Fundación Universitaria San Mateo

Sistema de Gestión de Incidentes de Seguridad en AWS

Documentación elaborada por

Maicol Nuñez - Nicolas Castro - Harold Neuta - Sebastian Garcia

Profesor a cargo

Ingeniero Joaquin Fernando Sánchez Cifuentes

Fecha: Enero 2026

Sistema de Gestión de Incidentes de Seguridad en AWS

1. Introducción y Contexto

1.1 Contexto del Proyecto

Las organizaciones actuales enfrentan un aumento constante de amenazas de seguridad informática. La gestión adecuada de incidentes es esencial para proteger la información de las empresas. CyberIncident es un sistema desarrollado para gestionar incidentes de seguridad utilizando servicios de Amazon Web Services (AWS), aprovechando las ventajas de la computación en la nube.

1.2 Objetivos del Sistema

Objetivo General

Implementar un sistema de información en la nube llamado CyberIncident para el registro, clasificación y análisis de incidentes de seguridad, utilizando servicios básicos de AWS con buenas prácticas de configuración y seguridad.

Objetivos Específicos

1. Desplegar una aplicación backend en una instancia EC2 con sistema operativo Linux
2. Utilizar una base de datos para almacenar información estructurada de incidentes
3. Implementar Amazon S3 para almacenamiento de evidencias
4. Integrar los servicios EC2, base de datos y S3 en una arquitectura básica
5. Documentar el proceso de despliegue y funcionamiento del sistema

2. Descripción del Sistema

2.1 Funcionalidades Principales

CyberIncident es una aplicación web que permite:

· Registrar incidentes de seguridad informática · Clasificar incidentes por tipo, severidad y estado · Adjuntar evidencias técnicas como logs, imágenes o documentos · Consultar el historial de incidentes registrados · Generar reportes y estadísticas

2.2 Arquitectura del Sistema

La arquitectura utiliza los siguientes servicios de AWS:

1. Amazon EC2: Instancia Linux que aloja la aplicación Flask
2. Base de Datos: Motor MySQL para almacenar información de incidentes
3. Amazon S3: Servicio de almacenamiento para evidencias
4. VPC: Red virtual para conectar los componentes
5. Security Groups: Control de acceso a los servicios

2.3 Flujo de Datos

1. Registro de Incidente · Usuario completa formulario · Aplicación valida datos · Se guarda en base de datos · Se registra en historial
2. Subida de Evidencias · Usuario selecciona archivo · Aplicación valida tipo y tamaño · Archivo se sube a S3 · Se guardan metadatos en base de datos · Se crea backup local
3. Consulta de Información · Aplicación consulta base de datos · Recupera información de incidentes · Genera URLs para acceder a evidencias · Presenta datos en interfaz web

3. Componentes Técnicos

3.1 Backend (Flask Application)

· Framework: Flask (Python) · Base de datos: MySQL · Almacenamiento: AWS S3 · Autenticación: Sistema básico de sesiones

3.2 Frontend

· Templates: HTML con Jinja2 · Estilos: Bootstrap 5 · JavaScript: Funcionalidades básicas

3.3 Base de Datos

Tablas principales:

· incidentes: Información de cada incidente · evidencias: Archivos adjuntos a incidentes · historial: Registro de actividades del sistema

3.4 AWS S3

· Bucket: cyberincident · Estructura: evidencias/{incidente_id}/ · Configuración: Acceso privado, encriptación SSE-S3

4. Configuración de Seguridad

4.1 EC2 Security Group

· Puerto 22 (SSH): Solo desde IP específica · Puerto 5000 (HTTP): Acceso público · Puerto 3306 (MySQL): Solo desde EC2

4.2 RDS Security Group

· Puerto 3306: Solo acceso desde EC2 Security Group

4.3 S3 Policies

· Bloqueo de acceso público · Políticas IAM restrictivas · Encriptación automática

4.4 Seguridad en la Aplicación

· Sanitización de inputs · Validación de archivos · Protección contra XSS · Límites de tamaño de archivo

5. Proceso de Despliegue

5.1 Paso 1: Configuración de AWS

1. Crear VPC y subredes
2. Configurar Internet Gateway
3. Crear Security Groups

5.2 Paso 2: Despliegue de RDS

1. Crear instancia MySQL
2. Configurar parámetros de seguridad
3. Establecer credenciales

5.3 Paso 3: Configuración de S3

1. Crear bucket

2. Configurar políticas de acceso
3. Establecer configuración de encriptación

5.4 Paso 4: Despliegue de EC2

1. Lanzar instancia Ubuntu
2. Configurar Security Group
3. Instalar dependencias
4. Desplegar aplicación

5.5 Paso 5: Configuración de Aplicación

1. Configurar conexión a base de datos
2. Establecer credenciales AWS
3. Configurar parámetros de seguridad
4. Iniciar servicio

6. Scripts y Configuraciones

6.1 Script de Inicialización EC2

```
#!/bin/bash
# Script de inicialización para instancia EC2

# Actualizar sistema
apt-get update
apt-get upgrade -y

# Instalar dependencias
apt-get install -y python3-pip python3-dev nginx git

# Instalar paquetes Python
```

```
pip3 install flask mysql-connector-python boto3 werkzeug

# Configurar Nginx
cat > /etc/nginx/sites-available/cyberincident << 'EOF'
server {
    listen 80;
    server_name _;

    location / {
        proxy_pass http://127.0.0.1:5000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
EOF

# Habilitar sitio
ln -s /etc/nginx/sites-available/cyberincident /etc/nginx/sites-enabled/
rm /etc/nginx/sites-enabled/default

# Reiniciar Nginx
systemctl restart nginx
systemctl enable nginx

# Configurar servicio Systemd
cat > /etc/systemd/system/cyberincident.service << 'EOF'
```

```
[Unit]
Description=CyberIncident Application
After=network.target

[Service]
User=ubuntu
WorkingDirectory=/var/www/cyberincident
ExecStart=/usr/bin/python3 app.py
Restart=always

[Install]
WantedBy=multi-user.target
EOF

# Iniciar servicio
systemctl daemon-reload
systemctl start cyberincident
systemctl enable cyberincident
```

6.2 Configuración de la Aplicación

```
# config.py
import os

class Config:
    # Configuración de base de datos
    DB_HOST = 'cyberincident-db.cxvvvkdnihbk.us-east-1.rds.amazonaws.com'
    DB_USER = 'Maik'
```

```
    DB_PASSWORD = 'cyberIncident123'
    DB_NAME = 'cyberincident'
    DB_PORT = 3306

    # Configuración de S3
    S3_BUCKET = 'cyberincident'
    S3_REGION = 'us-east-1'

    # Configuración de aplicación
    SECRET_KEY = 'clave-secreta-de-desarrollo'
    UPLOAD_FOLDER = 'uploads'
    MAX_CONTENT_LENGTH = 16 * 1024 * 1024  # 16MB
```

6.3 Estructura de Base de Datos

```
-- Tabla de incidentes
CREATE TABLE incidentes (
    id INT PRIMARY KEY AUTO_INCREMENT,
    titulo VARCHAR(200) NOT NULL,
    descripcion TEXT NOT NULL,
    tipo VARCHAR(50) NOT NULL,
    severidad VARCHAR(20) NOT NULL,
    estado VARCHAR(30) DEFAULT 'Abierto',
    usuario_reporta VARCHAR(100),
    fecha_creacion TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

-- Tabla de evidencias
```

```
CREATE TABLE evidencias (
  id INT PRIMARY KEY AUTO_INCREMENT,
  incidente_id INT NOT NULL,
  nombre_archivo VARCHAR(255) NOT NULL,
  tipo_archivo VARCHAR(30),
  ruta TEXT,
  s3_key VARCHAR(500),
  s3_url VARCHAR(1000),
  tamano BIGINT,
  fecha_subida TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  FOREIGN KEY (incidente_id) REFERENCES incidentes(id) ON DELETE CASCADE
);

-- Tabla de historial
CREATE TABLE historial (
  id INT PRIMARY KEY AUTO_INCREMENT,
  incidente_id INT NOT NULL,
  usuario VARCHAR(100) NOT NULL,
  accion VARCHAR(50) NOT NULL,
  descripcion TEXT,
  fecha TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  FOREIGN KEY (incidente_id) REFERENCES incidentes(id) ON DELETE CASCADE
);
```

---

7. Verificación y Monitoreo

7.1 Comandos de Verificación

```
# Verificar conexión a RDS
mysql -h cyberincident-db.cxvvvkdnihbk.us-east-1.rds.amazonaws.com -u Maik -p

# Verificar bucket S3
aws s3 ls s3://cyberincident

# Verificar aplicación
curl http://localhost:5000/status

# Verificar logs
journalctl -u cyberincident -f
tail -f /var/log/nginx/access.log
```

7.2 Monitoreo de Recursos

```
# Uso de CPU y memoria
top

# Uso de disco
df -h

# Conexiones de red
netstat -tulpn
```

---

8. Solución de Problemas

8.1 Problema: Conexión a base de datos fallida

Solución:

1. Verificar Security Groups

2. Confirmar que RDS está disponible
3. Verificar credenciales
4. Probar conexión desde EC2

8.2 Problema: Aplicación no responde

Solución:

1. Verificar estado del servicio
2. Revisar logs de error
3. Confirmar que puertos están abiertos
4. Reiniciar servicios

8.3 Problema: Archivos no se suben a S3

Solución:

1. Verificar credenciales AWS
2. Confirmar permisos del bucket
3. Verificar tamaño de archivo
4. Revisar tipos de archivo permitidos

---

9. Evidencias del Sistema

9.1 Evidencias de Amazon EC2

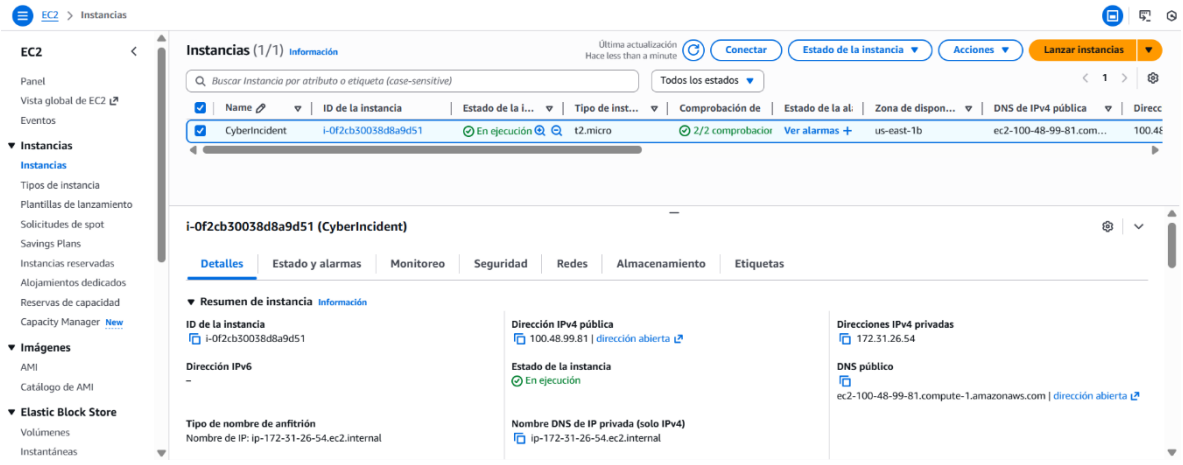
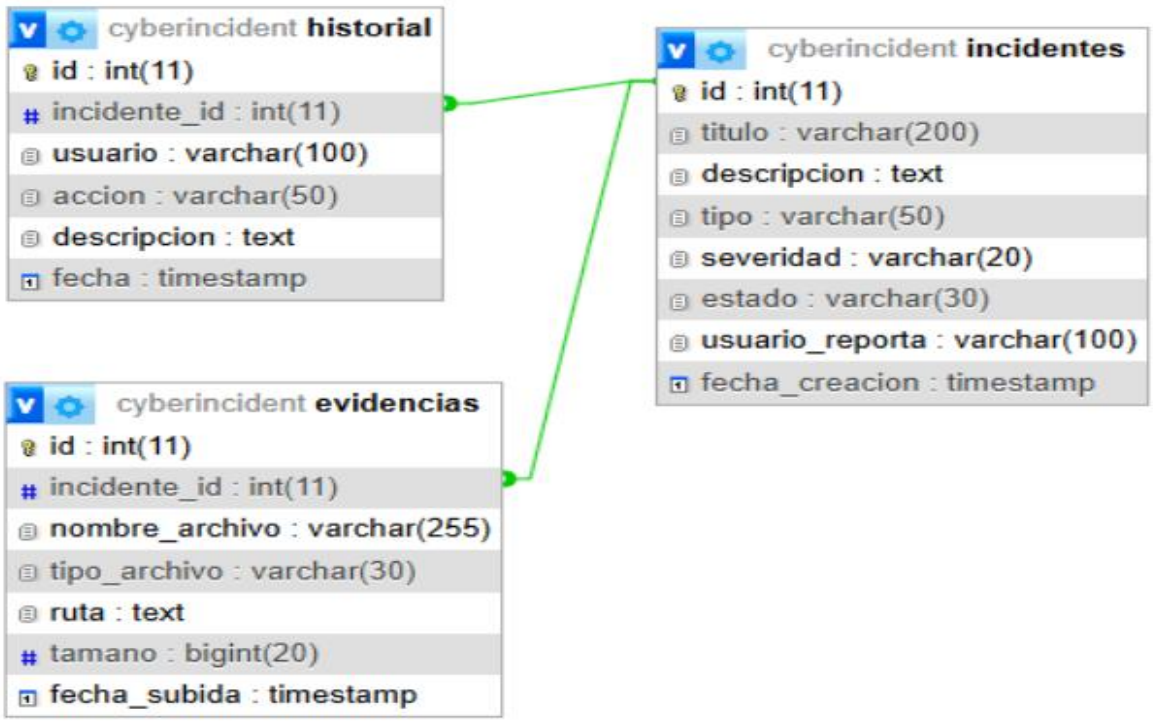
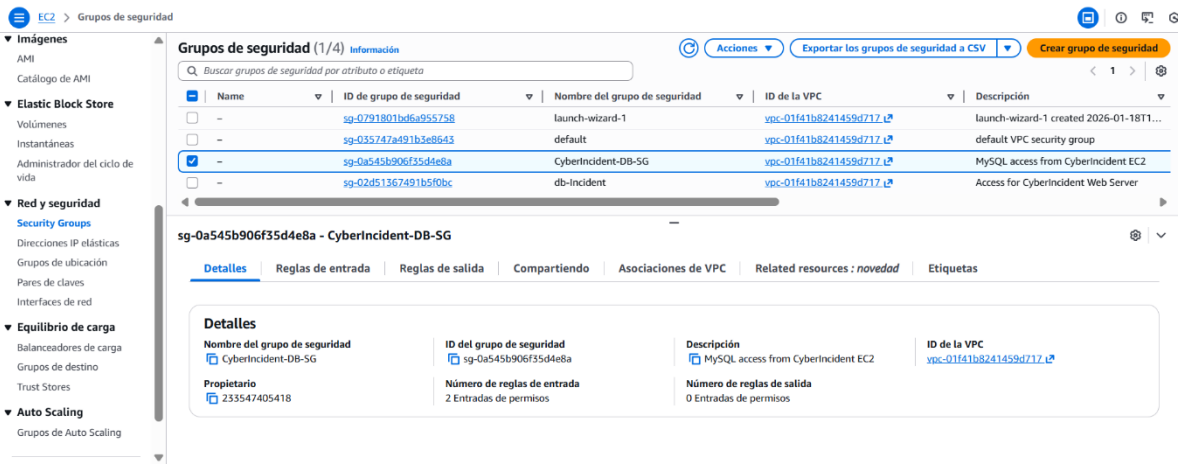
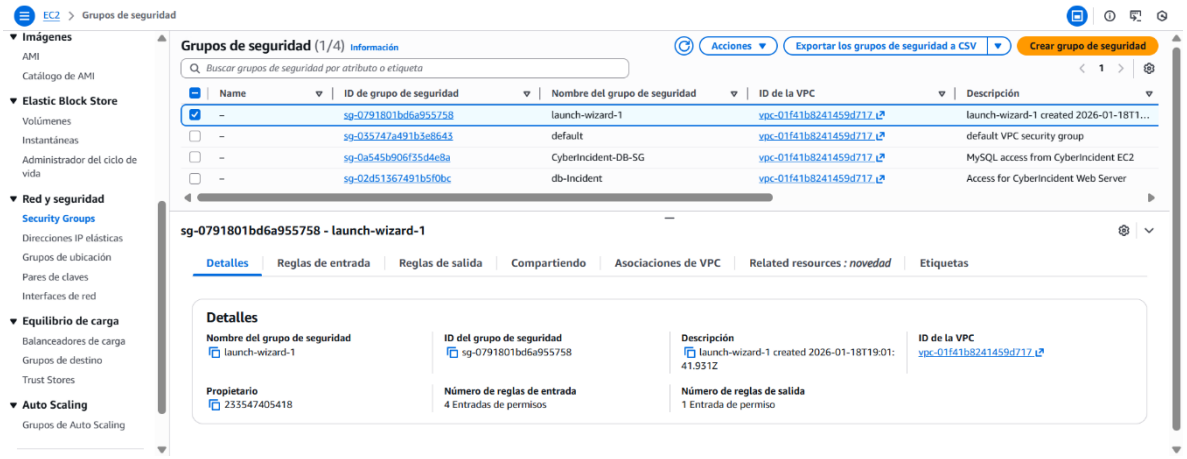


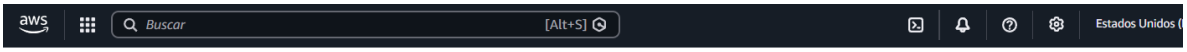
Figura 3: Configuración del Security Group asociado

Estructura de la base de datos










```
A newer release of "Amazon Linux" is available.
  Version 2023.10.20260120:
  Version 2023.10.20260120:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Jan 23 13:21:53 2026 from 18.206.107.29
[ec2-user@ip-172-31-26-54 ~]$
```

```
[ec2-user@ip-172-31-26-54 CyberIncident]$ python3 app.py
2026-01-23 14:09:51,307 - INFO - Found credentials from IAM Role: LabRole
2026-01-23 14:09:51,532 - INFO - Cliente S3 inicializado - Bucket: cyberincident

============================================================
CYBERINCIDENT - Sistema de Gestion de Incidentes
============================================================
BASE DE DATOS: AWS RDS MySQL
Host: cyberincident-db.cxvvvkdnihbk.us-east-1.rds.amazonaws.com
Usuario: Maik
Puerto: 3306
============================================================
ALMACENAMIENTO: AWS S3
Bucket: cyberincident
Region: us-east-1
Carpeta: evidencias/
S3 disponible: True
============================================================
URL principal: http://0.0.0.0:5000
Estado: http://0.0.0.0:5000/status
============================================================
2026-01-23 14:09:51,586 - INFO - Base de datos verificada/actualizada
Base de datos actualizada para S3
```

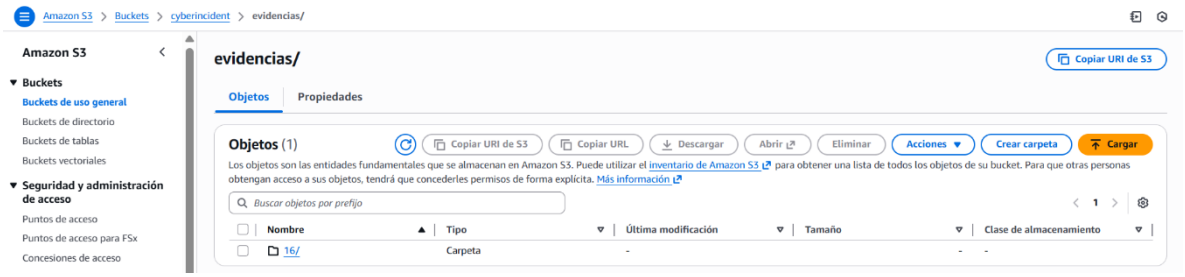
9.2 Evidencias de la Base de Datos (RDS / MySQL)


```
[ec2-user@ip-172-31-26-54 CyberIncident]$ mysql -h cyberincident-db.cxvvvkdnihbk.us-east-1.rds.amazonaws.com -u Maik -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1448
Server version: 8.0.43 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| cyberincident      |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.007 sec)
```

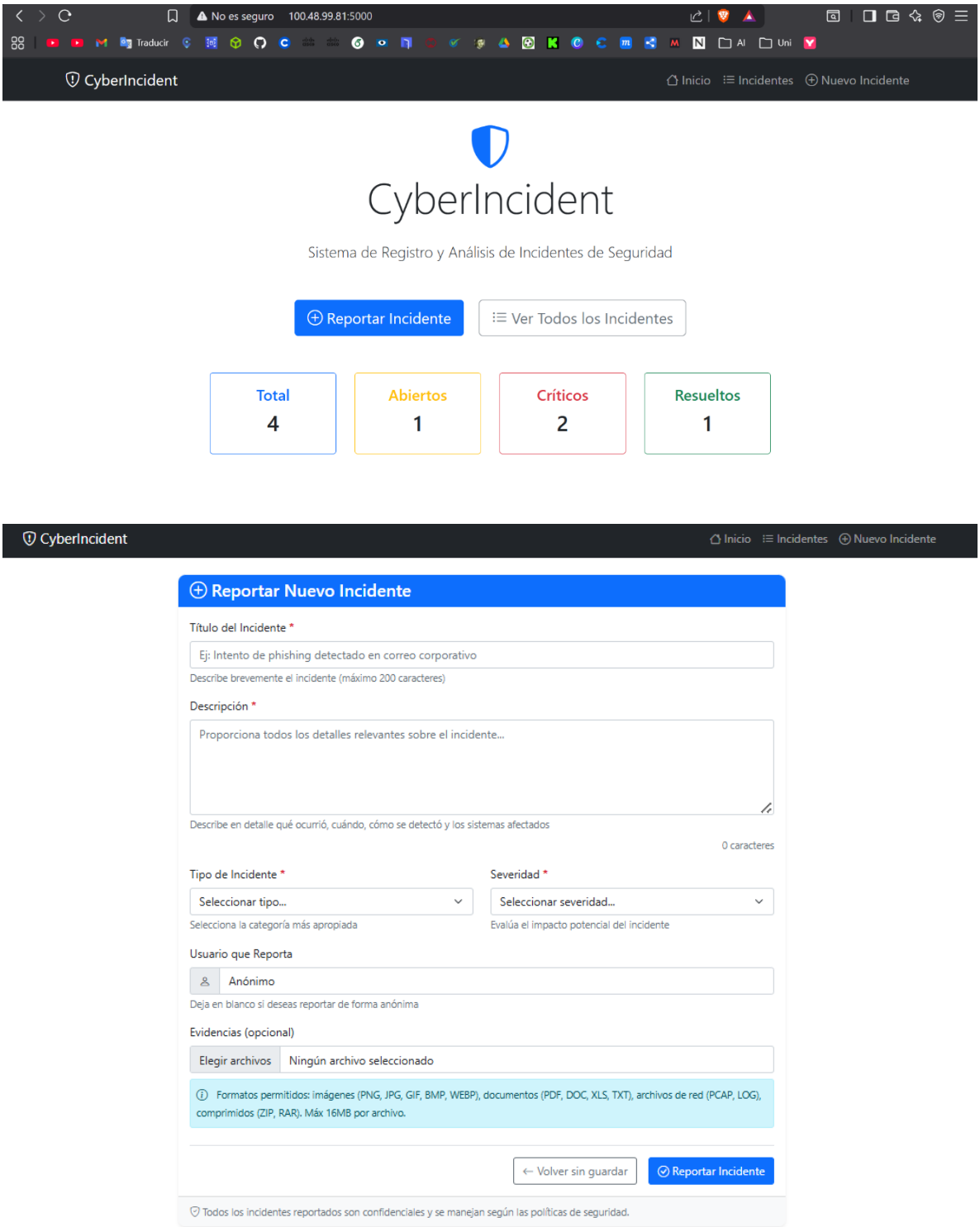
```
MySQL [(none)]> USE cyberincident;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [cyberincident]> SHOW TABLES;
+-------------------------+
| Tables_in_cyberincident |
+-------------------------+
| evidencias              |
| historial               |
| incidentes              |
+-------------------------+
3 rows in set (0.002 sec)

MySQL [cyberincident]>
```

```
MySQL [(none)]> USE cyberincident;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [cyberincident]> SHOW TABLES;
+-------------------------+
| Tables_in_cyberincident |
+-------------------------+
| evidencias              |
| historial               |
| incidentes              |
+-------------------------+
3 rows in set (0.002 sec)

MySQL [cyberincident]> SELECT * FROM incidentes;
+----+-------------------------------+-----------------------------------------+-----------+-----------+-----------------+----------------+---------------------+
| id | titulo                        | descripcion                             | tipo      | severidad | estado          | usuario_reporta | fecha_creacion      |
+----+-------------------------------+-----------------------------------------+-----------+-----------+-----------------+----------------+---------------------+
|  1 | Intento de phishing detectado | Se recibieron correos sospechosos       | phishing  | media     | Abierto         | admin          | 2026-01-23 01:24:41 |
|  2 | Malware en equipo             | Antivirus detectó troyano               | malware   | alta      | En Investigación | soporte        | 2026-01-23 01:24:41 |
|  3 | Acceso no autorizado          | Intentos de acceso desde IPs desconocidas | intrusion | critica   | Resuelto        | admin          | 2026-01-23 01:24:41 |
|  5 | Hola ayuda me jakian          | me jakiaron                             | malware   | critica   | En Investigación | Sebas          | 2026-01-23 01:35:54 |
+----+-------------------------------+-----------------------------------------+-----------+-----------+-----------------+----------------+---------------------+
4 rows in set (0.001 sec)

MySQL [cyberincident]>
```

9.3 Evidencias de Amazon S3



9.4 Evidencias del Funcionamiento de la Aplicación


No es seguro
100.48.99.81:5000
CyberIncident
Inicio
Incidentes
Nuevo Incidente
CyberIncident
Sistema de Registro y Análisis de Incidentes de Seguridad
Reportar Incidente
Ver Todos los Incidentes
Total
4
Abiertos
1
Críticos
2
Resueltos
1
CyberIncident
Inicio
Incidentes
Nuevo Incidente
Reportar Nuevo Incidente
Título del Incidente *
Ej: Intento de phishing detectado en correo corporativo
Describe brevemente el incidente (máximo 200 caracteres)
Descripción *
Proporciona todos los detalles relevantes sobre el incidente...
Describe en detalle qué ocurrió, cuándo, cómo se detectó y los sistemas afectados
0 caracteres
Tipo de Incidente *
Seleccionar tipo...
Selecciona la categoría más apropiada
Severidad *
Seleccionar severidad...
Evalúa el impacto potencial del incidente
Usuario que Reporta
Anónimo
Deja en blanco si deseas reportar de forma anónima
Evidencias (opcional)
Elegir archivos
Ningún archivo seleccionado
Formatos permitidos: imágenes (PNG, JPG, GIF, BMP, WEBP), documentos (PDF, DOC, XLS, TXT), archivos de red (PCAP, LOG), comprimidos (ZIP, RAR). Máx 16MB por archivo.
Volver sin guardar
Reportar Incidente
Todos los incidentes reportados son confidenciales y se manejan según las políticas de seguridad.

Incidente #26 - Acceso no autorizado al servidor web

Abierto

Tipo de Incidente

Intrusion

Severidad

Alta

Descripción

Se detectaron múltiples intentos de acceso no autorizado desde una IP extranjera. El sistema de monitoreo registró intentos de fuerza bruta contra el servicio SSH.

Reportado por

Maicol Nuñez

Fecha de Creación

23/01/2026 14:26

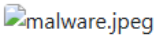
Cambiar estado: Abierto

Eliminar Incidente

Evidencias Adjuntas

1

Imágenes



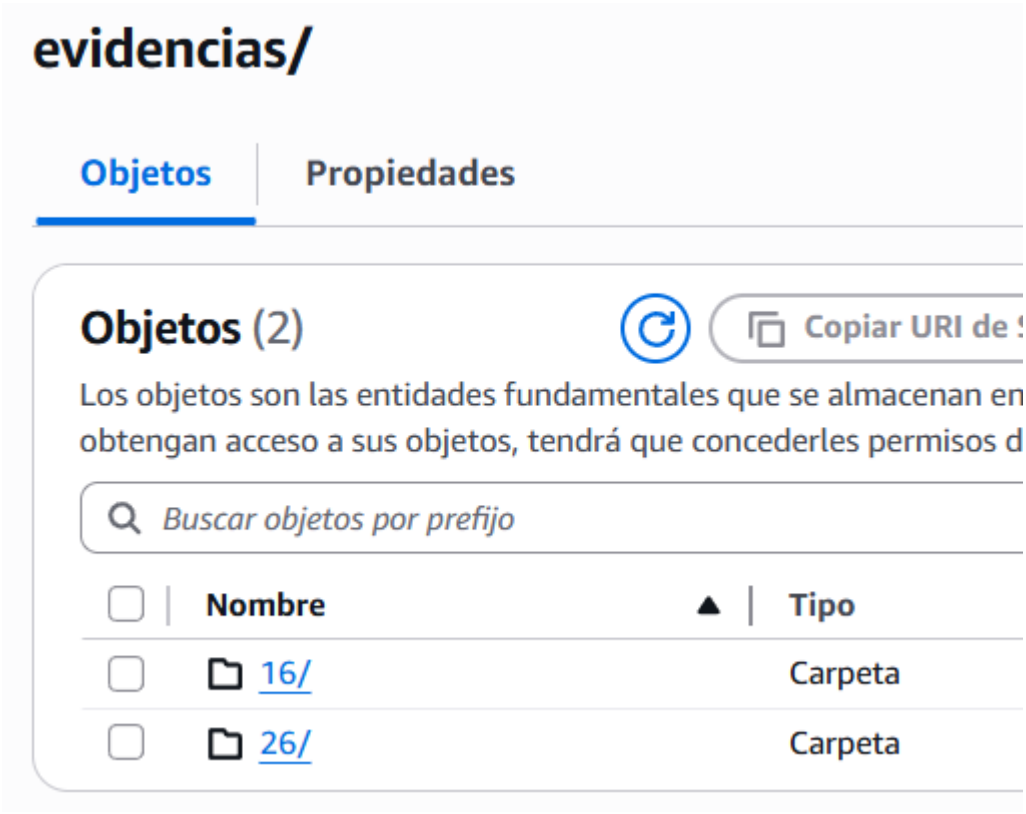
malware.jpeg

6.55 KB

Documentos

No hay documentos adjuntos

```
2026-01-23 14:21:52,116 - WARNING -  * Debugger is active!
2026-01-23 14:21:52,117 - INFO -  * Debugger PIN: 542-516-432
2026-01-23 14:22:07,886 - INFO - 190.145.6.251 - - [23/Jan/2026 14:22:07] "GET / HTTP/1.1" 200 -
2026-01-23 14:22:08,722 - INFO - 190.145.6.251 - - [23/Jan/2026 14:22:08] "GET /static/img/Codeic.png HTTP/1.1" 200 -
2026-01-23 14:22:33,033 - INFO - 190.145.6.251 - - [23/Jan/2026 14:22:33] "GET /incidentes/nuevo HTTP/1.1" 200 -
2026-01-23 14:26:54,513 - INFO - Archivo subido a S3: evidencias/26/f648a5d3-8d2c-4559-ae7c-c289ed3c24a3.jpeg
2026-01-23 14:26:54,523 - INFO - 190.145.6.251 - - [23/Jan/2026 14:26:54] "POST /incidentes/crear HTTP/1.1" 302 -
2026-01-23 14:26:54,656 - INFO - 190.145.6.251 - - [23/Jan/2026 14:26:54] "GET /incidentes/26 HTTP/1.1" 200 -
2026-01-23 14:26:55,037 - INFO - 190.145.6.251 - - [23/Jan/2026 14:26:55] "GET /ver_imagen/23 HTTP/1.1" 302 -
```



10. Anexos

Anexo A: Comandos AWS CLI Utilizados

EC2

aws ec2 describe-instances

aws ec2 run-instances

aws ec2 create-security-group

RDS

aws rds create-db-instance

```
aws rds describe-db-instances


# S3
aws s3api create-bucket
aws s3api put-public-access-block
aws s3 ls
```

Anexo B: Estructura del Proyecto

```
cyberincident/
├── app.py
├── config.py
├── requirements.txt
├── templates/
│   ├── base.html
│   ├── index.html
│   ├── incidentes.html
│   ├── nuevo_incidente.html
│   ├── detalle.html
│   ├── historial.html
├── static/
│   ├── css/
│   ├── js/
│   └── img/
├── uploads/
└── README.md
```

Anexo C: Referencias Técnicas

1. Documentación oficial AWS
2. Flask Documentation
3. MySQL Documentation
4. Bootstrap Documentation
5. Python Documentation

Arquitectura de Gestion de incidentes