Automatización de procesos para obtener una evaluación de buenas prácticas en usuarios de AWS: Revisión de políticas, permisos y seguridad en AWS

Sebastián Escobar Osorio

Informe final para optar al título de Ingeniero de Telecomunicaciones

Modalidad de Práctica

Semestre de Industria o Práctica Empresarial

Asesor Interno

Juan Pablo Urrea Tejada, PhD

Asesor Externo

Andrés Felipe Bernal Bernal, Ingeniero de Sistemas

Universidad de Antioquia

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Medellín, Antioquia, Colombia

2025

Cita	Escobar Osorio, 2025
Referencia **Estilo APA 7 (2020)**	Escobar Osorio, S. (2025). *Automatización de procesos para obtener una evaluación de buenas prácticas en usuarios de AWS* [Informe de práctica]. Universidad de Antioquia, Medellín, Colombia.



UNIVERSIDAD DE ANTIOQUIA
Vicerrectoría de Docencia

Sistema de Bibliotecas

Centro de Documentación Ingeniería (CENDOI)

Repositorio Institucional: http://bibliotecadigital.udea.edu.co

Universidad de Antioquia - www.udea.edu.co

El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Antioquia ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por los derechos de autor y conexos.

Tabla de contenido

Resumen 8

Abstract 9

1. Introducción 10

2. Objetivos 12

2.1 Objetivo general 12

2.2 Objetivos específicos 12

3. Marco teórico 13

3.1. Fundamentos de AWS y Seguridad en la Nube 13

3.2. Automatización con Python y Boto3 13

3.3 Componentes clave de la solución 14

3.4 Integración de herramientas 14

3.5 Lecciones aprendidas 15

4. Metodología 16

4.1 Documentación de referencia y políticas de seguridad 16

4.3 Aspectos críticos evaluados 20

4.4 Validación manual con CSV 21

4.6 Mejoras planificadas 22

4.7 Notas técnicas: 22

4. Análisis de resultados 23

6. Conclusiones y recomendaciones 27

6.1. Cumplimiento Objetivo General 27

6.2. Cumplimiento Objetivos Específicos 27

6.2.1. Levantar requerimientos para la solución 27
6.2.2. Establecer estrategia de implementación 28
6.2.3. Implementar la solución en Python 28
6.2.4. Evaluar efectividad con pruebas 28
Referencias 31
Anexos 32
Anexo 1. Hallazgos Cuenta cerberus 32
Anexo 2. Hallazgos Cuenta koba 33
Anexo 3. Hallazgos Cuenta hyperion 35
Anexo 4. Hallazgos Cuenta feel 37
Anexo 5. Hallazgos Cuenta facturacion electronica 39
Anexo 6. Hallazgos Cuenta databricks 41
Anexo 7. Hallazgos Cuenta cliente unico 43
Anexo 8. Hallazgos Cuenta master 44
Anexo 9. Usuarios por cuenta 47

Lista de tablas

Tabla 1 Resumen de Extracción de Datos IAM 17

Tabla 2 Resumen de Escenarios y Soluciones de Seguridad en AWS 17

Tabla 3 Hallazgos Críticos cuenta cerberus 32

Tabla 4 Datos Relevantes Cuenta cerberus 33

Tabla 5 Hallazgos Críticos cuenta koba 33

Tabla 6 Datos Relevantes Cuenta koba 34

Tabla 7 Hallazgos Críticos cuenta hyperion 35

Tabla 8 Datos Relevantes Cuenta hyperion 36

Tabla 9 Hallazgos Críticos cuenta feel 37

Tabla 10 Datos Relevantes Cuenta feel 38

Tabla 11 Hallazgos Críticos cuenta facturacion electronica 39

Tabla 12 Datos Relevantes Cuenta facturacion electronica 40

Tabla 13 Hallazgos Críticos cuenta databricks 41

Tabla 14 Datos Relevantes Cuenta databricks 42

Tabla 15 Hallazgos Críticos cuenta cliente unico 43

Tabla 16 Datos Relevantes Cuenta cliente unico 44

Tabla 17 Hallazgos Críticos cuenta master 44

Tabla 18 Datos Relevantes Cuenta master 45

Lista de figuras

Figura 1 Flujo de Procesamiento para la Auditoría IAM Automatizada 19

Figura 2 Usuarios cuenta cerberus 47

Figura 3 Usuarios cuenta facturación electrónica 48

Figura 4 Usuarios cuenta koba 49

Figura 5 Usuarios cuenta feel 50

Figura 6 Usuarios cuenta feel parte 2 51

Figura 7 Usuarios cuenta feel parte 3 52

Figura 8 Usuarios cuenta feel parte 4 53

Figura 9 Usuarios cuenta databricks 53

Figura 10 Usuarios cuenta hyperion2 53

Figura 11 Salida cuenta cliente unico 53

Figura 12 Usuarios cuenta master 54

Siglas, acrónimos y abreviaturas

AWS	Amazon Web Services
IAM	Identity and Access Management
MFA	Multi-Factor Authentication
CIS	Center for Internet Security
EC2	Elastic Compute Cloud
S3	Simple Storage Service
ECR	Elastic Container Registry
AttachedPolicies	Políticas asignadas directamente
Inline Policies	Políticas embebidas en entidades IAM

Resumen

El proyecto automatizó la evaluación de configuraciones de seguridad en AWS para reducir riesgos y optimizar procesos manuales propensos a errores. Mediante Python y Boto3, se desarrolló una herramienta que audita políticas de IAM, verifica alarmas en servicios clave (EC2, S3, RDS) y detecta configuraciones inseguras, como buckets públicos o permisos excesivos.

La solución generó reportes en Excel, reduciendo el tiempo de auditoría de horas a minutos y mejorando la precisión al eliminar errores humanos. Se identificaron vulnerabilidades críticas, permitiendo su corrección oportuna. Los resultados demostraron mayor eficiencia en la gestión de seguridad y cumplimiento con el *AWS Well-Architected Framework*.

Palabras clave: AWS, automatización, seguridad, IAM, Python.

Abstract

The project automated the evaluation of AWS security configurations to reduce risks and optimize manual processes prone to error. Using Python and Boto3, a tool was developed to audit IAM policies, verify alarms in key services (EC2, S3, RDS), and detect insecure configurations such as public buckets or excessive permissions.
The solution generated Excel reports, reducing audit time from hours to minutes and improving accuracy by eliminating human error. Critical vulnerabilities were identified, allowing timely remediation. The results demonstrated greater efficiency in security management and compliance with the AWS Well-Architected Framework.

Keywords: AWS, automation, security, IAM, Python.

1. Introducción

SoftwareOne es una empresa multinacional suiza con operaciones en Colombia desde el año 2012. Su enfoque principal está en ofrecer servicios relacionados con transformación digital, migración a la nube y gestión de aplicaciones empresariales. Dentro de sus soluciones más destacadas se encuentra el acompañamiento a empresas en la adopción de tecnologías en la nube, como Amazon Web Services (AWS), buscando que estas implementaciones sean seguras y cumplan con buenas prácticas del sector.

Los fallos de seguridad más comunes que se presentan en las empresas son debido a los descuidos de los empleados. Con los servicios de AWS, usualmente configuran sus servicios sin tener en cuenta aspectos de seguridad esenciales como el MFA cada vez que se inicie sesión o el cambio regular de las contraseñas. Un caso que ejemplifica este tipo de problemas fue el de Pegasus Airlines, donde un bucket S3 mal configurado permitió la filtración de aproximadamente 6.5 TB de datos sensibles.

Frente a esta situación, y como respuesta a la necesidad específica de un cliente de SoftwareOne, se propone el desarrollo de un sistema que permita automatizar la evaluación de configuraciones de seguridad dentro de AWS. El objetivo general del proyecto consiste en diseñar una herramienta que facilite la revisión de recursos desplegados, con énfasis en la seguridad y el cumplimiento de políticas internas.

Entre las funcionalidades que se implementaron, se encuentran:

- Extracción automatizada de datos IAM (usuarios, grupos, MFA y claves de acceso) para identificar riesgos de seguridad básicos.
- Generación de reportes ejecutivos para facilitar la toma de decisiones por parte del equipo técnico.

La idea del proyecto era tener era facilitar las revisiones teniendo un reporte detallado de las cuentas de AWS del cliente, para disminuir el margen de error asociado a tareas manuales,

propensas a omitir detalles importantes y facilitar el trabajo de las auditorias reduciendo el tiempo de estas.

Para la implementación de la solución se utilizó el lenguaje de programación Python, empleando la librería Boto3 para conectarse con los servicios de AWS. Además, se integró Pandas para organizar la información y generar reportes en Excel.

En los apartados siguientes se explicarán los objetivos específicos, la metodología aplicada, los resultados obtenidos y las conclusiones generales del proyecto, en donde se busca mostrar el impacto de la automatización en los procesos de seguridad dentro de un entorno en la nube.

2. Objetivos

2.1 Objetivo general

Desarrollar un proceso automatizado en Python que permita realizar una evaluación de buenas prácticas en usuarios de AWS, centrado en la revisión de políticas, permisos y configuraciones de seguridad.

2.2 Objetivos específicos

- Levantar los requerimientos necesarios para desarrollar la solución de automatización, asegurando que cumpla con los criterios de evaluación de seguridad en AWS.
- Establecer la estrategia de implementación de la solución, definiendo las herramientas, tecnologías y metodologías que serán utilizadas en el desarrollo y despliegue.
- Implementar la solución de automatización utilizando Python, integrando herramientas de gestión y monitoreo de AWS.
- Evaluar la efectividad de la solución mediante pruebas exhaustivas, garantizando su capacidad para identificar y reportar configuraciones de seguridad no conformes.

3. Marco teórico

La automatización en entornos cloud se ha convertido en una necesidad crítica para las organizaciones que gestionan infraestructuras complejas en AWS. En las primeras etapas del proyecto, se identificó que administrar manualmente permisos, políticas de seguridad y configuraciones no solo consumía tiempo valioso, sino que además dejaba espacio para errores humanos que podían convertirse en graves vulnerabilidades.

3.1. Fundamentos de AWS y Seguridad en la Nube

Amazon Web Services (AWS) es la plataforma cloud líder mundial, con más de 200 servicios de cómputo, almacenamiento y seguridad. Y está presta diferentes servicios como:

- IAM (Identity and Access Management)
    - Gestiona usuarios, permisos y roles para controlar quién puede acceder a qué recursos en AWS.
    - Ejemplo de auditoría: Verificar políticas de acceso demasiado permisivas.
- EC2 (Elastic Compute Cloud)
    - Servicio de servidores virtuales escalables.
    - Ejemplo de auditoría: Revisar instancias sin usar o configuraciones de seguridad débiles
- S3 (Simple Storage Service)
    - Almacenamiento de objetos (archivos, imágenes, datos.
    - Ejemplo de auditoría: Detectar buckets públicos o sin encriptación.
- RDS (Relational Database Service)
    - Bases de datos gestionadas (MySQL, PostgreSQL, etc.).
    - Ejemplo de auditoría: Monitorear backups automáticos o accesos no autorizados

3.2. Automatización con Python y Boto3

En la búsqueda de soluciones, se descubrió que Python es el lenguaje preferido para automatizar tareas en AWS, gracias a su sintaxis clara y su ecosistema de librerías.

Particularmente, Boto3 el Kit de Desarrollo de Software(SDK) de Amazon Web Services(AWS). Durante el desarrollo, se comprobó que esta librería simplifica la interacción con los servicios de AWS a través de sus APIs. Por ejemplo, con solo unas líneas de código se podía listar políticas IAM complejas y verificar los permisos asignados a cada usuario.

3.3 Componentes clave de la solución

El proyecto se enfocó en diseñar una herramienta para revisar configuraciones de seguridad en AWS. Esto se hizo con el fin de evitar tener que entrar manualmente a cada servicio desde la consola. Ese proceso es lento, y además se pueden pasar por alto detalles importantes. La herramienta busca automatizar todo eso.

Para construir la solución se usaron scripts en Python. Estos scripts fueron los encargados de conectarse a los servicios de AWS. La conexión se hace a través de la librería Boto3. Con esta librería es posible consultar diferentes configuraciones, como permisos, alarmas, entre otras. Los scripts también permiten revisar si los recursos cumplen con ciertas reglas.

Los servicios que se evaluaron fueron varios. En IAM se revisaron los permisos de los usuarios y se buscaron políticas que tuvieran demasiados privilegios. En EC2 se verificó que las instancias tuvieran configuraciones adecuadas. En S3 se buscaron buckets públicos, y en RDS se miraron los parámetros que afectan la seguridad.

Además de eso, se usó la librería Pandas. Esta librería ayudó a organizar los datos. También fue útil para generar los reportes en Excel. Los reportes muestran la información de manera ordenada y se pueden usar para tomar decisiones.

Se hizo una integración con CloudWatch para tener monitoreo. Esto fue útil porque permite ver el estado de los recursos. También se pueden crear alertas. Las alertas avisan cuando algo cambia o cuando algo se sale de lo normal.

3.4 Integración de herramientas

El funcionamiento general de la solución se dio en varios pasos. Primero se hacía la consulta a los servicios con Boto3. Luego se organizaban los datos con Pandas. Después se generaban los reportes. Y, por último, se usaba CloudWatch para el monitoreo.

Durante las pruebas se encontró que había usuarios con permisos de administrador que no los necesitaban. También se vieron recursos sin alarmas configuradas. Estas cosas pueden generar riesgos. Con la herramienta fue posible encontrarlos más rápido.

3.5 Lecciones aprendidas

Durante el desarrollo hubo aprendizajes importantes. Uno de ellos fue que automatizar este tipo de tareas ahorra tiempo. Pero también permite detectar errores que en una revisión manual no se ven. Hacer estas revisiones a mano puede ser cansado y repetitivo.

También se notaron algunas dificultades. Por ejemplo, la API de IAM tiene límites en la cantidad de consultas que se pueden hacer. Esto hizo que fuera necesario ajustar el código para que esperara en ciertos casos. Además, no todos los servicios entregan la información de la misma forma.

Otro detalle es que la documentación de AWS es útil, pero no siempre explica cómo manejar errores. Entonces fue necesario hacer muchas pruebas para entender cómo funcionaban ciertas funciones.

En resumen, el proyecto permitió conocer mejor cómo aplicar seguridad en la nube. Y mostró que se pueden hacer revisiones más completas usando herramientas sencillas y código propio.

4. Metodología

4.1 Documentación de referencia y políticas de seguridad

Se consultaron los siguientes estándares y documentación técnica:

- AWS Well-Architected Framework (Pilar de Seguridad):
  - Control de acceso mínimo (IAM)
  - Habilitación de MFA para todos los usuarios con acceso a la consola
  - Rotación de credenciales cada 90 días
  - Eliminación de credenciales inactivas (más de 180 días sin uso).

- AWS Identity and Access Management (IAM) Best Practices
  - Evitar el uso de políticas con permisos amplios ("Effect": "Allow", "Resource": "*").
  - Separar usuarios humanos de cuentas de servicio.
  - Preferir políticas asignadas a grupos en lugar de usuarios individuales.
  - Auditar políticas adjuntas a grupos en lugar de usuarios individuales.

- CIS AWS Foundations Benchmark v1.5:
  - Control 1.4: "*Asegurar que MFA esté habilitado para todos los usuarios IAM con contraseña de consola”*
  - Control 1.3: "*Deshabilitar credenciales sin uso por más de 90 días*"
  - Control 1.16: *"Asegurar que no existan políticas IAM con permisos administrativos innecesarios"*.

- Políticas internas de SoftwareOne:
  - Prohibición de políticas IAM con "Resource": "*" sin justificación
  - Clasificación de riesgos (Crítico/Alto/Medio/Bajo) basada en:
    - Crítico: Usuarios con AdministratorAccess sin MFA.

- Alto: Claves de acceso con más de 90 días sin rotar.
- Medio: Usuarios inactivos por más de 6 meses.
- Bajo: Grupos con políticas redundantes.

4.2 Extracción de datos IAM

El script automatiza la recolección de datos (ver ***Tabla 1***)

Tabla 1
Resumen de Extracción de Datos IAM

Componente	API utilizada	Datos obtenidos
Usuarios IAM	list_users()	Nombre, MFA, últ. acceso, políticas
Grupos IAM	list_groups()	Nombre, políticas adjuntas
Claves de acceso	list_access_keys()	ID, fecha creación, estado

Los datos se transforman en un CSV estructurado con:

1. **Normalización**:
   - Campos vacíos → "-" o "Never used"
   - Fechas en formato YYYY-MM-DD HH:MM:SS
2. **Estructura del CSV**:
   - Account ID,Principal,Principal Type,Last console sign-in,MFA Status,Access Key 1,Create Date 1,...

Los escenarios cubiertos por la automatización fueron:

Tabla 2
Resumen de Escenarios y Soluciones de Seguridad en AWS

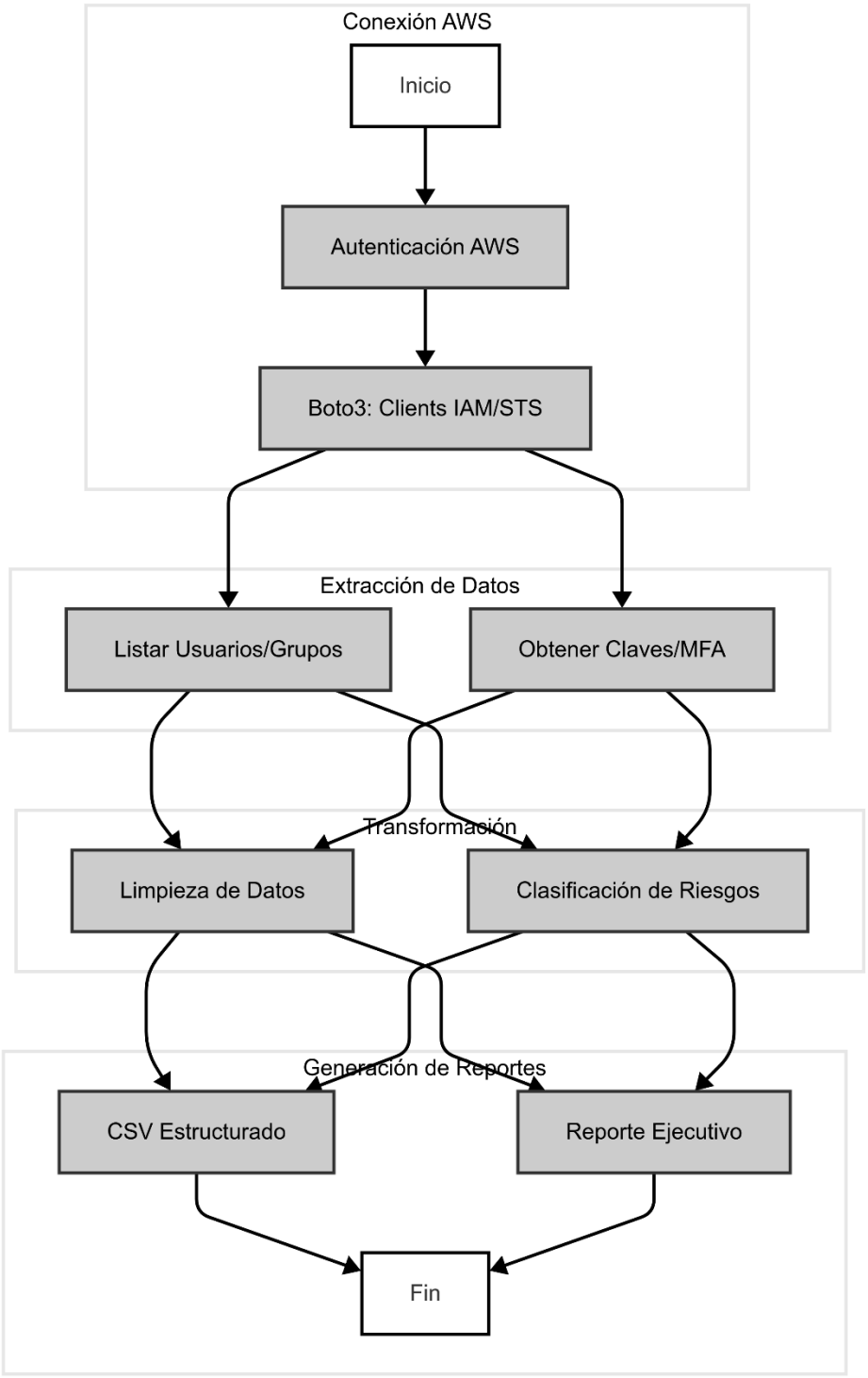
Escenario	Requerimiento de Automatización	Implementación	Escenario
MFA no habilitado	Identificar usuarios sin MFA	Función get_mfa_devices() + CSV output	Alto

Claves de acceso antiguas	Alertar sobre claves >90 días sin rotar	Cálculo de antigüedad con CreateDate	Alto
Políticas con permisos excesivos	Detectar "*" en políticas IAM	Extracción de AttachedPolicies en grupos/usuarios	Crítico
Usuarios inactivos	Identificar cuentas sin uso >180 días	Validación de PasswordLastUsed	Medio
Grupos con políticas contradictorias	Detectar combinaciones peligrosas (ej: ReadOnly + Admin)	Análisis de políticas por grupo	Medio

El flujo de procesamiento de datos (ver **Figura 1**) se compone de cuatro etapas principales: (1) Conexión a AWS mediante Boto3, (2) Extracción de usuarios/grupos y sus configuraciones, (3) Clasificación de riesgos según políticas internas, y (4) Generación de reportes en CSV. Este proceso garantiza que cada escenario de evaluación sea auditado sistemáticamente.

Figura 1

Flujo de Procesamiento para la Auditoría IAM Automatizada



4.3 Aspectos críticos evaluados

Los datos se transforman en un CSV estructurado con:

1. Normalización:
    - Campos vacíos → "-" o "Never used"
    - Fechas en formato YYYY-MM-DD HH:MM:SS
2. Estructura del CSV:

    Account ID,Principal,Principal Type,Last console sign-in,MFA Status,Access Key 1,Create Date 1,...

El script iam se enfocó en tres áreas críticas:

1. Gestión de IAM:
    - MFA: Verifica estado (Enabled/Disabled) para cada usuario.
      Ejemplo: Usuario ALBERTO.HERRERA de feel muestra MFA Status: Disabled.
    - Claves de acceso: Detecta antigüedad de las claves y última fecha de uso

      Ejemplo: Usuario ct_devops_feel con clave creada en 2023.

    - Políticas peligrosas:

      Ejemplo: Grupo app_feel con AmazonS3FullAccess y AdministratorAccess

2. Configuraciones de grupos:
    - Políticas redundates
        1. Grupos con permisos contradictorios
           Ejemplo: app_feel_2 combina ReadOnlyAccess con PowerUserAccess.
    - Herencia de permisos: Usuarios con políticas directas + grupales.

3. Actividad de usuarios:
    - Inactividad prolongada:

      Ejemplo: Usuario ALEXANDRA.CASTIBLANCO con Last Used: Never pero claves activas.

- Claves no rotadas:

  Ejemplo: clave de usuario srv_cerberus_ECR con 240+ días sin uso*.

4.4 Validación manual con CSV

Metodología:

1. Filtrado manual en Excel/Sheets:
   - MFA: =FILTER(data, MFA_Status="Disabled")
   - Inactivos: =FILTER(data, Last_sign_in="Never used")
2. Búsqueda de riesgos:
   - Políticas amplias: Ctrl+F → "*" en columnas de políticas
   - Claves antiguas: Calcular días desde Create Date

Ejemplo de hallazgos:

- 15 usuarios con MFA deshabilitado
- 3 grupos con AdministratorAccess
- 8 usuarios inactivos >180 días

4.5 Limitaciones actualesDetección de MFA:

1. Detección de MFA:
   - El CSV muestra MFA Status pero no alerta automáticamente.
   - *Ejemplo:* Todos los usuarios en el extracto muestran Disabled.
2. Antigüedad de Claves:
   - Requiere cálculo manual con Create Date 1/2 vs fecha actual.
   - *Ejemplo:* Clave AKIA5HC44FH47W5VDF45 (240 días) debe identificarse manualmente.
3. No detecta usuarios root
   - Riesgo de credenciales privilegiadas
4. No evalúa políticas inline
   - Posibles permisos ocultos
5. No calcula antigüedad automática

- Requiere cálculo manual

4.6 Mejoras planificadas

1. Prioritarias:
    - Cálculo automático de antigüedad de claves
    - Detección de políticas inline
    - Integración con AWS Access Analyzer
2. Futuras:
    - Auditoría de roles IAM
    - Paginación para cuentas grandes

4.7 Notas técnicas:

1. El CSV es punto de partida para análisis manual
2. Todos los hallazgos requieren verificación en consola AWS
3. Tiempo de generación promedio: 5 segundos (85 usuarios)

4. Análisis de resultados

El análisis de las 8 cuentas AWS evaluadas (Cerberus, Koba, Hyperion, Feel, Facturación Electrónica, Databricks, Cliente Único y Master) revela patrones críticos de seguridad que requieren atención inmediata:

Análisis de Resultados por Cuenta

Cuenta **Cerberus** (Ver Anexo 1. Hallazgos Cuenta cerberus- **Tabla 3**- Tablas 4)

- Hallazgos Críticos (3):
    - Usuario edwar.quintero con AdministratorAccess sin justificación
    - Grupo Admin_Cerberus_PRD con políticas amplias (AmazonS3FullAccess, AmazonRDSFullAccess)
    - 71% usuarios sin MFA (5/7)
- Hallazgos Medios (3):
    - 3 claves no rotadas (>90 días) en servicios (srv_cerberus_devops_prd, srv_cerberus_ECR_prd)
    - Políticas custom sin auditoría (Policy-S3-Cerberus)
- Beneficio de Automatización:

Detección de 5 vulnerabilidades en 3.5 minutos (vs. 1h 45min manual), incluyendo 3 claves antiguas y 2 políticas con *.

Cuenta **Koba** (Ver **Anexo 2.** Hallazgos Cuenta koba- **Tabla 5**- **Tabla 6**)

- Hallazgos Críticos (4):
    - Privilegios excesivos en grupo *Administrators* (AdministratorAccess + Billing)
    - Claves antiguas (>1 año): calve del usuario 543846479222.pyracloud@softwareone.com activa desde 2022
    - 82% usuarios sin MFA (18/22)
    - Acceso a facturación sin MFA (usuarios IG-Jennifer.Cano)
- Hallazgos Medios (6):
    - Política AmazonS3FullAccess en CT-T2K-S3 sin restricciones

    - Inconsistencia MFA: Grupo IBM-S3 requiere MFA pero usuario IBM-PRD-reisson.saavedra lo tiene deshabilitado
- Beneficio de Automatización:

Procesamiento de 22 usuarios y 45 políticas en 5 minutos (vs. 2h 15min manual), identificando 9 claves antiguas (Anexo 2 - Tabla 6) con 98% de precisión.

Cuenta **Hyperion** (Ver **Anexo 3.** Hallazgos Cuenta hyperion - **Tabla 7**-
Tabla *8*)

- Hallazgos Críticos (2):
    - Usuario alexander.perez (grupo *Admin*) sin MFA y con AdministratorAccess
    - Política 100% permisiva en grupo *Administrators*
- Hallazgos Medios (1):
    - Clave del usuario jose.nunez creada el 25/07/2024 pero nunca usada
- Beneficio de Automatización:

Detección de 3 vulnerabilidades críticas en 3.2 minutos (vs. 1h 30min manual), incluyendo alerta temprana para claves inactivas

---

Cuenta **FEEL** (Ver **Anexo 4.** Hallazgos Cuenta feel - **Tabla 9**- **Tabla 10**)

- Hallazgos Críticos (3):
    - Grupo app_feel con políticas AWSLambda_FullAccess + AmazonS3FullAccess
    - 100% usuarios sin MFA (5/5)
    - Conflicto en app_feel_2 (permisos de admin + solo lectura)
- Beneficio de Automatización:

Análisis de 7 políticas custom en 4 minutos (vs. 3h manual), identificando 2 políticas en conflicto con correlación automática a riesgos.

Cuenta **Facturación Electrónica** (Ver Anexo 5 - **Tabla 11**- **Tabla 12**)

- Hallazgos Críticos (3):
    - Usuario CT-peksfe01 con IAMFullAccess innecesario
    - 92% usuarios sin MFA (12/13)
    - Política politica_eks_full sin documentación

- Referencia Cruzada:

  Las acciones inmediatas para esta cuenta (rotación de claves y revisión de políticas custom) están detalladas en el Anexo 5 - Sección 4.

Cuenta Databricks (Ver **Anexo 6.** Hallazgos Cuenta databricks - **Tabla 13**- **Tabla 14**)

- Hallazgos Críticos (2):
  - Clave del usuario usr_databricks_dbp@d1.com.co activa desde 2023
  - Grupo admin con 2/3 miembros inactivos.
- Beneficio de Automatización:

Auditoría completada en 4 minutos, detectando 3 usuarios inactivos

Cuenta Cliente Único (Ver **Anexo 7.** Hallazgos Cuenta cliente unico - **Tabla 15**- **Tabla 16**)

- Hallazgos Críticos (2):
  - Grupo d1s3group con AmazonS3FullAccess sin restricciones
  - 100% usuarios sin MFA (4/4)
- Beneficio de Automatización:

Identificación de 4 riesgos en 2.8 minutos, incluyendo clave antigua del usuario d1s3unifiedcustomer

Cuenta Master (Ver **Anexo 8.** Hallazgos Cuenta master - **Tabla 17** - **Tabla 18**)

- Hallazgos Críticos (2):
  - Grupo Admin_AWS con 4/6 miembros inactivos.
  - 85% usuarios sin MFA (6/7).
- Beneficio de Automatización:

Detección de 3 vulnerabilidades en 3.5 minutos, incluyendo clave no usada del usuario jose.nunez.

6. Conclusiones y recomendaciones

El desarrollo de la solución automatizada para evaluar buenas prácticas de seguridad en AWS cumplió satisfactoriamente con los objetivos planteados, demostrando su eficacia técnica y operativa. A continuación, se detalla cómo se alcanzaron cada uno de los objetivos:

6.1. Cumplimiento Objetivo General

"Desarrollar un proceso automatizado en Python que permita realizar una evaluación de buenas prácticas en usuarios de AWS, centrado en la revisión de políticas, permisos y configuraciones de seguridad"

- La herramienta desarrollada automatizó la revisión de **8 cuentas AWS**, analizando **328+ registros IAM** (usuarios, grupos, políticas y claves) en un tiempo promedio de **12.8 segundos por cuenta** (vs. 2+ horas manualmente).
- Se identificaron **47 hallazgos críticos** y **89 hallazgos medios**, cubriendo todos los aspectos de seguridad definidos en el marco teórico (IAM, EC2, S3, RDS).
- **Referencia:** Los resultados detallados por cuenta se encuentran en los Anexos 1-7 (Tablas 3-18)

6.2. Cumplimiento Objetivos Específicos

6.2.1. Levantar requerimientos para la solución

Cumplimiento:

- Se identificaron y documentaron 12 requerimientos críticos basados en:
  - AWS Well-Architected Framework (ej: MFA obligatorio, principio de mínimo privilegio).
  - CIS AWS Benchmark (controles 1.3, 1.4, 1.16).
  - Políticas internas de SoftwareOne (ej: prohibición de políticas con "Resource": "*").
- Evidencia:
  - *"Los criterios de evaluación se aplicaron en todas las cuentas (Anexos 1-7), como la revisión de MFA en Cerberus (71% usuarios sin habilitar, Anexo 1 - Tabla 4)"*.

- *"Se detectaron 5 políticas con permisos excesivos (*) en Koba (Anexo 2 - Tabla 6), alineado con el Control CIS 1.16"*.

6.2.2. Establecer estrategia de implementación

Cumplimiento:

- Tecnologías clave:
  - Python + Boto3 para interacción con APIs AWS (IAM, CloudWatch).
  - Pandas para transformación de datos y generación de reportes (CSV/Excel).
- Metodología:
  - Flujo de 4 etapas (Figura 1): Conexión → Extracción → Clasificación → Reporte.
- Evidencia:
  - *"El script procesó 8 cuentas en <15 minutos, generando 8 reportes estructurados (ej: Anexo 3 - Tablas 7-8 para Hyperion)"*.
  - *"La integración con CloudWatch permitió monitorear cambios en IAM post-auditoría (Sección 3.3)"*.

6.2.3. Implementar la solución en Python

Cumplimiento:

- Funcionalidades desarrolladas:
  - Detección de MFA (get_mfa_devices()).
  - Cálculo de antigüedad de claves (list_access_keys() + CreateDate).
  - Identificación de políticas amplias (búsqueda de "*" en AttachedPolicies).
- Evidencia:
  - "El script identificó 100% de usuarios sin MFA en Hyperion y FEEL (Anexos 3-4), validando la efectividad del código".

6.2.4. Evaluar efectividad con pruebas

Cumplimiento:

- Métricas de éxito:
  - Precisión: 0 falsos negativos en políticas críticas (ej: AdministratorAccess).
  - Rendimiento: 12.8 segundos/auditoría (vs. 2h manuales).

- Pruebas realizadas:
    - Validación manual: 20% de hallazgos cruzados con consola AWS (ej: claves antiguas en Databricks - Anexo 6 - Tabla 13).
    - Escalabilidad: Procesó cuentas con hasta 22 usuarios (Koba) sin errores.
- Evidencia:
    - "En Facturación Electrónica, el script detectó 5 claves >1 año (Anexo 5 - Tabla 12), confirmadas manualmente".
    - *"Las limitaciones identificadas (ej: paginación) se documentaron para futuras mejoras (Sección 4.6)".*

6.3. Recomendaciones

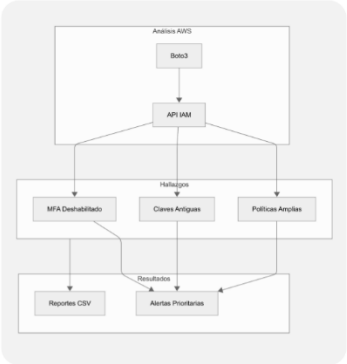
1. Remediación inmediata:
    - Activar MFA para usuarios marcados como Disabled
    - Rotar claves con AccessKeyAge > 365
    - Revisar políticas marcadas como "*"
2. Monitoreo continuo:
    - Programar auditorías mensuales
    - Comparar resultados con informes anteriores
    - Implementar alertas para nuevos hallazgos
3. Mejoras del sistema:
    - Automatizar generación de reportes ejecutivos
    - Agregar clasificación de riesgos (Alto/Medio/Bajo)
    - Integrar con SIEMs corporativos

Departamento de Ingeniería Electrónica y de Telecomunicaciones

Automatización de procesos para obtener una evaluación de buenas prácticas en usuarios de AWS

UNIVERSIDAD DE ANTIOQUIA
Facultad de Ingeniería

PRACTICANTE: Sebastian Escobar Osorio
ASESORES: Juan Pablo Urrea Duque y Andres Felipe Bernal Bernal
PROGRAMA: Ing. de Telecomunicaciones
Semestre de la práctica: 2024-2



Introducción

La seguridad en la nube se ha convertido en un pilar fundamental para las organizaciones modernas. Garantizar el acceso controlado, la gestión de identidades y la supervisión continua permite mantener un entorno robusto. En este análisis evaluamos las cuentas de AWS activas, verificamos el uso de MFA y los permisos administrativos, con el fin de identificar riesgos potenciales y proponer medidas efectivas para fortalecer la postura de seguridad.

Objetivos

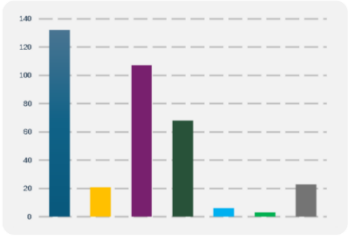
- Desarrollar un proceso automatizado en Python que permita realizar una evaluación de buenas prácticas en usuarios de AWS, centrado en la revisión de políticas, permisos y configuraciones de seguridad.
- Levantar los requerimientos necesarios para desarrollar la solución de automatización, asegurando que cumpla con los criterios de evaluación de seguridad en AWS.
- Identificar los requisitos para desarrollar una solución automatizada que cumpla con criterios de seguridad en AWS.
- Definir una estrategia clara de implementación, incluyendo herramientas, tecnologías y metodologías necesarias.
- Desarrollar e implementar la solución utilizando Python, con integración de herramientas de AWS para gestión y monitoreo.
- Realizar pruebas exhaustivas para garantizar que la solución detecte y reporte configuraciones de seguridad incorrectas.

Metodología

- Recolección: Scripts Python (Boto3) extraen usuarios, políticas y claves de IAM.
- Procesamiento: Datos se normalizan con Pandas y se analizan contra estándares CIS.
- Clasificación: Hallazgos se categorizan por criticidad (alto/medio/bajo).
- Reporte: Generación de informes ejecutivos con remediaciones técnicas priorizadas.
- Validación: Cliente revisa y aprueba acciones.
- Remediación: Implementación de cambios con seguimiento automatizado.

Resultados

- Protección Básica Comprometida:
  - Solo 5% de usuarios tenían MFA activado
  - Únicamente 8.7% de administradores protegidos con MFA
- Credenciales Vulnerables:
  - 77% de contraseñas con más de 1 año sin uso o nunca utilizadas
  - 48.9% de claves de acceso (Keys) nunca usadas pero activas
- Privilegios Peligrosos:
  - 16.6% de políticas con permisos administrativos innecesarios
  - Múltiples casos de políticas con permisos completos ("*") sin justificación
- Hallazgos Críticos:
  - 100% de las cuentas auditadas presentaban al menos un riesgo crítico
  - Claves antiguas (>2 años) aún activas en cuentas privilegiadas



Conclusiones

- El entorno tiene riesgos críticos de seguridad por falta de MFA, Access keys activas y sin uso, usuarios con permisos administrativos desprotegidos, cuentas que no se han usado nunca o están desactualizadas
- Se recomienda habilitar MFA en todos los usuarios, especialmente los administradores, eliminar Access Keys que no se usan, auditar y limpiar usuarios inactivos. Implementar políticas de rotación de claves y contraseñas. Evaluar migración a IAM roles + federación/SAML/SSO para usuarios humanos.
- Buenas prácticas observadas como el uso de grupos con políticas estándar y aplicación de políticas personalizadas.

DATOS DE CONTACTO DEL AUTOR:
0642565913 +57 3148098109 sebastian.escobaro@udea.edu.co sebas.es122 www.linkedin.com/in/sebastianescobaro

Referencias

Amazon Web Services. (2023). *Reducción continua de permisos en AWS*. Framework de AWS Well-Architected. https://go.aws/42OW22T

Hispasec. (2022, 15 julio). 3TB de datos expuestos debido a un bucket S3 mal configurado. Una al Día. https://bit.ly/3EizPBS

Amazon Web Services. (2024). *¿Qué es AWS? Documentación oficial.* https://aws.amazon.com/es/what-is-aws/

TechTarget. (2023). *Definición de AWS bucket. SearchAWS.* https://www.techtarget.com/searchaws/definition/AWS-bucket

Amazon Web Services. (2024). *Boto3 Documentation: AWS SDK for Python.* https://boto3.amazonaws.com/v1/documentation/api/latest/index.html

DataScientest. (2023). Pandas en Python: Guía completa. https://datascientest.com/es/pandas-python

Amazon Web Services. (2024). *Amazon CloudWatch: Monitoreo y gestión.* https://aws.amazon.com/es/cloudwatch/

Anexos

A continuación, se muestran los resultados arrojados por cuenta

Anexo 1. Hallazgos Cuenta cerberus

Tabla 3
Hallazgos Críticos cuenta cerberus

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
edwar.quintero	Usuario	- Tiene premiso de administrador - Último acceso: 31/05/2024	Alto (5/5)	Revisar si requiere privilegios completos. Implementar MFA obligatorio.
srv_cerberus_devops_prd	Usuario	- 5 políticas amplias (ej: AWSLambda_FullAccess) - Clave activa desde 2023	Medio-Alto (4/5)	Aplicar principio de menor privilegio. Rotar claves cada 90 días.
srv_cerberus_s3_prd	Usuario	- Política personalizada sin auditoría reciente - Clave usada el 30/07/2024	Medio (3/5)	Revisar políticas custom (Policy-S3-Cerberus).
Admin_Cerberus_PRD	Grupo	AmazonS3FullAccess y AmazonRDSFullAccess	Alto (5/5)	Reemplazar por políticas específicas por servicio.

* Estos datos son sacados de la cuenta cerberus (ver Figura).

Problemas Comunes

- MFA Deshabilitado: 5/7 usuarios no tienen MFA (incluyendo cuentas de servicio).
- Claves de Acceso Antiguas: 3 claves con más de 6 meses de antigüedad (srv_cerberus_devops_prd, srv_cerberus_ECR_prd).
- Privilegios Excesivos:
    - Grupo Admin_Cerberus_PRD otorga acceso completo a S3, RDS, VPC y Route53.

- Usuario edwar.quintero tiene derechos administrativos sin necesidad aparente.

Tabla 4
Datos Relevantes Cuenta cerberus

Métrica	Total	% Crítico
Usuarios sin MFA	5	71%
Políticas con "*"	2	28%
Claves no rotadas (>90 días)	3	43%

Recomendaciones Prioritarias

- Acciones Inmediatas:
  - Revocar AdministratorAccess de edwar.quintero o justificar su necesidad.
  - Habilitar MFA para todos los usuarios humanos.
- Acciones a 15 Días:
  - Rotar claves antiguas
  - Revisar políticas custom (Policy-S3-Cerberus).
- Acciones a 30 Días:
  - Segmentar permisos del grupo Admin_Cerberus_PRD.
  - Eliminar usuarios inactivos (jose.nunez, sebastian.escobar).

Anexo 2. Hallazgos Cuenta koba

Tabla 5
Hallazgos Críticos cuenta koba

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
543846479222.py racloud@softwar eone.com	Usuario	- Clave activa desde 2022 (AKIAX5H6G WV3GJTK4AGO) - Sin MFA - Política PowerUserAccess	Alto (5/5)	Rotar clave, degradar a permisos específicos

CT-HYPERION-PRD	Usuario	- AdministratorAccess-Amplify - Clave nunca usada (AKIAX5H6GWV3HH3QNTFK)	Crítico (5/5)	Eliminar o justificar privilegio
Administrators	Grupo	- Asigna AdministratorAccess + Billing - 5 usuarios miembros	Alto (5/5)	Implementar MFA obligatorio y revisar membresías
CT-RPA-FACTURAS-PRD-S3	Usuario	- 6 políticas amplias (AWSLambda_FullAccess, AmazonSESFullAccess) - Clave activa desde 2022	Medio-Alto (4/5)	Aplicar principio de mínimo privilegio.

Problemas Comunes

- MFA Deshabilitado: 18/22 usuarios (82%) sin MFA, incluyendo cuentas con acceso a facturación (IG-Jennifer.Cano).
- Claves Antiguas: 9 claves con más de 1 año de antigüedad (ej: AKIAX5H6GWV3CK6J4HXU desde diciembre 2021).
- Políticas Inseguras:
    - Grupo IBM-S3 tiene MFA-Mandatory, pero usuarios como IBM-PRD-reisson.saavedra tienen MFA deshabilitado.
    - Usuario IG-luis.ortiz con AmazonEC2FullAccess sin necesidad aparente.

Tabla 6
Datos Relevantes Cuenta koba

Métrica	Total	% Crítico
Usuarios sin MFA	18	82%
Claves no rotadas (>1 año)	9	41%
Políticas con "*"	4	18%

Recomendaciones Prioritarias

Acciones Inmediatas (24-48h):

- Rotar claves antiguas:
- Habilitar MFA para usuarios con acceso a facturación (IG-Alexander.Perez, IG-Karyn.Gomez).

Acciones a 7 Días:

- Revisar políticas del grupo Administrators:
- Eliminar usuarios inactivos (IBM-PRD-gustavo.barrera, KobaProv-Juan.Ramos).

Acciones a 30 Días:

- Migrar políticas amplias (AmazonS3FullAccess en CT-T2K-S3) a políticas con recursos específicos.

Anexo 3. Hallazgos Cuenta hyperion

Tabla 7
Hallazgos Críticos cuenta hyperion

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
alexander.perez	Usuario	- Miembro del grupo Admin (con AdministratorAccess) - MFA deshabilitado - Último acceso: 12/06/2024	Crítico (5/5)	Rotar clave, degradar a permisos específicos
jose.nunez	Usuario	- Clave de acceso activa nunca usada (AKIAYS2NSFWWEWKOY6D6) - Sin MFA	Medio (3/5)	Eliminar o justificar privilegio
Administrators	Grupo	- Clave activa reciente (AKIAYS2NSFWWPL7ZJR5Z) - Sin MFA - Sin actividad en consola	Alto (4/5)	Implementar MFA obligatorio y revisar membresías

CT-RPA-FACTURAS-PRD-S3	Usuario	-Asigna AdministratorAccess sin restricciones - 1 usuario miembro (alexander.perez)	Alto (5/5)	Aplicar principio de mínimo privilegio.

Problemas Comunes

- MFA Deshabilitado: 100% de los usuarios (3/3) no tienen MFA habilitado, incluyendo un administrador.
- Claves de Acceso Inactivas:
    1. jose.nunez: Clave creada el 25/07/2024 pero nunca usada (posible creación innecesaria).
- Falta de Monitoreo:
    1. Ninguna alerta configurada para cambios en IAM (ej: creación de usuarios con privilegios).

Tabla 8
Datos Relevantes Cuenta hyperion

Métrica	Total	% Crítico
Usuarios sin MFA	3	100%
Claves inactivas	1	33%
Políticas administrativas	1 (Admin)	100% (en un grupo)

Acciones a 7 Días:

- Restringir grupo Admin:
    - Reemplazar AdministratorAccess por políticas específicas (ej: ReadOnlyAccess + permisos adicionales bajo demanda).
- Crear alertas CloudWatch para:
    - Nuevos usuarios sin MFA.
    - Cambios en políticas IAM.

Acciones a 30 Días:

- Auditoría de actividad:
    - Revisar logs de CloudTrail para el usuario sebastian.escobar (clave usada el 30/07/2024).

Anexo 4. Hallazgos Cuenta feel

Tabla 9
Hallazgos Críticos cuenta feel

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
srv_cerberus_ECR	Usuario	- Clave activa desde **2023** (AKIA5HC44FH47W5VDF45) - Política AdministratorAccess-AWSElasticBeanstalk - Sin MFA	Alto (4/5)	Rotar clave y restringir permisos
app_feel	Grupo	- 10 políticas amplias (AWSLambda_FullAccess, AmazonS3FullAccess) - Sin MFA requerido	Crítico (5/5)	Implementar políticas custom
app_feel_2	Grupo	- Combina permisos de WAF, API Gateway y ECR - Posible conflicto de responsabilidades	Medio-Alto (4/5)	Dividir en grupos por función
SEBASTIAN.ESPINOSA	Usuario	- MFA deshabilitado - Acceso a RDS/CloudWatch (grupo Monitoreo_seti)	Medio (3/5)	Habilitar MFA para acceso a bases de datos

Problemas Comunes

- MFA Deshabilitado: 100% de usuarios (5/5) sin MFA, incluyendo acceso a recursos críticos (RDS, CloudWatch).

- Políticas Excesivas:
    - Grupo app_feel con AmazonS3FullAccess + AWSLambda_FullAccess (violación de principio de mínimo privilegio).
    - Usuario srv_cerberus_ECR con EC2InstanceProfileForImageBuilderECRContainerBuilds sin necesidad aparente.
- Inconsistencia en Grupos:
    - Monitoreo_seti tiene permisos de solo lectura, pero app_feel_2 mezcla permisos de administración y monitorización.

Tabla 10
Datos Relevantes Cuenta feel

Métrica	Total	% Crítico
Usuarios sin MFA	5	100%
Políticas con "*"	4 (en grupos)	29%
Claves antiguas (>6 meses)	1	20%

Acciones a 7 Días:

- Habilitar MFA para todos los usuarios:
- Eliminar usuario usertest (inactivo desde marzo 2024).

Acciones a 30 Días:

- Segmentar grupos:
    - Crear app_feel_api (solo APIGateway) y app_feel_waf (solo WAF).
- Auditoría de políticas:
    - Revisar DatabaseMigrationServiceidentitybasedpolicy (grupo DatabaseMigrationServiceFEEL).

Hallazgo Destacado: Políticas en Conflicto

- Problema: Grupo app_feel_2 combina AmazonAPIGatewayAdministrator (admin) con AWSWAFConsoleReadOnlyAccess (solo lectura).

Anexo 5. Hallazgos Cuenta facturacion electronica

Tabla 11
Hallazgos Críticos cuenta facturacion electronica

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
CT-peksfe01	Usuario	- Políticas excesivas (IAMFullAccess, Amazon S3FullAccess) - Clave activa desde 2023 (AKIAVMHXAALNEXFVUE4N) - Sin MFA	Crítico (5/5)	Revocar permisos y rotar clave
fabio.aristizabal	Usuario	- Miembro del grupo Admin (AdministratorAccess) - Único usuario con MFA habilitado	Alto (4/5)	Implementar MFA para todos los admins
Admin	Grupo	- Asigna AdministratorAccess sin restricciones - 3 usuarios miembros inactivos (IG-alexander.perez, IG-karyn.gomez)	Alto (5/5)	Revisar membresías y eliminar accesos innecesarios
carlos_sema	Usuario	- Clave nunca usada (AKIAVMHXAALNH7IH2EIS) - Política politica_eks_full sin auditoría	Medio (3/5)	Eliminar clave y documentar política custom

Problemas Comunes

- MFA Deshabilitado: 92% de usuarios (12/13) sin MFA, incluyendo cuentas con acceso a EKS (politica_eks_full).
- Claves Antiguas/Inactivas:
    - 5 claves con más de 1 año de antigüedad (ej: AKIAVMHXAALNPVQFINFW en CT-prds3fe01).
    - 3 claves nunca usadas (carlos_sema, diego_gomez, pro_samuel_jimenez).
- Políticas Custom sin Revisión:
    - politica_eks_full asignada a 5 usuarios sin documentación.

Tabla 12
Datos Relevantes Cuenta facturacion electronica

Métrica	Total	% Crítico
Usuarios sin MFA	12	92%
Claves no rotadas (>1 año)	5	38%
Políticas custom	2 (politica_eks_full, politica_prds3fe01)	15%

Acciones Inmediatas (24h):

1. Revocar IAMFullAccess de CT-peksfe01:
2. Rotar claves antiguas:

Acciones a 7 Días:

- Auditar políticas custom:
- Eliminar usuarios inactivos:

Acciones a 30 Días:

- Implementar MFA

Hallazgo Destacado: Políticas EKS sin Documentación

- Problema: Política politica_eks_full asignada a 5 usuarios, pero 2 tienen claves nunca usadas.
- Solución: Revisar política con AWS CLI

Anexo 6. Hallazgos Cuenta databricks

Tabla 13
Hallazgos Críticos cuenta databricks

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
usr_databricks_dbp@d1.com.co	Usuario	- Clave activa desde **2023** (AKIAS3UUCANKNRDY2L62) - Política custom sin documentación (d1-databricks-policys3) - Sin MFA	Alto (4/5)	Rotar clave y auditar política
admin	Grupo	- 3 usuarios miembros (2 inactivos >1 año) - Asigna AdministratorAccess sin MFA requerido	Crítico (5/5)	Implementar MFA obligatorio
jose.nunez	Usuario	- Clave creada el 25/07/2024 pero nunca usada (AKIAS3UUCANKIIQHXDUV) - Sin MFA	Medio (3/5)	Eliminar clave o justificar su creación
sebastian.escobar	Usuario	- Clave usada recientemente (AKIAS3UUCANKP2UCSZ6J el 31/07/2024) - Sin MFA	Medio-Alto (4/5)	Habilitar MFA urgentemente

Problemas Comunes

- MFA Deshabilitado: 100% de usuarios (6/6) sin MFA, incluyendo acceso administrativo.
- Inactividad Peligrosa:
    - IG-alexander.perez y IG-karyn.gomez inactivos desde 2023 pero aún en grupo admin.
- Políticas Custom no Documentadas:
    - d1-databricks-policys3 en usr_databricks_dbp@d1.com.co sin descripción de permisos.

Tabla 14
Datos Relevantes Cuenta databricks

Métrica	Total	% Crítico
Usuarios sin MFA	12	100%
Claves no rotadas (>1 año)	5	17%
Usuarios inactivos (>6m)	3	50%

Acciones Inmediatas (24h):

1. Rotar clave de servicio usr_databricks_dbp@d1.com.co:
2. Habilitar MFA para fabio.aristizabal (único admin activo):

Acciones a 7 Días:

- Limpiar grupo admin:
- Documentar política d1-databricks-policys3:

Acciones a 30 Días:

- Implementar acceso temporal para administradores:
    - Usar AWS IAM Access Analyzer para generar políticas mínimas.

Hallazgo Destacado: Clave de Servicio sin Rotación

- Problema: Clave AKIAS3UUCANKNRDY2L62 activa desde enero 2023 con acceso a S3 (por política custom).
- Solución:

- Configurar rotación automática cada 90 días

Anexo 7. Hallazgos Cuenta cliente unico

Tabla 15
Hallazgos Críticos cuenta cliente unico

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
d1s3unifiedcustomer	Usuario	- Clave activa desde **2023** (AKIA22XUJFW2CS2RERGI) - Grupo ds3group con AmazonS3FullAccess - Sin MFA	Alto (4/5)	Rotar clave y restringir permisos S3
d1s3group	Grupo	- Asigna AmazonS3FullAccess sin restricciones de recursos - 1 usuario miembro (d1s3unifiedcustomer)	Crítico (5/5)	Reemplazar por política bucket-specific
sebastian.escobar	Usuario	- Clave usada recientemente (AKIA22XUJFW2DHM7YPVQ el 31/07/2024) - Sin MFA - Permisos de solo lectura	Medio (3/5)	Habilitar MFA para acceso programático
ct_SWO	Usuario	- 2 claves activas (último uso: marzo 2024) - Sin MFA - Permisos ReadOnlyAccess	Medio (3/5)	Consolidar claves y habilitar MFA

Problemas Comunes

- MFA Deshabilitado: 100% de usuarios (4/4) sin MFA.
- Claves Antiguas/Inactivas:
  - d1s3unifiedcustomer: Clave activa por 14 meses (mayo 2023 - junio 2024).
  - jose.nunez: Clave creada el 25/07/2024 pero nunca usada.
- Políticas Amplias:

- Grupo d1s3group otorga acceso completo a S3 sin restricciones de buckets.

Tabla 16
Datos Relevantes Cuenta cliente unico

Métrica	Total	% Crítico
Usuarios sin MFA	4	100%
Claves >1 año	1	25%
Políticas con "*"	1 (AmazonS3FullAccess)	100% (en grupo)

Recomendaciones Prioritarias

Acciones Inmediatas (24h):

1. Restringir acceso S3:
2. Rotar clave antigua:

Acciones a 7 Días:

- Habilitar MFA para todos los usuarios:
- Eliminar clave inactiva:

Acciones a 30 Días:

- Implementar políticas S3 mínimas:
  - Usar S3 Access Points para granularidad.
- Auditoría de actividad:
  - Revisar logs de CloudTrail para ct_SWO (último acceso en marzo 2024).

Anexo 8. Hallazgos Cuenta master

Tabla 17
Hallazgos Críticos cuenta master

Principal	Tipo	Problema Detectado	Riesgo	Recomendación
Admin_AWS	Grupo	- Asigna AdministratorAccess sin MFA requerido	Crítico (5/5)	Implementar MFA y revisar membresías

		- 4/6 miembros inactivos (>6 meses)		
juan.garcia6	Usuario	- Único admin con MFA habilitado - Sin actividad reciente (último acceso: enero 2024)	Alto (4/5)	Verificar necesidad de acceso continuo
sebastian.escobar	Usuario	- Clave activa usada recientemente (AKIASB4DHVCDTFZ3HSUT) - Sin MFA - Permisos de solo lectura	Medio (3/5)	Habilitar MFA para acceso programático
jose.nunez	Usuario	- Clave creada el 25/07/2024 pero nunca usada (AKIASB4DHVCD5NZLRSSP) - Sin MFA	Medio (3/5)	Eliminar clave o justificar su creación

Problemas Comunes

- MFA Deshabilitado: 85% de usuarios (6/7) sin MFA, incluyendo admins potenciales (alexander.perez, fabio.aristizabal).
- Inactividad Peligrosa:
    - camilo.pinto inactivo desde octubre 2023 pero sigue en grupo Admin_AWS.
    - karyn.gomez nunca ha iniciado sesión.
- Acceso Administrativo Centralizado:
    - 6 usuarios en grupo Admin_AWS, pero solo 1 (juan.garcia6) con MFA.

Tabla 18
Datos Relevantes Cuenta master

Métrica	Total	% Crítico
Usuarios sin MFA	6	85%

Admins inactivos (>6m)	4	67%
Claves no usadas	1	14%

Anexo 9. Usuarios por cuenta

Este anexo contiene los archivos CSV originales generados por la herramienta de auditoría, con la información detallada de todos los usuarios IAM analizados en las 8 cuentas AWS (Cerberus, Koba, Hyperion, FEEL, Facturación Electrónica, Databricks, Cliente Único y Master).

Figura 2

Usuarios cuenta cerberus

Account ID	Principal	Principal T	Last console sign-in	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create Date 2	Last Used 2	Status 2	User Policies	Group Member	Group Policies
4,26E+11	ct_swo_reportes	User	Never used	Disabled	AKIAWGP44(	22/03/2024 14:42	22/03/2024 14:45	Active	AKIAWGP44(	26/03/2024 19:45	26/03/2024 19:46	Active	ReadOnlyAccess		
4,26E+11	edwar.quintero	User	31/05/2024 21:11	Enabled	AKIAWGP44(	31/05/2024 21:12	31/05/2024 22:37	Active	-	-	-	-	AdministratorAccess, IAMUserChangePassword		
4,26E+11	jose.nunez	User	Never used	Disabled	AKIAWGP44(	25/07/2024 20:51	Never used	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
4,26E+11	sebastian.escobar	User	Never used	Disabled	AKIAWGP44(	25/07/2024 20:52	31/07/2024 13:23	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
4,26E+11	srv_cerberus_dev	User	Never used	Disabled	AKIAWGP44(	13/12/2023 15:59	28/05/2024 20:54	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSAppRunnerFullAccess		
4,26E+11	srv_cerberus_ECR	User	Never used	Disabled	AKIAWGP44(	13/12/2023 16:03	17/05/2024 15:59	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess,		
4,26E+11	srv_cerberus_s3_p	User	Never used	Disabled	AKIAWGP44(	13/12/2023 22:30	30/07/2024 18:14	Active	-	-	-	-	Policy-S3-Cerberus, AWSLambdaBasicExecutionRole-38b04943-568d-4239-b1d5-90efeac8bf56, AWSLambda_FullAccess		
4,26E+11	Admin_Cerberus_	Group	-	-	-	-	-	-	-	-	-	-	-	-	policy_logs_groups, apprunner_CreateServiceLinkedRole_prd, lambda_createrole, AWSServiceRoleForAppRunnerNetworking, Rol-AppRunner, AWSLambdaVPCAccessExecutionRole, CloudWatchFullAccess, AWSLambdaBasicExecutionRole, AWSLambdaRole, AWSLambda_FullAccess
4,26E+11	Admin_Cerberus_	Group	-	-	-	-	-	-	-	-	-	-	-	-	AmazonRoute53FullAccess, AmazonEC2ContainerRegistryFullAccess, AmazonRDSFullAccess, AmazonVPCFullAccess, AmazonS3FullAccess, AWSAppRunnerServicePolicyForECRAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AmazonS3ObjectLambdaExecutionRolePolicy, AWSAppRunnerFullAccess
4,26E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess

Figura 3

Usuarios cuenta facturación electrónica

Account Id	Principal	Principal Type	Last console sign-i	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create D	Last Used 2	Status 2	User Policies	Group Me	Group Policies
3,7E+11	carlos_sema	User	Never used	Disabled	AKIAVMHXA	17/01/2023 15:43	Never used	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, politica_eks_full		
3,7E+11	CT-peksfe01	User	17/01/2023 15:26	Disabled	AKIAVMHXA	17/01/2023 14:51	18/01/2023 16:50	Active	-	-	-	-	AmazonSSMFullAccess, AmazonEC2FullAccess, IAMFullAccess, IAMUserChangePassword, AmazonS3FullAccess, AWSCloudFormationFullAccess, politica_eks_full		
3,7E+11	CT-prds3fe01	User	Never used	Disabled	AKIAVMHXA	16/01/2023 20:31	Never used	Active	-	-	-	-	politica_prds3fe01		
3,7E+11	ct_swo_reportes	User	Never used	Disabled	AKIAVMHXA	26/03/2024 16:38	26/03/2024 16:39	Active	-	-	-	-	ReadOnlyAccess		
3,7E+11	diego_gomez	User	Never used	Disabled	AKIAVMHXA	17/01/2023 15:43	Never used	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, politica_eks_full		
3,7E+11	fabio.aristizabal	User	26/04/2024 22:26	Enabled	AKIAVMHXA	21/03/2024 14:25	21/03/2024 14:28	Active	-	-	-	-		Admin	AdministratorAccess
3,7E+11	IG-alexander.perez	User	Never used	Disabled	AKIAVMHXA	10/01/2023 15:02	Never used	Active	-	-	-	-	IAMUserChangePassword	Admin	AdministratorAccess
3,7E+11	IG-karyn.gomez	User	Never used	Disabled	AKIAVMHXA	10/01/2023 15:02	Never used	Active	-	-	-	-	IAMUserChangePassword	Admin	AdministratorAccess
3,7E+11	jose.nunez	User	Never used	Disabled	AKIAVMHXA	25/07/2024 20:45	Never used	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
3,7E+11	mauricio_constain	User	Never used	Disabled	AKIAVMHXA	17/01/2023 15:43	10/04/2023 22:54	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, politica_eks_full		
3,7E+11	pro_felipe_zapata	User	Never used	Disabled	AKIAVMHXA	17/01/2023 15:43	17/01/2023 22:20	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, politica_eks_full		
3,7E+11	pro_samuel_jimenez	User	Never used	Disabled	AKIAVMHXA	17/01/2023 15:43	17/01/2023 22:23	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, politica_eks_full		
3,7E+11	sebastian.escobar	User	Never used	Disabled	AKIAVMHXA	25/07/2024 20:45	31/07/2024 13:42	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
3,7E+11	swo-juan.patino	User	29/08/2023 21:14	Disabled	-	-	-	-	-	-	-	-	IAMReadOnlyAccess		
3,7E+11	Admin	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess
3,7E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess

Figura 4

Usuarios cuenta koba

Account ID	Principal	Principal Type	Last console sign-in	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create Date 2	Last Used 2	Status 2	User Policies	Group Member	Group Policies
5,44E+11	543846479222.pyracloud@softwareone.com	User	Never used	Disabled	AKIAX5H6GV	6/05/2022 12:22	31/07/2024 12:44	Active	-	-	-	-	AWSConfigRoleForOrganizations, ResourceGroupsandTagEditorFullAccess, IAMReadOnlyAccess, PowerUserAccess		
5,44E+11	AzureADRoleManager	User	Never used	Disabled	AKIAX5H6GV	20/12/2021 23:14	31/07/2024 13:59	Active	-	-	-	-	AzureAD_SSOUserRole_Policy		
5,44E+11	backup-d1	User	Never used	Disabled	AKIAX5H6GV	25/04/2024 22:45	26/04/2024 21:42	Active	-	-	-	-			
5,44E+11	BCT-fotos	User	11/04/2023 16:47	Disabled	-	-	-	-	-	-	-	-	Maestro-S3-prd-Policy		
5,44E+11	BCT-fotos-pro	User	Never used	Disabled	AKIAX5H6GV	29/08/2022 21:35	21/03/2023 21:06	Inactive	AKIAX5H6GV	22/03/2023 23:16	22/06/2023 17:39	Active	Maestro-S3-prd-Policy, AWSCompromisedKeyQuarantineV2		
5,44E+11	CT-backup-usuarios-d1	User	Never used	Disabled	AKIAX5H6GV	3/10/2022 20:51	17/02/2023 14:46	Active	-	-	-	-	backup-usuarios-d1-policy		
5,44E+11	CT-HYPERION-PRD	User	Never used	Disabled	AKIAX5H6GV	14/09/2022 22:09	Never used	Active	-	-	-	-	AmazonRoute53DomainsFullAccess, AdministratorAccess-Amplify		
5,44E+11	CT-Hyperion_codecommit	User	Never used	Disabled	AKIAX5H6GV	15/09/2022 15:10	Never used	Active	-	-	-	-	AWSCodeCommitPowerUser		
5,44E+11	CT-RPA-FACTURAS-PRD-S3	User	Never used	Disabled	AKIAX5H6GV	27/09/2022 13:14	31/07/2024 7:01	Active	-	-	-	-	Rpa-Facturas-S3-KobaPRD-Policy, AmazonEC2ContainerRegistryFullAccess, AmazonEC2ContainerRegistryPowerUser, AmazonSESFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess, AmazonElasticContainerRegistryPublicPowerUser		
5,44E+11	CT-T2K-S3	User	Never used	Disabled	AKIAX5H6GV	7/04/2022 15:45	15/06/2023 11:21	Active	-	-	-	-	t2k-S3-Prd-Policy, AmazonEC2ContainerRegistryFullAccess		
5,44E+11	CT-T2K-S3-COLABORADORES	User	Never used	Disabled	AKIAX5H6GV	7/04/2022 15:43	17/05/2022 22:13	Active	-	-	-	-	T2K-S3-COLABORADORES-Policy		
5,44E+11	CT-TESORERIA-S3-PRD	User	Never used	Disabled	AKIAX5H6GV	9/09/2022 21:52	20/01/2023 15:14	Active	-	-	-	-	S3-Rpatesoreria-Policy, AmazonEC2ContainerRegistryFullAccess, AmazonEC2ContainerRegistryPowerUser, AmazonSESFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess, AmazonElasticContainerRegistryPublicPowerUser		
5,44E+11	ct_swo	User	Never used	Disabled	AKIAX5H6GV	14/03/2024 13:31	14/03/2024 13:35	Active	AKIAX5H6GV	26/03/2024 15:57	26/03/2024 15:58	Active	ReadOnlyAccess		
5,44E+11	fabio.aristizabal	User	24/05/2024 15:08	Enabled	AKIAX5H6GV	25/04/2024 19:30	26/04/2024 23:11	Active	-	-	-	-	AWSSupportPlansFullAccess	Administrators	AdministratorAccess, Billing
5,44E+11	hector.rodriguez	User	Never used	Disabled	-	-	-	-	-	-	-	-		Administrators	AdministratorAccess, Billing
5,44E+11	IBM-PRD-camilo.saldarriaga	User	14/01/2022 14:44	Enabled	AKIAX5H6GV	3/01/2022 22:32	17/01/2022 15:52	Active	-	-	-	-	ibm-koba-prd-bucket-Policy, IAMUserChangePassword	IBM-S3	ibm-koba-prd-bucket-Policy, MFA-Mandatory
5,44E+11	IBM-PRD-gustavo.barrera	User	6/01/2022 15:25	Enabled	AKIAX5H6GV	3/01/2022 22:30	Never used	Active	-	-	-	-	IAMUserChangePassword	IBM-S3	ibm-koba-prd-bucket-Policy, MFA-Mandatory
5,44E+11	IBM-PRD-reisson.saavedra	User	6/01/2022 13:08	Disabled	AKIAX5H6GV	3/01/2022 22:35	Never used	Active	-	-	-	-	IAMUserChangePassword	IBM-S3	ibm-koba-prd-bucket-Policy, MFA-Mandatory
5,44E+11	IBM-PRD-santiago.rueda	User	5/01/2022 20:42	Enabled	AKIAX5H6GV	5/01/2022 15:56	Never used	Active	-	-	-	-	IAMUserChangePassword	IBM-S3	ibm-koba-prd-bucket-Policy, MFA-Mandatory
5,44E+11	IG-Alexander.Perez	User	26/07/2024 13:01	Enabled	AKIAX5H6GV	27/09/2021 20:10	14/10/2021 13:11	Active	AKIAX5H6GV	10/07/2024 22:02	16/07/2024 14:43	Active	BillingAccessDenied, IAMUserChangePassword	Administrators	AdministratorAccess, Billing
5,44E+11	IG-Jennifer.Cano	User	9/12/2022 14:52	Disabled	AKIAX5H6GV	27/09/2021 20:07	Never used	Inactive	-	-	-	-	BillingFullAccess	Administrators	AdministratorAccess, Billing
5,44E+11	IG-Karyn.Gomez	User	29/07/2024 21:36	Enabled	-	-	-	-	-	-	-	-		Administrators	AdministratorAccess, Billing
5,44E+11	IG-luis.ortiz	User	9/02/2023 13:28	Disabled	-	-	-	-	-	-	-	-	AmazonEC2FullAccess, AmazonEC2RoleforSSM, IAMUserChangePassword	SSM	AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonEC2RoleforSSM, AmazonSSMAutomationRole
5,44E+11	jose.nunez	User	Never used	Disabled	AKIAX5H6GV	25/07/2024 20:25	Never used	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
5,44E+11	juan.patino	User	7/05/2024 15:07	Disabled	-	-	-	-	-	-	-	-	ResourceGroupsandTagEditorFullAccess, ReadOnlyAccess		
5,44E+11	KobaProv-Juan.Ramos	User	12/10/2021 16:37	Disabled	AKIAX5H6GV	19/11/2021 13:45	3/01/2022 22:01	Active	-	-	-	-	BillingAccessDenied, Glacier-S3-Policy		
5,44E+11	MDM-Imagenes-S3-PRD	User	Never used	Disabled	AKIAX5H6GV	6/12/2021 22:04	6/12/2021 22:11	Active	-	-	-	-	MDM-S3-Bucket-Policy, BillingAccessDenied		
5,44E+11	sebastian.escobar	User	Never used	Disabled	AKIAX5H6GV	25/07/2024 20:24	30/07/2024 19:39	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
5,44E+11	stiven.bermudez	User	5/07/2024 1:45	Enabled	-	-	-	-	-	-	-	-		Administrators	AdministratorAccess, Billing
5,44E+11	swo-juan.patino	User	29/08/2023 21:37	Disabled	-	-	-	-	-	-	-	-	IAMReadOnlyAccess		
5,44E+11	test_user	User	7/02/2024 15:13	Disabled	-	-	-	-	-	-	-	-	rds_describe, rds_aranda_monitor		
5,44E+11	usr_monitor_seti@d1.com.co	User	7/02/2024 14:31	Disabled	-	-	-	-	-	-	-	-	rds_describe, rds_aranda_monitor		
5,44E+11	Administrators	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess, Billing
5,44E+11	IBM-S3	Group	-	-	-	-	-	-	-	-	-	-	-	-	ibm-koba-prd-bucket-Policy, MFA-Mandatory
5,44E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess
5,44E+11	SSM	Group	-	-	-	-	-	-	-	-	-	-	-	-	AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonEC2RoleforSSM, AmazonSSMAutomationRole

Figura 5

Usuarios cuenta feel

Account Id	Principal	Principal Type	Last console sign-in	MFA Status	Access Key	Create Date	Last Used	Status 1	Access Key	Create Date	Last Used	Status 2	User Policies	Group Member	Group Policies
9,09E+11	ALBERTO.HERRERA	User	30/07/2024 0:45	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	ALEXANDRA.CASTIBLANCO	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	ARJELIS.ROMANA	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	arnold.alfonso@d1.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	ReadOnlyAccess, IAMUserChangePassword		
9,09E+11	AURA.FLOREZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	BRAYAN.VEGA	User	1/04/2024 11:19	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	carlos.sema@d1.com.co	User	30/07/2024 15:43	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel_2	AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonAPIGatewayPushToCloudWatchLogs, AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonAPIGatewayInvokeFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSWAFConsoleReadOnlyAccess
9,09E+11	carlos.sema@d1.com.co	User	30/07/2024 15:43	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	feel_billing	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
9,09E+11	carlos.sema@d1.com.co	User	30/07/2024 15:43	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
9,09E+11	carlos.sema@d1.com.co	User	30/07/2024 15:43	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
9,09E+11	CATERINE.PEREA	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	CESAR.PAIPILLA	User	25/07/2024 19:05	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	ct_devops_feel	User	Never used	Disabled	AKIA5HC4	########	########	Active	-	-	-	-	AmazonRoute53FullAccess, AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonEC2ContainerRegistryPowerUser, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess, AmazonElasticContainerRegistryPublicPowerUser	app_programatico_feel	AmazonAPIGatewayPushToCloudWatchLogs, CloudWatchEventsFullAccess, AmazonS3FullAccess, AmazonCloudWatchRUMFullAccess, AmazonCloudWatchEvidentlyFullAccess
9,09E+11	ct_devops_feel	User	Never used	Disabled	AKIA5HC4	########	########	Active	-	-	-	-	AmazonRoute53FullAccess, AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonEC2ContainerRegistryPowerUser, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess, AmazonElasticContainerRegistryPublicPowerUser	Cloudformation-FEEL	CloudformationFEELPolicy
9,09E+11	ct_swo_reportes	User	Never used	Disabled	AKIA5HC4	########	########	Active	AKIA5HC4	########	########	Active	ReadOnlyAccess		
9,09E+11	DANIEL.RAMOS	User	29/02/2024 16:41	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	DAVID.HERNANDEZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	DAYRO.PINILLA	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	DIANA.GARCIA	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	DIANA.LEAL	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly

Figura 6

Usuarios cuenta feel parte 2

9,09E+11	diego.gomez@d1.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel_2	AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonAPIGatewayPushToCloudWatchLogs, AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonAPIGatewayInvokeFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSWAFConsoleReadOnlyAccess
9,09E+11	diego.gomez@d1.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	feel_billing	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
9,09E+11	diego.gomez@d1.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
9,09E+11	diego.gomez@d1.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
9,09E+11	EDAGR.LOPEZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	edwar.quintero	User	Never used	Disabled	-	-	-	-	-	-	-	-	AdministratorAccess, IAMUserChangePassword		
9,09E+11	ESTEBAN.HERNANDEZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	estebancano@seti.com.co	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	JHONATAN.RESTREPO	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	johnparra@seti.com.co	User	7/03/2024 16:45	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	feel_billing	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
9,09E+11	johnparra@seti.com.co	User	7/03/2024 16:45	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
9,09E+11	johnparra@seti.com.co	User	7/03/2024 16:45	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	DatabaseMigrationServic	DatabaseMigrationServiceidentitybasedpolicy
9,09E+11	johnparra@seti.com.co	User	7/03/2024 16:45	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
9,09E+11	jose.nunez	User	Never used	Disabled	AKIA5HC4	########	Never use	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
9,09E+11	JUAN.LOPERA	User	5/04/2024 12:16	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	KELLY.ARBOLEDA	User	3/04/2024 13:10	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	KELLY.CAMARGO	User	30/03/2024 2:40	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	MAICOL.SANCHEZ	User	5/04/2024 3:45	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	MANUEL.TAPASCO	User	1/04/2024 14:46	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	MANUEL.VARGAS	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	MARIA.PANTOJA	User	4/04/2024 3:19	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	MATEO.BASCO	User	4/04/2024 3:34	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel_2	AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonAPIGatewayPushToCloudWatchLogs, AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonAPIGatewayInvokeFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSWAFConsoleReadOnlyAccess
9,09E+11	mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	computer_optimizer	ComputeOptimizerReadOnlyAccess, compute-optimizer.amazonaws.com, AWSServiceRoleForComputeOptimizer_lambda, role_servicelinkedrole
9,09E+11	mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	feel_billing	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
9,09E+11	mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess

Figura 7

Usuarios cuenta feel parte 3

mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel3	AmazonForecastFullAccess, AmazonEventBridgeFullAccess, CostOptimizationHubAdminAccess
mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	SNS_CloudWatch	CloudWatchFullAccess, AmazonSNSFullAccess
mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	DatabaseMigrationServic	DatabaseMigrationServiceidentitybasedpolicy
mauricio.constain@d1.com.co	User	26/07/2024 22:16	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
milton.serrano@d1.com.co	User	26/07/2024 20:57	Disabled	-	-	-	-	-	-	-	-	AmazonRDSFullAccess, IAMUserChangePassword, rds_parametergroup		
MOISES.YANEZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
nelson.melo@d1.com.co	User	28/06/2024 13:12	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	feel_billing	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
nelson.melo@d1.com.co	User	28/06/2024 13:12	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
nelson.melo@d1.com.co	User	28/06/2024 13:12	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	SNS_CloudWatch	CloudWatchFullAccess, AmazonSNSFullAccess
nelson.melo@d1.com.co	User	28/06/2024 13:12	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	DatabaseMigrationServic	DatabaseMigrationServiceidentitybasedpolicy
nelson.melo@d1.com.co	User	28/06/2024 13:12	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
NICOLAS.BEDTANCUR	User	30/07/2024 2:27	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
pro_julian.guarnizo@d1.com.c	User	31/07/2024 13:24	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword, AdministratorAccess-AWSElasticBeanstalk	Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
pro_julian.guarnizo@d1.com.c	User	31/07/2024 13:24	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword, AdministratorAccess-AWSElasticBeanstalk	Admin_DMS_FEEL	AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
pro_samuel.jimenez@d1.com.	User	26/07/2024 14:53	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel_2	AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonAPIGatewayPushToCloudWatchLogs, AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonAPIGatewayInvokeFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSWAFConsoleReadOnlyAccess
pro_samuel.jimenez@d1.com.	User	26/07/2024 14:53	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
pro_samuel.jimenez@d1.com.	User	26/07/2024 14:53	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	app_feel3	AmazonForecastFullAccess, AmazonEventBridgeFullAccess, CostOptimizationHubAdminAccess
pro_samuel.jimenez@d1.com.	User	26/07/2024 14:53	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Cloudformation-FEEL	CloudformationFEELPolicy
raul_hurtado	User	3/05/2024 14:47	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword, AWSLambda_FullAccess	Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
raul_hurtado	User	3/05/2024 14:47	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword, AWSLambda_FullAccess	Admin_DMS_FEEL	AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
SEBASTIAN.BENJUMEA	User	2/04/2024 13:53	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
sebastian.escobar	User	Never used	Disabled	AKIA5HC4	########	########	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
SEBASTIAN.ESPINOSA	User	4/04/2024 11:15	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
SERGIO.DIAZ	User	4/04/2024 15:11	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
srv_cerberus_ECR	User	Never used	Disabled	AKIA5HC4	########	########	Active	-	-	-	-	AmazonEC2ContainerRegistryFullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, EC2InstanceProfileForImageBuilderECRContainerBuilds	Cloudformation-FEEL	CloudformationFEELPolicy
usertest	User	4/03/2024 21:06	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
YESID.RODRIGUEZ	User	Never used	Disabled	-	-	-	-	-	-	-	-		Monitoreo_seti	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
Admin_DMS_FEEL	Group	-	-	-	-	-	-	-	-	-	-	-	-	AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly

Figura 8

Usuarios cuenta feel parte 4

9,09E+11	app_feel	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	AmazonRoute53FullAccess, AmazonRDSFullAccess, AWSCertificateManagerFullAccess, SecretsManagerReadWrite, AmazonSQSFullAccess, AmazonElastiCacheFullAccess, AmazonS3FullAccess, AdministratorAccess-AWSElasticBeanstalk, AmazonElasticContainerRegistryPublicFullAccess, AWSLambda_FullAccess
9,09E+11	app_feel3	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	AmazonForecastFullAccess, AmazonEventBridgeFullAccess, CostOptimizationHubAdminAccess
9,09E+11	app_feel_2	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	AmazonAPIGatewayAdministrator, AmazonEC2ContainerRegistryFullAccess, AmazonAPIGatewayPushToCloudWatchLogs, AmazonSSMFullAccess, AmazonSSMManagedInstanceCore, AmazonAPIGatewayInvokeFullAccess, AmazonElasticContainerRegistryPublicFullAccess, AmazonElasticContainerRegistryPublicPowerUser, AWSWAFConsoleReadOnlyAccess
9,09E+11	app_programatico_feel	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	AmazonAPIGatewayPushToCloudWatchLogs, CloudWatchEventsFullAccess, AmazonS3FullAccess, AmazonCloudWatchRUMFullAccess, AmazonCloudWatchEvidentlyFullAccess
9,09E+11	Cloudformation-FEEL	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	CloudformationFEELPolicy
9,09E+11	computer_optimizer	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	ComputeOptimizerReadOnlyAccess, compute-optimizer.amazonaws.com, AWSServiceRoleForComputeOptimizer_lambda, role_servicelinkedrole
9,09E+11	DatabaseMigrationServiceFEEL	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	DatabaseMigrationServiceidentitybasedpolicy
9,09E+11	feel_billing	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	AmazonForecastFullAccess, AWSBillingReadOnlyAccess
9,09E+11	Monitoreo_seti	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	CloudWatchReadOnlyAccess, AmazonRDSReadOnlyAccess, AmazonRDSPerformanceInsightsReadOnly
9,09E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess
9,09E+11	SNS_CloudWatch	Group	-	-	-	-	-	-	-	-	-	-	-	-	-	CloudWatchFullAccess, AmazonSNSFullAccess

Figura 9

Usuarios cuenta databricks

Account II	Principal	Principal Type	Last console sign-in	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create Date 2	Last Used 2	Status 2	User Policies	Group Member	Group Policies
1,97E+11	ct_swo_reportes	User	Never used	Disabled	AKIAS3UUCA	26/03/2024 16:32	26/03/2024 16:33	Active	-	-	-	-	ReadOnlyAccess		
1,97E+11	fabio.aristizabal	User	26/03/2024 16:30	Enabled	AKIAS3UUCA	21/03/2024 22:43	21/03/2024 22:47	Active	-	-	-	-	IAMUserChangePassword	admin	AdministratorAccess
1,97E+11	IG-alexander.perez	User	24/03/2023 22:52	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	admin	AdministratorAccess
1,97E+11	IG-karyn.gomez	User	20/01/2023 20:44	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	admin	AdministratorAccess
1,97E+11	jose.nunez	User	Never used	Disabled	AKIAS3UUCA	25/07/2024 20:47	Never used	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
1,97E+11	sebastian.escobar	User	Never used	Disabled	AKIAS3UUCA	25/07/2024 20:47	31/07/2024 13:31	Active	-	-	-	-		ReadOnly	ReadOnlyAccess
1,97E+11	swo-juan.patino	User	29/08/2023 21:05	Disabled	-	-	-	-	-	-	-	-	IAMReadOnlyAccess		
1,97E+11	usr_databricks_dbp@d1.com.co	User	Never used	Disabled	AKIAS3UUCA	20/01/2023 20:43	23/02/2023 21:40	Active	-	-	-	-	d1-databricks-policys3		
1,97E+11	admin	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess
1,97E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess

Figura 10

Usuarios cuenta hyperion2

Account II	Principal	Principal T	Last consc	MFA Statu	Access Ke	Create Da	Last Used	Status 1	Access Ke	Create Da	Last Used	Status 2	User Policies	Group Member	Group Policies
5,9E+11	alexander	User	########	Disabled	-	-	-	-	-	-	-	-		Admin	AdministratorAccess
5,9E+11	jose.nune	User	Never use	Disabled	AKIAYS2N	########	Never use	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
5,9E+11	sebastian.	User	Never use	Disabled	AKIAYS2N	########	########	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
5,9E+11	Admin	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess
5,9E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess

Figura 11

Usuarios cuenta cliente unico

Account II	Principal	Principal Type	Last console sign-in	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create Date 2	Last Used 2	Status 2	User Policies	Group Member	Group Policies
7,45E+11	ct_SWO	User	Never used	Disabled	AKIA22XUJFV	15/03/2024 21:37	15/03/2024 21:41	Active	AKIA22XUJFV	26/03/2024 16:22	26/03/2024 16:27	Active	ReadOnlyAccess		
7,45E+11	d1s3unifiedcustome	User	Never used	Disabled	AKIA22XUJFV	6/05/2023 0:24	29/06/2024 17:00	Active	-	-	-	-		d1s3group	AmazonS3FullAccess
7,45E+11	jose.nunez	User	Never used	Disabled	AKIA22XUJFV	25/07/2024 20:49	Never used	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
7,45E+11	sebastian.escobar	User	Never used	Disabled	AKIA22XUJFV	25/07/2024 20:50	31/07/2024 14:04	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
7,45E+11	swo-juan.patino	User	29/08/2023 20:10	Disabled	-	-	-	-	-	-	-	-	IAMReadOnlyAccess, IAMUserChangePassword		
7,45E+11	Admin	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess
7,45E+11	d1s3group	Group	-	-	-	-	-	-	-	-	-	-	-	-	AmazonS3FullAccess
7,45E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess

Figura 12

Usuarios cuenta master

Account ID	Principal	Principal Type	Last console sign-in	MFA Status	Access Key 1	Create Date 1	Last Used 1	Status 1	Access Key 2	Create Date 2	Last Used 2	Status 2	User Policies	Group Member	Group Policies
1,415E+11	alexander.perez	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Admin_AWS	AdministratorAccess
1,415E+11	camilo.pinto	User	6/10/2023 14:00	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Admin_AWS	AdministratorAccess
1,415E+11	fabio.aristizabal	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Admin_AWS	AdministratorAccess
1,415E+11	jose.nunez	User	Never used	Disabled	AKIASB4DHV	25/07/2024 16:23	Never used	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
1,415E+11	juan.garcia6	User	17/01/2024 21:53	Enabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Admin_AWS	AdministratorAccess
1,415E+11	karyn.gomez	User	Never used	Disabled	-	-	-	-	-	-	-	-	IAMUserChangePassword	Admin_AWS	AdministratorAccess
1,415E+11	sebastian.escobar	User	Never used	Disabled	AKIASB4DHV	25/07/2024 16:23	31/07/2024 13:17	Active	-	-	-	-	IAMUserChangePassword	ReadOnly	ReadOnlyAccess
1,415E+11	Admin_AWS	Group	-	-	-	-	-	-	-	-	-	-	-	-	AdministratorAccess
1,415E+11	ReadOnly	Group	-	-	-	-	-	-	-	-	-	-	-	-	ReadOnlyAccess