periódicos:** Los respaldos deben realizarse de manera periódica, de acuerdo con la criticidad de los datos. Se recomienda que los datos considerados críticos sean respaldados de forma **diaria** y, siempre que sea posible, de manera **automática**. Esto asegura una protección constante y una recuperación rápida en caso de incidentes.
- **Almacenamiento en múltiples zonas geográficas:** Para asegurar la redundancia y protegerse contra eventos que puedan afectar una sola ubicación (como desastres naturales o fallos en la infraestructura), es crucial almacenar los respaldos en

 Universidad de los Andes	Universidad de los Andes Maestría en Seguridad de la Información - MESI	Abril 2025
---	--	------------

múltiples zonas geográficas. De esta manera, se reduce el riesgo de pérdida total de los datos.

- **Cifrado de datos en tránsito y en reposo:** Tanto los datos en tránsito como los almacenados deben ser cifrados para proteger la confidencialidad e integridad de la información. El cifrado previene que los datos sean interceptados o manipulados durante su transferencia o mientras están almacenados.
- **Validación periódica de la restauración de datos:** Realizar pruebas de restauración de datos de manera **regular** es esencial para asegurar que los respaldos sean realmente funcionales. Estas pruebas deben realizarse de manera programada para garantizar que los datos se puedan recuperar correctamente en cualquier momento.

Seguridad de los Backups:

La seguridad de los respaldos es un aspecto crítico que debe ser cuidadosamente gestionado. Las siguientes prácticas deben ser implementadas para fortalecer la protección de los datos respaldados:

- **Cifrado en reposo:** Para los datos almacenados, se debe utilizar **cifrado en reposo** con claves de cifrado gestionadas por el cliente (CMEK, Customer-Managed Encryption Keys) o por el proveedor. Esto garantiza que solo las partes autorizadas puedan acceder a los datos sensibles.
- **Control de acceso estricto:** Solo los usuarios con roles específicos, como los **administradores de backups**, deben tener acceso a los respaldos. Es esencial implementar un control de acceso **granular** para minimizar el riesgo de exposición de los datos. Además, se recomienda el uso de **autenticación multifactor** para aumentar la seguridad.
- **Transferencia segura de datos:** La transferencia de respaldos debe realizarse a través de canales seguros, como **HTTPS** o **VPN** (Virtual Private Network), para garantizar que los datos no sean interceptados durante su movimiento entre sistemas o ubicaciones.

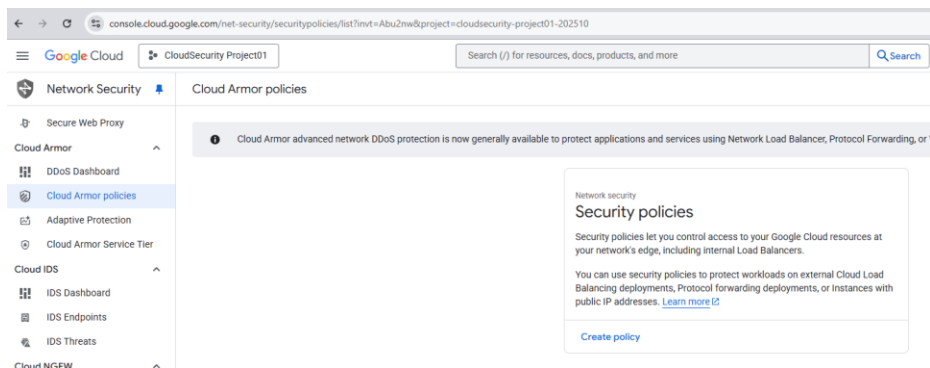
- **Simulacros de restauración regular:** Para validar la efectividad de los respaldos, es necesario llevar a cabo **simulacros de restauración** de forma regular. Estos simulacros aseguran que los procesos de restauración funcionen correctamente y que los tiempos de recuperación sean los esperados.
- **Monitoreo y alertas proactivas:** Es fundamental contar con un sistema de **monitoreo constante** que vigile los trabajos de respaldo. Configurar **alertas** automáticas ante fallos o retrasos en los procesos de respaldo es clave para identificar y resolver problemas rápidamente, minimizando los riesgos de pérdida de datos.

Con la implementación de estas mejores prácticas, se puede asegurar que los datos estén protegidos de manera eficiente y estén siempre disponibles cuando sea necesario, independientemente de los eventos inesperados que puedan ocurrir.

9. Preparación WAF:

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

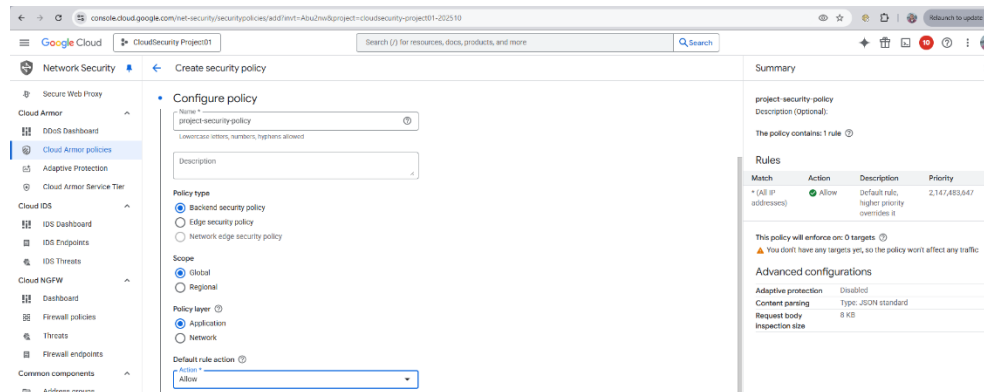
En la sección "Network Security", se selecciona la opción "Cloud Armor policies" para crear una nueva política de seguridad.



Se establece un nombre descriptivo para la política, en este caso: project-security-policy.



Se dejan los valores por defecto y, para la regla predeterminada, se selecciona la acción "Allow" para que la política funcione inicialmente en modo permisivo, tal como se solicita.



Una vez completada esta configuración, se verifica que la política se crea exitosamente.

Filter Enter property name or value						
<input type="checkbox"/>	Name ↑	Type	Scope	Rules	Targets ⓘ	Description
<input type="checkbox"/>	project-security-policy	Backend security policy	global	1	0	⋮

10. Configuración de Google Cloud Armor:

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

Para añadir una regla que bloquee tráfico de IPs sospechosas, se hace lo siguiente:

- En el apartado "Condition", se selecciona el modo básico.
- En el campo "Match", se especifica la IP que se desea bloquear.
- Se asigna la acción "Deny" (denegar).
- Se establece una prioridad relativamente baja (6000).



Summary

project-security-policy
Description (Optional):
The policy contains: 2 rules

Match	Action	Description	Priority
10.41.8.122	Deny (403)	Traffic based on IP's sospechosas	6,000
* (All IP addresses)	Allow	Default rule, higher priority overrides it	2,147,483,647

This policy will enforce on: 0 targets

Advanced configurations

Adaptive protection: Disabled
Content parsing: Type: JSON standard
Request body inspection size: 8 KB

- Intentos de inyección (SQL/XSS), DDoS y otros 2 ataques OWASP Top 10.

Se agregan dos reglas usando WAF preconfigurado:

- `evaluatePreconfiguredWaf('sqli-v33-stable')`

Detecta y bloquea intentos de inyección SQL (SQLi), una técnica que intenta manipular consultas a bases de datos insertando código malicioso en campos de entrada.

- `evaluatePreconfiguredWaf('xss-v33-stable')`

Detecta y bloquea ataques de Cross-Site Scripting (XSS), donde el atacante inyecta scripts en páginas vistas por otros usuarios, buscando robar información o manipular el contenido.

Summary

project-security-policy
Description (Optional):
The policy contains: 3 rules

Match	Action	Description
evaluatePreconfiguredWaf('xss-v33-stable') evaluatePreconfiguredWaf('sqli-v33-stable')	Deny (403)	Intentos de inyección (SQL/XSS)
10.41.8.122	Deny (403)	Traffic based on IP's sospechosas
* (All IP addresses)	Allow	Default rule, higher priority overrides it

This policy will enforce on: 1 target

Target name	Target endpoints	Target type
blog-backend-lb	serverless-lb (external application load balancer)	Backend service

Se habilita la opción Adaptive Protection, que permite a Cloud Armor detectar patrones anómalos de tráfico que podrían indicar un ataque de denegación de servicio distribuido (DDoS), y responder dinámicamente a estas amenazas.

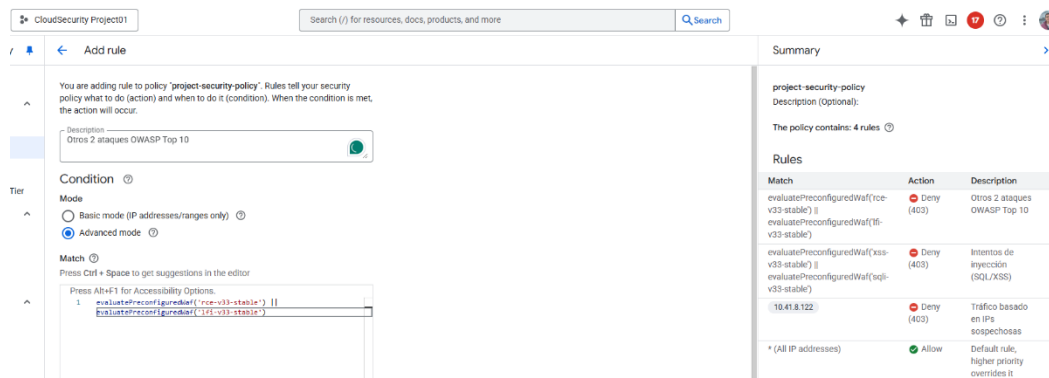
Adaptive protection configuration

Cloud Armor Adaptive Protection helps protect backend services from Layer 7 DDoS attacks by learning normal traffic patterns, detecting and alerting on potential attacks, and providing Cloud Armor WAF rules to mitigate them.
[Learn more](#)

☒ Enable Adaptive Protection

Se incorporan reglas adicionales para amenazas del OWASP Top 10:

- `evaluatePreconfiguredWaf('rce-v33-stable')`
 Protege contra ataques de Remote Code Execution (RCE), donde el atacante intenta ejecutar código malicioso de forma remota en el servidor.
- `evaluatePreconfiguredWaf('lfi-v33-stable')`
 Detecta y bloquea ataques de Local File Inclusion (LFI), los cuales intentan acceder o ejecutar archivos internos del servidor a través de rutas manipuladas.



CloudSecurity Project01

Search (/) for resources, docs, products, and more

Add rule

You are adding rule to policy 'project-security-policy'. Rules tell your security policy what to do (action) and when to do it (condition). When the condition is met, the action will occur.

Description: Otros 2 ataques OWASP Top 10

Condition

Mode

Basic mode (IP addresses/ranges only)

Advanced mode

Match

Press Ctrl + Space to get suggestions in the editor

Press Alt+F1 for Accessibility Options

1. evaluatePreconfiguredWaf('rce-v33-stable') || evaluatePreconfiguredWaf('lfi-v33-stable')

Summary

project-security-policy

Description (Optional):

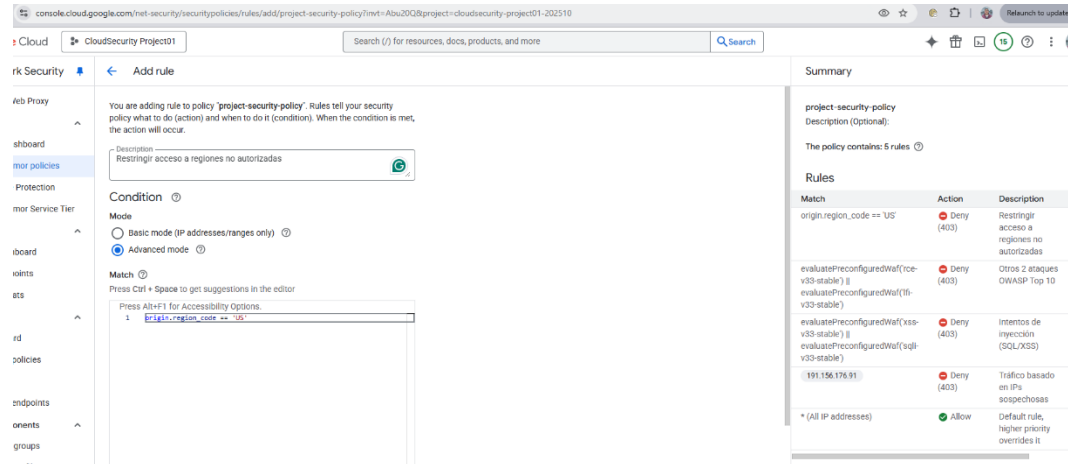
The policy contains: 4 rules

Rules

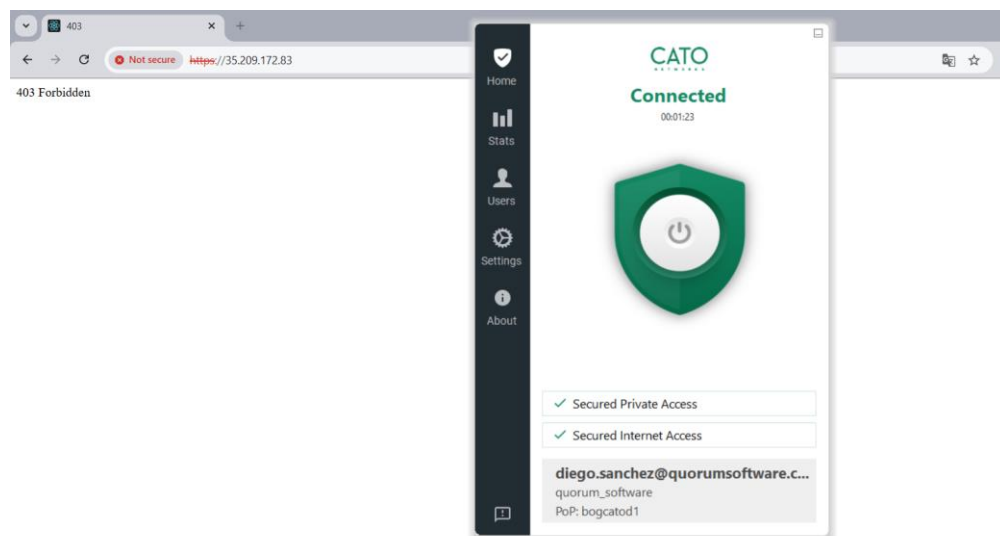
Match	Action	Description
evaluatePreconfiguredWaf('rce-v33-stable') evaluatePreconfiguredWaf('lfi-v33-stable')	Deny (403)	Otros 2 ataques OWASP Top 10
evaluatePreconfiguredWaf('xss-v33-stable') evaluatePreconfiguredWaf('sql-v33-stable')	Deny (403)	Intentos de inyección (SQL/XSS)
10.41.8.122	Deny (403)	Tráfico basado en IPs sospechosas
* (All IP addresses)	Allow	Default rule, higher priority overrides it

- Aplicar reglas de geolocalización para restringir acceso a regiones no autorizadas.

Para efectos de la práctica, se configura una regla que bloquea tráfico con origen en Estados Unidos, utilizando el código de región "US". Esta funcionalidad puede ser útil para restringir tráfico desde regiones no deseadas.



Conectado a una VPN en Estados Unidos, se puede observar que efectivamente no se puede acceder a la aplicación y se muestra el error 403 (Forbidden) como se espera.



- Concatenar reglas para ahorro de costos en Google Cloud Armor.

Se procede a concatenar múltiples condiciones dentro de una misma regla. Cabe resaltar que Cloud Armor permite concatenar hasta 5 condiciones por regla.



CloudSecurity Project01

Search (/) for resources, docs, products, and more

Search

15

ty

← Add rule

You are adding rule to policy 'project-security-policy'. Rules tell your security policy what to do (action) and when to do it (condition). When the condition is met, the action will occur.

Description

Concatenated rules

Condition

Mode

☐ Basic mode (IP addresses/ranges only)

☒ Advanced mode

Match

Press Ctrl + Space to get suggestions in the editor

Press Alt+F1 for Accessibility Options.

```
1 (origin.region_code == 'US') ||  
2 evaluatePreconfiguredWaf('rce-v33-stable') ||  
3 evaluatePreconfiguredWaf('lfi-v33-stable') ||  
4 evaluatePreconfiguredWaf('xss-v33-stable') ||  
5 evaluatePreconfiguredWaf('sql-v33-stable')
```

Summary

project-security-policy

Description (Optional):

The policy contains: 6 rules

Rules

Match	Action	Description
(origin.region_code == 'US') evaluatePreconfiguredWaf('rce-v33-stable') evaluatePreconfiguredWaf('lfi-v33-stable') evaluatePreconfiguredWaf('xss-v33-stable') evaluatePreconfiguredWaf('sql-v33-stable')	Deny (403)	Concatenated rules
origin.region_code == 'US'	Deny (403)	Restringir acceso a regiones no autorizadas

Para evitar duplicidad, las reglas seleccionadas se pueden eliminar dado que fueron concatenadas.

Filter Enter property name or value						
	Action	Type	Match	Description	Priority ↑	
<input type="checkbox"/>	Deny (403)		(origin.region_code == 'US') evaluatePreconfiguredWaf('rce-v33-stable') evaluatePreconfiguredWaf('lfi-v33-stable') evaluatePreconfiguredWaf('xss-v33-stable') evaluatePreconfiguredWaf('sql-v33-stable')	Concatenated rules	2,000	⋮
<input checked="" type="checkbox"/>	Deny (403)		origin.region_code == 'US'	Restringir acceso a regiones no autorizadas	3,000	⋮
<input checked="" type="checkbox"/>	Deny (403)		evaluatePreconfiguredWaf('rce-v33-stable') evaluatePreconfiguredWaf('lfi-v33-stable')	Otros 2 ataques OWASP Top 10	4,000	⋮
<input checked="" type="checkbox"/>	Deny (403)		evaluatePreconfiguredWaf('xss-v33-stable') evaluatePreconfiguredWaf('sql-v33-stable')	Intentos de inyección (SQL/XSS)	5,000	⋮
<input type="checkbox"/>	Deny (403)	IP addresses/ranges	191.156.176.91	Tráfico basado en IPs sospechosas	6,000	⋮
<input type="checkbox"/>	Allow	IP addresses/ranges	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647	⋮

11. Integración con el Balanceador de Carga:

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

Finalmente, se asocia la política de seguridad al balanceador de carga correspondiente, asegurando que el tráfico entrante a la aplicación pase por los filtros definidos en la política project-security-policy.



console.cloud.google.com/net-services/loadbalancing/backends/details/backendService/blog-backend-lb?project=cloudsecurity-project01-202510&inv=Abu20Q

Google Cloud CloudSecurity Project01 Search (/) for resources, docs, products, and more

Network Services Load balancing

Cloud DNS Cloud CDN Cloud NAT Cloud Service Mesh (Traff... Service Directory Cloud Domains Private Service Connect SSL policies Service Extensions

Backends

In order to edit backend service use load balancer mutations, gcloud or REST API.

blog-backend-lb

General properties

Load balancer type	Classic Application Load Balancer (EXTERNAL)
Endpoint protocol	HTTPS
In use by	serverless-lb
IP address selection policy	Only IPv4
Health check	--
Backend security policy	project-security-policy
Session affinity	None
Cloud CDN	Disabled
Connection draining timeout	0 seconds
Custom request headers	Currently there are no custom request headers configured
Custom response headers	Currently there are no custom response headers configured
Logging	Enabled
Sample rate	1
Backend authentication	Disabled

Backends

Name	Type	Scope	Healthy	Autoscaling	Balancing mode	Capacity	Preference level
externalserver	Serverless network endpoint group	us-central1	N/A	No configuration	N/A	N/A	None

Rules Targets Logs

Targets are Google Cloud resources that you want to control access to. Access is controlled by policies, which are applied to targets.

Apply policy to new target Remove

Filter Enter property name or value

Target name	Target endpoints	Target type
blog-backend-lb	serverless-lb	Backend service (external application load balancer)

12. Pruebas de Simulación:

- Efectuar un ataque simple sobre la infraestructura de la aplicación en GCP, con herramientas similares a OWASP ZAP y Burp Suite.

La herramienta seleccionada para realizar el ataque fue OWASP ZAP, donde se realizó un escaneo automatizado indicando la URL de la aplicación <https://myfrontend-613756850426.us-central1.run.app> y <https://35.209.172.83>.



ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
243	4/15/25, 9:15:58 PM	4/15/25, 9:15:58 PM	GET	https://35.209.172.83/central:run.app?size=206&filter=all	200 OK		635 ms	320 bytes	235 bytes
244	4/15/25, 9:15:58 PM	4/15/25, 9:15:58 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	200 OK		689 ms	325 bytes	7,281 bytes
245	4/15/25, 9:15:59 PM	4/15/25, 9:15:59 PM	GET	https://35.209.172.83/central:run.app?size=206&filter=all	200 OK		288 ms	320 bytes	235 bytes
246	4/15/25, 9:15:59 PM	4/15/25, 9:16:00 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	200 OK		1,07 s	321 bytes	7,281 bytes
247	4/15/25, 9:16:01 PM	4/15/25, 9:16:01 PM	OPTIONS	https://35.209.172.83/central:run.app?size=16&filter=all	200 OK		348 ms	510 bytes	2 bytes
248	4/15/25, 9:16:01 PM	4/15/25, 9:16:02 PM	GET	https://35.209.172.83/central:run.app?size=16&filter=all	200 OK		436 ms	320 bytes	235 bytes
249	4/15/25, 9:16:02 PM	4/15/25, 9:16:02 PM	GET	https://35.209.172.83/central:run.app?size=206&filter=all	200 OK		201 ms	320 bytes	235 bytes
250	4/15/25, 9:16:02 PM	4/15/25, 9:16:02 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	200 OK		264 ms	350 bytes	5,347 bytes
251	4/15/25, 9:16:02 PM	4/15/25, 9:16:02 PM	GET	https://35.209.172.83/central:run.app?size=206&filter=all	200 OK		271 ms	321 bytes	7,281 bytes
252	4/15/25, 9:16:03 PM	4/15/25, 9:16:04 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	200 OK		314 ms	321 bytes	6,446 bytes
253	4/15/25, 9:16:07 PM	4/15/25, 9:16:07 PM	GET	https://35.209.172.83/central:run.app?size=206&filter=all	200 OK		493 ms	320 bytes	235 bytes
254	4/15/25, 9:16:07 PM	4/15/25, 9:16:07 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	200 OK		572 ms	322 bytes	7,281 bytes
255	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		182 ms	317 bytes	169 bytes
256	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		168 ms	317 bytes	169 bytes
257	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
258	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
259	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
260	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
261	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
262	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
263	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
264	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
265	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	GET	https://35.209.172.83/central:run.app?size=126&filter=all	301 Moved Permanently		165 ms	317 bytes	169 bytes
266	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	POST	https://35.209.172.83/central:run.app?size=126&filter=all	400 Bad Request		133 ms	213 bytes	273 bytes
267	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	POST	https://35.209.172.83/central:run.app?size=126&filter=all	400 Bad Request		141 ms	274 bytes	559 bytes
268	4/15/25, 9:16:41 PM	4/15/25, 9:16:41 PM	CONNECT	https://35.209.172.83/central:run.app?size=126&filter=all	400 Bad Request		141 ms	274 bytes	559 bytes

A continuación, se presentan las alertas reportadas:

Alerts (8)

- > Content Security Policy (CSP) Header Not Set (2)
- > Missing Anti-clickjacking Header
- > Strict-Transport-Security Header Not Set (8)
- > X-Content-Type-Options Header Missing (7)
- > Information Disclosure - Suspicious Comments
- > Modern Web Application
- > Re-examine Cache-control Directives (3)
- > User Agent Fuzzer (7)

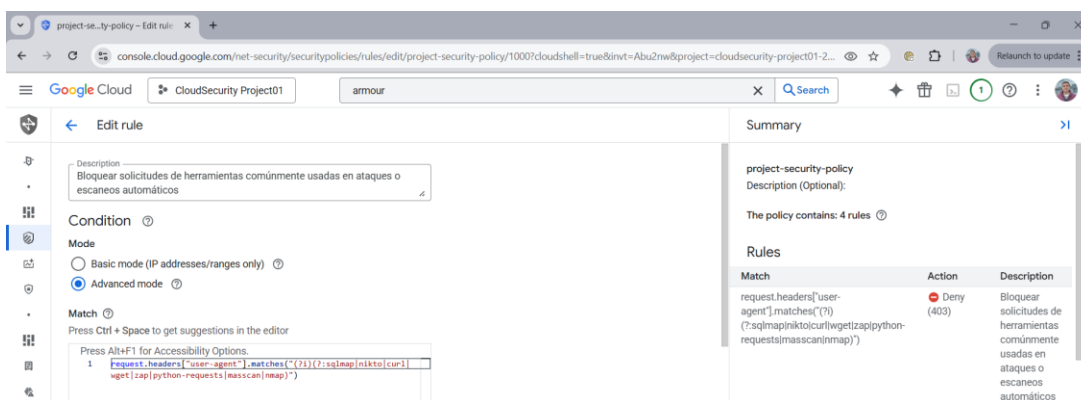
- **Content Security Policy (CSP) Header Not Set:** La ausencia de la política CSP deja a la aplicación vulnerable a ataques como Cross-Site Scripting (XSS), ya que no hay restricciones sobre qué fuentes externas pueden cargar contenido en el navegador.
- **Missing Anti-clickjacking Header:** Falta el encabezado X-Frame-Options, lo que permite que la aplicación sea embebida en otros sitios mediante iframes, facilitando ataques de clickjacking para engañar al usuario y robar datos.
- **Strict-Transport-Security Header Not Set:** Sin el encabezado HSTS (Strict-Transport-Security), los navegadores no están obligados a usar HTTPS en visitas futuras, lo que permite ataques de tipo downgrade o MITM si el usuario accede mediante HTTP.
- **X-Content-Type-Options Header Missing:** La ausencia del encabezado X-Content-Type-Options: nosniff permite a los navegadores interpretar archivos como un tipo MIME distinto, lo que puede usarse para ejecutar scripts maliciosos.

- Information Disclosure – Suspicious Comments: Se encontraron comentarios en el código fuente que podrían revelar información confidencial o lógica interna de la aplicación, lo cual es una mala práctica de seguridad.
- Modern Web Application: La aplicación fue clasificada como moderna, lo cual es informativo, pero no representa una amenaza directa. Sirve para entender mejor el tipo de tecnologías empleadas.
- Re-examine Cache-control Directives: Las directivas de caché no están correctamente configuradas, lo que podría permitir que contenido sensible sea almacenado en cachés públicas, exponiendo información a usuarios no autorizados.
- User Agent Fuzzer: Se observaron variaciones en las respuestas del servidor según el User-Agent, lo que puede indicar comportamientos inconsistentes que podrían ser explotados para evasión de controles o fingerprinting.

- Ajustar las reglas del WAF basándose en los resultados de las pruebas

Aunque la mayoría de las alertas están relacionadas con encabezados de seguridad que deben ser configurados en el servidor web, se pueden añadir una regla para reforzar la seguridad:

- Se bloquean las solicitudes de herramientas comúnmente usadas en ataques o escaneos automáticos, se inspecciona el encabezado “User-Agent” filtrando valores como sqlmap, nikto, curl, wget, ZAP, nmap, etc.



The screenshot shows the Google Cloud console interface for editing a WAF rule. The rule is named "project-security-policy" and is in "Advanced mode". The condition is set to "request.headers[\"user-agent\"][matches(\"(?:sqlmap|nikto|curl|wget|python-requests|masscan|nmap)\")]" and the action is "Deny (403)". The description is "Bloquear solicitudes de herramientas comúnmente usadas en ataques o escaneos automáticos".

Match	Action	Description
request.headers[\"user-agent\"][matches(\"(?:sqlmap nikto curl wget python-requests masscan nmap)\")]	Deny (403)	Bloquear solicitudes de herramientas comúnmente usadas en ataques o escaneos automáticos

Diagrama de arquitectura GCP

