# Arquitecturas de Sistemas para la Seguridad de la Información en las EPS de Colombia

Juan Pablo Daza Pinzon, Juan Sebastian Rodriguez Peña

Septiembre 2023

## 1. Abstract

In recent years, Healthcare Promoting Entities (EPS) in Colombia have experienced a significant increase in cyber threats and information security vulnerabilities. This document addresses the cybersecurity issues that have affected Colombian EPS and analyzes the system architectures designed to address these concerns.

This document aims to provide a comprehensive overview of the cybersecurity challenges facing EPS in Colombia and offer key recommendations to strengthen information security in this critical healthcare sector.

## 2. Introducción

En los últimos años, las Entidades Promotoras de Salud (EPS) en Colombia han experimentado un aumento significativo en las amenazas cibernéticas y las vulnerabilidades de seguridad de la información. Este documento aborda las problemáticas de ciberseguridad que han afectado a las EPS colombianas y analiza las arquitecturas de sistemas diseñadas para abordar estas preocupaciones.

En última instancia, este documento busca proporcionar una visión integral de las problemáticas de ciberseguridad que enfrentan las EPS en Colombia y ofrecer recomendaciones clave para fortalecer la seguridad de la información en este sector crítico de la atención médica.

## 3. Descripción y Caracterización del Problema

El sistema de salud en nuestra nación se ha convertido en un tema de gran controversia, especialmente debido a las extensas esperas para obtener citas médicas y las largas filas para obtener documentos esenciales. Agravando aún más esta

situación, se encuentra la problemática que detallamos en este documento: nuestros servicios de salud han caído víctimas de ciberataques. Esta situación ha dado lugar a que las personas tengan que soportar aún más demoras para acceder a los mencionados servicios. Además, ha obligado a muchos profesionales de la salud que, en el pasado, habían adoptado la digitalización en su trabajo, a regresar a métodos más convencionales, como el uso de papel. Esto representando un problema multifacetico el cual involucra que se lleguen a filtrar datos sensibles, continuidad en la atencion medica e incluso la atencion en los centros; por lo cual es necesario abordar estos para garantizar a los usuarios integridad, confidencialidad y disponibilidad de la informacion de la salud en el pais.

# 4. Objetivos

## 4.1 Objetivo General

Realizar la implementación de una arquitectura para la mejora de la ciberseguridad y la protección de la privacidad de los usuarios de las EPS.

## 4.2 Objetivos especificos

- Investigar el porque se han realizado diferentes ataques a las EPS.
- Crear una arquitectura que mejore la seguridad del sistema.
- Implementación de un SOAR para el manejo y control de incidentes.

# 5. Marco Teórico

## 5.1 Ciberseguridad

Al ciberseguridad es la practica de proteger sistemas, redes y programas de ataques digitales. El objetivo principal de la ciberseguridad es garantizar la confidencialidad, la integridad y la disponibilidad de la información en entornos digitales.

## 5.2 EPS

Las Entidades Promotoras de Salud son parte del sistema de salud colombiano, su función es administrar los recursos destinados a la salud de los afiliados y coordinar la atención médica que estos reciben. Una definicion dada por el Gobierno de Colombia es:

Entidades responsables de la afiliación y registro de los afiliados al sistema de la regularidad social en Colombia. Se encargan también del recaudo de las cotizaciones y su función básica es organizar y garantizar la prestación del plan obligatorio de salud.

## 5.3 SOAR

Es la estrategia y herramientas diseñadas para mejorar la capacidad de una organización para abordar y responder a amenazas cibernéticas de manera mas eficiente y efectiva.

Sus siglas representan Security Orchestation, Automation and Response, su principal objetivo es monitorizar el sistema y tener predefinidos ciertas directrices si se presenta un ataque o se detecta una amenaza.

## 5.4 Sanitas

Sanitas es una compañía de seguros de salud que ofrece una amplia gama de seguros médicos y servicios de salud para cada necesidad y momento. Esta compañía se especializa en la mejora de la calidad de vida, la salud y el bienestar de las personas. Sanitas proporciona seguros de salud con las mejores coberturas médicas, hospitales y centros propios, clínicas dentales y cuidado de mayores.

## 5.5 Cafam

Cafam es una Caja de Compensación Familiar en Colombia con más de 65 años de trayectoria. Ofrece bienestar a los usuarios y a más de 800 mil afiliados con sus familias, a través de un completo portafolio de productos y servicios. Cafam proporciona servicios como vivienda, turismo, salud integral, educación, recreación, cultura, eventos, subsidios, empleo, créditos y seguros.

## 5.6 Keralty

Keralty es un grupo de empresas privadas comprometidas en mantener saludable a la población, a través de un Modelo de Salud Integral propio. Este modelo se basa en la prevención, identificación y gestión de riesgos en la salud, así como en el control y cuidado de la enfermedad y la dependencia.

Keralty ofrece un modelo de servicios socio-sanitarios dedicado al cuidado, manejo y acompañamiento de la fragilidad y la dependencia a lo largo de la vida de las personas. Este modelo se implementa mediante un grupo de empresas especializadas, que logran un mayor valor en salud y generan bienestar en la población atendida, en sus familias y en la comunidad.

Además, Keralty tiene presencia en varios países como Colombia(Sanitas), Estados Unidos, México, Brasil, España, Perú, Venezuela, Filipinas, República Dominicana y Puerto Rico. En cada país, Keralty se asocia localmente con entidades que les permiten entender la cultura y las necesidades de la población para adaptar sus servicios a las realidades particulares de cada región.

En resumen, Keralty es una organización global que ofrece servicios sanitarios, sociales y comunitarios para mantener saludables a las personas que confían en su cuidado.

### 5.7 RansomHouse

RansomHouse es un nuevo grupo de extorsión que se infiltra en las redes de sus víctimas explotando vulnerabilidades para robar datos y obliga a las víctimas a pagar, a menos que sus datos sean vendidos al mejor postor. Y si ningún criminal está interesado en comprar los datos, el grupo los filtra en su sitio de filtraciones.

Este grupo también es único en la forma en que extorsiona dinero de las víctimas. Parecen comercializarse a sí mismos como probadores de penetración y cazadores de recompensas por errores más que como el típico extorsionista en línea. Después de robar datos de los objetivos, ofrecen eliminarlos y luego proporcionan un informe completo sobre qué vulnerabilidades explotaron y cómo.

Al igual que los grupos de ransomware, también tienen canales establecidos, una cuenta de Telegram y un sitio de filtraciones, para comunicarse con las víctimas, los periodistas y aquellos que quieren seguir sus actividades.

Se cree que RansomHouse surgió en diciembre de 2021 y actualmente tiene cuatro víctimas, la primera de las cuales fue la Autoridad de Licores y Juegos de Saskatchewan (SLGA) de Canadá, un regulador del alcohol, el cannabis y la mayoría del juego en la provincia, que informó por primera vez de una violación en ese mismo mes y año.

Según la página "Acerca de" en el sitio Onion de RansomHouse, se llaman a sí mismos "una comunidad profesional de mediadores".

### 5.8 SOC

Son las siglas para Security Operations Center, es el centro de operaciones de una organización para todo el tema de seguridad TI, con ls finalidad de tener todo el registro y monitoreo de la información en un solo lugar y que el equipo de seguridad tenga a su disposición todas las herramientas que requieran para poder llevar a cabo su tarea de proteger los activos de la organización.

Se encarga de preparar los recuros para poder responder ante un ataque, planea estrategias de seguridad para mantener la organizacion en buen estado y previene cualquier afectacion a los servicios que sean prestados.

## 6. Estado del arte

### 6.1 Actualidad del SOAR

Los ciberataques son mas comunes que nunca, y cada vez son mas sofisticados que nunca, esto está causando que muchas organizaciones destinen más recursos a la ciberseguridad de sus negocios. Aunque exista mas presupuesto para proteger los activos, no ha sido suficiente ante las contantes amenazas que existen hoy en día. Se generan demasiadas alertas de seguridad ralentizando los SOC (Security Operations Center) y responder a todas estas alertas es una tarea laboriosa y conlleva mucho tiempo y aquí es donde entran los SOAR.

La tecnología SOAR ofrece un sistema que logra identificar automáticamente las vulnerabilidades y responde a ellas sin necesidad de intervención humana. Además, cada organización puede definir y establecer como desea reaccionar a un evento, lo que permite liberar tiempo y presupuesto para centrarse en proyectos más prioritarios.

## 6.2 Lideres

Las grandes empresas de software destinan muchos recursos al desarrollo de herramientas destinadas a la ciberseguridad, por ejemplo:

- Microsoft: Tiene a su disposición SIEM y XDR
- IBM: Presta su servicio con IBM Security QRadar SOAR
- Red Hat: Utiliza un software opensource llamado Red Hat Ansible Automation Platform
- Amazon: Dentro de sus módulos ofrece Amazon GuardDuty

## 6.3 Situacion de las EPS

El sistema de salud en nuestra nación se ha convertido en un tema de gran controversia, especialmente debido a las extensas esperas para obtener citas médicas y las largas filas para obtener documentos esenciales. Agravando aún más esta situación, se encuentra la problemática que detallamos en este documento: nuestros servicios de salud han caído víctimas de ciberataques.

Un ejemplo de este más relevante es el ataque que fue realizado a la EPS Sanitas en Colombia. En el cual el grupo Ransomhouse, logro vulnerar el sistema impuesto por el grupo Keralty, el cual es contratado por sanitas para alojar sus datos digitalmente, este ciberataque dio paso en noviembre del 2022 y dio como resultado la filtración de datos personales de pacientes y empresas con las cuales sanitas hizo negociaciones, entre los datos que se filtraron se pueden encontrar documentos personales, historial médico, entre otros. Esta situación da lugar a que las personas tengan que soportar aún más demoras para acceder a los servicios que la EPS ofrece, y obligo a que muchos profesionales de la salud, que en el pasado habían optado por la digitalización de su trabajo, a volver a métodos antiguos, como el uso del papel.

Esto representa un problema multifacético porque involucra datos sensibles, la continuidad en la atención medica e incluso la atención en los centros médicos, por lo cual se debe abordar para así garantizar a los usuarios integridad, confidencialidad y disponibilidad de la información de la salud en el país.

# 7. Propuesta de solución

## 7.1 Explicacion

La gran cantidad de datos personales que se almacenan para el sistema de salud hace que sean un objetivo de los atacantes debido aque pueden secuestrar estos datos y solicitar un rescate por parte de la EPS atacada, por esto, es de vital importancia que la arquitectura de un sistema tan delicado sea monitorazada y controlada.

Dando la solucion, se puede implementar un sistema SOAR para lograr que la informacion sea monitorizada y la respuesta a incidentes sea rapida y efectiva.

Por medio de la automatización se pueden llevar a cabo funciones que sean tediosas y repetitivas con el objetivo de delegarlas al sistema y reubicar los recursos humanos a zonas donde sea mas necesario. Para responder ante cualquier incedente se debe plantear una buena arquitectura y se debe estructurar un plan de acción para la proteccion de los datos de los usuarios.

## 7.2 Arquitectura

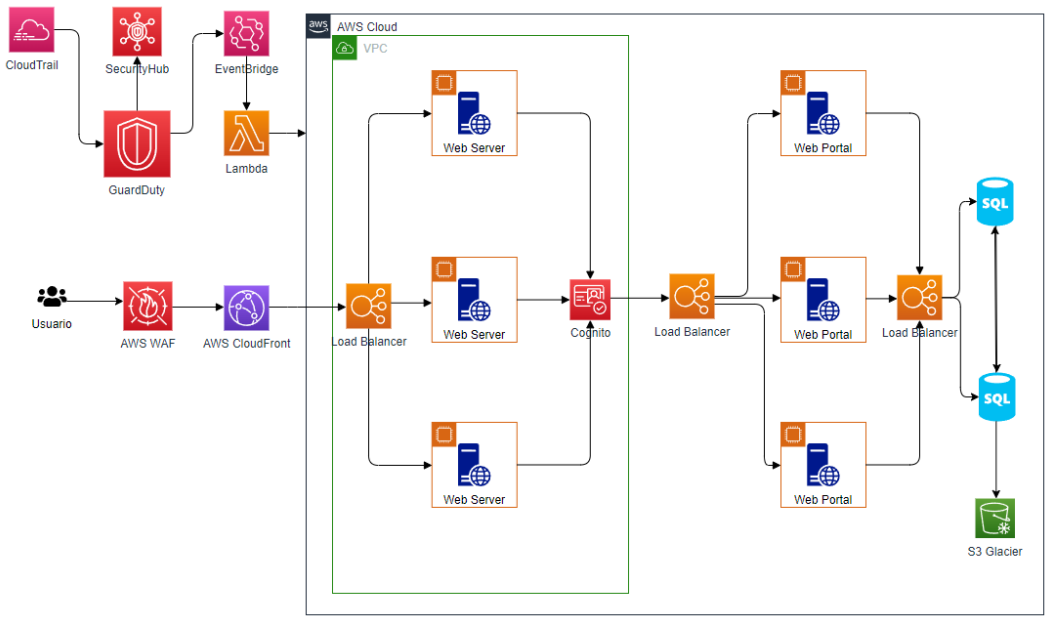


Figure 1: Arquitectura propuesta

En nuestra arquitectura queremos establecer diferentes modulos que ofrece AWS, el primero seria su WAF, el cual presta la protección contra ataques web comunes que afecten la disponibilidad. Nuestra intención es mostrar una pagina

de fachada que muestre los servicios de la organizacion y que dentro de esta exista un apartado para iniciar sesion.

AWS CloudFront es un módulo para optimizar las conexiones y mejorar el servicio y su repuesta, AWS Cognito es el módulo encargado de la configuración de cuentas de usuarios, maneja el Inicio de Sesión y el Registro y su objetivo es proteger la aplicación web de accesos no autorizados y demás.

El usuario puede acceder a un Web Server a travez de un balanceador de carga que lo redigirá a un servidor que este disponible. El usuario podrá iniciar sesión con el objetivo de ver su información personal. Una vez el usuario acccede a travez de Cognito, otro balanceador de carga lo redirige a un servidor en donde esta el portal Web y este puede realizar las consultas a las bases de datos, las cuales estan sincronizadas y guardan un Back Up de la información en un módulo S3 Glacier.

Toda la actividad esta siendo monitorizada por AWS GuardDuty, quien se va a encargar de detectar comportamientos extraños, alertar y responder frente a estos. GuardDuty utiliza AWS EventBridge para poder tomar accion frente a los incidentes de seguridad. Las funciones Lambda juegan un papel importante ya que por medio de estas se pueden tomar medidas frente a los incidentes y lograr mantener el sistema seguro.

## 7.3 Arquitectura POC

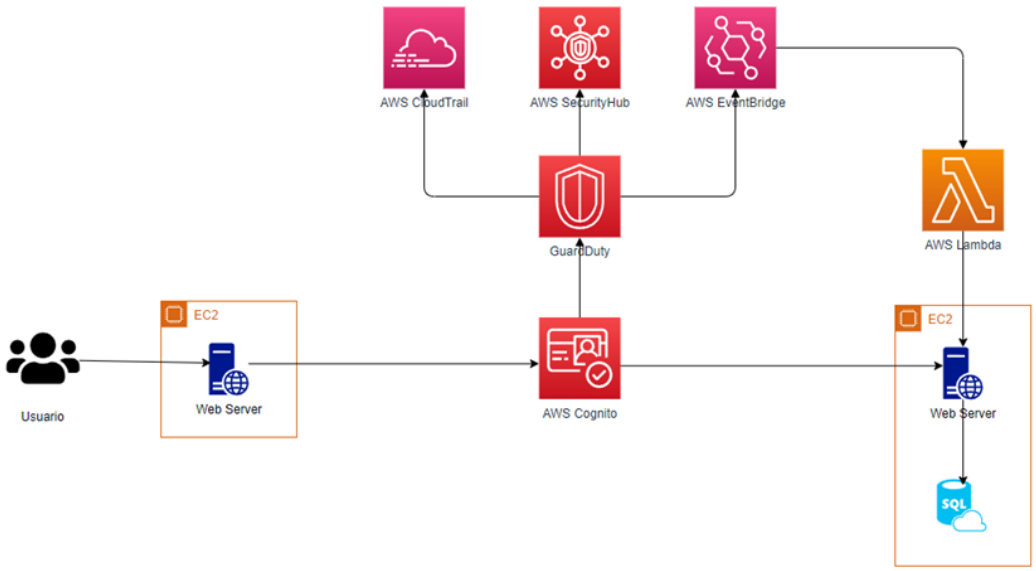


Figure 2: Arquitectura POC

Para nuetra POC (Proof of Concept), tenemos una arquitectura mas pequeña

que solo va probar el funcionamiento del SOAR frente a una instancia EC2 que haya sido comprometida y se esta intentando conectar a una IP fuera de la red.

GuardDuty es capaz de detectar la actividad y la instancia es apagada para mantener la seguridad del sistema.

### 7.4 Resultados

Realizamos 20 incidentes dentro de la instancia y calculamos el tiempo de respuesta:

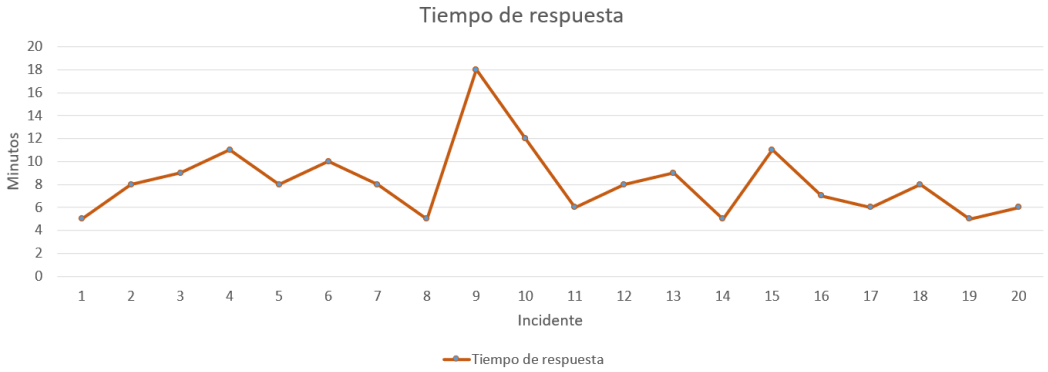


Figure 3: Tiempo de respuesta

Podemos ver que el promedio fue de 8.25 minutos y tuvimos un pico de 18 minutos, el cual puede ser evidenciado en la gráfica. Esto nos deja como conclusion que GuardDuty si detecta los incidentes pero algunas veces su tiempo de respuesta no es el esperado.

## 8. Conclusiones

- Las EPS deben implementar un mejor sistema de seguridad ya que la informacion que almacenan es muy delicada y es necesario protegerla.
- El SOAR ayuda a la automatización con la finalidad de mejorar la respuesta y la proteccion de los datos.
- Si se implementa un SOAR se puede controlar la información de una manera mas eficiente y mejorar la respuesta ante posibles incidentes que pongan en peligro la información de los usuarios.

## References

[1] Cisco®. Ciberseguridad. https://www.cisco.com/c/es$_mx$/*products*/*security*/*what*−*is* − *cybersecurity.html*.

[2] Gobierno de Colombia. Eps. https://www.sdp.gov.co/transparencia/informacion-interes/glosario/entidad-promotora-de-salud-eps.

[3] Red Hat. Soar. https://www.redhat.com/es/topics/security/what-is-soar.

[4] Amazon. Aws waf. https://aws.amazon.com/waf/?nc1=h$_l s$.

[5] Amazon. Aws cognito. https://aws.amazon.com/cognito/?nc1=h$_l s$.

[6] Gartner. Security orchestation automation and response solution reviews and ratings. https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions.

[7] Hackeo Sanitas. Ciberataque a sanitas: hackers revelaron más información clasificada de la eps. https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/.

[8] Hackeo Cafam. Atención: falla en el sistema de cafam en bogotá es un ciberataque. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cafam-esta-siendo-victima-de-un-ciberataque-hay-fallas-en-servicios-778440: :text=Laura

[9] Red Hat. Red hat ansible automation platform. https://www.redhat.com/es/topics/security/what-is-soar.

[10] Microsoft. Xdr. https://www.microsoft.com/en-us/security/business/solutions/siem-xdr-threat-protection.

[11] IBM. Ibm security qradar soar. https://www.ibm.com/products/qradar-soar.

[12] Amazon. Amazon guardduty. https://aws.amazon.com/guardduty/.

[13] IBM. Ibm soc. https://www.ibm.com/topics/security-operations-center.

[14] Jovi Umawing. Threat profile: Ransomhouse makes extortion work without ransomware. https://www.malwarebytes.com/blog/news/2022/05/threat-profile-ransomhouse-makes-extortion-work-without-ransomware.

[15] Sanitas es. Sanitas. https://www.sanitas.es/.

[16] Cafam. Caja de compensación familiar cafam. https://www.cafam.com.co/.