

Bitácora Individual – Estancia Profesional ESIT

Fase: Fase 2 – Implementación de la plataforma de monitoreo en la nube

Nombre del proyecto: Sistema de Monitoreo de Recursos Cloud con Grafana

Integrante: Carlos José Fletes Alduvín

Equipo: Grupo 13

Tutor: Carlos Guillermo Rodríguez Álvarez

Ciclo: 06

1. Información general

La siguiente bitácora contiene actividades realizadas que fueron asignadas por el líder desde antes que se entregara la fase 1, también se encontrarán actividades realizadas por el rol que desempeño y actividades asignadas por el tutor

2. Actividades realizadas

Actividad realizada	Descripción técnica	Responsable	Evidencia
Apoyo en la creación y configuración de las instancias	Apoyo en la creación de y configuración de la instancia en AWS Apoyo en la creación de la VM en GCP Se apoyó al compañero Carlos Sopón y René Pinto	Carlos Fletes	1 - Apoyo en la creación y configuración de las instancias
Apoyo en la configuración de red y seguridad básica	Apoyo en la configuración de la red y seguridad básica implementada en GCP en la siguiente: Control del tráfico entrante, para Grafana mediante TCP: 3000, para Node Exporter TCP:9100 y para Prometheus: 9090 Mediante la IP privada 10.138.0.4 y la IP	Carlos Fletes	2 – Apoyo en la red básica y Seguridad

La implementación para AWS es la siguiente, el control de acceso, mediante un TCP personalizado: 9100 y la IP 34.169.162.44/32 que es el puerto y la IP donde GCP tendrá acceso

Y SSH para permitir conexión de cualquier IPV4, que es la que se utiliza para que el equipo de trabajo pueda conectarse, pero que se deshabilitará cuando ya no se necesite

Se apoyó al compañero Carlos Sopón y René Pinto

Creación de rol para acceder a la instancia de AWS mediante SSM	<p>Se creó un rol para poder hacer conexión a la instancia de AWS mediante SSM y que los compañeros no tengan que conectarse mediante SSH desde la Shell de su PC</p> <p>el cual me estuvo apoyando el compañero René Pinto</p>	Carlos Fletes	3 – Creación de rol y configuración de SSM
Reestructuración del repositorio del proyecto en GitHub	<p>Se reestructuró el repositorio, creando la carpeta de docs, que actualmente contienen los archivos README.md y Runbook.md del proyecto</p>	Carlos Fletes	4 – Reestructuración del repositorio en GitHub

	Además contiene la bitácora de la fase 2		
	el cual me estuvo apoyando el compañero René Pinto		
Creación del archivo runbook.md	Se creó un archivo runbook.md que contiene información de como correr el proyecto y que hacer en casos de que falle, e información necesaria	Carlos Fletes	5 – Creación del runbook.md
	el cual me estuvo apoyando el compañero René Pinto		
Creación del archivo README.md	Se creó el archivo readme.md que contiene información sobre el proyecto en general, y documentación de la seguridad mínima aplicada, que el detalle se encuentra en el entregable	Carlos Fletes	6 – Creación del readme.md
	el cual me estuvo apoyando el compañero René Pinto		
Apoyo en la documentación de la fase actual	Se apoyó al compañero René Pinto en el proceso de la documentación de la fase actual	Carlos Fletes	7 – Apoyo en la documentación

3. Herramientas utilizadas

Herramienta / Servicio	Propósito
WhatsApp	Comunicación entre los compañeros del equipo de trabajo, para coordinar y apoyo de consultas entre nuestras actividades

Visual Estudio Code

Creación de los archivos de runbook.md y readme.md que se encuentran en la plataforma de GitHub en la carpeta docs
GitHub
AWS
GCP
Reestructuración en el directorio del proyecto
Configuración de la instancias, sus herramientas de conexión, roles y medidas de seguridad de redes
Apoyo en el proceso de configuración de la VM

9. Registro de evidencias

1 – Apoyo en la creación y configuración de las instancias

Capturas de Carlos Fletes
 VPC montada en AWS
 Nombre: MONITORING GRAFANA
 VPC ID: [vpc-03704d60bf47d4c9](#)
 IP: [172.31.0.0/16](#)
 (cambió el nombre de la VPC a MONITORING GRAFANA)

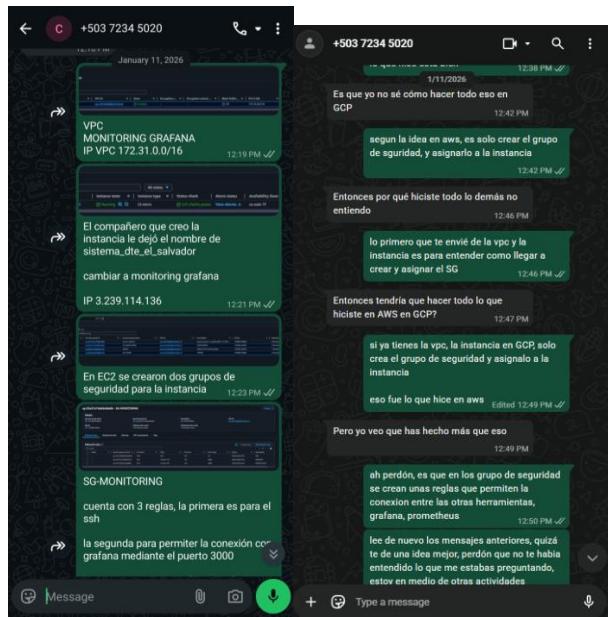


Tenemos una instancia con el nombre de: sistema_dte_el_salvador
 IP: IP 3.239.114.136

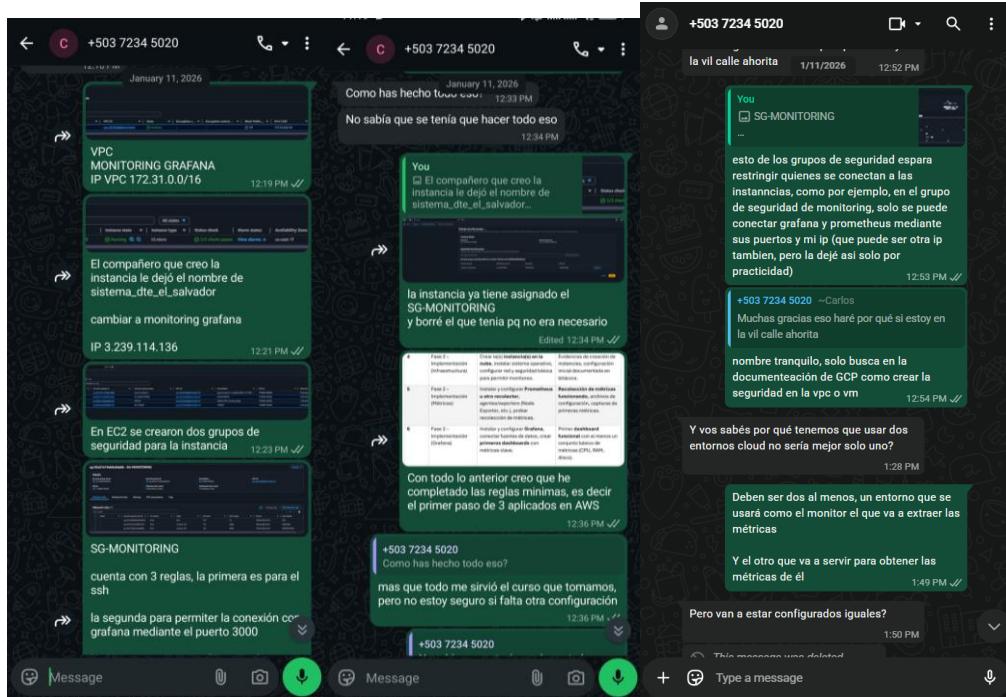


En EC2 se crearon dos grupos de seguridad para la instancia





2 - Apoyo en la red básica y Seguridad

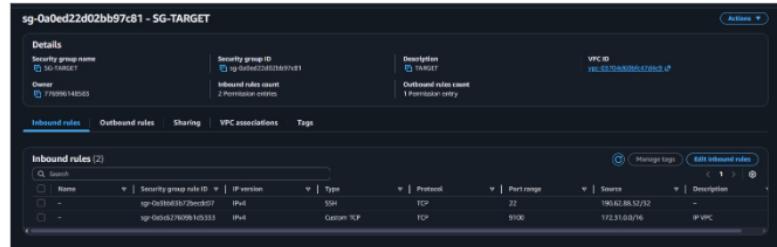


SG - TARGET

cuenta con 2 reglas

la primera para el ssh

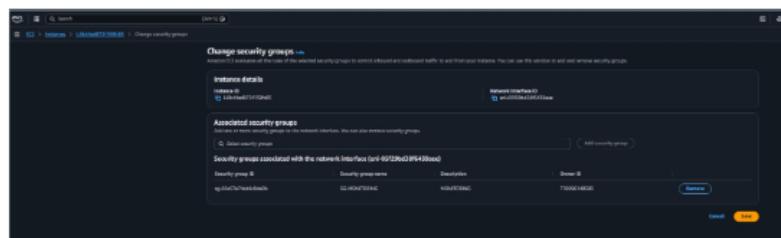
la segunda regla para poder ~~permintir~~ que para que Node exporter y prometheus puedan extraer las ~~metricas~~



The screenshot shows the AWS CloudFormation stack details for 'sg-0a0ed22d02bb97c81 - SG-TARGET'. It displays the security group's inbound rules:

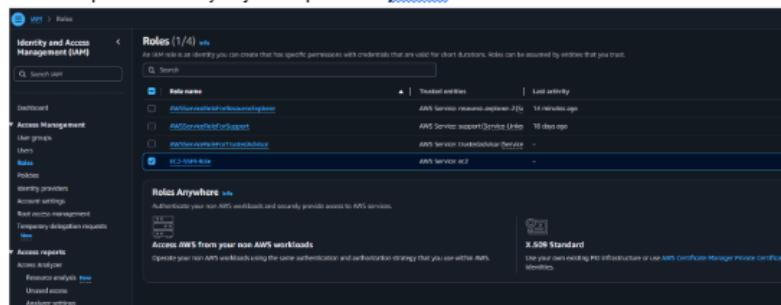
Name	Security group rule ID	Type	Protocol	Port range	Source	Description
-	sg-0a0ed22d02bb97c81-0ed5f57	IPv4	TCP	22	192.62.88.52/32	-
-	sg-0a0ed22d02bb97c81-0533	IPv4	TCP	9100	172.31.0.0/16	IP VPC

Previamente la instancia ya tenía asignado un SG diferente, que viene por default cuando se crea el EC2, pero se nos pidió crear nuestro SG adecuados al proyecto por medidas de seguridad, entonces ahora la instancia tiene asignado el SG-MONITORING



The screenshot shows the 'Change security groups' interface for an instance. It lists the associated security groups and their details, including the network interface and security group ID.

Role creado en IAM [EC2-SMM-Role](#) para poder acceder el gestor de las instancias en EC2 sin tener que usar SSH y dejarlo expuesto al público



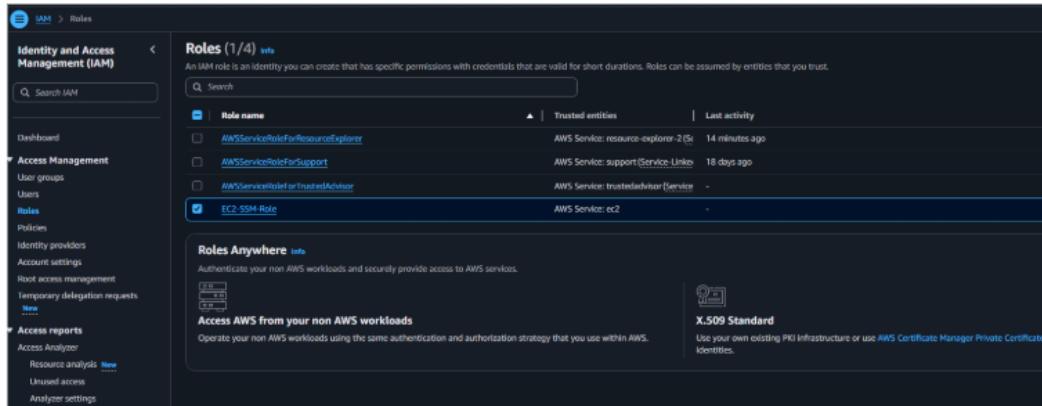
The screenshot shows the AWS IAM Roles page. It lists the roles available, including the newly created 'EC2-SMM-Role'.

La instancia [sistema_dte_el_salvador](#) ahora tienen asignado el nuevo rol



The screenshot shows the 'Modify IAM role' interface for the 'EC2-SMM-Role'. It shows the selected role and the option to 'Add role'.

Role creado en IAM **EC2-SSM-Role** para poder acceder el gestor de las instancias en EC2 sin tener que usar SSH y dejarlo expuesto al público

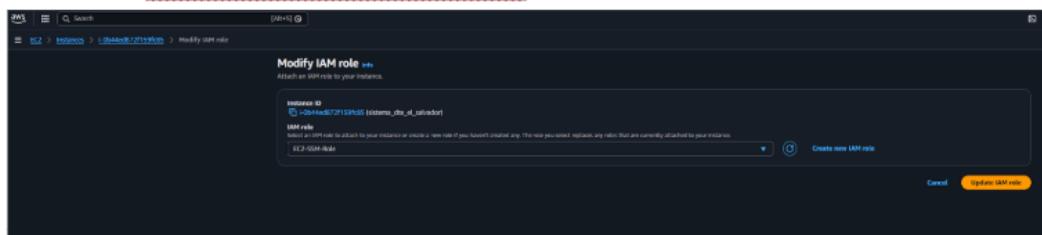


The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation options like Dashboard, Access Management, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests, Access reports, Access Analyzer, Resource analysis, Unusual access, and Analyzer settings. The main area is titled "Roles (1 / 4)" and contains a table with one row:

Role name	Trusted entities	Last activity
<input checked="" type="checkbox"/> EC2-SSM-Role	AWS Service: ec2	-

Below the table, there are sections for "Access AWS from your non AWS workloads" and "X.509 Standard".

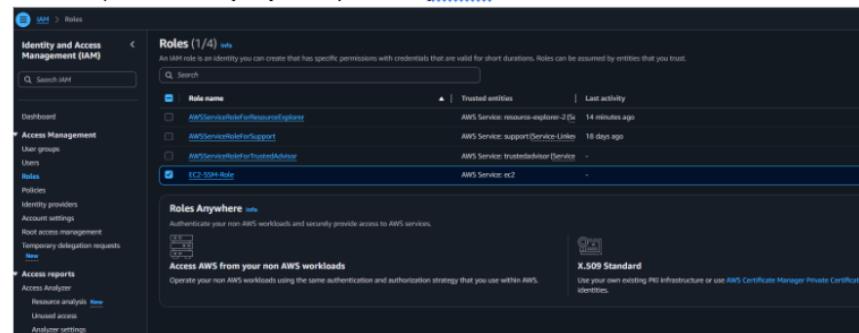
La instancia **sistema_dte_el_salvador** ahora tienen asignado el nuevo rol



The screenshot shows the "Modify IAM role" page for the instance **sistema_dte_el_salvador**. It has a sidebar with similar navigation options as the previous screenshot. The main form has a "Role" dropdown menu where **EC2-SSM-Role** is selected. At the bottom right, there are "Cancel" and "Update IAM role" buttons.

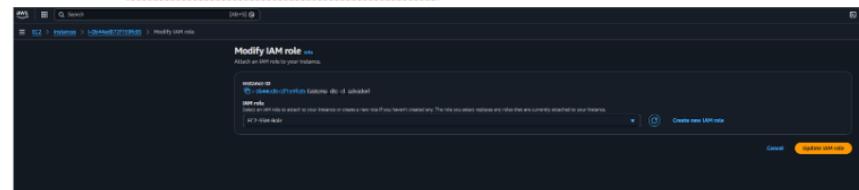
3 – Creación de rol y configuración de SSM

Role creado en IAM **EC2-SSM-Role** para poder acceder el gestor de las instancias en EC2 sin tener que usar SSH y dejarlo expuesto al público



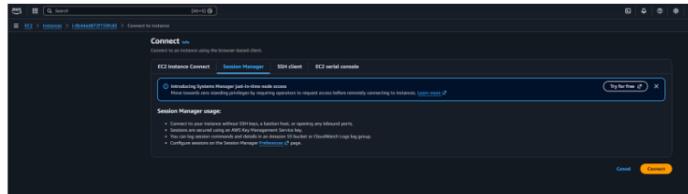
This screenshot is identical to the one above, showing the AWS IAM Roles page with the newly created **EC2-SSM-Role** listed.

La instancia **sistema_dte_el_salvador** ahora tienen asignado el nuevo rol



This screenshot is identical to the one above, showing the "Modify IAM role" page for the instance **sistema_dte_el_salvador** with the **EC2-SSM-Role** selected.

Ahora con el rol asignado, se puede conectar a la instancia sin usar el SSH, sino que también mediante SSM



4 – Reestructuración del repositorio en GitHub

sistema-de-monitoreo-cloud / docs / README.md

Preview Code Blame 285 lines (152 loc) - 5.81 kB

No subir credenciales al repositorio (usar variables de entorno/archivos fuera de Git).

- Exponer solo puertos necesarios y restringir por IP (Security Groups/Firewall).
- Crear usuarios dedicados (p. ej. `node_exporter`) con permisos mínimos.
- Preferir SSM / acceso administrado cuando aplique, y restringir SSH.

Estructura recomendada del repositorio

```

docs/
  |- fase-1-analisis-y-diseno.pdf
  |- bitacora-fase-2.docx
  |- capturas/
infra/
  |- prometheus/
    |- prometheus.yml
      |- rules/          # alert rules (opcional)
  |- systemd/
    |- prometheus.service
    |- node_exporter.service
  |- nginx/
    |- grafana.conf     # reverse proxy (opcional)
  dashboards/
    |- dashboards.json  # export de dashboards (opcional)

```

File Edit Selection View Go Run Terminal Help

Restricted Mode is intended for safe code browsing. Trust this window to enable all features. [Manage](#) [Learn More](#)

RUNBOOK.md README.md

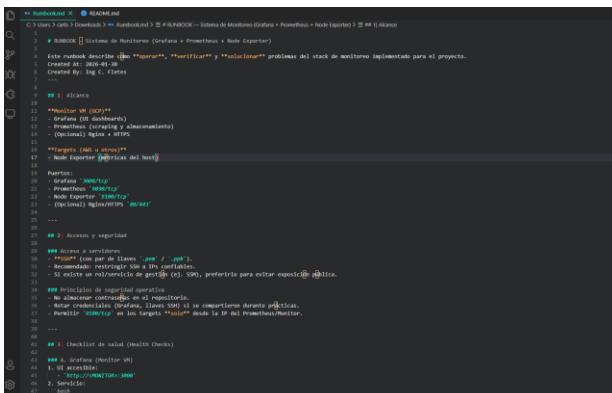
C: > Users > carlo > Downloads > README.md > # Sistema de Monitoreo de Recursos Cloud con Grafana

```

1  # Sistema de Monitoreo de Recursos Cloud con Grafana
56 ## Estructura recomendada del repositorio
59
60
61   docs/
62     |- fase-1-analisis-y-diseno.pdf
63     |- bitacora-fase-2.docx
64     |- capturas/
65   infra/
66     |- prometheus/
67       |- prometheus.yml
68         |- rules/          # alert rules (opcional)
69     |- systemd/
70       |- prometheus.service
71       |- node_exporter.service
72     |- nginx/
73       |- grafana.conf     # reverse proxy (opcional)
74   dashboards/
75     |- dashboards.json  # export de dashboards (opcional)

```

5 – Creación del runbook.md



```

# Runbook.md
C:\Users\Carlo\Downloads> more runbook.md
# RUNBOOK — Sistema de Monitoreo (Grafana + Prometheus + Node Exporter)

Este runbook describe como operar, verificar y solucionar problemas del stack de monitoreo implementado para el proyecto.
Created At: 2026-01-30
Created By: Ing C. Fletes

1) Alcance
  • Monitor VM (GCP)
    - Grafana (UI dashboards)
    - Prometheus (scraping y almacenamiento)
    - (Opcional) Nginx + HTTPS
  **Targets (AWS u otros)**
    - Node Exporter (targets de host)

Puertos:
  • Grafana: http://127.0.0.1:3000
  • Prometheus: http://127.0.0.1:9090
  • Grafana: https://127.0.0.1:3001
  • (Opcional) Nginx: https://127.0.0.1:443
  ...
  ...

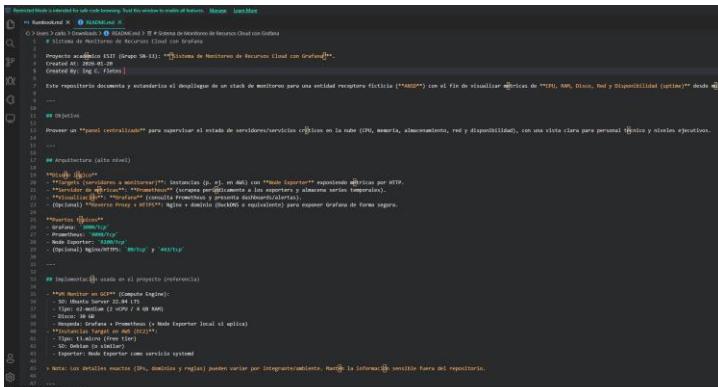
2) Acceso y seguridad
  • Acceso a servicios
    - SSH: (por default) https://127.0.0.1:22
      - Si existe un red/service de getSSH (ej., SSH), preferirlo para evitar exposición pública.
  # Principios de seguridad operativa
  • No almacenar credenciales en el repositorio.
  • Usar claves SSH para los hosts (SSH se comparten durante prácticas).
  • Permitir https:// en los targets **targets** desde la IP del Prometheus/Monitor.
  ...
  ...

3) Checklist de salud (Health Checks)
  • A. Grafana (Monitor VM)
  • B. accesibilidad
  • 2. servicios
  ...
  ...

Resumen:
```



6 – Creación del readme.md



```

# README.md
C:\Users\Carlo\Downloads> more README.md
# Sistema de Monitoreo de Recursos Cloud con Grafana

Este repositorio documenta y estandariza el despliegue de un stack de monitoreo para una entidad receptora ficticia (**ANSI**) con el fin de visualizar métricas de **CPU, RAM, Disco, Red y Disponibilidad (uptime)** desde múltiples recursos.

...
  ...

## Objetivo
  Proveer un panel centralizado para supervisar el estado de servidores/servicios críticos en la nube (CPU, memoria, almacenamiento, red y disponibilidad), con una vista clara para personal técnico y niveles ejecutivos.

...
  ...

## Arquitectura (alto nivel)
  * **Monitoreo:** Se encarga de recopilar datos (CPU, RAM, Disco, Red, Uptime) de los nodos y enviarlos a Grafana. Los datos se obtienen mediante scraping de Prometheus y Node Exporter.
  * **Visualización:** Grafana es el sistema centralizado que recibe los datos y los visualiza en forma de dashboards interactivos.
  * **Integración:** Node Exporter (que actúa como middleware entre los nodos y Grafana) para expor datos de forma segura.

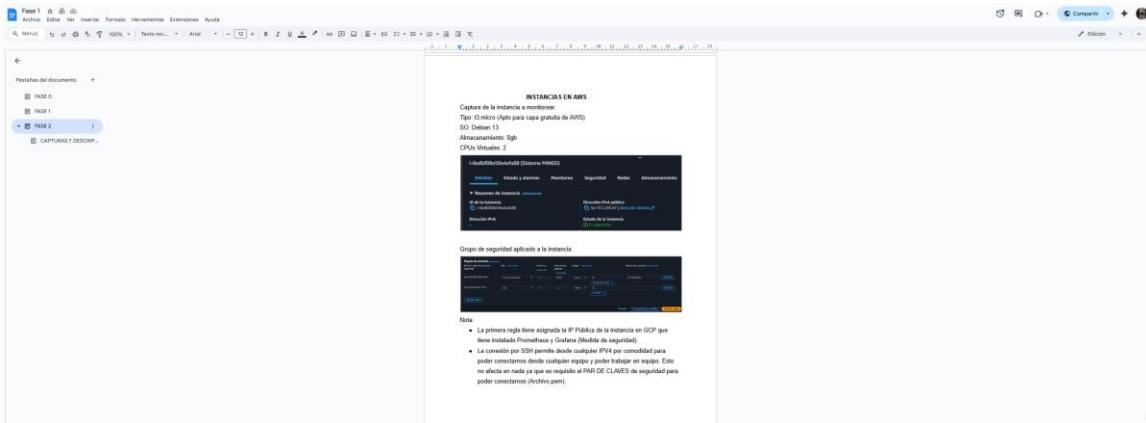
  Notas: Los detalles exactos (puertos, direcciones y reglas) pueden variar por entorno/ambiente. Mantén la información sensible fuera del repositorio.

  ...
  ...

Resumen:
```



7 – Apoyo en la documentación



The image shows a Microsoft Word document with a screenshot of a CloudWatch Metrics Insights interface. The screenshot displays a list of metrics and a detailed view of one metric named 'CPUUtilization'. The detailed view includes a graph showing CPU utilization over time, a table with specific data points, and a section titled 'Reglas de respuesta aplicadas a la instancia' (Response rules applied to the instance) with two items listed.

INSTANCIAS EN AWS

Captura de la instancia en AWS

Tipo: EC2 micro (Algo para copia gratuita de AWS)

SC: Detalles 13

Administrador de grupos de máquinas virtuales 2

CloudWatch Metrics Insights (Última ejecución)

Estado y alcance

Mensajes

Seguridad

Index

Almacenamiento

Reglas de respuesta

Alta

- La primera regla tiene asignada la IP Pública de la instancia en GCP que tiene instalado Prometheus y Grafana (Medida de seguridad).
- La otra regla por SSH permite desde cualquier IPV4 permitir conexión a través de SSH. No afecta en nada ya que no se requiere un PIVI DE CLAVO de seguridad para poder conectarse (Archivos perm).