Vol.10 No.3 (2026): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR.2026.e477

Evaluation of the pilot implementation of an open-source SIEM for monitoring and incident detection at the Municipal Government of Pichincha Canton.

Evaluación de la implementación piloto de un SIEM de código abierto para el monitoreo y la detección de incidentes en el GAD Municipal del cantón Pichincha.

Autores:

Zambrano-Cedeño, Gilbert Stalin
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca-Ecuador
stalinzamce@hotmail.com
https://orcid.org/0009-0002-6049-0593

Cuenca-Tapia, Juan Pablo
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca-Ecuador
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Andrade-Paredes, Roberto Omar
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca-Ecuador
roberto.andrade@ucacue.edu.ec
https://orcid.org/0000-0002-7120-281X

Fechas de recepción: 01-JUN-2026 aceptación: 09-JUL-2026 publicación: 30-SEP-2026
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La digitalización de los gobiernos locales ecuatorianos ha aumentado la dependencia de redes, servidores y sistemas administrativos que sostienen servicios públicos esenciales. En el GAD Municipal del cantón Pichincha se identifican limitaciones asociadas con la ausencia de monitoreo centralizado, red plana sin segmentación, falta de políticas de respuesta y recursos técnicos reducidos. El estudio tuvo como propósito evaluar, desde un diseño piloto, el uso de un sistema de gestión de información y eventos de seguridad de código abierto para mejorar la capacidad de monitoreo y detección temprana de incidentes. Se aplicó una investigación de tipo aplicada, con enfoque mixto y diseño cuasi experimental de preprueba y posprueba, estructurada en fases de diagnóstico, selección técnica, arquitectura piloto, validación controlada e indicadores. La matriz comparativa ubicó a OSSIM como alternativa viable por su arquitectura con agentes, servidor, indexador y tablero, además de su relación con MITRE ATT&CK. Los resultados preliminares del diseño muestran una ruta de implementación y validación medible mediante cobertura de activos, fuentes de log, tasa de detección, falsos positivos, tiempo medio de detección y tiempo medio de triaje inicial. Se concluye que el fortalecimiento no debe asumirse antes de la medición, ya que requiere validación técnica, autorización institucional y seguimiento posterior.

Palabras clave: Ciberseguridad; código abierto; gobierno local; monitoreo; SIEM.

Abstract

The digitalization of Ecuadorian local governments has increased their dependence on networks, servers, and administrative systems that support essential public services. In the Municipal GAD of Pichincha canton, limitations were identified related to the absence of centralized monitoring, a flat network without segmentation, a lack of response policies, and limited technical resources. The purpose of this study was to evaluate, through a pilot design, the use of an open-source Security Information and Event Management system to improve monitoring capacity and early incident detection. Applied research was conducted with a mixed approach and a quasi-experimental pretest-posttest design, structured into phases of diagnosis, technical selection, pilot architecture, controlled validation, and indicators. The comparative matrix identified OSSIM as a viable alternative due to its architecture with agents, server, indexer, and dashboard, as well as its relationship with MITRE ATT&CK. The preliminary design results show a measurable implementation and validation path through asset coverage, log sources, detection rate, false positives, mean time to detection, and mean initial triage time. It is concluded that strengthening should not be assumed before measurement, since it requires technical validation, institutional authorization, and subsequent monitoring.

Keywords: Cybersecurity; local government; monitoring; open source; SIEM.

Introducción

La digitalización del sector público ha transformado la forma de prestar servicios, gestionar información y atender a la ciudadanía por parte de los municipios, pero también ha ampliado la superficie de exposición a amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información que gestionan. En este marco, la Estrategia Nacional de Ciberseguridad del Ecuador plantea la importancia de fortalecer capacidades institucionales para proteger la información pública e implementar respuestas determinantes ante los riesgos digitales (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Los Gobiernos Autónomos Descentralizados presentan particularidades ante esta situación. Muchas entidades locales tienen un presupuesto escaso, equipamientos técnicos reducidos, infraestructuras de distinta tipología y poca documentación sobre activos, redes y procedimientos de respuesta. Estas particularidades hacen difícil la detección temprana de eventos anómalos, lo cual aumenta la probabilidad de que un incidente afecte la continuidad de los servicios municipales.

El GAD Municipal del cantón Pichincha pone de manifiesto esta situación por la ausencia de un monitoreo centralizado de la red, la existencia de una red plana, sin segmentación adecuada, la falta de políticas de respuesta ante incidentes y las restricciones presupuestarias para adquirir soluciones comerciales. Esta situación requiere de una alternativa técnica acorde con recursos limitados, pero que, a la vez, pueda trabajarse con criterios de evaluación verificables y no solo con afirmaciones generales de mejora.

Los sistemas para la gestión de la información y eventos de seguridad, conocidos como SIEM, permiten recopilar, centralizar, correlacionar y analizar logs que provienen de servidores, estaciones de trabajo, dispositivos de red y servicios críticos, lo cual resulta útil para detectar patrones anómalos y generar alertas que permitan al equipo técnico iniciar una respuesta oportuna (González et al., 2021).

No obstante, el rendimiento de un SIEM depende del nivel de calidad de los logs, de las reglas que se hayan configurado, de la capacidad en la cobertura del activo y de la medición de esos resultados (Kent y Souppaya, 2006). La utilización de plataformas de código abierto disminuye las barreras que en torno a las licencias de uso puede tener y resulta una opción válida para las instituciones públicas que no cuentan con suficientes recursos. Wazuh, Graylog, OSSIM y ELK Stack se disponen con diferentes alcances en la recolección, el análisis, la visualización y la correlación. Wazuh (2026) está compuesto por agente, interfaz de servidor, indexador y tablero, lo que permite facilitar la recolección de datos desde endpoints y su procesamiento y análisis centralizado, así como su integración MITRE ATT&CK para relacionar alertas e informar acerca de aquellas tácticas y técnicas de los adversarios. La intención es comprobar en qué medida un piloto de SIEM de código abierto

puede mejorar la capacidad de monitoreo y detección temprana de incidentes en la infraestructura crítica del GAD Municipal del cantón de Pichincha, a partir de cobertura del activo, tasa de detección, tasa de falsos-positivos y el tiempo medio en la detección.

La pregunta que da sentido al estudio es la siguiente: ¿en qué medida la implementación piloto de un SIEM de código abierto mejora la capacidad de monitoreo y detección temprana de incidentes en la infraestructura crítica del GAD Municipal del cantón Pichincha? A partir de ella se formula como hipótesis de trabajo que un piloto de SIEM de código abierto, configurado con fuentes de logs críticas y escenarios alineados a MITRE ATT&CK, puede aumentar la visibilidad técnica y reducir el tiempo de detección inicial, siempre y cuando se valide con métricas objetivas y con autorización institucional.

Material y métodos

El estudio fue de tipo aplicado, pues se orientó a la resolución de una situación problema concreta, relacionada con la necesidad de monitoreo y detección de incidentes en una determinada entidad pública local. En lo que respecta al tipo de orientación del estudio, se trató de un estudio mixto con predominancia cuantitativa, en la medida en que la evaluación se apoyó fundamentalmente en indicadores técnicos como la cobertura, detección, falsos positivos y tiempos de respuesta, mientras que el componente cualitativo incluyó entrevistas al personal de tecnologías de la información orientadas a la determinación de restricciones operativas, necesidades de soporte y condiciones de adopción de la herramienta. En cuanto al diseño, por la consideración de una medida inicial del estado de la situación tecnológica y una segunda medida posterior asociada con la implementación piloto del SIEM, fue un diseño de tipo cuasi experimental.

La unidad de análisis fue la infraestructura tecnológica crítica del GAD Municipal del cantón Pichincha. La línea base facilitó identificar la situación inicial de los activos, de las fuentes de log, de los procedimientos de respuesta y de la visibilidad sobre eventos de seguridad. La medición posterior estuvo ligada a la configuración de OSSIM, a la integración de fuentes de datos, a la recepción de eventos y a la validación mediante situaciones controladas. Esta organización permitió contrastar el punto inicial con la situación esperada tras el piloto, pero sin hacer ningún tipo de asunción sobre los beneficios que se obtendrían sin medición.

La población técnica estuvo compuesta por servidores, estaciones de trabajo, dispositivos de red, servicios administrativos y personal del área de tecnologías de la información. La muestra fue no probabilística por conveniencia y estuvo centrada en los activos que tienen mayor relación con la continuidad institucional. Entre los activos que se consideraron están el servidor de correo institucional Zextras Carbonio sobre CentOS 7, el servidor de aplicaciones DELL PowerEdge T330 con Windows Server, el servidor de base de datos, SQL Server y PostgreSQL, el router MikroTik CRS326-24G-2S+, el switch Ruijie NBS3200-24GT4XS-P, puntos de acceso inalámbrico, estaciones de trabajo y el servidor OSSIM para

monitoreo. La investigación se desarrolla en cinco fases. La primera fase corresponde al diagnóstico, mediante inventario de activos críticos, revisión de arquitectura, entrevistas al personal técnico, revisión de documentos y línea base con el NIST CSF 2.0. Este marco organiza la gestión del riesgo a partir de las funciones Govern, Identify, Protect, Detect, Respond y Recover, lo que permite ubicar las brechas del GAD en gestión, identificación, protección, detección, respuesta y recuperación (National Institute of Standards and Technology, 2024). La revisión de documentos consideró normas de control interno, la política de tratamiento de datos del GAD, el portal institucional, la documentación técnica de OSSIM, OSSEC, Syslog, NIST CSF 2.0 y MITRE ATT&CK.

La fase dos fue la selección y justificación de la herramienta. Se tienen en cuenta criterios técnicos, económicos y funcionales como costos totales, facilidad de despliegue, compatibilidad con Windows y Linux, integración con Syslog o firewall, dashboards, relación con MITRE ATT&CK, soporte de la comunidad y requisitos de hardware. OSSIM ha sido considerado viable al ser open source, al ofrecer la posibilidad de centralizar eventos, integrarse con OSSEC, Syslog y DataSource Plugins, y ser apropiado para una institución pública con limitaciones económicas.

La fase tres es la arquitectura piloto de OSSIM. Se ha utilizado OSSIM como un servidor dedicado para recibir eventos procedentes de los diferentes dispositivos y sistemas. La arquitectura consideró la integración del router MikroTik mediante Syslog UDP puerto 514, el switch Ruijie mediante Syslog, los servidores Linux mediante rsyslog o Syslog, los servidores Windows mediante OSSEC Agent Manager o eventos de Windows, así como el servicio crítico Zextras Carbonio Server. Este modelo de arquitectura, entonces, permite pasar de una revisión dispersa de eventos a una supervisión centralizada.

La cuarta fase fue la validación técnica. Se generaron escenarios controlados y defensivos alineados a MITRE ATT&CK, sin ejecutar ataques reales en servicios productivos. Las pruebas se orientaron a comprobar que OSSIM recibía eventos, generaba alertas, clasificaba riesgos y permitía dar inicio al análisis técnico del incidente. Cada prueba debía documentar la fecha, hora, activo implicado, fuente de log, tipo de alerta, tiempo de detección, responsable de la revisión y la acción emprendida.

La quinta fase fue la medición de desempeño. Los indicadores elegidos fueron el porcentaje de activos críticos integrados, el número de fuentes de log incorporadas, la tasa de detección por escenario, la tasa de falsos positivos, el tiempo medio de detección, el tiempo medio de triaje inicial y la relación entre alertas útiles y ruido; los cuales fueron capaces de establecer una correlación entre una línea base anterior, caracterizada por logs dispersos y no centralizados, y una posterior en la que OSSIM centraliza eventos provenientes de Syslog, OSSEC, MikroTik, switch, Linux, Windows y servidor de correo.

Tabla 1

Operacionalización metodológica del piloto SIEM

Fase	Propósito	Instrumentos	Producto verificable
Diagnóstico	Identificar las brechas de monitoreo, activos críticos, red, políticas y respuesta ante incidentes en el GAD Municipal del cantón Pichincha.	Inventario de activos críticos, revisión documental, entrevistas al personal técnico y línea base NIST CSF 2.0.	Mapa de activos críticos, brechas iniciales y nivel de visibilidad antes del piloto.
Selección	Comparar herramientas SIEM de código abierto según criterios técnicos, económicos y operativos.	Matriz comparativa de costo total, despliegue, compatibilidad Windows/Linux, integración Syslog/firewall, dashboards, MITRE ATT&CK, soporte comunitario y hardware.	Justificación técnica de la herramienta seleccionada para el piloto.
Arquitectura piloto	Definir los componentes técnicos, fuentes de log y activos que serán incorporados al monitoreo.	Diagrama lógico, lista de fuentes de log, servidor SIEM, Syslog, agentes OSSEC, plugins y activos críticos.	Diseño piloto con servidor SIEM, fuentes Syslog, agentes, activos registrados, dashboards y alertas.
Validación	Probar la capacidad de detección de la herramienta mediante escenarios controlados y defensivos.	Casos de uso alineados a MITRE ATT&CK, registros de eventos, alertas, capturas y bitácora técnica.	Evidencia de eventos detectados, reglas activadas, alertas generadas y respuesta inicial del equipo TIC.
Medición	Comparar la situación inicial y la situación esperada después del piloto.	Indicadores de cobertura, fuentes de log, tasa de detección, falsos positivos, tiempo medio de detección, triaje inicial y alertas útiles.	Tabla de desempeño, línea base, metas iniciales y discusión de limitaciones.

Resultados

El diagnóstico técnico fue capaz de identificar los activos críticos que soportan la operación institucional del GAD Municipal del cantón Pichincha, que se concretan en el servidor de correo institucional, el servidor de aplicaciones, el servidor de base de datos, el router de salida a Internet, el switch principal, los puntos de acceso inalámbrico, las estaciones de trabajo y el servidor OSSIM.

Esta identificación permitió priorizar los componentes a incorporar al monitoreo, conforme a la relación con la comunicación institucional, los sistemas administrativos, así como con la información financiera, tributaria, catastral y ciudadana.

La línea base organizada con NIST CSF 2.0 identificó las principales brechas en las funciones Govern, Identify, Protect, Detect, Respond y Recover, las cuales son las siguientes: en Govern, se evidenció la necesidad de disponer de lineamientos formales para gestión de riesgos, revisión de roles, monitoreo y respuesta. En Identify se recogió el inventario de servidores, router, switch, puntos de acceso, bases de datos y endpoints, aunque este inventario no se encontraba centralizado en alguna herramienta de eventos. En Protect se identificaron debilidades en segmentación, reglas de firewall y control de acceso, y en Detect se dio cuenta de la ausencia de monitoreo centralizado en tiempo real. Por último, Respond demostró una respuesta predominantemente reactiva y la ausencia de tiempos definidos para detección, triaje o escalamiento. En Recover se ha considerado la necesidad de llevar a cabo la documentación de los procedimientos de recuperación, respaldos, restauraciones y lecciones aprendidas.

Tabla 2

Matriz comparativa ponderada para selección de SIEM de código abierto

Criterio	Peso	Wazuh	Graylog	OSSIM	ELK Stack
MITRE ATT&CK	20 %	5	3	4	4
Despliegue	15 %	4	4	5	3
Requisitos de hardware	15 %	4	4	4	3
Costo total / costo operativo	10 %	5	4	5	3
Windows/Linux	10 %	5	3	4	4
Syslog/firewall	10 %	4	5	5	4
Tableros	10 %	4	4	5	5
Soporte comunitario / documentación	10 %	4	4	4	5
Puntaje ponderado total	100 %	87/100	76/100	88/100	76/100
Resultado para el piloto		Alternativa potente por sus agentes, documentación y relación con MITRE ATT&CK	Alternativa aceptable para la gestión de logs.	Seleccionado por su equilibrio técnico, operativo y económico para el piloto municipal.	Alternativa potente para analítica avanzada, pero con una curva técnica más pronunciada.

Nota. La matriz no presenta a OSSIM como una solución ideal, sino como una alternativa técnicamente viable para un piloto municipal. Su mayor fortaleza es la centralización de logs, la

integración con Syslog y OSSEC, el bajo costo de licencia y la posibilidad de sacar provecho de infraestructuras existentes.

La decisión de escoger OSSIM fue argumentada por ser de código abierto y por poder integrar múltiples funciones de seguridad en la misma plataforma. Esta herramienta le concede al usuario la posibilidad de gestionar eventos, correlacionar alertas, centralizar logs, integrar agentes OSSEC, activar DataSource Plugins y recibir eventos mediante Syslog. Esta función era relevante para el GAD Municipal del cantón Pichincha, en virtud de sus restricciones presupuestarias, a la vez que tenía la necesidad de reutilizar infraestructura existente.

Tabla 3
Matriz de justificación técnica de OSSIM para el piloto

Criterio	**Resultado en OSSIM**	**Relación con el piloto**
Costo total / costo operativo	OSSIM no genera costo de licenciamiento comercial, aunque requiere infraestructura, horas técnicas, soporte, capacitación y mantenimiento.	Permite implementar una solución SIEM en una institución con presupuesto limitado, sin asumir que el costo total es cero.
Facilidad de despliegue	Se instaló como servidor dedicado con interfaz web, gestión de activos, plugins y pruebas de recepción de eventos.	Facilita la centralización de eventos, aunque requiere planificación, configuración de red y capacitación técnica.
Compatibilidad Windows/Linux	Permite integrar Windows mediante OSSEC Agent Manager o eventos de Windows, y Linux mediante Syslog, rsyslog u OSSEC.	Se ajusta a la infraestructura mixta del GAD, que combina servidores Windows, Linux, correo institucional y endpoints.
Integración Syslog/firewall	Recibe eventos mediante Syslog UDP puerto 514 desde MikroTik, switch Ruijie, Linux y otros dispositivos.	Permite monitorear el perímetro, eventos de red, errores, advertencias, DHCP, autenticación y cambios de configuración.
Dashboards y visualización	Dispone de vistas para eventos de seguridad, activos, agentes, plugins, alarmas, correlación y reportes.	Permite pasar de una revisión manual y dispersa a una supervisión centralizada.
Relación con MITRE ATT&CK	Sus eventos, reglas de correlación, OSSEC, Syslog, IDS y DataSource Plugins permiten relacionar eventos con tácticas y técnicas adversarias.	Ayuda a interpretar eventos técnicos como comportamientos de ataque, aunque no siempre exista un mapeo nativo completo.

Soporte comunitario / documentación	Cuenta con apoyo de comunidades y componentes asociados como OSSEC, OpenVAS, Suricata, Snort y Syslog.	Reduce dependencia de proveedores comerciales y facilita la continuidad del aprendizaje técnico.
Requisitos de hardware	Se utilizó un servidor con Intel Core i7 11700K, 32 GB de RAM, 1 TB SSD y conectividad Gigabit.	Resulta adecuado para un piloto, aunque se recomienda ampliar almacenamiento si aumenta el volumen de logs.

La arquitectura del piloto fue concebida como una implementación incremental y no como un despliegue institucional completo, de forma que se pudiera ajustar a las restricciones presupuestarias y disminuir el riesgo operativo. OSSIM fue instalado como servidor dedicado para centralizar los eventos de seguridad que provenían de fuentes críticas de la red municipal. El router MikroTik CRS326-24G-2S+, el switch Ruijie NBS3200-24GT4XS-P, los servidores Linux, los servidores Windows, el servidor de correo Zextras Carbonio y los endpoints priorizados fueron considerados fuentes de log para el seguimiento.

La integración con Syslog fue un resultado técnico significativo, porque permitió que dispositivos de red y servidores enviaran registros a OSSIM para su análisis y correlación. La activación del plugin Syslog y la recepción mediante el puerto UDP 514 permitieron incorporar eventos del router MikroTik, el switch Ruijie, servidores Linux y el servidor de correo. La adopción del router perimetral cumple un papel importante, dado que representa el punto de salida hacia Internet y a la vez permite observar tráfico sospechoso, cambios de configuración, intentos de acceso y sucesos relacionados con el perímetro.

OSSIM también posibilitó operar con datos provenientes de Windows y Linux. En Windows se propuso el uso de OSSEC Agent Manager para enviar eventos hasta OSSIM. En Linux se propuso el envío de logs utilizando Syslog o rsyslog hasta la IP del servidor OSSIM. La compatibilidad fue importante porque la infraestructura del GAD consiste en servidores Windows, servidores Linux, correo institucional, bases de datos y terminales administrativos.

El modo de validar se definió a partir de casos de uso controlados y defensivos, sin perjudicar la operación institucional. No era suficiente con observar eventos aislados, pues había que preservar capturas de pantalla, logs de OSSIM, fecha y hora de cada evento, activo involucrado y conclusión técnica. Esta metodología, acorde a la estructura de los escenarios controlados, ha dejado constancia de que la herramienta recibía los eventos, generaba alertas, clasificaba los riesgos y apoyaba con trazabilidad el análisis inicial del incidente.

Tabla 4

Escenarios controlados de validación técnica

Escenario	Técnica MITRE ATT&CK relacionada	Fuente de log	Procedimiento controlado de prueba	Evidencia esperada en OSSIM	Indicador asociado
Intentos de fuerza bruta	Credential Access / T1110 - Brute Force	Windows, Linux, MikroTik, OSSEC y Syslog.	Generar, en un entorno controlado, varios intentos fallidos de autenticación con una cuenta de prueba autorizada.	Eventos de autenticación fallida y alerta por repetición anómala de intentos.	Tasa de detección, falsos positivos y tiempo medio de detección.
Ejecución sospechosa en PowerShell	Execution / T1059.001 - PowerShell	Windows Event Logs y OSSEC.	Ejecutar comandos administrativos benignos y autorizados para verificar si quedan registrados como actividad inusual.	Evento de ejecución inusual o uso no habitual de consola administrativa.	Tasa de detección y tiempo medio de detección.
Persistencia en endpoint	Persistence / T1547 - Boot or Logon Autostart Execution	Windows, Linux y OSSEC.	Verificar cambios controlados en servicios, tareas programadas o elementos de arranque dentro de un entorno de prueba.	Evento de cambio en configuración, servicio persistente o mecanismo de arranque.	Tasa de detección y evidencia de integridad del endpoint.
Elevación de privilegios	Privilege Escalation / T1068 - Exploitation for Privilege Escalation	Windows Server, Linux y OSSEC.	Validar eventos de cambio de rol, asignación de permisos o uso de cuentas administrativas en un ambiente autorizado.	Evento de cambio de privilegios, asignación de rol o alerta de riesgo alto.	Tasa de detección, falsos positivos y tiempo medio de triaje inicial.
Cambios no autorizados en archivos	Impact / T1565 - Data Manipulation	OSSEC HIDS y módulo de integridad de archivos.	Modificar un archivo de prueba monitoreado, sin alterar	Evento de modificación de archivo y trazabilidad	Tasa de detección y relación entre alertas útiles y ruido.

			archivos reales de producción.	del cambio realizado.	
Evento anómalo de red	Discovery / T1046 - Network Service Discovery	MikroTik, switch Ruijie, IDS/Syslog y firewall.	Detectar variaciones inusuales de tráfico o escaneo controlado desde un host autorizado hacia un segmento de prueba.	Evento de tráfico sospechoso, escaneo o anomalía presentada en el dashboard.	Tasa de detección, tiempo medio de detección y falsos positivos.

Nota. Las pruebas deben ejecutarse únicamente en un entorno autorizado y controlado.

Los indicadores fueron definidos para evaluar la capacidad operativa y no únicamente el número de alertas. Un número elevado de eventos no se traduce en mejor seguridad, ya que podría también estar ligado a un aumento del ruido y saturar con ello a los técnicos en su día a día. Por ello, la relación entre alertas útiles y falsos positivos es tan importante como la tasa de detección. La matriz de indicadores permite comparar la línea base previa a OSSIM con la posterior al piloto, dado que se espera disponer de activos registrados, fuentes de log integradas, detección automática de eventos, tiempos medidos y clasificación de alertas en útiles, duplicadas o irrelevantes.

Tabla 5

Indicadores para comparar la línea base y el piloto

Indicador	**Fórmula o criterio**	**Línea base**	**Meta / umbral**	**Fuente de datos**	**Unidad de medida**	**Lectura esperada**
Cobertura de activos críticos	Activos críticos integrados / total de activos críticos x 100.	No existía registro centralizado de activos críticos en una herramienta SIEM.	Integrar el 80 % o más de los activos críticos identificados.	Inventario de activos y consola OSSIM.	Porcentaje.	Mayor cobertura mejora la visibilidad institucional.
Fuentes de log incorporadas	Conteo de fuentes activas enviando eventos al SIEM.	Los logs se encontraban dispersos o no centralizados.	Incorporar mínimo cinco fuentes: MikroTik, switch, Windows, Linux y	OSSIM, Data Sources, Syslog y agentes OSSEC.	Número absoluto.	Mayor diversidad de fuentes permite mejor correlación de eventos.

			servidor de correo.			
Tasa de detección por escenario	Escenarios detectados / escenarios probados x 100.	La detección era manual, tardía o no documenta da.	Detectar el 80 % o más de los escenarios controlados .	Matriz de validación, alertas OSSIM y bitácora de pruebas.	Porcentaje.	Mide la capacidad de detección por caso de uso.
Tasa de falsos positivos	Alertas no relevantes / total de alertas x 100.	No se contaba con medición previa de falsos positivos.	Mantener una tasa menor al 20 % después del ajuste inicial de reglas.	Revisión de alertas y clasificació n técnica.	Porcentaje.	Permite ajustar reglas y reducir ruido operativo.
Tiempo medio de detección	Promedio entre la generación del evento y la alerta en OSSIM.	Indetermin ado por ausencia de monitoreo centralizad o.	Lograr un tiempo medio menor a 5 minutos.	Logs, timestamps y dashboard OSSIM.	Minutos.	Debe reducirse frente a la detección manual o tardía.
Tiempo medio de triaje inicial	Promedio entre la alerta y la primera revisión del analista.	No documenta do antes del piloto.	Lograr una primera revisión en menos de 30 minutos.	Registro de atención, bitácora de triaje y entrevistas al personal TIC.	Minutos.	Mide la capacidad operativa del equipo técnico.
Alertas útiles vs. ruido	Alertas útiles / total de alertas x 100.	No existía clasificació n sistemática de alertas útiles, duplicadas o irrelevantes .	Alcanzar más del 60 % de alertas útiles después del ajuste inicial.	Clasificaci ón manual de eventos y dashboard OSSIM.	Porcentaje.	Evalúa la calidad del alertamient o y evita saturación del personal técnico.

Desde este punto de vista, la literatura y la documentación técnica analizadas indican que la efectividad de un SIEM open source se encuentra condicionada por la calidad de las fuentes de logs, la idoneidad de las reglas, la capacidad operativa del personal que lo implementa y la vigilancia sistemática de los indicadores. Así, la toma de decisiones tecnológicas puede interpretarse como una condición necesaria, pero no suficiente, para la mejora de la visibilidad institucional y para la detección de incidentes de seguridad. ENISA, responsable del desarrollo del informe de threat landscape, establece que este informe debería ayudar a

la propuesta de medidas de mitigación, lo que refuerza la postura de que se necesita un seguimiento que procure evidencias y que no sea meramente una adquisición oportunista de tecnología. En este contexto, la adopción de OSSIM tiene sentido porque permite vincular el seguimiento de la red municipal con activos críticos, fuentes de log, escenarios de validación y métricas de desempeño.

Como limitación del estudio, se encuentra que el piloto debe estar validado, debe contar con autorización institucional, activos disponibles y un entorno de prueba que no comprometa operaciones reales. Por esta razón, en el trabajo no se puede señalar que se da una disminución definitiva de incidentes ni una mejora total de los tiempos de respuesta. Sin embargo, sí supone poder mostrar una ruta técnica de implementación, capaz de alcanzar la centralización y evaluación, fundamentada en una integración de fuentes críticas y en la determinación de indicadores verificables.

Conclusiones

La metodología determina secuencias de evaluación en el diagnóstico inicial, en la selección de la herramienta, en la arquitectura piloto, en la validación y en la medición, permitiendo que las brechas iniciales se relacionen con el modelo de seguridad NIST CSF 2.0 y, a la par, que los escenarios de prueba lo hagan con MITRE ATT&CK, sin proclamar resultados antes de la verificación.

OSSIM se defiende como herramienta piloto; la razón se encuentra en su carácter open source, en su fácil integración con Syslog, OSSEC, MikroTik, servidores Windows/Linux, DataSource Plugins y dashboards de eventos. Esto proviene de la posibilidad de utilizarla según la disponibilidad institucional, de reutilizar infraestructura existente, de resolver la necesidad de centralizar logs en un entorno municipal y de ajustarse a las restricciones presupuestarias.

El refuerzo de la ciberseguridad no se proclama como resultado final antes de la verificación. A la par, la conclusión correcta es que el piloto propuesto da acceso a la mejora de la visibilidad y la detección, siempre que sea ejecutado en un entorno institucional, en condiciones controladas, con fuentes de log suficientes, con reglas ajustadas y medición de indicadores.

El artículo deja como contribución aplicada una ruta de validación repetible por parte de una institución municipal con restricciones presupuestarias. Esta ruta puede ayudar a las implementaciones futuras en otros gobiernos locales, siempre que se adapten activos, fuentes de log, escenarios de prueba y umbrales de verificación a cada contexto institucional.

Referencias bibliográficas

Center for Internet Security. (2021). *CIS Critical Security Controls Version 8.* Center for Internet Security. https://www.cisecurity.org/controls/v8

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Elastic. (2009). *Elastic Security Detection Rules*. Retrieved 2 de junio de 2026, from https://elastic.github.io/detection-rules-explorer/

Elastic. (2026). *Manage detection rules*. Retrieved 2 de junio de 2026, from https://www.elastic.co/docs/solutions/security/detect-and-alert/manage-detection-rules

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024.* ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors, 21*(14), 4759. https://doi.org/10.3390/s21144759

Graylog. (2026). *Graylog: SIEM, log management & API protection*. Retrieved 2 de junio de 2026, from https://graylog.org/

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO. https://www.iso.org/standard/27001

International Organization for Standardization. (2022). *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.* ISO. https://www.iso.org/standard/75652.html

International Organization for Standardization. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* ISO. https://www.iso.org/standard/80585.html

International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process.* ISO. https://www.iso.org/standard/78973.html

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024.* ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Política de Ciberseguridad.* Quito: Gobierno del Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Agenda de Transformación Digital del Ecuador 2022-2025.* Quito: Gobierno del Ecuador. https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2022/12/Agenda-transformacion-digital-2022-2025.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador.* Quito: Gobierno del Ecuador. https://gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

MITRE ATT&CK. (2026). *Enterprise matrix*. Retrieved 2 de junio de 2026, from https://attack.mitre.org/matrices/enterprise/

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Organización de los Estados Americanos y Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Banco Interamericano de Desarrollo. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Rahman, M., & Williams, L. (2022). An investigation of security controls and MITRE ATT&CK techniques. *arXiv*, arXiv:2211.06500. https://arxiv.org/abs/2211.06500

Rosenberg, M., Schneider, B., Scherb, C., & Asprion, P. (2023). An Adaptable Approach for Successful SIEM Adoption in Companies. *arXiv*, arXiv:2308.01065. https://arxiv.org/abs/2308.01065

Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S., & Loukas, G. (2023). SoK: The MITRE ATT&CK Framework in Research and Practice. *arXiv*, arXiv:2304.07411. https://arxiv.org/abs/2304.07411

Shen, X., Li, Z., Burleigh, G., Wang, L., & Chen, Y. (2024). Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments. *arXiv*, arXiv:2401.15878. https://arxiv.org/abs/2401.15878

SourceForge. (2026). *AlienVault OSSIM: Open Source SIEM*. Retrieved 2 de junio de 2026, from https://os-sim.sourceforge.net/

Wazuh. (2026). *Architecture*. Retrieved 2 de junio de 2026, from https://documentation.wazuh.com/current/getting-started/architecture.html

Wazuh. (2026). *MITRE ATT&CK framework*. Retrieved 2 de junio de 2026, from https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html

Wazuh. (2026). *The Open Source Security Platform*. Retrieved 2 de junio de 2026, from https://wazuh.com/

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.