INVESTIGACIÓN

Herramienta para el monitoreo y análisis de trazas en la Fiscalía Provincial de Mayabeque

Tool for monitoring and trace analysis in the Provincial Prosecutor's Office of Mayabeque

TS. Laura Celín Sosa Martínez*

Recibido: 11/2025 | Aceptado: 11/2025 | Publicado: 12/2025

Resumen

Este estudio abordó la implementación de una herramienta especializada para el monitoreo y análisis de trazas, con el objetivo de fortalecer la supervisión de los sistemas informáticos y reducir la exposición ante amenazas. Se establecieron criterios para la selección e integración de la herramienta, priorizando la centralización de registros, el análisis en tiempo real y la visualización accesible de la información. La solución fue implementada en un entorno controlado, lo que permitió la detección de eventos relevantes, la identificación de patrones anómalos y la clasificación de amenazas según su nivel de impacto. La validación de la herramienta evidenció mejoras significativas en la capacidad para interpretar datos críticos y responder de forma oportuna ante posibles fallos, optimizando así la supervisión de la infraestructura tecnológica. Los resultados obtenidos confirmaron que el análisis de trazas con soporte visual representa una estrategia efectiva para garantizar la continuidad operativa y la protección de los sistemas en instituciones públicas.

Palabras clave: amenazas, análisis de trazas, monitoreo, visualización de datos, seguridad informática

* Dirección de Seguridad Informática de la UCI, Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba.lsosa@uci.cu.

Abstract

This study addressed the implementation of a specialized tool for monitoring and analyzing traces, with the goal of strengthening the oversight of information systems and reducing exposure to threats. Criteria were established for the selection and integration of the tool, prioritizing the centralization of logs, real-time analysis, and accessible visualization of information. The solution was implemented in a controlled environment, allowing for the detection of relevant events, identification of anomalous patterns, and classification of threats based on their level of impact. The validation of the tool demonstrated significant improvements in the ability to interpret critical data and respond promptly to potential failures, thus optimizing the supervision of technological infrastructure. The results confirmed that trace analysis with visual support represents an effective strategy for ensuring operational continuity and protecting systems in public institutions.

Keywords: *threats, trace analysis, monitoring, data visualization, cybersecurity*

Introducción

El monitoreo y análisis de trazas se ha vuelto una práctica esencial para el correcto funcionamiento de los sistemas informáticos en instituciones públicas y privadas. En el contexto actual, donde los sistemas informáticos están cada vez más interconectados y dependen de la tecnología para operar, es fundamental poder supervisar las actividades de las redes y los servidores para identificar problemas de rendimiento, fallos en los procesos y posibles amenazas (Alzahrani et al., 2025).

A medida que las organizaciones se digitalizan y dependen más de los sistemas tecnológicos; la seguridad de la información y la eficiencia operativa se convierten en prioridades claves. Las trazas registran información detallada sobre cada evento dentro de los sistemas, lo que permite no solo realizar diagnósticos precisos de los problemas, sino también asegurar la confidencialidad e integridad de los datos (Ahmed et al., 2023).

En el caso de Cuba, el monitoreo y análisis de trazas se ha vuelto una prioridad creciente a medida que el país avanza en su proceso de informatización de la sociedad. Con la adopción de nuevas tecnologías y la digitalización de los servicios públicos, la necesidad de implementar soluciones efectivas para monitorear los sistemas informáticos es más importante que nunca. A pesar de los desafíos tecnológicos y de conectividad, Cuba ha logrado avances significativos en el fortalecimiento de su infraestructura tecnológica, priorizando la seguridad y el desempeño de sus sistemas (Álvarez & Andrés, 2023).

La Fiscalía Provincial de Mayabeque, fundada en el año 2010, tiene como objetivo velar por el cumplimiento de la Constitución, las leyes y demás disposiciones legales, tanto de los organismos del Estado como de los ciudadanos. Su misión es ejercer el control de la investigación penal y la acción penal pública en representación del Estado, asegurando el estricto cumplimiento normativo, protegiendo los datos y la información. Esto implica un compromiso con la seguridad y la privacidad de la información manejada, todo lo anterior garantiza no solo la transparencia en sus funciones, sino también el respeto a los derechos de las personas.

En la Fiscalía Provincial de Mayabeque se evidenció una grave deficiencia en el monitoreo de trazas. Uno de los hallazgos más preocupantes fue la falta de un sistema efectivo para rastrear y documentar las trazas de información, lo que afecta directamente la capacidad de la Fiscalía para detectar anomalías y fallos recurrentes en sus sistemas informáticos, esto pone en riesgo la eficiencia de los servicios que ofrece.

A partir de lo antes expuesto se plantea el siguiente problema de investigación: ¿Cómo contribuir al mejoramiento del monitoreo y análisis de trazas en la Fiscalía Provincial de Mayabeque?

Para dar solución a dicho problema, se tiene como objetivo general: implementar una herramienta para el monitoreo y análisis de trazas en la Fiscalía Provincial de Mayabeque con el fin de detectar anomalías.

Materiales y métodos

Para seleccionar la herramienta adecuada para el monitoreo y análisis de trazas, se realizó una búsqueda exhaustiva de soluciones tecnológicas reconocidas por su capacidad de análisis avanzado y su eficacia en la detección de problemas. Entre las opciones evaluadas se identificaron Grafana, Prometheus y ELK Stack, todas de código abierto y ampliamente utilizadas en entornos de observabilidad y supervisión de sistemas.

Grafana es una herramienta de visualización que analiza datos en tiempo real mediante paneles interactivos y personalizables. Se integra con múltiples fuentes como Prometheus, Elasticsearch e InfluxDB y ofrece funcionalidades como alertas configurables, integración con OpenTelemetry y diseño de paneles gráficos (Leppänen, 2021).

Prometheus, por su parte, está orientada a la recopilación de métricas en forma de series temporales. Su modelo de datos multidimensional y su lenguaje de consulta PromQL permite realizar análisis detallados y generar alertas personalizadas. Aunque su visualización es limitada, se complementa de manera eficaz con Grafana (Kim et al., 2024).

ELK Stack se destaca por su capacidad para centralizar y analizar trazas de múltiples fuentes en sistemas distribuidos. Su arquitectura escalable gestiona grandes volúmenes de datos, correlaciona eventos en tiempo real y detecta patrones de comportamiento. Además, facilita la visualización detallada mediante Kibana, lo que mejora la interpretación de datos y la toma de decisiones (Gatsi et al., 2023).

Para responder a las necesidades específicas de la Fiscalía Provincial de Mayabeque, se definieron criterios clave para la selección de la herramienta: compatibilidad con los sistemas existentes, costo nulo por ser de código abierto, capacidad avanzada de análisis de trazas, eficiencia en la búsqueda de datos, facilidad de uso para personal no técnico y amplias opciones de visualización.

A continuación, se presenta una tabla comparativa (Tabla 1) que resume las características de las herramientas evaluadas:

Tabla 1. Comparación de las herramientas para monitoreo de trazas

Herramientas	Compatibilidad	Costo	Análisis de Trazas	Búsqueda de Datos	Usabilidad	Visualización
Grafana	Se integra con Windows, Linux y MacOS.	Gratuito	Limitado, depende de integración externa.	No realiza búsquedas directas.	Interfaz gráfica personalizable.	Interfaz gráfica personalizable.
Prometheus	Se integra con Windows, Linux y MacOS.	Gratuito	Buena capacidad para patrones complejos.	Consultas avanzadas.	Requiere conocimientos técnicos.	Visualización limitada, se complementa con Grafana.
ELK Stack	Se integra con Windows, Linux y MacOS.	Gratuito	Alta capacidad para detectar patrones.	Búsquedas rápidas y eficientes.	Interfaz intuitiva y flexible.	Visualización dinámica y en tiempo real.

Con base en esta comparación, se determinó que ELK Stack es la herramienta más adecuada para implementar en la Fiscalía Provincial de Mayabeque. Su versatilidad, capacidad de análisis, eficiencia en la búsqueda de datos y facilidad de uso la convierten en la solución ideal para mejorar el monitoreo de trazas.

La interfaz gráfica de Kibana permite una adopción rápida por parte del personal, mientras que la integración con Logstash y Elasticsearch garantiza una centralización efectiva de los registros. ELK Stack cumple con todos los requisitos establecidos, y ofrece una plataforma robusta para la supervisión de sistemas, la detección de anomalías y la generación de informes visuales que facilitan la toma de decisiones informadas.

Resultados y discusión

La herramienta ELK Stack fue implementada en un entorno controlado dentro de la Fiscalía Provincial de Mayabeque, con el propósito de validar su efectividad en el monitoreo y análisis de trazas. Se configuraron los componentes principales: Logstash, para la recolección y procesamiento de datos; Elasticsearch, para el almacenamiento y búsqueda eficiente; y Kibana, para la visualización interactiva de los registros.

Durante la implementación, se definieron variables de entorno específicas (Figura 1) que permitieron adaptar la herramienta a las características de la infraestructura tecnológica de la Fiscalía. Se verificó el funcionamiento de los índices generados por Elasticsearch

y se activó el servidor de Kibana para la visualización en tiempo real de los eventos registrados.

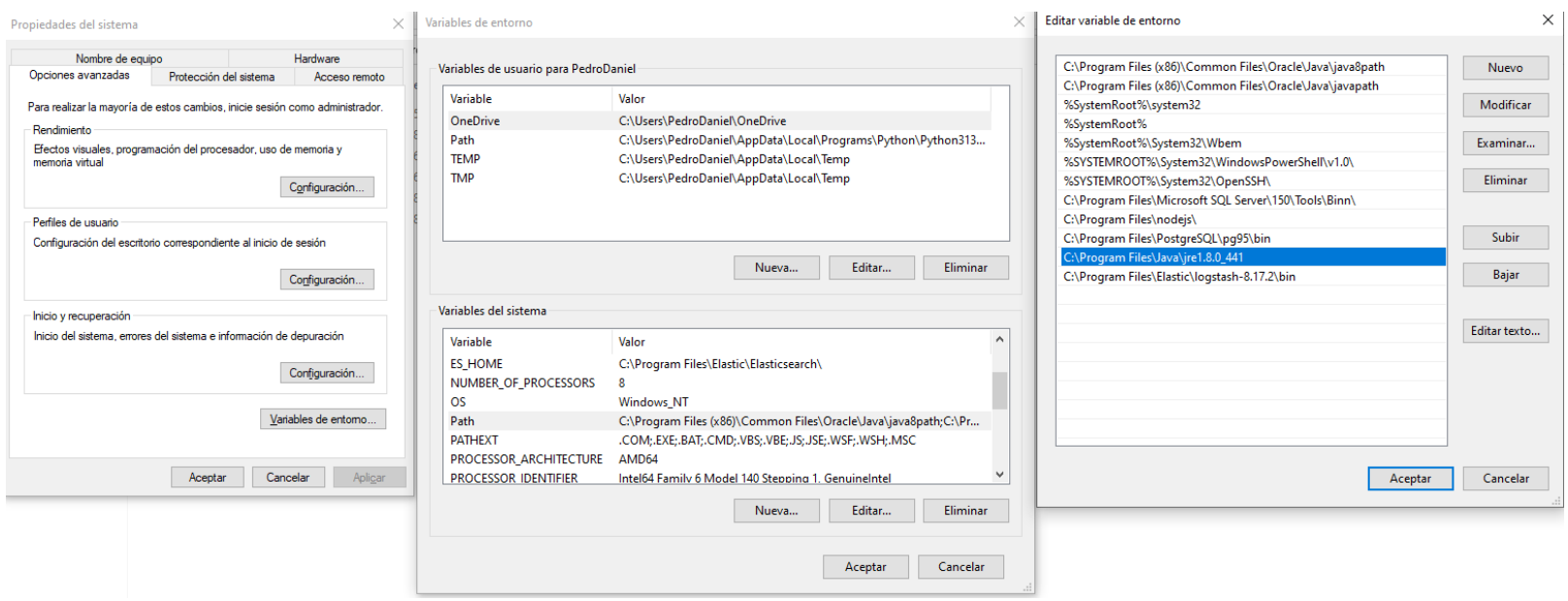

Figura 1. Variables de entorno

Una vez completada la configuración, se procedió a la validación funcional de la herramienta. Se realizaron pruebas de detección de eventos, comprobación de alertas y análisis de trazas en distintos escenarios simulados (Figura 2). Los resultados mostraron que la herramienta fue capaz de identificar patrones anómalos, clasificar amenazas según su nivel de impacto y generar alertas oportunas ante posibles fallos (Figura 3 y Figura 4).

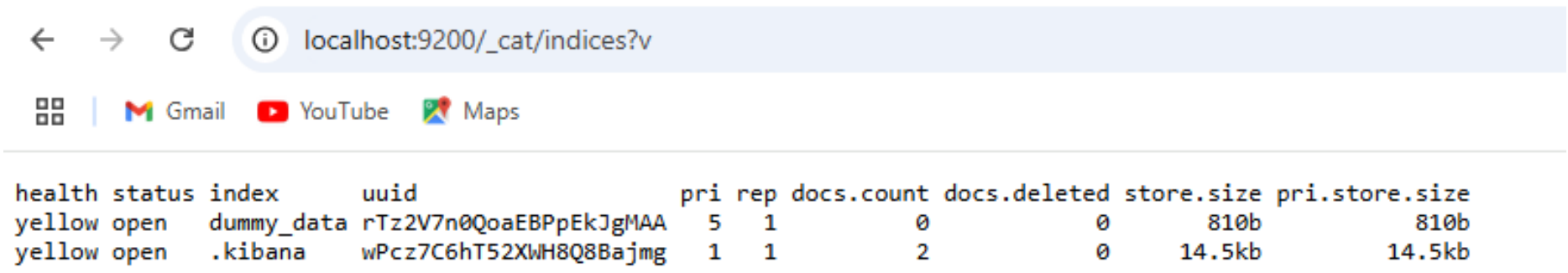

Figura 2. Comprobación de los índices

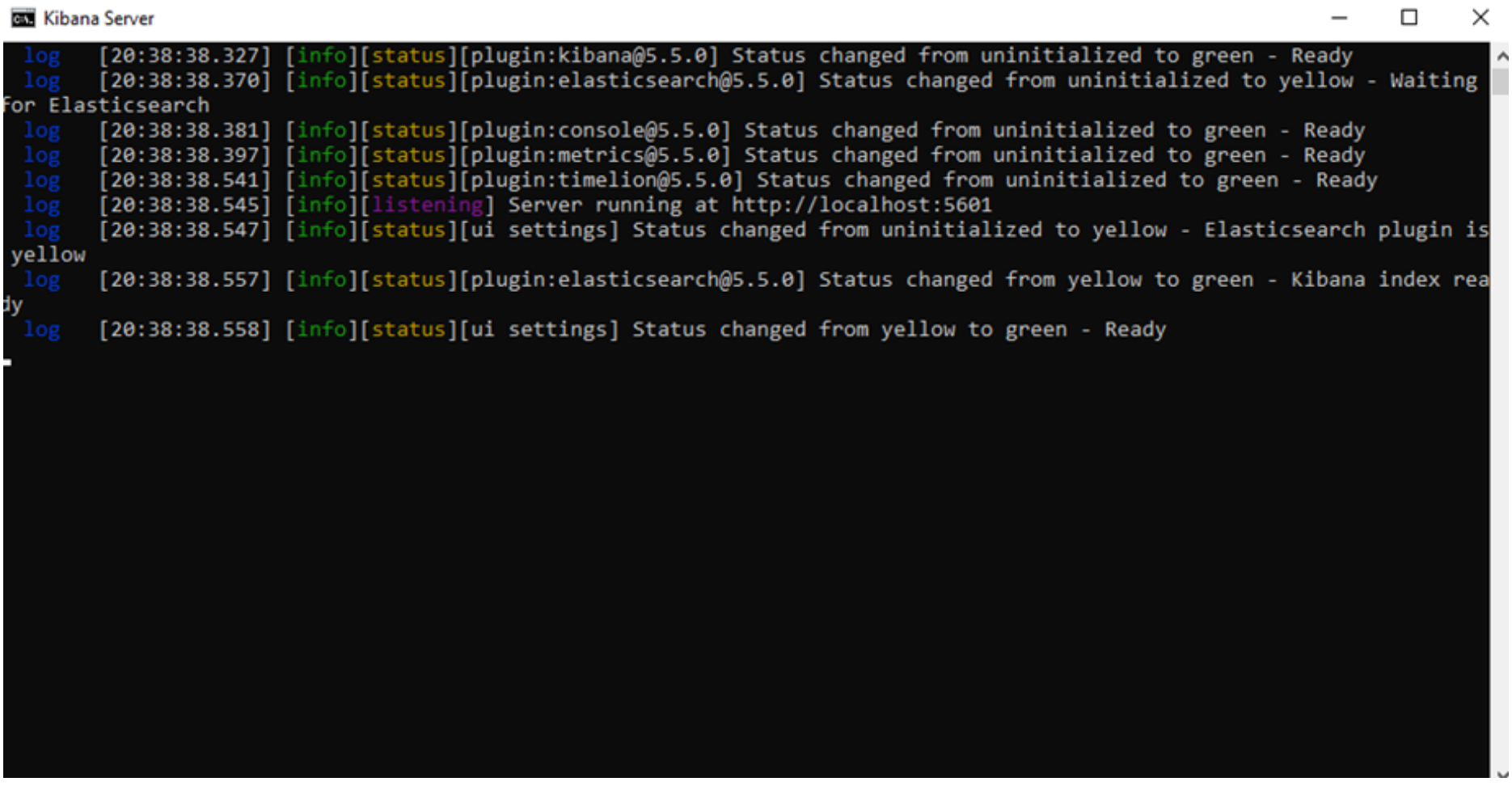

Figura 3. Servidor de Kibana activo

logstash.conf.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
input {
     file {
          path => "Escritorio/dummy_data.log"
          start_position => "beginning"

     }
}

filter {
     json {
     source => "message"
   }
}

output {
     elasticsearch {
          hosts => ["http://localhost:9200"]
          index => "dummy_data"
     }
stdout {codec => rubydebug }
}
```

Figura 4. Configuración del Logstash

La visualización de los eventos detectados permitió al personal técnico interpretar los datos de forma clara y rápida, lo anterior facilitó la toma de decisiones informadas. Además, se logró una mejora significativa en la capacidad de respuesta ante incidentes y esto contribuyó a optimizar la supervisión de los sistemas informáticos (Figura 5; Figura 6; Tabla 2; Tabla 3; Tabla 4).

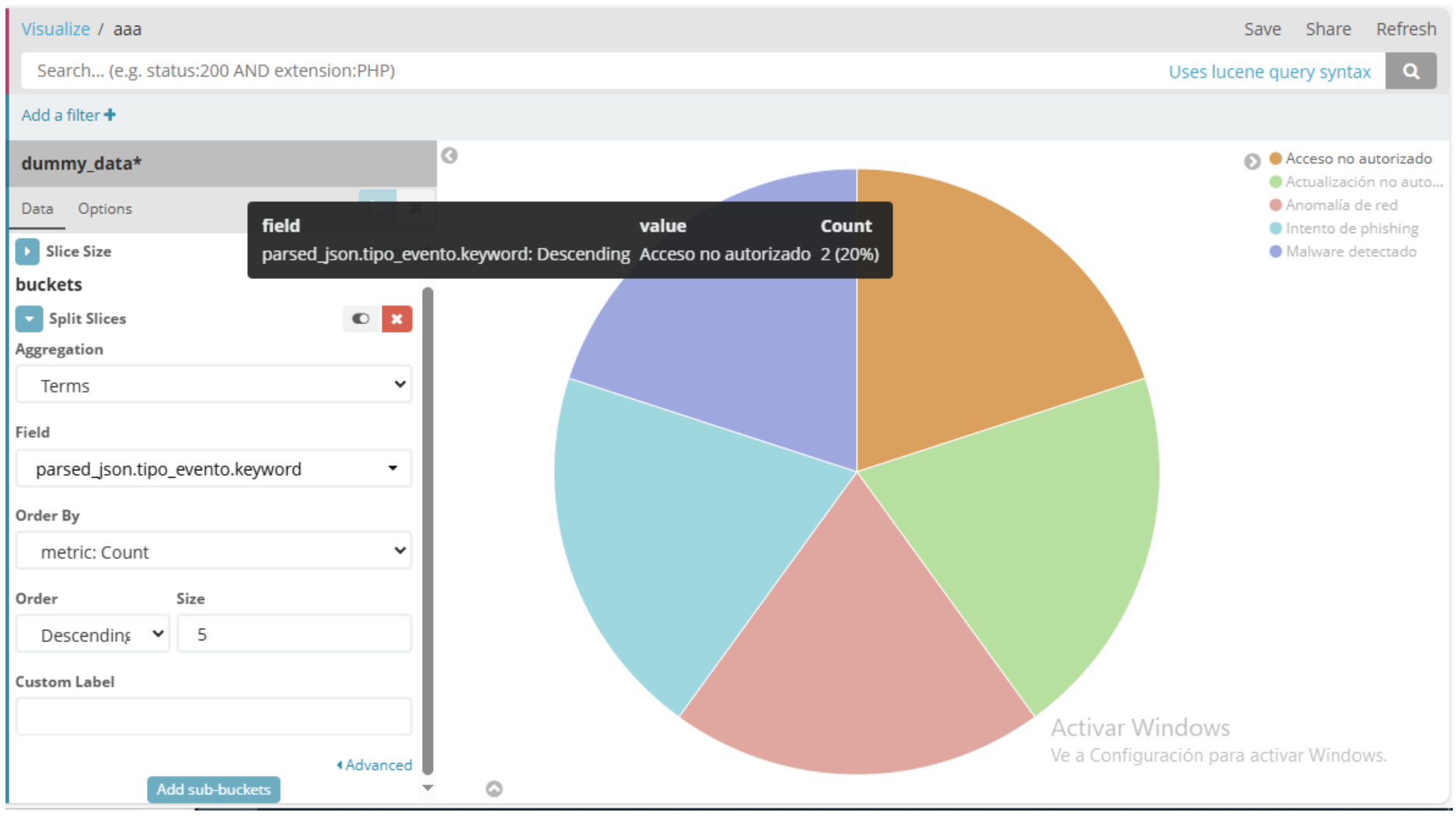

Figura 5. Eventos detectados

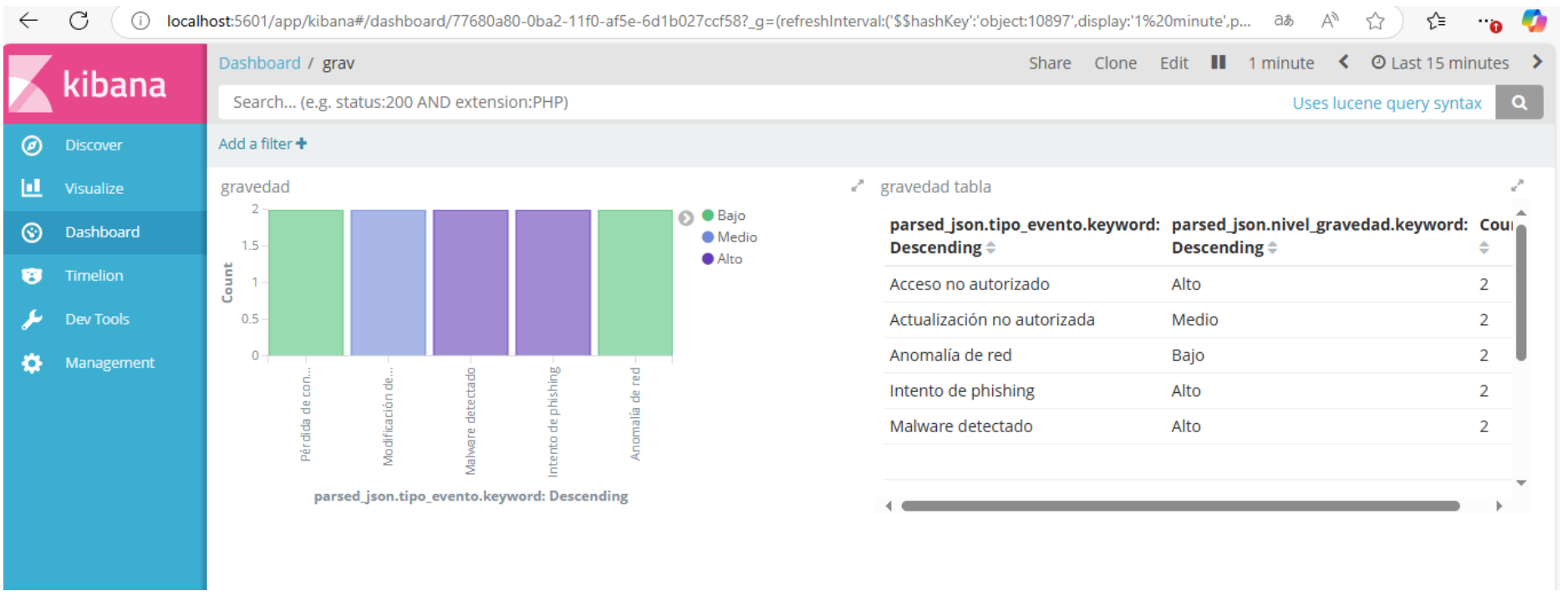

Figura 6. Clasificación de amenazas

Tabla 2. Clasificación de eventos detectados

Evento	Cantidad Detectada	Gravedad	Acción Realizada
Intentos de acceso no autorizado.	15	Crítico	Bloqueo de IP y ajustes de *firewall*.
Descargas sospechosas.	10	Medio	Restricción de descargas.
Actividades sospechosas.	5	Bajo	Monitoreo continuo.

Tabla 3. Clasificación de amenazas identificadas

Amenaza Identificada	Descripción	Clasificación de Gravedad	Acciones Recomendadas
Servicio expuesto vulnerable	Configuración deficiente que permite acceso no autorizado desde Internet.	Crítico	Actualizar configuraciones y aplicar políticas estrictas
Descargas no autorizadas	Descargas que pueden introducir *malware* al sistema sin intervención de usuarios.	Medio	Restringir descargas.
Ataques basados en ingeniería social	Aplicaciones maliciosas entregadas por correo electrónico o descargadas por usuarios.	Bajo	Implementar filtros de correo y educar a usuarios.

Tabla 4. Resumen de problemas y resoluciones

Problema	Acción Correctiva	Estado
Servicio vulnerable expuesto.	Reconfiguración y aplicación de restricciones.	Resuelto
Actividades sospechosas.	Capacitación de usuarios y monitoreo continuo.	En proceso

Los resultados obtenidos evidencian que la solución propuesta constituye una mejora sustancial respecto a las prácticas anteriores. La centralización de registros, el análisis avanzado de trazas y la visualización dinámica representan una novedad en el contexto de la Fiscalía Provincial de Mayabeque, donde no existía una herramienta con estas capacidades.

ELK Stack demostró ser superior a otras soluciones similares en términos de funcionalidad, adaptabilidad y facilidad de uso, lo que confirma el cumplimiento de los objetivos planteados en este estudio. Su implementación no solo fortaleció la seguridad informática de la institución, sino que también sentó las bases para futuras mejoras en la gestión tecnológica.

Conclusiones

La implementación de la herramienta ELK Stack en la Fiscalía Provincial de Mayabeque mejoró de forma significativa el monitoreo y análisis de trazas en sus sistemas informáticos. Esta solución tecnológica respondió de manera efectiva al problema identificado en la auditoría, al proporcionar una plataforma capaz de centralizar registros, detectar eventos relevantes y visualizar datos de forma clara y dinámica.

Se cumplió el objetivo general del estudio, al establecer una herramienta que facilita la identificación de anomalías, fortalece la seguridad de la infraestructura tecnológica y optimiza la supervisión operativa. Los resultados obtenidos evidencian que el uso de trazas con soporte visual representa una estrategia eficiente para garantizar la continuidad de los servicios institucionales.

El trabajo realizado constituye un aporte relevante en el campo de la administración de redes y seguridad informática, al demostrar que es posible implementar soluciones avanzadas con recursos accesibles y de código abierto. La experiencia adquirida en este proceso puede servir de referencia para otras instituciones públicas que enfrenten desafíos similares en la gestión de sus sistemas tecnológicos.

Como proyección futura, se recomienda continuar el desarrollo de la herramienta incorporando mecanismos de inteligencia artificial para la detección predictiva de amenazas, así como ampliar su integración con otros sistemas de monitoreo existentes. Además, se sugiere capacitar al personal técnico en el uso de estas tecnologías para garantizar su aprovechamiento pleno y sostenible.

Referencias bibliográficas

Ahmed, A., Khan, M., & Hussain, S. (2023). Trace analysis for anomaly detection in distributed systems. *Journal of Computer Networks and Security*, 15(2), 45–58.

Álvarez, J., & Andrés, R. (2023). Seguridad informática en entornos gubernamentales: desafíos y soluciones. *Revista Cubana de Tecnología*, 29(1), 12–20.

Gatsi, T., Mensah, K., & Boateng, E. (2023). Enhancing system observability using ELK Stack in large-scale infrastructures. *International Journal of Information Systems*, 18(4), 101–115.

Haykal, A., & Siswanto, R. (2020). Monitoring and threat detection in cloud-native environments. *Cybersecurity Review*, 7(3), 88–97.

Kim, J., Park, S., & Lee, H. (2024). Prometheus-based monitoring for scalable cloud applications. *Journal of Cloud Computing*, 22(1), 33–49.

Leppänen, M. (2021). Grafana dashboards for real-time system analytics. *Software Engineering Insights*, 10(2), 67–74.