Diseño e Implementación de un sistema de monitoreo y alertamiento de control de acceso a datos de una entidad pública que suministra información a terceros

Carlos Alberto Rodríguez, Mario Diaz Carrasco
Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes Bogotá, Colombia
Mayo de 2022

1. Introducción

De acuerdo con lo establecido en la Ley 019 de 2012, conocida como Ley Anti-trámites, las entidades públicas se vieron en la necesidad de poner a disposición la información que producen y administran, habilitando herramientas de interoperabilidad para facilitar y agilizar la consulta por parte de la ciudadanía, otras entidades y actores tanto privados como públicos. Sin embargo, varias de las entidades del estado colombiano, y aun ante la criticidad de la información que es consultada; no cuentan con una herramienta que permita realizar el monitoreo y generar alertas que permita alertar de manera automática e inmediata de la extracción de datos de manera abusiva, a través de las diferentes consultas realizadas por las entidades públicas y privadas, así como otros actores.

A partir del año 2020 a causa de la pandemia ocasionada por el virus SARS-COV2, las consultas a las bases datos administradas por entidades públicas, se incrementaron significativamente, en el caso de la entidad que hace parte del presente proyecto, en más de un 100% en comparación al año 2019, pasando de 654 millones a más de 1300 millones. El incremento de las consultas realizadas fue ocasionado por las ayudas y beneficios otorgados por el gobierno nacional a los colombianos en condición de pobreza y/o colombianos clasificados en los niveles más bajos del SISBEN, requiriendo la verificación de sus datos para evitar asignar ayudas a personas suplantadas.

Debido al notorio incremento de las consultas, la implementación de actividades de monitoreo, alertamiento y aseguramiento de datos han cobrado una mayor relevancia para la entidad; esto teniendo en cuenta que en años recientes se han presentado una cantidad significativa de incidentes asociados a la fuga de datos, los cuales afectan ya no solo a entidades privadas, sino también a instituciones públicas, y pueden llegar a tener efectos adversos a nivel económico, disciplinario y reputacional. Es de especial atención que al tratar específicamente con datos personales, la base de datos con información de los colombianos está sujeta al cumplimiento de la ley 1581 de 2012, en la cual se constituye el marco de la protección de los datos personales en Colombia, por lo cual al no contar actualmente con un sistema que permita realizar las debidas acciones para prevenir y controlar los riesgos a los que se encuentra expuesta esta base de datos; se podría llegar a incurrir en incumplimientos de la ley anteriormente mencionada (Belli, 2021) (contributors, Bulgarian revenue agency hack, 2022) (contributors, Commission on Elections data breach, 2021).

Es importante tener en cuentas las cifras de delitos informáticos publicados en la página del CAI Virtual de la Policía Nacional (https://caivirtual.policia.gov.co/). El comportamiento de algunos delitos informáticos durante el período covid-19 como el acceso abusivo a un sistema informático y la interceptación de datos informáticos ha aumentado de forma significativa, lo que podría materializarse en la entidad extrayendo la información de los colombianos (Nacional, Policia, 2021).

Como herramienta estadística, una de las oficinas de la entidad, cuenta con un sistema que permite generar el reporte de consultas por entidad en un período determinado, este período debe ser seleccionado por el

funcionario. Dicho reporte debe ser generado de forma manual y a petición del funcionario, actividad que no se realiza continuamente ya que depende de la disponibilidad del funcionario.

Debido a lo mencionado anteriormente, incidentes presentados con el acceso a la base de dato con información biográfica de los colombianos no fueron detectados por las herramientas con las que cuenta la entidad, sino posteriormente, a través de los procesos de generación y análisis de los reportes estadísticos, lo que ha permitido, más de una vez, la consulta de millones de registros. Estos incidentes se han presentado tanto con entidades públicas como privadas, por lo cual es necesario que se implemente otro tipo de sistema que permita generar alertas automáticas y desarrollar tableros de control amigables, con información actualizada y que se encuentren disponible para los funcionarios autorizados al interior de la entidad, esto con el objeto de tomar acciones correctivas a nivel técnico y administrativo.

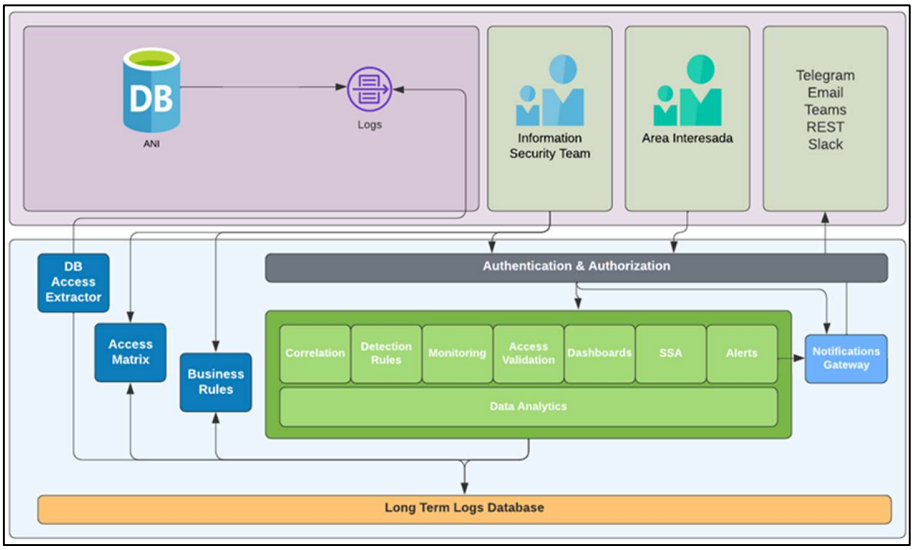
2. Propuesta de Solución

Como solución a la problemática expuesta anteriormente, se realizó el diseño e implementación de un sistema de monitoreo y generación de alertas que permita obtener visibilidad y mayor conocimiento sobre las diferentes transacciones realizadas por terceros, así como desarrollar reglas que permitan identificar actividades, consultas y accesos no autorizados sobre la información presente en la base de datos. Como característica adicional, el sistema se encuentra compuesto por herramientas de código abierto; eliminando así completamente los costos asociados al licenciamiento de los componentes.

El sistema permite mejorar el control de acceso a través de identificación de la actividad desarrollada por los diferentes actores, y la generación automática de alertas sobre las consultas que se presentan a la base de datos; identificando de forma proactiva y automatizada posibles brechas de seguridad, acceso no autorizados, o abusos sobre los accesos existentes, permitiéndole a la entidad desarrollar acciones de monitoreo, prevención, identificación y respuesta ante la posible materialización de estos riesgos; al obtener una mejor visibilidad de las consultas que se desarrollan a la base de datos.

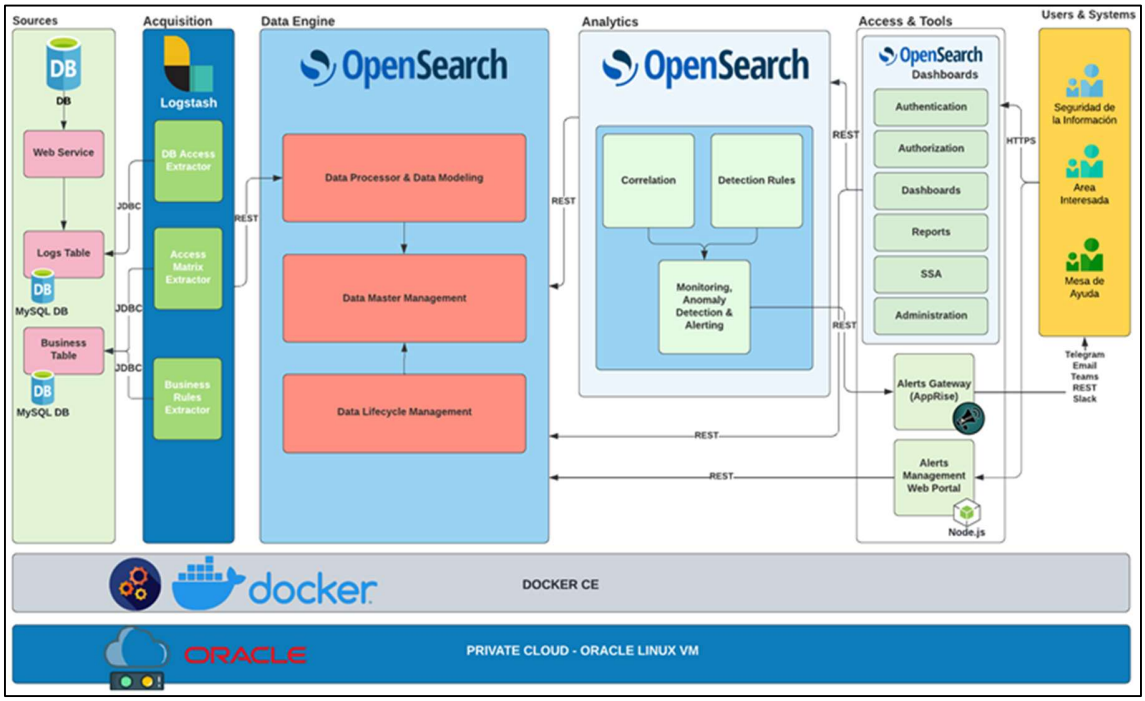
3. Diseño

De acuerdo con la propuesta de solución, se desarrolla una arquitectura de alto nivel la cual se presenta en la Figura 1, con los componentes del sistema y los actores que interactúan con el mismo.



Dentro de la propuesta de solución planteada, se muestra en fondo color azul claro, la arquitectura de alto nivel del sistema de información que será diseñado e implementado para la recolección, correlación, análisis a partir de los registros generados por el sistema que controla el acceso a la base de datos utilizado para el acceso a la misma; el sistema diseñado de igual forma, desarrollará los procesos de analítica, alertamiento y visualización de los accesos, permitiéndole a los usuarios del sistema analizar grandes cantidades de información de forma simple, gráfica, precisa y confiable, de tal manera que le permita a la entidad estar informada en tiempo real y reaccionar en el menor tiempo a posibles incidente de seguridad que ponga en riesgo la confidencialidad de la información y la disponibilidad del sistema.

La arquitectura de alto nivel está basada en plataforma de contenedores "Docker" en su edición "Community", desplegada sobre una máquina virtual con sistema operativo Linux Oracle versión 8.5; lo anterior tiene como propósito poder aprovechar de mejor forma los recursos disponibles y tener una mayor densidad de aplicaciones dadas las limitaciones tecnológicas de la entidad. Dentro de la ilustración 2 es posible identificar cada uno de los componentes de la arquitectura de solución detallada, así como los elementos que la componen y los protocolos utilizados en la interrelación de estos.



A continuación, se describen los diferentes elementos de la solución propuesta:

- **Sources:** Las fuentes de información de la arquitectura, se encuentran centralizados principalmente en una base de datos MySQL, utilizada para almacenar la información referente a los convenios y contratos que se encuentran actualmente vigentes, así como las respectivas consultas desarrolladas por las entidades que hacen parte de estos. Esta información es la que sirve como base para obtener los registros de las consultas realizadas, así como las entidades con acceso, fechas de expiración de los convenios y contratos, reglas de negocio en cuanto a consumo de consultas, entre otros.

- **Acquisition:** La plataforma utilizada para realizar la adquisición de los registros es Logstash en su versión de código abierto, este funciona como herramienta de Extracción, Transformación y Carga de datos (ETL por sus siglas en ingles), realizando consultas JDBC hacia las diversas fuentes con una periodicidad especifica; una vez obtenidos los datos, se realiza la transformación de los mismos de acuerdo al esquema

de datos desarrollado y posteriormente se carga a través de un servicio REST al componente de motor de datos, esto último con el fin de poder realizar los diferentes procesos de almacenamiento, tratamiento y análisis de los mismos en posteriores etapas.

- **Data Engine:** El motor de base de datos utilizado en la arquitectura corresponde a Open Search, esta base de datos NoSQL fue elegida debido a la versatilidad que posee para el manejo y búsqueda de datos específicos dentro de grandes cantidades de información, así como, las posibilidades de funcionar en modo clúster y desarrollar funciones analíticas; adicionalmente cuenta con una alta integración con una plataforma de visualización de contenido versátil y altamente probada. Dentro del motor de datos, se realizan los procesos de almacenamiento y procesamiento de los datos asociados a los registros de acceso al web service, reglas de negocio, matriz de acceso y alertas presentadas sobre el sistema; dentro de las funciones que desarrolla, también se encuentran las relacionadas con el manejo del ciclo de vida de los datos, permitiendo la eliminación de los datos una vez se considera que han cumplido su ciclo de vida.

- **Analytics**: El motor de analítica utilizado en el sistema, hace parte de Open Search en forma varios complementos (plugins), los cuales añaden capacidades al sistema, permitiendo realizar búsquedas sobre la información y estableciendo reglas para la correlación y detección de posibles situaciones de riesgo; adicionalmente cuenta con un módulo especializado en el monitoreo, detección de anomalías y alertamiento; las búsquedas son realizadas directamente sobre el motor de base de datos de Open Search a partir de peticiones REST. Adicionalmente las alertas que se generan a partir de los análisis desarrollados son enviadas al componente Alerts Gateway mediante un servicio REST, el cual es el encargado de realizar la distribución a través de múltiples protocolos de envió de mensajes.

- **Access & Tools:** Dentro del componente de acceso y autenticación, se encuentran varios productos; el principal es “Open Search Dashboards”, el cual es el encargado de proveer la autenticación, autorización, tableros de control, reportes, Self Service Analytics (SSA) y administración general de la plataforma de gestión de la información; adicionalmente y como el rol más importante, es el componente con el cual interactúan de forma principal los usuarios de la plataforma; este componente realiza peticiones REST directamente al motor de base de datos y sus complementos; esto con el objetivo de poder desarrollar búsquedas, parametrizaciones y visualizaciones de la información presente en el mismo.

  Adicionalmente a “Open Search Dashboards”, dentro de la arquitectura existen otras dos herramientas, la primera corresponde al “Alerts Gateway”, el cual se encarga de recibir notificaciones a través de una interfaz REST, para luego distribuir estas mismas mediante otros canales de comunicación, como lo son Telegram, Email, servicios REST, Slack y Microsoft Teams, entre otros. La segunda herramienta es el “Alerts Management Web Portal”, la cual se encarga de servir de interfaz gráfica entre el usuario y la administración de los estados y detalles de las alertas generadas por el sistema, esto con el objetivo de poder actualizar las mismas de acuerdos a los procesos de gestión que se desarrollen al interior de la entidad.

- **Users & Systems:** Los usuarios principales de la aplicación corresponden al equipo de seguridad de la información y el área misional de la entidad; ambos equipos acceden al sistema para realizar consultas, visualizar y monitorear los accesos que se realizan a la base de datos, y ejecutar actividades operativas y administrativas sobre el sistema. Adicionalmente se encuentra el grupo de mesa de ayuda y los sistemas de información, los primeros desempeñando el rol de receptores de las alertas generadas por el sistema; y los segundos como potenciales elementos sobre los cuales es posible desarrollar integraciones que puedan ayudar en la automatización de la gestión y acciones derivadas de las alertas generadas por el sistema.

4. Métricas.

De acuerdo con lo identificado con la entidad y tomando como base la información histórica relacionada con los incidentes presentados dentro de la misma; se han seleccionado dos criterios de evaluación, los cuales permiten identificar el nivel de éxito del proyecto una vez se encuentre completamente implementado y funcional dentro de la entidad. Las métricas previas a la implementación del proyecto se muestran a continuación.

4.1. Tiempo Promedio de Detección (MTTD por sus siglas en ingles)

Si bien previo a la implementación del proyecto, la entidad no cuenta con un sistema que permita el cálculo preciso de esta métrica; a través de la evaluación histórica de los incidentes presentados y la identificación de estos; los cuales corresponden en promedio a uno por mes. La identificación de los incidentes se produce mayormente en los periodos de inicio de mes, en los cuales se generan los reportes del mes vencido; por lo que se estableció que la métrica de MTTD previo a la implementación del proyecto es de aproximadamente 2.2 días para el año 2022. El cálculo de esta métrica se desarrolla mediante la suma de todos los tiempos de detección de los incidentes presentados, divido el número de incidentes presentados en un periodo.

$$MTTD = \frac{\sum_{i=1}^{n} Tiempo\ de\ Detección_i}{n}$$

4.2. Tiempo Promedio de Respuesta (MTTR por sus siglas en ingles)

De igual forma que sucede con la métrica de MTTD, tampoco existe un sistema en el cual se consigne la información relacionada con la gestión de este, como lo es cuando se presentó, cuando se detectó y cuando se le dio respuesta al mismo. Sin embargo, a partir de las entrevistas y la recolección de información, se identificó que el tiempo de respuesta a un incidente previo a la implementación del proyecto es de aproximadamente 2 horas y 30 minutos para el año 2022; esto teniendo en cuenta que, una vez identificado el incidente, el funcionario que lo identifica actúa rápidamente para iniciar el proceso de remediación del mismo y garantizar que este no continue afectando el sistema si es que llega a ser el caso que el incidente se siga presentando. El cálculo de esta métrica se desarrolla realizando la suma de todos los tiempos de respuesta una vez se ha recibido una alerta, dividió el número de incidentes presentados en un periodo.

$$MTTR = \frac{\sum_{i=1}^{n} Tiempo\ de\ Respuesta_i}{n}$$

4.3. Resultado de las métricas

A través de la implementación del proyecto, se tiene como meta que al realizar la evaluación del éxito de este; estas métricas se vean reducidas a los siguientes valores:

- **Tiempo Promedio de Detección (MTTD)**

  Reducción al 0.09% del valor previo a la implementación del proyecto, el valor original expresado en minutos es de **3168** con una desviación estándar de **368 minutos**; a través de la implementación del proyecto; se espera que este tiempo se vea reducido a un valor aproximado de **3 minutos** con una deviación estándar aproximado de **1 minuto** para la detección de los incidentes. Lo anterior debido a que la evaluación e identificación de estos, se desarrolla de manera automática.

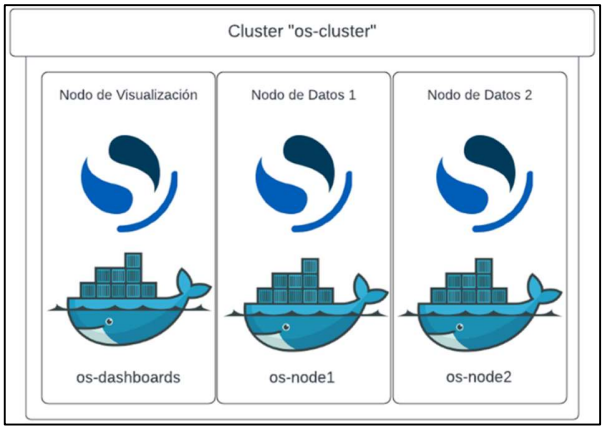
– **Tiempo Promedio de Respuesta (MTTR)**

Reducción al 40% del valor previo a la implementación del proyecto; a través del sistema se espera que este tiempo se vea reducido a un aproximado de **1 hora** con una desviación estándar de aproximadamente **30 minutos** para la respuesta ante los incidentes; esto debido a que la información expuesta a través de los tableros de control permite identificar de forma significativamente más sencilla la situación presentada y las respectivas entidades que pueden encontrarse involucradas en el incidente.

5. Implementación

5.1. Despliegue de la plataforma

Dentro de la implementación se realizó el despliegue y parametrización de una instancia de Open Search en la infraestructura provista por la entidad; la instancia se encuentra conformada por un total tres contenedores de Docker distribuidos como se puede observar en la ilustración 3.



- **Nodo de Visualización:** Nodo de Open Search Dashboards, encargado de la visualización de los tableros de control, e interfaz de administración de la funcionalidad del clúster. Permite realizar el proceso de análisis de registros y visualización de datos a través de gráficos, indicadores, mapas, entre otros; adicionalmente tiene como rol administrar y supervisar los elementos del clúster, controlando qué usuarios tienen acceso a qué funciones.

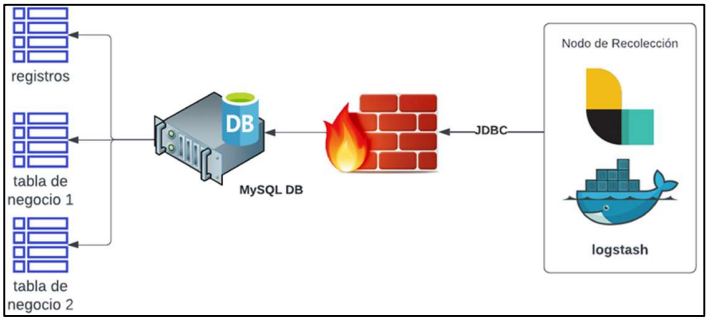
- **Nodo de Datos 1 y 2:** Nodo de OpenSearch, encargado de realizar la búsqueda e ingesta de los datos recolectados y mantenerlos por el periodo de retención definido, este nodo provee la funcionalidad de almacenar copias primarias de los datos, y las réplicas de aquellos que se encuentren en otro nodo de datos; lo cual le permite al sistema operar con un solo nodo de datos.

Las características generales del clúster son las siguientes:

Ambiente	Producción
Versión	1.3.0
Cantidad de Nodos	3
Almacenamiento Total	500 GB
Memoria Total del Clúster	16 GB
Total de Procesadores	4

5.2. Integraciones y Ciclo de Vida de Datos.

A partir de la arquitectura de solución detallada, se definió que, a nivel lógico, se realizaría la recolección de registros mediante el uso de la plataforma “Logstash” en su versión de código libre, desplegada a través de un contenedor de Docker sobre la infraestructura proporcionada por la entidad; esto dio como resultado una arquitectura de recolección de datos como la arquitectura lógica de la recolección de datos como se muestra en la ilustración 4.



Una vez se llevó a cabo la integración, se realizó un proceso para enriquecer, filtrar, modificar y dar formato a los datos recolectados, mejorando el nivel de seguridad y separación de ambientes e índices de la solución, segregando los índices utilizados y permitiendo entregar un nivel de administración más granular sobre los registros recolectados.

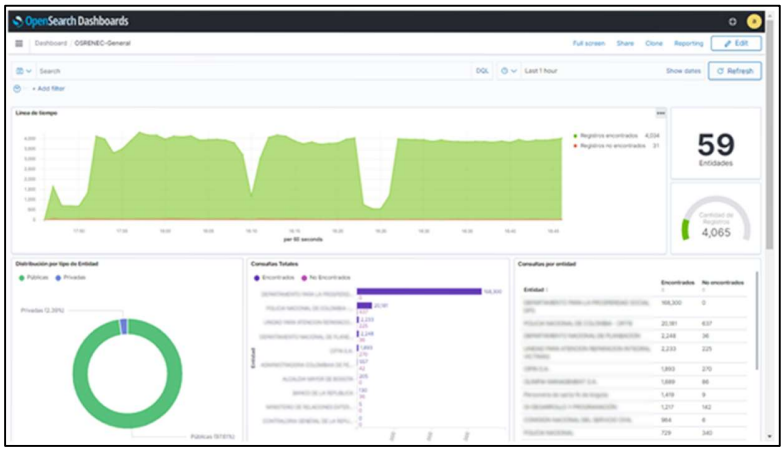
Asimismo, se realizó la definición de los elementos objetivo de la recolección de los registros, para realizar la agrupación y mejorar la segregación de los registros, para lo cual se definió el índice inicial.

De acuerdo con la recolección de los eventos, se realizó la definición de las políticas de ciclo de vida, esto con el fin de poder conservar, y por requerimiento de la entidad, al menos el último mes para ser consultado de forma eficiente y que permitan un óptimo desempeño en las búsquedas y 400 días adicionales de retención de datos, los cuales permiten almacenar de manera eficiente los datos que no son consultados de forma recuente, pero que siguen siendo relevantes para la compañía; la política de ciclo de vida definida fue la siguiente:

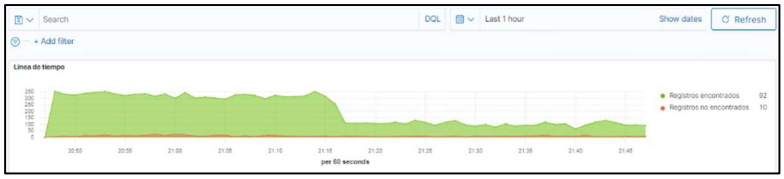
- Estado “Inicial”: Ejecuta una acción de cambio de índice cada 7 días; posteriormente realiza la transición del índice al estado “histórico” una vez el índice tenga 30 días de antigüedad.
- Estado “historico”: No ejecuta ninguna acción, realiza la transición del índice al estado “borrado” una vez el índice tenga 400 días de antigüedad.
- Estado “borrado”: Ejecuta la acción de eliminación de los datos.

5.3. Tableros de Control

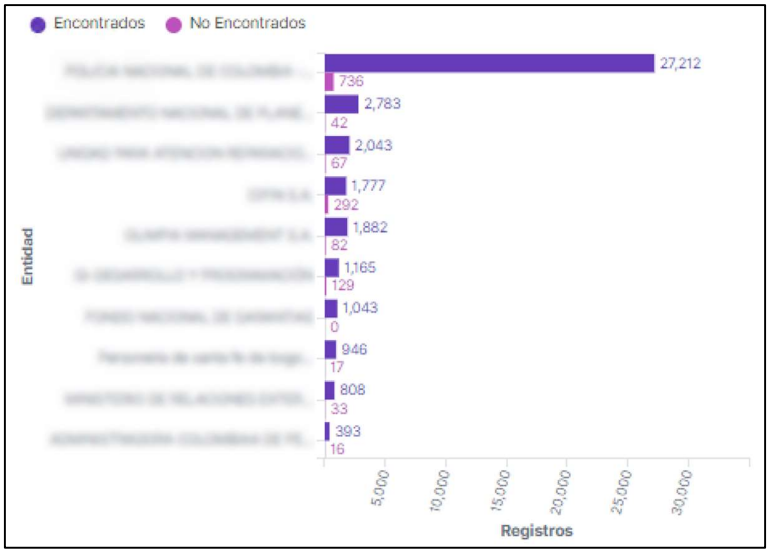
Una vez integrado el sistema a la base de datos expuesta por el área técnica de la entidad, integración que consistió en el análisis de los registros y el modelamiento de los datos para integrarlos a Open Search, se dio comienzo a la creación de diferentes visualizaciones, como Línea de Tiempo, Distribución por entidad, Consultas totales, entre otros. A continuación, se exponen algunas de las visualizaciones implementadas en el tablero de control que se muestra en la ilustración 5.



- **Visualización de Línea de tiempo**: Muestra el comportamiento de las consultas en un período que puede seleccionado por el usuario, como se muestra en la ilustración 6.

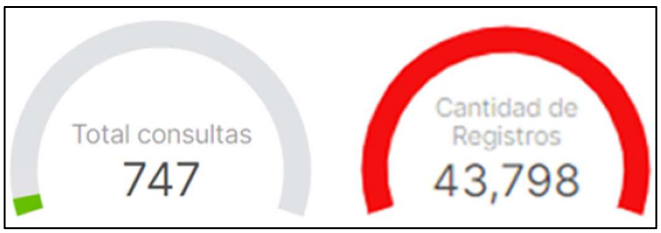


- **Visualización consultas por entidades:** Muestra el top 10 de las entidades que mayor registros consultas realizan de acuerdo con el filtro o filtros establecidos por el usuario. La visualización se muestra en la ilustración 7.

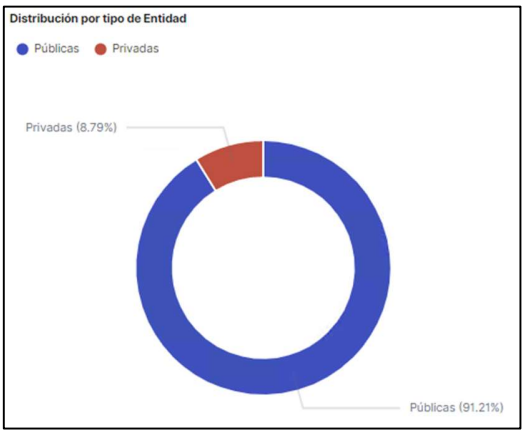


- **Consolidado de entidades consultando:** Muestra la total de entidades que realizan las consultas, de acuerdo con el filtro o filtros establecidos por el usuario, como se muestra en la ilustración 8

- **Consolidado Total de Consultas:** Grafica tipo Gauge como se muestra en la ilustración 9; el cual contiene la información del total de consultas de acuerdo con el filtro o filtros establecidos por el usuario, además, muestra el desempeño de sistema de acuerdo con la capacidad de carga por minuto de los servidores de la entidad, que para el caso es de 24000 consultas por minuto.



- **Visualización de Distribución por tipo de entidad:** Gráfica tipo torta que muestra la distribución de las entidades públicas y privadas, información que refleja el comportamiento de acuerdo con el filtro o filtros establecidos por el usuario. Esta visualización se muestra en la ilustración 10.



6. Visibilidad y monitoreo

A partir de la implementación del tablero de control general y la exploración de los datos recolectados, se identificó nuevos tipos de situaciones sobre las cuales no se tenía conocimiento o visibilidad de la información; a partir de esto, la entidad solicitó la generación de un tablero de control adicional; el cual permite realizar la identificación de los contratos con entidades privadas próximos al vencimiento, así como los respectivos saldos de estos contratos; esto con el fin de poder contar con un elemento gráfico en el cual es posible anticipar situaciones en las cuales se deban realizar la generación de un nuevo contrato o la generación de la prórroga del contrato, establecidos con entidades privadas.

7. Criterios de evaluación

De acuerdo con lo identificado con la entidad y tomando como base la información histórica relacionada con los incidentes presentados durante el funcionamiento del proyecto, se realizó la identificación de las métricas asociadas al éxito de este dando como resultado los siguientes valores:

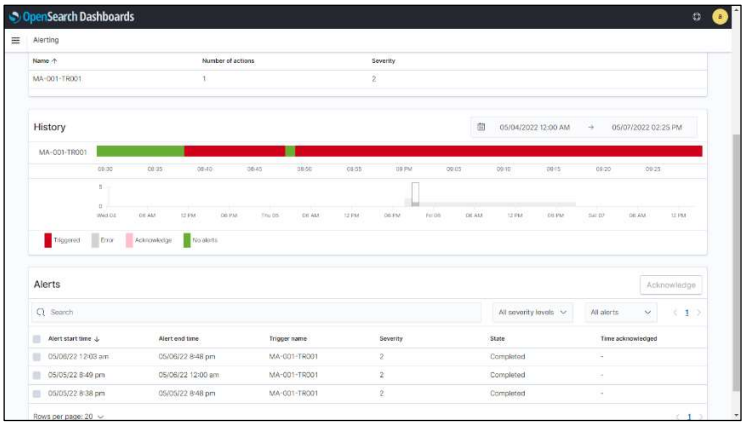
- **MTTD:** Valor medio de 1.65 minutos con una desviación estándar de 0.87 minutos (52 segundos).
- **MTTR:** Valor medio de 47 minutos con una desviación estándar de 37 minutos.

8. Alertas

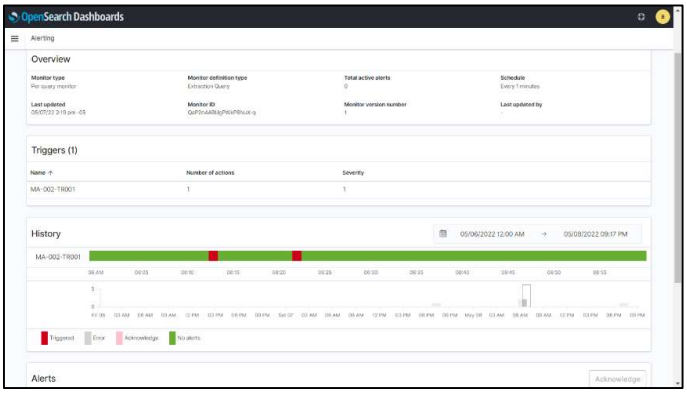
Teniendo en cuenta las necesidades de la entidad, se establecieron diferentes alertas automáticas que serán enviadas por correo electrónico a las áreas encargadas de gestionar el componente técnico y jurídico-administrativo, cuando se cumplan los criterios definidos en cada una de las alertas.

Las alertas definidas y configuradas en el sistema son las siguientes:

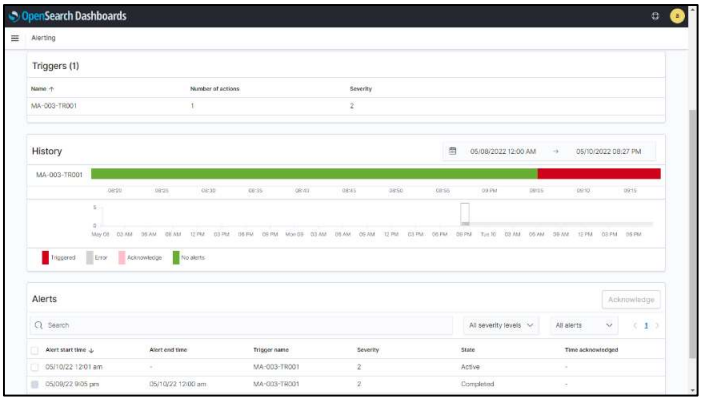
- **MA-001**: Alerta aplicada solo para entidades privades que evalúa si el valor del saldo por las consultas pagadas es menor o igual a cero. Una vez se detecte esta condición, el sistema envía correo electrónico al grupo de protección de datos, reenviando la alerta cada 30 minutos en caso de que la situación no se resuelva.



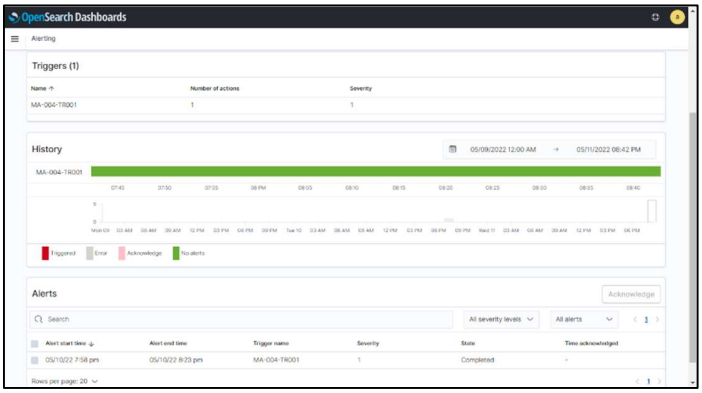
- **MA-002**: Alerta aplicada solo a entidades públicas y que evalúa el comportamiento general de las consultas realizadas a la base de datos; específicamente la cantidad de “Registros no encontrados” y su relación con respecto a los “Registros encontrados”. Si una entidad presenta una cantidad de registros no encontrados mayor a 100 por minuto y a su vez estos corresponden a más del 50% del total de los registros consultados; el sistema envía un correo electrónico al grupo de protección de datos, reenviando la alerta cada 10 minutos en caso de que la situación no se resuelva.



- **MA-003**: Alerta aplicada solo a entidades privadas y evalúa que el valor del saldo del convenio sea igual o menor al 10% del valor contrato. Una vez se detecte la condición, el sistema envía correo electrónico al grupo de protección de datos, con una frecuencia de un (1) día.

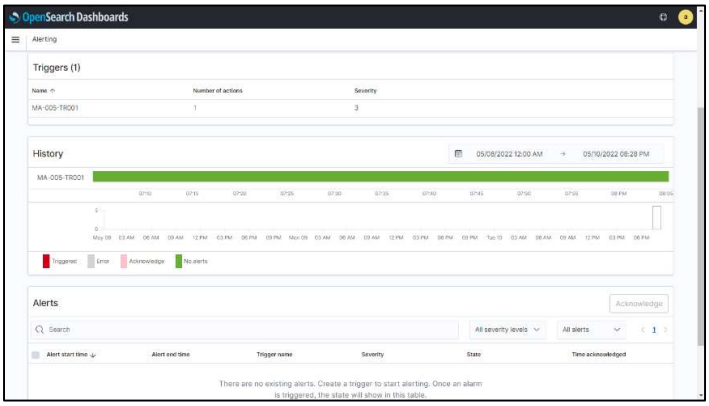


- **MA-004**: Alerta aplicada a entidades tanto públicas como privadas, la cual evalúa si la cantidad de consultas por minuto supera las dieciocho (18) mil consultas, lo cual corresponde al 70% de la capacidad por minuto del sistema. Una vez se detecta la condición, el sistema envía correo electrónico al grupo de protección de datos y al grupo de soporte técnico, con una frecuencia de diez (10) minuto.



- **MA-005**: Alerta aplicada solamente a entidades privadas, y que evalúa que la fecha final del contrato se encuentre dentro de los siguientes 40 días a la fecha del sistema. Una vez se

detecte la condición, el sistema envía correo electrónico al grupo de protección de datos con una frecuencia de una semana.



Las alertas automáticas configuradas en el sistema, le permite a la entidad tener información en tiempo real y reaccionar, de manera oportuna, ante posibles incidentes de seguridad sobre la información y el sistema de información expuesto a terceros con datos biográficos de los colombianos.

9. Evolución de la herramienta

Teniendo en cuenta los resultados obtenidos en el corto tiempo de implementada la herramienta y la aceptación por parte de los interesados al interior de la entidad, éstos han planteado la necesidad de ampliar la cobertura del sistema a otros sistemas de información que son expuestos a entidades públicas y privadas con información de reserva legal que contiene datos privados y sensibles; y que en algunos casos se encuentran en infraestructuras externas a la sede principal de la entidad.

Así mismo, han considerado la necesidad de ampliar el alcance de la herramienta al interior de la entidad para los diferentes procesos misionales, y así mismo integrarse con diferentes artefactos de seguridad, los cuales permitirían desarrollar actividades de remediación automatizada y ayudarían a ampliar la cobertura que tiene el sistema sobre la infraestructura de la entidad en términos de seguridad de la información.

10. Conclusiones

- El sistema le permite a la entidad identificar de forma proactiva y automática posibles brechas de seguridad y accesos no autorizados, desarrollando acciones de prevención ante la posible materialización de riesgos sobre los datos y sobre el servicio expuesto a terceros.

- La implementación del tablero de control al interior de la entidad optimiza el monitoreo sobre las consultas realizadas por entidades públicas y privadas a la base de datos con información biográfica de los colombianos, permitiendo reaccionar de manera proactiva ante posibles incidentes de seguridad que pongan el riesgo la confidencialidad de la información y disponibilidad del sistema.

- La generación de alertas a partir del comportamiento no deseado sobre las consultas a la base de datos biográfica de los colombianos le permite a la entidad reaccionar de manera oportuna para evitar la extracción datos fuera de los rangos permitidos por la entidad y la indisponibilidad del servicio a las demás

entidades autorizadas; teniendo también como un beneficio adicional reducir el tiempo de detección y respuesta ante posibles incidentes de seguridad que afecten el servicio.

- Dentro de las entidades públicas, los métodos utilizados para evidenciar los beneficios de los proyectos suelen diferir de las entidades o compañías privadas; sin embargo, es importante resaltar que a partir del uso de tecnologías libres y una correcta arquitectura de información; es posible desarrollar sistemas que permitan obtener de forma relativamente rápida beneficios en cuanto a la eficiencia de los procesos, visibilidad de la información y seguridad de los datos sobre los cuales trabajan estos sistemas de información.

- Previo al desarrollo de las capacidades directamente asociadas a la Seguridad de la Información, es necesario desarrollar un componente que permita obtener una mejor visibilidad sobre los problemas y datos, de las posibles situaciones de riesgo a las cuales se encuentran expuestas las compañías; para posteriormente desarrollar procesos de exploración, analítica y descubrimiento de patrones e información que, permita definir de una mejor forma las reglas y elementos de seguridad que se deben implementar en el mediano y largo plazo para asegurar la información.

- Con el fin de poder avanzar en la implementación de soluciones de seguridad de la información, más robustas y que puedan perdurar y ofrecer una mayor funcionalidad a futuro; es necesario desarrollar una relación de confianza y asesoría con las entidades en las cuales se implementa el sistema; esto permite superar varios de los posibles problemas asociados a la confianza en soluciones desconocidas, así como tramites que puedan resultar en retrasos sobre el desarrollo del proyecto.

- A partir del apoyo recibido por parte de la entidad, una vez se comenzaron a evidenciar los beneficios del proyecto; este ya no se entiende como un esfuerzo aislado por parte de la entidad, sino como la base de una arquitectura de seguridad, en la cual a través del proyecto se crean las capacidades base necesarias para soluciones más completas, las cuales tienen como objetivo desarrollar funcionalidades que permitan tomar acciones en tiempo casi real, que van dirigidas a incrementar los beneficios y disminuir la dependencia de llevar a cabo las acciones por parte de actores humanos.

- A través de la implementación del proyecto, se evidencia que es posible realizar la implementación de herramientas de código abierto con funcionalidades de monitoreo y alertamiento, a partir de documentación de acceso libre en internet, sin incurrir en altos costos de licenciamiento y sistemas altamente complejos y propietarios; conservando y bridando herramientas para los equipos de seguridad de la información; que le permitan optimizar las tareas desarrolladas y proteger los sistemas de la entidad.

9. Bibliografía

Belli, L. (3 de 02 de 2021). *openDemocracy*. Obtenido de openDemocracy: https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/

contributors, W. (12 de 12 de 2021). *Commission on Elections data breach*. Obtenido de The Free Encyclopedia: https://en.wikipedia.org/wiki/Commission_on_Elections_data_breach

contributors, W. (11 de 1 de 2022). *Bulgarian revenue agency hack*. Obtenido de The Free Encyclopedia:

https://en.wikipedia.org/w/index.php?title=2019_Bulgarian_revenue_agency_hack&oldid=1064991294

Nacional, Policia. (2021). *CAI Cibernetico Virtual*. Obtenido de CAI Virtual: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf