Instalación del Servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4

Cruz Guachilema, Eduardo Antonio y Meza Navarrete, Bryan Esteban

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de integración curricular, previo a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

12 de febrero de 2023

CERTIFICADO DE ANÁLISIS
magister

TESIS SIEM CRUZ - MEZA

4% Similitudes

< 1% Texto entre comillas
< 1% similitudes entre comillas
0% Idioma no reconocido

Nombre del documento: TESIS SIEM CRUZ - MEZA.pdf
ID del documento: fe14c241628344d325726bd1abb4939e393ef878
Tamaño del documento original: 5,09 Mo

Depositante: RAMIRO NANA DELGADO RODRIGUEZ
Fecha de depósito: 15/3/2023
Tipo de carga: interface
fecha de fin de análisis: 15/3/2023

Número de palabras: 29.214
Número de caracteres: 204.625

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**manageengine.com.mx** | 3 pasos para configurar su solución SIEM: implementación,... https://manageengine.com.mx/log-management/3-pasos-para-configurar-la-solucion-siem	1%		Palabras idénticas : 1% (341 palabras)
2	**repositorio.pucesa.edu.ec** | Implementación de una solución "security information a... http://repositorio.pucesa.edu.ec/bitstream/123456789/3291/2/77446.pdf.txt **3 fuentes similares**	< 1%		Palabras idénticas : < 1% (243 palabras)
3	**polux.unipiloto.edu.co** http://polux.unipiloto.edu.co:8080/00003801.pdf **3 fuentes similares**	< 1%		Palabras idénticas : < 1% (188 palabras)
4	**repositorio.pucesa.edu.ec** | Repositorio PUCESA: Implementación de una solución "s... https://repositorio.pucesa.edu.ec/handle/123456789/3291	< 1%		Palabras idénticas : < 1% (151 palabras)
5	**repositorio.uisrael.edu.ec** http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf **3 fuentes similares**	< 1%		Palabras idénticas : < 1% (118 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repository.unipiloto.edu.co** | Implementación de un sistema de correlación de even... http://repository.unipiloto.edu.co/handle/20.500.12277/11530	< 1%		Palabras idénticas : < 1% (37 palabras)
2	**repositorioslatinoamericanos.uchile.cl** | Implementación de un correlacionador de ... https://repositorioslatinoamericanos.uchile.cl/handle/2250/4587419?show=full	< 1%		Palabras idénticas : < 1% (32 palabras)
3	**repositorio.uisek.edu.ec** | Repositorio de la Universidad Internacional SEK Ecuador: ... https://repositorio.uisek.edu.ec/handle/123456789/4865	< 1%		Palabras idénticas : < 1% (35 palabras)
4	**tecmanagement.org** | ITIL 4 - Las 4 Dimensiones de la Gestión de Servicio https://tecmanagement.org/itil-4-las-4-dimensiones-de-la-gestion-de-servicio/	< 1%		Palabras idénticas : < 1% (15 palabras)
5	**hdl.handle.net** | Marco para la definición y adecuación de una "service management... http://hdl.handle.net/10016/18079	< 1%		Palabras idénticas : < 1% (16 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://especare.freshdesk.com/support/home
2 http://repository.unipiloto.edu.co/handle/20.500.12277/2821
3 http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242
4 https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI7.pdf
5 https://www.cisco.com/c/es_mx/solutions/automation/what-is-network

Firmado electrónicamente por:
MARIO BERNABE RON
EGAS

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación, **"Instalación del servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4"** fue realizado por los señores Cruz Guachilema Eduardo Antonio y Meza Navarrete Bryan Esteban el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 13 de marzo de 2023

Firma:

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2023.03.14 10:41:18 -05'00'

.....

Ing. Ron Egas, Mario Bernabe Ms.C

C. C 1704229747

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Responsable de la autoría

Nosotros, **Cruz Guachilema Eduardo Antonio y Meza Navarrete Bryan Esteban**, con cédulas de ciudadanía n° 1723281794 y 1727432534, declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Instalación del servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 12 de febrero de 2023

Firma

.....

Cruz Guachilema Eduardo Antonio

C.C.: 1723281794

Firma

.....

Meza Navarrete Bryan Esteban

C.C.: 1727432534

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Autorización de publicación

Nosotros, **Cruz Guachilema Eduardo Antonio y Meza Navarrete Bryan Esteban,** con cédulas de ciudadanía n° 1723281794 y 1727432534 autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Instalación del servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 12 de febrero de 2023

Firma

.....

Cruz Guachilema Eduardo Antonio

C.C.: 1723281794

Firma

.....

Meza Navarrete Bryan Esteban

C.C.: 1727432534

Dedicatoria

Para toda mi querida familia, en especial para mis padres, Antonio y Patricia; mis abuelitas, Reneé y María de Lourdes; mis tíos Humberto y Susana; quienes me han ayudado desde la primera vez que puse un pie en la universidad, me dieron cobijo y cariño a lo largo de los años.

Eduardo Cruz

Dedico este logro a mis seres queridos que me han acompañado en este proceso, haciendo énfasis en mi padre Víctor y mi madre Yolanda, que sin ellos no habría llegado tan lejos.

Bryan Meza

Agradecimientos

En primer lugar, quiero agradecer a mi padres, Antonio y Patricia por apoyarme día tras día a lo largo de mi vida universitaria, ha sido un camino largo, pero siempre han estado a mi lado apoyándome cualquier cosa que necesite. También quiero agradecer a mis profesores, aquellos que me han demostrado lo que es ser tanto una buena persona como profesional. Por último, pero no menos importante agradecer a todos los amigos que he podido hacer a lo largo de estos años, gracias a ellos el camino fue más interesante y divertido. Bryan, Patricio, Kevin, Mishell, María José, Nicole, Alisson, David, Jordy, Daniel, Alexis, Nicolás, Mateo, Génesis. Cada persona ha puesto su grano de arena para ayudarme en la vida, crecer como persona y así poder salir adelante, por lo que, les estoy muy agradecido. Muchas gracias a todos, espero también haber aportado algo a su vida.

"Fue un buen viaje…"- E.O.

Eduardo Cruz

Quiero agradecer a Dios por siempre haberme bendecido y permitirme vivir este momento, además darme el discernimiento para abarcar y superar los retos que me he planteado en mi vida. Agradezco a mi madre, que siempre me dio su cariño y supo alentarme en las ocasiones que me sentía agotado, gracias por todas esas tasas de café que me ofreciste cuando el sueño me dominaba. Agradezco a mi padre que, a pesar de mis errores y desobediencias, nunca me dio la espalda y estuvo para mí siempre que lo necesitara, gracias por siempre buscar la manera de sacarme hacia adelante a pesar de las dificultades que vivimos. Aunque sea algo poco convencional, agradezco a mi mascota Kitty que siempre estuvo a mi lado y fue mi compañera en las desveladas por estudiar. Por último, quiero agradecer a las personas que estuvieron y a las que están aún en mi vida universitaria, gracias por formar parte de maravillosas experiencias y ayudarme a lograr lo que soy hoy, ha sido la mejor etapa de mi vida.

Bryan Meza

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

Con el creciente avance tecnológico que existe en la actualidad, las organizaciones tienen que afrontar múltiples retos. Uno de los retos que ha llamado más la atención de los expertos durante los últimos años, ha sido la ciberseguridad. Con el uso cada vez más frecuente de la tecnología, encontrarse con ciberdelincuentes ya no es algo tan extraño como lo era hace varios años. De hecho, se ha visto una mayor actividad en estos tiempos, tanto que su aumento es preocupante. Es por ello que se han implementado dispositivos de seguridad perimetral para salvaguardar la información de las personas y las organizaciones. Sin embargo, el inconveniente surge cuando cada dispositivo genera su propio *log,* alerta o alarma y no se tiene una plataforma centralizada en donde se pueda recopilar y visualizar esta información en conjunto. El área del ESPE-CERT presenta esta necesidad, por lo cual, en el presente trabajo de titulación, se planteó la instalación de un servicio de monitoreo mediante un correlacionador de eventos (SIEM), que permita satisfacer las necesidades del negocio, que no interrumpa el funcionamiento de los demás servicios y que sirva como una herramienta de apoyo para los mismos. Para conseguir esto, en primer lugar, se realizó una revisión sistemática de literatura, donde se expusieron trabajos similares; en segundo lugar, se aplicó el proceso marcado por la *Information Technology Infrastructure Library* (por sus siglas en inglés, ITIL) para gestionar de manera eficiente un servicio de tecnologías de la información (por sus siglas, TI), este desarrollo tiene las actividades: plan, diseño y transición, entrega y soporte, operación y mejora. Al pasar por cada una de ellas y llegar a la entrega y soporte, se pudo observar que el funcionamiento de SIEM Wazuh (herramienta seleccionada) cumplía con los requisitos, recopilaba la información en un nodo central y no afectaba al funcionamiento de los demás servicios del nodo. Finalmente, se desarrollaron las conclusiones y recomendaciones, teniendo en cuenta los resultados observados durante la operación y las mejoras sugeridas por el evaluador.

Palabras clave: SIEM, ITIL, correlación de eventos, eventos de seguridad, incidentes de seguridad.

Abstract

With the growing technological advance that exists today, organizations have to face multiple challenges. One of these challenges, that has attracted the most attention from experts in recently years, has been cybersecurity. With frequent use of technology, encountering cybercriminals is not strange as it was several years ago. In fact, there has been a greater activity in these times, so much so that its increase is worrying. That is why perimeter security devices have been implemented to safeguard the information of people and organizations. However, the drawback arises when each device generates its own log, alert or alarm and there is no centralized platform where this information can be recollected and viewed as a whole. The ESPE-CERT area presents this need, for which reason in this titling work, the installation of a monitoring service through an event correlator (SIEM) was proposed, which allows satisfying the needs of the business, which does not interrupt the operation of the other services and that serves as a support tool for them. To achieve this, firstly, a systematic review of the literature was carried out, in this stage, we presented similar works; Secondly, the process marked by the Information Technology Infrastructure Library (ITIL) was applied to efficiently manage an information technology (IT) service. This development has the activities: plan, design and transition, delivery and support, operation and improvement. When going through each one of these phases and arriving at the delivery and support, it was possible to observe that the operation of SIEM Wazuh (selected tool) fulfilled the requirements, collected the information in a central node and did not affect the operation of the other node services. Finally, the conclusions and recommendations were developed, taking into account the results observed during the operation stage and the improvements stage suggested by the evaluator.

Keywords: SIEM, ITIL, event correlation, security events, security incidents.

Capítulo I:

Introducción

Las organizaciones se enfrentan a múltiples retos de ciberseguridad, particularmente por los delitos cibernéticos o cibercrímenes que cada día se vuelven más habituales y están creciendo de forma exponencial. Es por ello que la información es el bien más preciado para toda organización y en el intento por gestionar cualquier incidente de seguridad informática que pueda poner en riesgo la confidencialidad, integridad y disponibilidad de esta, han surgido dispositivos de seguridad perimetral, como los IDS, IPS, Firewalls, entre otros.

Los inconvenientes se generan en el momento que se da un ataque informático, ya que cada dispositivo configurado genera sus propios logs, que también dependen de su fabricante y debido a esto, el procesamiento de estos no es tan sencilla, ya que, los mismos poseen gran tamaño y son incompatibles entre sí, razón por la cual es necesario la normalización y centralización de estos, que nos permita de una manera más fácil generar alertas y detectar ataques informáticos en tiempo real.

En el presente documento se muestra el proceso de instalación del servicio de monitoreo de amenazas mediante un SIEM, su ejecución y evaluación de resultados obtenidos en el ESPE CERT, todo este procedimiento se realizó mediante los lineamientos establecidos en ITIL V4 para realizar un trabajo bajo buenas prácticas y seguir una metodología adecuada que permita obtener una gestión del nuevo servicio efectiva.

Con la instalación del servicio de monitoreo, se ayudará a tener una plataforma de información centralizada acerca de los eventos de seguridad ocurridos en los sensores configurados a ser monitoreados por el SIEM, los administradores tendrán acceso a un conjunto de reportes en base a criterios y el monitoreo en tiempo real de estos sensores.

Planteamiento del Problema

Las amenazas de seguridad aumentan continuamente y estas se pueden originar desde diferentes fuentes internas o externas. Entre los riesgos analizados tenemos la

probabilidad de que se configuren de manera inadecuada los dispositivos y controles previstos para mitigar esos riesgos, así mismo existe la posibilidad de que ocurran falsos negativos en los controles automáticos por falta de eficacia y actualización de las salvaguardas implantadas: firewalls, IPS, IDS, DLP y otros.

El empleo de dispositivos de control parcial y semiautomático o de monitoreo supervisado, hace difícil la detección de los ataques al sistema de gestión de seguridad de la Información (SGSI) y consecuentemente la reacción oportuna y eficaz del equipo de respuesta ante incidentes informáticos.

Se identificó que en el ESPE-CERT, hace falta una herramienta que realice la recolección de eventos y permita dar una respuesta acertada con el fin de generar una reacción oportuna ante los incidentes de seguridad y así, poder minimizar los daños sin que se afecten, dañen, o amenacen las operaciones de la institución.

Justificación del Tema

Teniendo en cuenta que ESPE-CERT ofrece varios servicios a la universidad, surge la necesidad de implantar el servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) que centralice toda la información y así poder: recolectar, almacenar, gestionar y monitorear los eventos que se produzcan desde cualquier tipo de activo de información importante de la universidad por la criticidad que representa en la gestión. El objetivo de un correlacionador de eventos (SIEM), consiste en detectar las anomalías intrusivas que intentan impactar de forma negativa a los activos y facilitar a los encargados de ESPE-CERT un análisis detallado de posibles eventos anómalos que puedan afectar a estos mismos activos.

Existe la posibilidad de que accidentalmente los funcionarios configuren de manera errónea los ajustes de seguridad, esto es una preocupación que está en constante aumento y puede dejar los datos expuestos a un ataque. Para prevenir esto, las organizaciones de IT han adquirido sistemas con el fin de tener una protección sólida ante intrusiones y otras formas de ataques.

El ESPE-CERT, tiene previsto entre sus servicios el monitoreo de amenazas de seguridad de la información mediante un correlacionador de eventos y herramientas que realizan el análisis de eventos, que permiten generar alarmas e iniciar la respuesta con el fin de ofrecer una reacción oportuna ante los incidentes de seguridad y así minimizar el impacto a las operaciones de la institución.

Objetivo General

Implantar el Servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4, para la Universidad de las Fuerzas Armadas ESPE, para estar en capacidad de ampliar el servicio a otras universidades.

Objetivo Específico

- Establecer el estado del Arte
- Establecer la Estrategia del Servicio en el portafolio de servicios del ESPE-CERT, publicar el catálogo de servicios actualizado en concordancia con el Plan Operativo Anual de la ESPE.
- Realizar el Diseño del Servicio en concordancia con la comunidad establecida y las capacidades actuales del ESPE-CERT.
- Transición del servicio según ITIL V4, que consiste en implantar el nuevo servicio, de acuerdo a la comunidad objetivo, en los servidores del ESPE-CERT del DCCO.
- Operación del servicio, en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO, se dará inicio y continuidad del nuevo servicio, incorporándose al catálogo de servicios del CERT-ESPE del DCCO.
- Mejora del Servicio y resolución de las no conformidades.

Alcance

En base al proyecto de investigación en donde se va a realizar la implementación del CERT académico mediante ITIL V4, se van a ejecutar las fases respectivas de estrategia, diseño, transición, operación y mejora para realizar la instalación del servicio de monitoreo de amenazas utilizando un correlacionador de eventos (SIEM). Se realizará la definición de las competencias, alcance, comunidad de servicio y se instalará la herramienta bajo supervisión y responsabilidad del ESPE-CERT. Posteriormente, se realizará la organización del servicio y se darán inicio a las operaciones de manera progresiva en toda la ESPE, posteriormente se va a evaluar el servicio implementado para la ejecución de mejoras.

Para la implementación de este nuevo servicio, se hará uso de los recursos otorgados por el Departamento de Ciencias de la Computación (DCCO) y utilizados directamente en el ESPE-CERT. El desarrollo de este trabajo dará inicio una vez recibida la aprobación por parte del ESPE-CERT, así como de la directiva del DCCO. Cuando la implementación del proyecto haya finalizado, el ESPE-CERT contará con un SIEM funcional, el cual servirá para monitorear los eventos de seguridad ocurridos en la universidad y con esto, se pueden establecer medidas preventivas para evitar la pérdida de información sensible.

Para ampliar la propuesta al alcance del proyecto planteado, se han plateado las siguientes preguntas de investigación, donde se consideraron dos preguntas para cada uno de los objetivos específicos, esto con el fin de establecer una base para el progreso de la investigación.

Tabla 1

Objetivos y preguntas

Objetivo específico	Pregunta de investigación
Establecer el estado del Arte	¿Cómo ayudará la implementación de un SIEM en el ESPE-CERT?

Objetivo específico	Pregunta de investigación
Establecer la Estrategia del Servicio en el portafolio de servicios del ESPE-CERT, publicar el catálogo de servicios actualizado en concordancia con el Plan Operativo Anual de la ESPE.	¿Cuál es la estrategia que se va seguir para establecer un servicio de monitoreo de amenazas?
Realizar el Diseño del Servicio en concordancia con la comunidad establecida y las capacidades actuales del ESPE-CERT.	¿Cómo se planea diseñar y comprobar el correcto funcionamiento del nuevo servicio de monitoreo de amenazas?
Transición del servicio según ITIL V4, que consiste en implantar el nuevo servicio, de acuerdo a la comunidad objetivo, en los servidores del ESPE-CERT del DCCO.	¿De qué forma se realizará la implementación de servicio de monitoreo?
Operación del servicio, en conformidad con el compromiso de disponibilidad del servicio y los niveles de servicio establecidos con la Dirección del DCCO, se dará inicio y continuidad del nuevo servicio, incorporándose al catálogo de servicios del CERT-ESPE del DCCO.	¿Cómo será la operación del SIEM que se va implementar en el ESPE-CERT? ¿Cómo se incorporará el SIEM al catálogo de servicios del CERT-ESPE del DCCO?
Mejora del Servicio y resolución de las no conformidades.	¿Qué se tomará a consideración para realizar las mejoras del servicio? ¿Cómo será la evaluación de las acciones para evaluar el funcionamiento del sistema?

Hipótesis

Hi = La implantación de un servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el área del ESPE-CERT de la Universidad de las Fuerzas Armadas ESPE, ayudará a recopilar los registros de actividad (*log)* de cada sensor en un nodo centralizado para ayudar al operador del ESPE-CERT. También brindará apoyo a la seguridad de los activos de información y facilitará la recolección de eventos, alertas y alarmas.

Beneficios o Impacto del Tema

Instalar un servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) permite desplegar una infraestructura de recopilación de registros. Esto ayuda al área de ESPE-CERT en la verificación del cumplimiento de normas de seguridad. El uso de la tecnología SIEM puede detectar actividades asociadas con un ataque, bloquear las amenazas en las redes, evitando que haya filtraciones de datos y fallos en los procesos del sistema. También permite buscar amenazas en registros archivados y por último ayuda a detener amenazas desconocidas hasta el momento. Para todo esto el SIEM se apoya en la tecnología de Machine Learning (Becerra Acosta & Paramo Calderón, 2021)

Entre otras ventajas que ofrecen el correlacionador de eventos SIEM, tenemos:

- Centralización de información.
- Automatización de tareas.
- Respuesta automática frente a eventos y/o amenazas.
- Alarmas de seguridad.
- Seguimiento de eventos
- Análisis y correlación de logs en tiempo real.
- Evaluación de vulnerabilidades.
- Detección de intrusiones.
- Monitoreo del comportamiento.

Metodología

Para el desarrollo del presente trabajo de investigación, se decidió utilizar la metodología design science research (DSR), la cual propone la construcción de artefactos mediante un enfoque de investigación riguroso con el objetivo de brindar una solución útil y efectiva a un problema de un dominio dado. El desarrollo del artefacto implica un ciclo de actividades de diseño-construcción-evaluación, que iteran tantas veces como sean necesarias antes que el artefacto sea finalmente verificado, validado y comunicado para su utilización. Para el abarcar de una formar adecuada esta metodología, se establecieron los siguientes pasos propuestos por Peffers, Tuunanen, Rothenberger & Chatterjee (2014), además, se describe brevemente en que consiste cada uno:

- Identificación del problema y motivación: Definir el problema de investigación específico y justificar el valor de una solución. Justificar el valor de una solución logra dos cosas: motivar al investigador y al equipo a buscar la solución, aceptar los resultados y ayuda a comprender el razonamiento asociado con la comprensión del problema por parte del investigador. Los recursos necesarios incluyen el conocimiento del estado del problema y la importancia de su solución.
- Definición de objetivos para una solución: definir los objetivos de una solución a partir de la definición del problema. Los recursos necesarios para esto incluyen el conocimiento del estado de los problemas y las soluciones actuales, si las hay, y su eficacia.
- Diseño y desarrollo: Consiste en crear el artefacto. Los artefactos son potencialmente construcciones, modelos, métodos o instanciaciones o nuevas propiedades de los recursos técnicos, sociales o informativos. Conceptualmente, un artefacto de investigación de diseño puede ser cualquier objeto diseñado en el que una contribución de investigación esté integrada en el diseño. Los recursos necesarios para pasar de los objetivos

al diseño y desarrollo incluyen el conocimiento de la teoría que se puede utilizar en una solución.

- Demostración: Se demuestra el uso del artefacto para resolver una o más instancias del problema. Esto podría implicar su uso en experimentación, simulación, estudio de casos, prueba u otra actividad apropiada. Los recursos necesarios para la demostración incluyen un conocimiento efectivo de cómo usar el artefacto para resolver el problema.
- Evaluación: Consiste en la observación y medición del desempeño del artefacto en el apoyo a una solución del problema. Esta actividad implica comparar los objetivos de una solución con los resultados reales observados del uso del artefacto en la demostración. Conceptualmente, la evaluación podría incluir cualquier evidencia empírica o prueba lógica apropiada. Al final de esta actividad, los investigadores pueden decidir si repetir el diseño y desarrollo para tratar de mejorar la efectividad del artefacto o continuar con la comunicación y dejar mejoras adicionales para proyectos posteriores.
- Comunicación: Comunicar el problema y su importancia, comunicar sobre el artefacto su utilidad y novedad, el rigor de su diseño y su eficacia a los investigadores y otras audiencias relevantes.

La razón por la cual se eligió esta metodología, es debido a que se adapta al marco de desarrollo de un trabajo de titulación en donde se va a realizar la prestación de un servicio haciendo uso de ITIL V4, además de que DSR puede ser aplicado a nuestro dominio que es la seguridad de la información. A continuación, se describe la adaptación a cada uno de los pasos propuestos de la metodología en el presente trabajo:

- Identificación del problema y motivación: en el planteamiento del problema, se identificó que el ESPE-CERT ofrece varios servicios configurados en sus equipos tecnológicos, además de que la universidad cuenta con una serie de dispositivos e infraestructura destinada a complementar y apoyar los

objetivos de la institución. Es por esto que, es necesario tener una plataforma en donde se pueda centralizar toda la información sobre los eventos de seguridad emitidos por los equipos informáticos mencionados anteriormente.

- Definición de objetivos para una solución: en base a la definición del problema, se plantean tanto el objetivo general como los específicos con el fin de intentar solventar la problemática mencionada en el paso anterior.
- Diseño y desarrollo: se procede con la identificación del artefacto a crear, que para este caso será el SIEM, ya que es una nueva propiedad agregada a la infraestructura actual del ESPE-CERT y que permitirá tener una vista centralizada de los equipos a monitorear. Además, también se involucran las actividades diseño y el plan de ITIL V4, en donde se plantea el diseño del nuevo servicio y su respectiva gestión para que este alineado a los objetivos de la institución. En lo que respecta al conocimiento de la teoría, se investigó y resumió los aspectos más importantes de un SIEM además de los subtemas relacionados al mismo, en la sección correspondiente a la fundamentación teórica se documentó la información estudiada para entender sobre el tema y realizar la implementación de manera satisfactoria.
- Demostración: con una extensa revisión de documentación sobre el SIEM a ser implementado, se procede a realizar la actividad de entrega y soporte de ITIL V4 que se ajusta a este paso, en donde se realizará una primera instalación y configuración del nuevo servicio para observar si existen errores en su funcionamiento.
- Evaluación: en el ciclo de vida de ITIL V4, la entrega y soporte del servicio se ajusta a este paso, ya que al realizar la implementación del SIEM en el entorno de producción, es posible identificar posibles mejoras para el servicio, además de que realizan revisiones sobre el desempeño del servicio para asegurarse que los clientes estén satisfechos y se cumplan los acuerdos de nivel de servicio (SLA) establecidos.

- Comunicación: del ciclo de vida de ITIL V4, también se ajusta la fase de entrega y soporte, adicionalmente, también la fase de mejora. Por parte de la entrega y soporte, los encargados de la implementación, deben informar y documentar los problemas importantes que surjan. De la fase de mejora, se puede mencionar que se debe informar si se cumplen los indicadores establecidos en donde se contraste que el servicio está funcionando correctamente, también se establecen nuevos objetivos para que la mejora siga en constate desarrollo, estos objetivos serán documentados y comunicados a los encargados de gestionar el SIEM.

Capítulo II:

Fundamentación Teórica y Estado del Arte

Fundamentación Teórica

Para el desarrollo del presente trabajo, es necesario tener claro algunos conceptos, como son: la seguridad de la información; seguridad informática; sistemas de seguridad; dispositivos de seguimiento y monitoreo; que es un correlacionador de eventos (SIEM), cómo ayudan estos a preservar la seguridad en la infraestructura tecnológica, cuáles son sus componentes y por último, qué es ITIL V4 y cómo aplicarlo en el desarrollo de la investigación, siguiendo las actividades necesarias para una correcta gestión del nuevo servicio.

Seguridad de la información

Para definir lo que es la seguridad de la información, se puede utilizar el estándar ISO/IEC 27001, el cual nos indica que la seguridad de la información tiene que velar por la integridad, confidencialidad y disponibilidad de la información de la organización o sistema al que pertenezca. Otros aspectos que se pueden asegurar es la autenticidad, confiabilidad y no repudio.

Se puede decir que la seguridad de la información se encarga de la protección de la información y sus elementos críticos, incluidos los sistemas y el hardware que usan, almacenan y transmiten esa información. No obstante, no protege únicamente el medio informativo, sino que abarca cualquier medio que pueda tener información, esto la convierte en un tema más extenso que la seguridad informática.

Seguridad informática

La seguridad informática es uno de los temas que más importancia ha tomado en la actualidad y a diferencia de la seguridad de la información, esta se encarga de la seguridad únicamente del medio informático. Según diversos autores la informática es la ciencia que

se encarga de distintos procesos, técnicas y métodos que tienen por objetivo el procesar, almacenar y transmitir información. (Romero Castro, y otros, 2018)

A la seguridad informática se la puede definir como aquella disciplina que se encarga de plantear, diseñar normas, procedimientos, métodos y técnicas para mantener un sistema de información seguro, confiable y que se encuentre disponible. (Romero Castro, y otros, 2018)

Para este tipo de seguridad existen distintas prácticas que por lo general consisten en la restricción del acceso al sistema o parte del sistema. El acceso al sistema está permitido solo para ciertas personas que se encuentren acreditadas, así como la modificación limitada por su nivel de autorización. Las amenazas que se pueden presentar se dan debido a que el mismo usuario no es consciente o no se da cuenta de las vulnerabilidades que existen al hacer mal uso del sistema. Por ejemplo, los usuarios al descargar archivos maliciosos o cuando eliminan archivos importantes del sistema. (Calderón Arateco, 2015)

Sistemas de Seguridad Integrada

Los sistemas de seguridad son conjuntos de elementos y métodos instalados e intercomunicados entre sí y que se encargan de proteger la integridad de los equipos, datos o información que se encuentran dentro de un área. Los sistemas de seguridad tienen como objetivo prevenir, detectar y eliminar las intrusiones (posibles ataques).

Sistemas de Gestión de Seguridad de la Información.

Un SGSI (Sistema de Gestión de la Seguridad de la información), también conocido como ISMS (por sus siglas en inglés). El SGSI es una herramienta con la que se puede identificar, atender y minimizar los riesgos que afectan de manera negativa a la confidencialidad integridad y disponibilidad de la organización. El SGSI abarca la estructura organizacional, actividades de planificación, políticas, responsabilidades, procedimientos, proceso y recursos.

Para implementar de un SGSI en cualquier organización se ha creado un conjunto de estándares conocido como ISO/IEC 27000. El uso de estas normas no es obligatorio, sin embargo, su uso muestra un compromiso con la calidad, aumento en la competitividad y facilita el entendimiento a otras personas, países u organizaciones. Cabe mencionar que la ISO/IEC 27000, no es una sola norma, sino, una familia de normas. En la ISO/IEC 27000 se agrupan las definiciones y términos utilizados por el resto de normas de esta familia.

Contar un con SGSI es beneficioso tanto para la organización como para sus clientes:

- En la organización:
  - Establece políticas de seguridad de la información.
  - Favorece a la imagen institucional.
  - Protege los activos de información.
  - Reduce las perdidas por incidentes de seguridad.
- Para los clientes:
  - Recepción de servicios de calidad.
  - Seguridad y confianza. (Lara, 2022) (iso27000.es, 2022)

Controles y Salvaguardas.

Como se mencionó anteriormente la seguridad de la información se encarga de proteger sus tres pilares (confidencialidad, integridad y disponibilidad), implementando medidas como controles o salvaguardas.

Siguiendo con el trabajo de un SGSI se puede utilizar la norma ISO/IEC 27002 (perteneciente a la familia de normas de la ISO/IEC 27000), que ofrece una guía acerca de buenas prácticas las cuales describen los objetivos de los controles recomendados en el campo de la seguridad de la información. (iso27000.es, 2022)

Según INCIBE (2022), la evaluación de los activos de la información se relaciona a los tres pilares de la seguridad de la información. Se debe tener en cuenta que un determinado control para un pilar puede afectar de manera positiva o negativa a los otros pilares, por lo cual es importante conocer cual pilar es primordial proteger para cada sistema de información.

Las salvaguardas son medidas indispensables para proteger la información del negocio. Para la selección de estas medidas se tiene que tener en cuenta los siguientes aspectos:

- Hay que determinar la importancia de la información que se maneja en la empresa/institución.
- Se debe identificar, clasificar y valorar la información según los pilares de la seguridad (dimensiones).
- Es importante también conocer la naturaleza de los controles que se implementarán.
- El presupuesto es un factor a considerar ya que el costo de las medidas puede variar o ser proporcional al nivel de riesgo que se quiere evitar.

Dispositivos de seguimiento y monitoreo

El monitoreo de red otorga la información necesaria a los administradores de la red para saber en tiempo real, si el funcionamiento de una red es adecuado. (cisco.com, 2022)

Firewall de Nueva Generación

Un firewall tradicional es un sistema que consta de software y/o hardware que está diseñado para evitar el acceso no autorizado a una red o dispositivo, estos supervisan el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad (Voronkov, Horn Iwaya, Martucci, & Lindskog, 2017).

Los firewalls de nueva generación, además de tener las funcionalidades de un firewall tradicional, permiten mejorar el desempeño de la red ya que están equipados con más características descritas por Neupane, Haddad & Chen (2018):

- Control de tráfico cifrado: Los firewalls de nueva generación deben tener la capacidad de descifrar e inspeccionar el tráfico SSL/TLS para eliminar las amenazas de puntos ciegos ya que, aunque SSL/TLS proporciona un método de autenticación, crea un punto ciego que desafía las defensas tradicionales en capas por donde los atacantes pueden vulnerar una red.
- Salto de puertos: a menudo los atacantes usan saltos de puertos de forma aleatoria para ir más allá de los firewalls tradicionales. Es por eso que los firewalls de próxima generación deben poder detectar esos puertos cuando se utilizan.
- Control de aplicaciones: un firewall de próxima generación no debe enfocarse en analizar encabezado estructurado en las capas 3 y 4, sino que debe tener más énfasis en las aplicaciones, de tal modo que tenga la capacidad de restringir el acceso a las aplicaciones web.
- Control basado en la identidad: debe poder asignar políticas de seguridad específicas a grupos de usuarios e individuos definidos.
- Filtrado de URL: debe poder restringir la navegación web para limitar la exposición a sitios dañinos e inapropiados.
- Protección contra la fuga de datos: el firewall de próxima generación debe poder restringir la salida de datos confidenciales.
- Control de la red Wi-Fi: debe garantizar que las redes Wi-Fi tengan altas capacidades de seguridad.
- Control de acceso a la red: debe garantizar que cada dispositivo de punto final conectado tenga la seguridad adecuada.

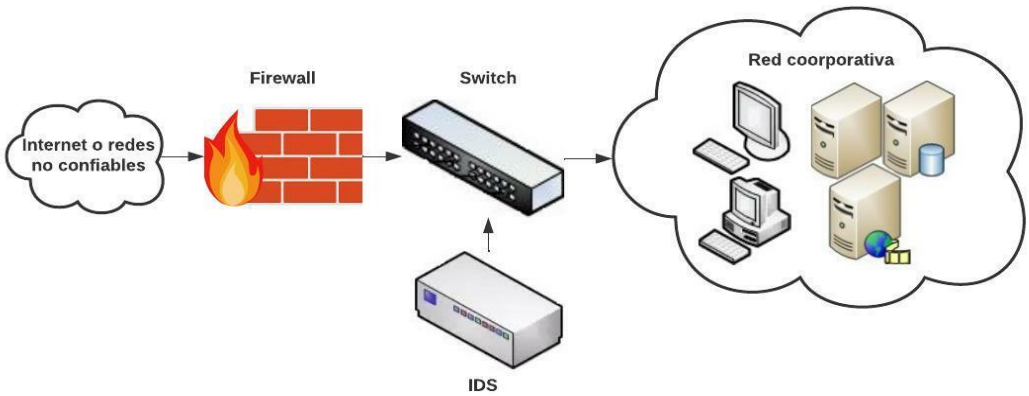
IDS (Intrusion Detection System)

Un IDS es la combinación de las palabras “intrusión” y “sistema de detección'', en donde la intrusión hace referencia a un acceso no autorizado a la información dentro de un computador o los sistemas de red, con el objetivo de comprometer su integridad, confidencialidad o disponibilidad, mientras que los sistemas de detección, son mecanismos de seguridad para la detección de tal actividad ilegal (Ahmad, Shahid, Wai, Abdullah, & Ahmad, 2020). Por tanto, un IDS es una herramienta de seguridad que monitorea constantemente a los dispositivos y el tráfico de la red con el fin de detectar cualquier comportamiento sospechoso que viole la política de seguridad y comprometa la confidencialidad, integridad y disponibilidad. El IDS generará alertas sobre el comportamiento malicioso detectado para los administradores del host o de la red.

Su modo de operación se fundamenta en examinar minuciosamente el flujo de tráfico de la red, el cual, al ser ingresado en el analizador, se coteja con registros y patrones de amenazas identificadas previamente, o conductas irregulares, como la exploración de puertos, paquetes defectuosos, entre otros. El IDS no solo examina la naturaleza del tráfico, sino que también analiza su comportamiento y contenido. (Janjua, Vecchio, & Antonelli, 2020)

Figura 1

Configuración típica de un IDS



Existen dos tipos de IDS principales, a continuación, se describe cada uno de ellos:

- IDS basados en host (HIDS). Analizan distintas áreas con el fin de determinar el uso inadecuado de los dispositivos o alguna intrusión, consultan diferentes tipos de registros de archivos como el del sistema, servidores kernel, red, firewall, etc., y los comparan con una base de datos interna de registros comunes sobre ataques conocidos, así mismo, pueden verificar la integridad de ejecutables importantes y de los datos de archivos. (RedHat, 2022)
- IDS basados en la red (NIDS). Escanean los paquetes de red al nivel de un router o host con el objetivo de auditar los datos contenidos en los paquetes y así, poder registrar los paquetes sospechosos en registro especial con información extendida. En base a estos paquetes sospechosos, estos IDS pueden realizar escaneos dentro de su propia base de datos de firmas de ataques registrados en red para asignar un nivel de severidad a cada paquete. Cuando se identifican niveles de severidad lo suficientemente altos, se envía un mensaje de advertencia al personal encargado de la seguridad para que puedan identificar la procedencia de la anomalía. (RedHat, 2022)

IPS (Intrusion Prevention System)

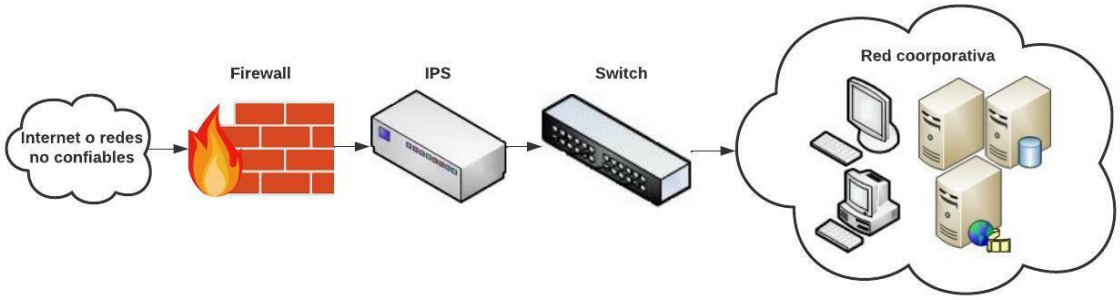
Los sistemas de prevención de intrusiones (IPS) son dispositivos de red que detectan, bloquean y reportan contenido malicioso en el tráfico de red que pasa a través de ellos, un IPS analiza el flujo de tráfico y su contenido, en busca de eventos maliciosos. (Särelä, Kyöstilä, Kiravuo, & Manner, 2017)

Si bien la utilidad de la prevención de intrusiones se ha cuestionado desde el principio, los dispositivos de prevención de intrusiones se han convertido en parte de la arquitectura de seguridad de la red. La razón es que un IPS proporciona profundidad adicional al perímetro de seguridad y un único punto de control. Se puede utilizar para detectar errores de configuración y proteger dispositivos con vulnerabilidades sin tratar.

En la **Figura 2**, se muestra el funcionamiento de un IPS en línea: el tráfico de la red pasa por el IPS para su análisis y el dispositivo puede bloquearlo según sea necesario.

Figura 2

Configuración típica de un IPS



Los dispositivos del sistema de prevención de intrusiones requieren configuración y administración para una operación eficiente y producen registros e informes resumidos sobre las amenazas detectadas y prevenidas.

DLP (Data Loss Prevention)

Por lo general, un sistema DLP representa un conjunto de herramientas y procesos incorporados que se utilizan para garantizar que los datos confidenciales no se pierdan, se utilicen indebidamente o los usuarios no autorizados accedan a ellos (Falah Faiz, Arshad, Alazab, & Shalaignov, 2019), un sistema DLP logra esto proporcionando una visión profunda del uso de datos y el transporte dentro de una organización. Con el aumento significativo de los ataques cibernéticos dirigidos al robo de datos, el uso de sistemas como DLP también ha aumentado con un estudio reciente llevado a cabo por *Bickerstaffe* que indica que el 62% de las organizaciones adoptan tales soluciones como parte de su arquitectura de seguridad organizacional. (Bickerstaffe, 2018)

Hay muchos tipos de herramientas de seguridad además de DLP que pueden ser utilizadas, como los sistemas de prevención de intrusiones (IPS) y los sistemas de detección de intrusiones (IDS). Aunque se consideran herramientas de seguridad, tienen

una diferencia principal. DLP es responsable únicamente de capturar e identificar información confidencial. Sin embargo, IPS e IDS se encargan de todo tipo de peligros o amenazas a los que puedan enfrentarse los datos. DLP tiene dos fases principales para identificar información importante o confidencial. El primero es generar huellas dactilares o patrones predefinidos que se basan en extraer ciertas características de archivos conocidos y la segunda es comparar las huellas dactilares de nuevos archivos con las huellas dactilares existentes que se derivan de la primera etapa (Husham Ali, Adeeb Jalal, & Ibrahem Al-Obaydy Al-Obaydy, 2020). Finalmente, si el resultado de la comparación fue positivo, el archivo detectado puede cifrarse, bloquearse, eliminarse o transferirse a un lugar seguro.

SIEM (Security Information and Event Management)

Constituyen la plataforma central de los centros de operaciones de seguridad modernos, ya que recopilan eventos de múltiples sensores (sistemas de detección de intrusos, antivirus, firewalls, etc.), correlacionan estos eventos y brindan vistas sintéticas de las alertas para el manejo de amenazas e informes de seguridad (González, González, & Diaz, 2021). En particular, un SIEM puede agregar, normalizar y correlacionar varios eventos de seguridad generados por una infraestructura administrada, identificando así posibles violaciones de seguridad (Radoglou, y otros, 2021). Un evento de seguridad se considera un mensaje normalizado relacionado con el estado de seguridad de la infraestructura monitoreada. La progresión continua de los ataques cibernéticos y el malware requiere la evolución y adopción simultáneas de las contramedidas necesarias. Los SIEM se caracterizan por una falta de comprensión entre las complicadas relaciones de las instancias de intrusión real y las alertas falsas. (Milajerdi, Gjomemo, Eshete, Sekar, & Venkatakrishnan, 2019)

Los SIEM surgen de la unión de tecnologías SIM como gestión de información de seguridad y SEM como gestión de eventos de seguridad:

- SIM: Es un software que automatiza la recopilación de datos emitidos por dispositivos de seguridad con respecto al registro de eventos, estos dispositivos pueden ser firewalls, IDS o antivirus. Estos datos luego se traducen a formatos correlacionados y simplificados. La SIM muestra informes, tablas y gráficos sobre eventos relacionados con la seguridad. (Technopedia, 2022)
- SEM: Es un software que tienen como objetivo reconocer, recolectar, supervisar y comunicar los incidentes vinculados con la seguridad en un software, sistema o ambiente de tecnología de la información. SEM permite registrar y analizar los eventos, y asiste a los administradores de sistemas o seguridad para examinar, adaptar y manejar la estructura, normativas y procesos de seguridad de la información. (Technopedia, 2015)

Cómo Funcionan. Los SIEM hacen uso de herramientas tales como los protocolos SNMP y WMI, además del envío de mensajes por medio de Syslog, con el objetivo de recolectar la información generada por los dispositivos, almacenarla y organizarla para que pueda ser interpretada de una forma adecuada. (García Arias & Rodríguez Duarte, 2021)

En su estructura, consta de una base de datos destinada a almacenar los dispositivos que van a ser monitoreados, así como la información generada por los mismos. También posee módulos más desarrollados destinados a funcionalidades más específicas, como la gestión de incidentes de seguridad o la generación de reportes.

Un SIEM también tiene la funcionalidad de normalizar la información cronológicamente, esto con la finalidad de poder identificar patrones a través del tiempo, realizar búsquedas sencillas de usuarios y eventos para determinar el origen de los incidentes y finalmente, puede interpretar de manera inteligente cada evento con el objetivo de identificar vulnerabilidades y amenazas en la infraestructura tecnológica.

Protocolos de Comunicación Empleados por un SIEM. El funcionamiento de un SIEM se basa en distintos protocolos de comunicación con el fin otorgar información sobre los dispositivos y así, poder obtener la mayor cantidad de logs posibles y que estos se

encuentren estructurados de una forma estándar. A continuación, se presentan algunos de estos protocolos empleados mencionados por García Arias & Rodríguez Duarte (2021) y Becerra Acosta & Paramo Calderón (2021):

- Syslog (*System Logging Protocol*)*:* Es utilizado para él envió y recopilación de eventos ocurridos en los dispositivos, cada uno de estos tiene un registro de eventos interno el cual es enviado a otro dispositivo con mayores capacidades de almacenamiento con el fin de tener la información centralizada. Estos logs generalmente se encuentran en texto plano para que sean más ligeros de almacenar y transportar. Este protocolo es extremadamente útil ya que una gran cantidad de dispositivos conectados a red pueden tener el habilitado el protocolo, como conmutadores, enrutadores, cortafuegos, incluso ciertas impresoras.
- SNMP (*Simple Network Monitoring Protocol*)*:* Este protocolo es empleado para la transferencia de información y monitoreo en gestión de redes. SNMP genera tráfico con los datos de monitoreo al servidor de los activos de información registrados en su base de datos. Los dispositivos conectados a la red emplean el protocolo UDP para él envió de datos de sí mismos hacia el servidor, el cual los interpreta para generar estadísticas y alarmas programadas, así mismo ayuda a la generación de informes sobre el comportamiento de la red.
- *Windows Event Log*: Es un registro que detalla los eventos relacionados con el sistema, la seguridad y la aplicación almacenados en un sistema operativo Windows. Los registros de eventos se pueden usar para rastrear el sistema y algunos problemas de aplicaciones y pronosticar problemas futuros. Estos registros almacenan información sobre diferentes eventos que ocurren dentro del sistema. El tipo de información almacenada varía según la categoría de

un registro de eventos. Los datos se registran comúnmente para cuatro tipos de registro de eventos de Windows:

  - sistema
  - solicitud
  - configuración
  - seguridad

- Rsyslog (*Rocket-fast System for log processing*): es el programa de registro predeterminado distribuciones Debian y Red Hat. Es una extensión del protocolo syslog original, con características adicionales como configuración flexible, capacidades de filtrado enriquecidas y filtrado basado en contenido. Es posible emplear Rsyslogd para reunir mensajes de registro provenientes de programas y servidores, para luego enviarlos a archivos de registro locales, dispositivos o servidores de registro remotos.

Integración de Datos. Luego de recolectar los datos de las diferentes fuentes, estos se unifican y son almacenados en un único lugar con el fin de facilitar la correlación de los eventos, las otras funcionalidades complementan la solución con base al análisis forense y la generación de informes. Ciertas características vienen integradas en la herramienta y pueden traer problemas en la implementación debido a que su arquitectura varía en base a las necesidades de las organizaciones.

Estandarización de Datos. Los SIEM recolectan una enorme cantidad de datos provenientes de los dispositivos conectados a la red, lo que significa que todos los datos van a estar en formatos distintos y estos deben ser interpretados por el SIEM. El proceso de estandarizar los datos, debe realizarse de una forma correcta con el objetivo de mostrar los datos de manera entendible, para así poder realizar la correlación de los eventos y hallar las anomalías de las diversas fuentes.

Componentes de un SIEM. En la **Figura 3** se muestran aquellos componentes que son básicos para que un SIEM pueda funcionar adecuadamente.

Figura 3

Componentes de un SIEM

- Capa de recolección de eventos. recolecta todos los eventos generados por los dispositivos de seguridad o de red.
- Capa de normalización. estandariza todos los eventos que son recolectados en el SIEM, de manera que todos estos posean un mismo formato de datos y así, puedan ser enviados e interpretados por la capa de correlación.
- Capa de correlación. identifica patrones en común de los logs y registros que se encuentran ya normalizados.
- Capa de reporte. Se encarga de analizar los resultados generados por la capa de correlación, los procesa y genera distintos informes sobre los eventos que ocurren en los dispositivos de red.

Ventajas de un SIEM. Con un SIEM, el personal de IT tiene a su disposición un método efectivo para realizar la automatización de procesos además de centralizar la gestión de seguridad, de tal manera que se ayude a simplificar la complicada labor de proteger información sensible. Es por ello que, una de las principales ventajas de un sistema SIEM es proporcionar al personal de TI información con la cual, se pueda diferenciar entre una amenaza de bajo riesgo y una que pueda ser determinante para las operaciones del negocio. Algunas otras ventajas son:

- Información de seguridad centralizada.

- Automatizar tareas
- Automatización de respuestas ante amenazas y eventos
- Menor tiempo en la detección de ataques
- Información oportuna para el análisis forense
- Alertas de seguridades eficientes
- Correlación de logs en tiempo real
- Seguimiento de eventos
- Mejor manejo del riesgo
- Gestión de métricas de seguridad

Correlación de Eventos. Es la función de relacionar varios eventos de seguridad y alarmas dentro de un rango de tiempo en varios dispositivos o sistemas con el fin de identificar actividades anormales que no son observables en eventos individuales y generar reglas que ayuden a diferenciar entre un evento normal y un evento anómalo persistente. En la gestión, se destacan algunos de los siguientes ítems:

- Administración Centralizada. Es un tablero de control que sirve para interactuar con las demás propiedades de un SIEM. Esta interfaz permite realizar en tiempo real el monitoreo de eventos además de que ayuda a realizar un análisis detallado en base a los resultados recolectados.
- Reportes. El SIEM por medio de consultas, paneles o plantillas, debe otorgar una vista global sobre el estado de los diferentes dispositivos que se encuentran agregados al monitoreo del SIEM, esta presentación debe ser sencilla de crear y fácilmente personalizable.
- Análisis Forense. Es una técnica en donde se hacen búsquedas de alertas y registros de actividades anormales con el fin de correlacionar los eventos de manera que los análisis recolectados, muestran los resultados que uno esperaría. Con esto, se busca encontrar, enfrentar y responder a cualquier evento anormal dentro de la red en tiempo real.

- Alertas. Los dispositivos conectados a la red, pueden de notificar problemas de software o hardware gracias a las propiedades implementadas por sus fabricantes. Con esto, es posible informar por medio de correos electrónicos o tableros de instrumentos.

En base a los conocimientos, similitudes y estadísticas, hay algunos tipos de correlación los cuales pueden desempeñarse.

- Correlación basada en el conocimiento: debe existir un conocimiento base de la sobre los tipos de amenazas.
- Correlación basada en similitud: realiza una comparación con respecto a las demás alertas que se estén dando.
- Correlación estadística: No se depende de un conocimiento que exista, más bien se basa de las actividades que ya estén detalladas.

Soluciones SIEM Open Source. Actualmente existen varias herramientas *Open Source* destinadas a la correlación de eventos de seguridad, estas tienen el fin de detectar tempranamente los ataques informáticos, además de satisfacer las necesidades de las organizaciones. A continuación, se describen algunas de estas herramientas en la **Tabla 2**.

Tabla *2*

Comparación entre soluciones SIEM open source

SIEM *open source*	**Descripción**	**Características esenciales**
Wazuh	Solución de monitoreo de seguridad de código abierto utilizada para recopilar, agregar, indexar y analizar datos de seguridad, lo que ayuda a las organizaciones a detectar intrusiones,	Gestión de cumplimiento y seguridad Detección de eventos anormales, respuesta a incidentes Detección de vulnerabilidades y remediación

SIEM *open source*	Descripción	Características esenciales
	amenazas y anomalías de comportamiento. (wazuh.com, 2022)	Detección y respuesta de punto final (EDR)
OSSIM	Permite dar tratamiento a la información generada, almacenarla y dar prioridad mediante técnicas de correlación para obtener una visión global de los eventos de seguridad, posee un análisis de registros en tiempo real y un análisis de vulnerabilidades. (Pazmiño Gómez & Pazmiño Gómez, 2018)	Presenta informes técnicos y ejecutivos. Su arquitectura es escalable Permite realizar análisis sobre el comportamiento de la red. Permite detectar a bajo nivel y en tiempo real actividades anómalas. Permite realizar análisis de los riesgos de seguridad. Gestión de registros forenses
OSSEC	Sistema de detección de intrusos basado en host (HIDS) escalable, multiplataforma y de código abierto, tiene un poderoso motor de análisis y correlación, que integra análisis de registros, monitoreo de integridad de archivos, monitoreo de registros de Windows, cumplimiento de políticas centralizado, detección de *rootkits*, alertas en tiempo real y respuesta activa. (ossec.net, 2022)	Detección de intrusos basada en registros (LID). Monitoreo de integridad de archivos (FIM). Inventario del sistema. Detección de *rootkits* y malware. Auditoría de cumplimiento.

SIEM *open source*	Descripción	Características esenciales
Elastic stack	Conjunto de tecnologías compuestas por Elasticsearch, Logstash y Kibana (ELK) diseñado para ayudar a los usuarios a tomar datos de cualquier tipo de fuente y en cualquier formato con el fin de buscar, analizar y visualizar esos datos en tiempo real, se puede implementar en las instalaciones o estar disponible como SaaS. (Kotenko, Kuleshov, & Ushakov, 2017)	Funcionalidad de correlación de eventos y sistema de alertas. Escalable y resistente a los cambios. Optimización en la detección y respuesta de puntos finales. Correlación y análisis en tiempo real.

Comparación y Selección de SIEM. A continuación, se presenta en la **Tabla 3** una comparativa con características generales que fueron determinadas para la selección del SIEM a implementar en base a al hardware disponible y algunas funcionalidades esenciales para el nuevo servicio.

Tabla 3

Clasificación de los servicios de acuerdo a la demanda

Característica	Wazuh	OSSIM	OSSEC	Elastik stack
Open Source	Si	Si	Si	Si
Almacenamiento y procesamiento de logs	Si	No	Si	Si

Característica	Wazuh	OSSIM	OSSEC	Elastik stack
Se puede instalar en un SO	Si	No	Si	Si
Transferencia segura de datos	Si	Si	Si	Si
Monitoreo de amenazas	Si	Si	Si	Si
Visualización en base a criterios como días, semanas, meses, etc.	Si	Si	No	Si
Gestión de incidentes	Si	Si	Si	Si
Análisis de vulnerabilidades	Si	Si	Si	Si
Alertas de intrusión	Si	Si	Si	Si
Soporte y documentación	Si	Si	Si	Si
Sitio web de comunidad activa	Si	Si	Si	No
Puntaje	11	9	10	10

En base a los puntajes obtenidos, se determina como solución la implementación del SIEM Wazuh.

Instalación y Configuración. La instalación de una solución SIEM consiste esencialmente en un procedimiento de tres pasos descritos a continuación:

1. Despliegue

Previo a realizar la instalación de un SIEM, se debe corroborar que el sistema en donde va a ser implementado, disponga de los recursos adecuados que solicita, esto es importante debido a que generalmente, estos requieren de altas capacidades computacionales para funcionar de manera óptima. Una vez que cumpla con los requisitos previos correctos, se puede continuar con la implementación utilizando uno de los siguientes tres modos que se mencionan a continuación:

- Basado en la nube: el SIEM se ejecuta en el servidor del proveedor de servicios en la nube. Una de las principales ventajas es la flexibilidad y escalabilidad que ofrece. Se puede agregar o quitar características y recursos según la demanda, ya que los servicios se pueden agregar o eliminar convenientemente desde el proveedor.
- Basado en dispositivos: el SIEM tiene la forma de un dispositivo físico que recopila y analiza los datos de registro de la red. Este modo se adapta de mejor manera en las organizaciones que albergan recursos de red dentro de sus propias instalaciones y requieren una seguridad estricta.
- Basado en software: la implementación del software requiere que se compré e instale una versión del software del SIEM para que se ejecute en un dispositivo local, donde se recopilan y procesan los registros.

Durante la fase de implementación, los administradores del sistema se familiarizan con la solución SIEM y su funcionamiento. En esta fase inicial, también se determinarán las proyecciones de almacenamiento, los volúmenes de registro promedio y los requisitos de CPU, lo que lo ayudará a tomar decisiones adecuadas. Para el caso de realizar la implementación de un SIEM *Open Source,* para que este funcione óptimamente y se adecue al sistema anfitrión, la eficiente sería montarlo sobre un sistema operativo también *Open Source* como podría ser una distribución Linux, aunque este no puede ser el caso para todos los SIEM, es importante leer la documentación y recomendaciones dadas por los creadores.

2. Afinación

Cada organización es diferente y también lo son sus necesidades. Un SIEM debe estar en concordancia con las necesidades específicas de una organización. La afinación es el proceso de configurar el SIEM para satisfacer las demandas organizacionales. Para ajustar el SIEM a las necesidades, se puede realizar lo siguiente:

- Para alimentar el SIEM con la información correcta, es importante haber habilitado las políticas de auditoría correctas y de haberlas ajustado para generar exactamente los datos que necesita para el análisis y la supervisión de la seguridad.
- Cuando el SIEM se encuentre implementado, se debe asegurar de que todos los dispositivos y fuentes de datos en la red estén configurados para enviar los logs generados a la herramienta. Algunos SIEM pueden configurar automáticamente dispositivos y aplicaciones que necesitan enviar logs.
- Debido al gran volumen de registros generados, es posible que se pasen por alto registros importantes. Para evitar esto y aprovechar al máximo el ancho de banda disponible, se debe asegurar de configurar los filtros de recopilación de registros para recopilar solo los logs necesarios. Además de reducir los costos de almacenamiento, esto ayudará a reducir la cantidad de falsos positivos y a detectar amenazas y vulnerabilidades en sus primeras etapas.

3. Mantenimiento

Los SIEM necesitan un mantenimiento constante para garantizar que funcionen sin problemas y que sus capacidades se aprovechen al máximo. Con el entorno de ciberseguridad en constante cambio y una red organizativa dinámica, a continuación, se presentan algunas cosas que debe hacer para mantener un SIEM optimizado:

- Actualizar periódicamente las reglas de correlación de registros para mantenerse al día con los patrones cambiantes de amenazas y ataques.
- Crear nuevos perfiles de alerta para configurar flujos de trabajo de respuesta a incidentes.
- Realizar copias de seguridad de las bases de datos con regularidad para asegurarse de que no se pierdan datos.

- Asegurar los logs para que sean a prueba de manipulaciones. Esto asegurará que se puedan volver a importar registros cuando sea necesario, como durante un análisis forense.

Estos pasos asegurarán que un SIEM esté en la mejor posición para mantener la salud cibernética de la organización además de ayudar a mantener un paso por delante de los atacantes.

Como Usar un SIEM. Con la información recopilada en forma de logs sobre los eventos de seguridad ocurridos en los sensores controlados y resguardados por el SIEM, los encargados de TI pueden acceder la interfaz de control del SIEM, en donde se brindan opciones especificas en base al SIEM que haya sido contratado. Sin embargo, se presentan opciones en común para todas las soluciones SIEM las cuales son utilizadas para la generación de reportes, monitoreo de los sensores, detección de aplicaciones maliciosas, entre otras opciones. A continuación, se describe la forma más común de cómo usar las funcionalidades prestadas por un SIEM:

- Amenazas internas. Es posible generar informes centrados en recopilar los datos acerca de las amenazas internas, ya que esta es una de las causas más comunes detrás de los incidentes de seguridad. Se puede configurar las reglas de alertas integradas junto con el motor de correlación para identificar y filtrar acciones como escalamiento de privilegios sospechosa, credenciales de usuario comprometidas, exfiltración de datos entre otras amenazas internas.
- Monitoreo de seguridad. Permite el acceso al monitore en tiempo real de los sensores de la red. Brida una vista única sobre los incidentes de seguridad ya que tiene acceso a múltiples fuentes de datos y gracias a esto, puede combinar alertas de un IDS con información de un antivirus y registros de autenticación, generando reportes y vistas personalizadas en base a los criterios seleccionados por el administrador.

- *Insiders* malintencionados. El SIEM puede ser utilizado para realizar el análisis forense de un navegador, de los datos de la red, de la autenticación y otros datos con el fin de identificar a los *insiders* que planean o llevan a cabo un ataque.
- Ataques de fuerza bruta. Al agrupar parámetros importantes como la frecuencia de los intentos de inicio de sesión, el nombre de usuario y la dirección IP, un SIEM registra un incidente de seguridad después de que se superan los límites de umbral. Se pueden configurar análisis de comportamiento para obtener falsos positivos y marcar a una parte como el atacante, además de configurar notificaciones al equipo encargado a través de correos electrónicos y mensajes.
- Visualización de informes variados. El uso más frecuente de un SIEM es la visualización de informes en tiempo real sobre posibles eventos de seguridad, los administradores están en la condición se agregar o quitar filtros de búsqueda y obtener los resultados en base a un criterio, gracias a esto, es posible la generación de informes para verificar la autenticación de usuario, los intentos de acceso a archivos, las modificaciones en usuarios, grupos y servicios, así como eventos de ataques emitidos por los sensores.

ITIL V4

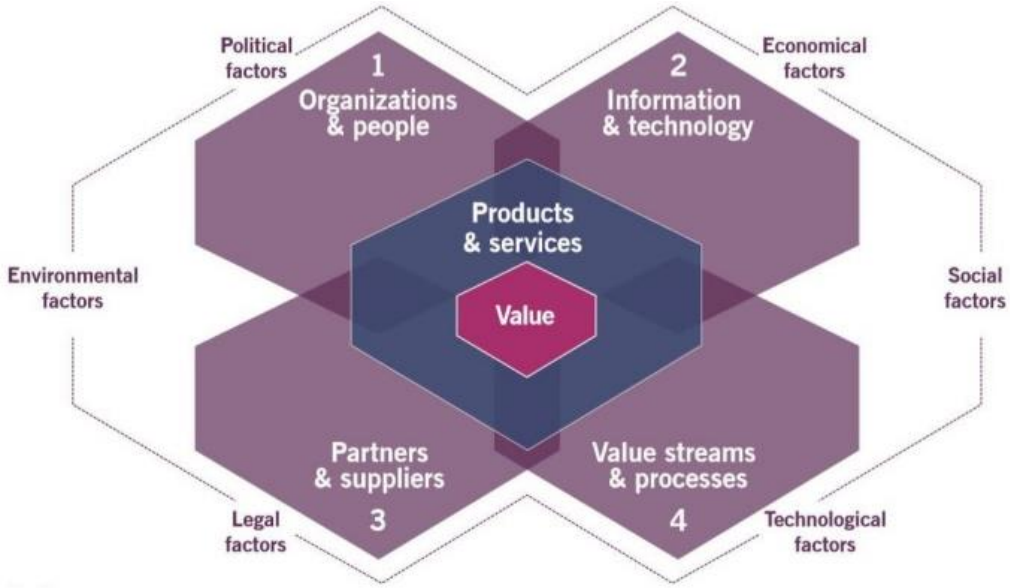
Publicada por primera vez en 1989, la Biblioteca de Infraestructura de Tecnología de la Información (*Information Technology Infrastructure Library, ITIL*) ha crecido hasta convertirse en el marco ITSM más popular y completo que contiene una serie de mejores prácticas que alinean los servicios de TI con las necesidades comerciales, describe los enfoques de las mejores prácticas en la gestión de servicios de TI, desde la generación de estrategias hasta las mejoras continuas del servicio en esencia, ITIL se centra en el servicio y prescribe una infraestructura organizacional para brindar servicios de TI a través de procesos (Marrone & Kolbe, 2011). En ITIL V4, se tiene como ciclo de vida el sistema de

valor, el cual cambia el antiguo modelo de servicio lineal por competencias que están interconectadas dentro de un sistema de valores (Remache Típan, 2022). El cambio de procesos a prácticas ayuda al personal de TI a que tengan un enfoque en lo que deben entregar, sin el inconveniente de realizar procesos repetitivos. El nuevo enfoque que tomó ITIL busca adaptarse a las nuevas tendencias tecnológicas.

Las 4 Dimensiones de la Gestión de Servicios. La entrega y el soporte de diferentes servicios y productos requiere una combinación diferente de componentes. Ningún componente puede generar valor por sí solo, por lo que se requiere una perspectiva holística: considerar todas las dimensiones al diseñar y cambiar productos y servicios. Las 4 dimensiones identifican los recursos organizacionales que se aprovechan para desarrollar prácticas y respaldar flujos de valor, así como resaltar los factores externos que pueden afectar estos recursos. En la Figura 4, se pueden observar las dimensiones establecidas en ITIL V4.

Figura 4

Las 4 dimensiones de la Gestión de Servicios ITIL V4



Nota: El gráfico fue tomado de *Marcos de gestión de tecnologías de información, análisis del marco de gestión V4* (p. 20), por Remache Maritza (2022), biblioteca digital de la EPN.

A continuación, se describen las dimensiones:

- **Organizaciones y personas:** garantiza que la forma en que se estructura y gestiona una organización, así como sus roles, responsabilidades, sistemas de autoridad y comunicación, estén bien definidos y respalden su estrategia general y modelo operativo.
- **Información y tecnología:** la información y el conocimiento que se utilizan para prestar servicios, y la información y las tecnologías que se utilizan para gestionar todos los aspectos del sistema de valor del servicio.
- **Socios y proovedores:** abarca las relaciones que una organización tiene con otras organizaciones que están involucradas en el diseño, desarrollo, implementación, entrega, soporte y/o mejora continua de los servicios.
- **Flujos de valor y procesos:** esta dimensión define las actividades, flujos de trabajo, controles y procedimientos necesarios para lograr los objetivos acordados.

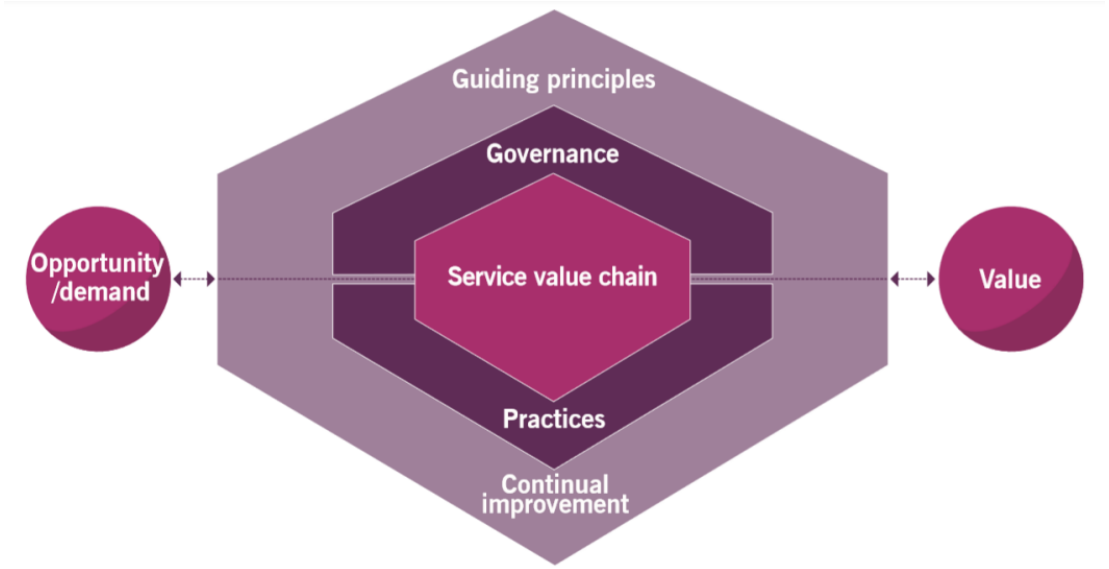
Sistema de Valor de Servicio (SVS). El sistema de valor de servicio de ITIL describe cómo todos los componentes y actividades de la organización funcionan juntos como un sistema para permitir la creación de valor. El sistema de valor del servicio de cada organización tiene interfaces con otras organizaciones, formando un ecosistema que puede, a su vez, facilitar el valor para esas organizaciones, sus clientes y otras partes interesadas. A continuación, se describen cada uno de los componentes:

- **Principios básicos:**
    - Estas son recomendaciones que pueden orientar a una organización en cualquier situación, sin importar los cambios que puedan ocurrir en sus objetivos, estrategias, tipo de trabajo o estructura de gestión.
- **Governanza:**
    - Se refiere a los mecanismos mediante los cuales una organización es dirigida y controlada. Esto implica establecer políticas, procesos y estructuras para garantizar que los servicios de TI se entreguen de manera efectiva y que se cumplan los objetivos del negocio.

- **Cadena de valor del servicio:**
    - Es conjunto de actividades interconectadas que realiza una organización con el fin de proporcionar un producto o servicio valioso a sus clientes y facilitar la creación de valor.
- **Prácticas:**
    - Son conjuntos de recursos organizacionales diseñados para realizar un trabajo o alcanzar un objetivo específico.
- **Mejora continua:**
    - Se refiere a una actividad organizacional recurrente realizada en todos los niveles con el objetivo de garantizar que el desempeño de una organización satisfaga constantemente a sus partes interesadas.

Figura 5

Sistema de Valor de Servicio ITIL V4



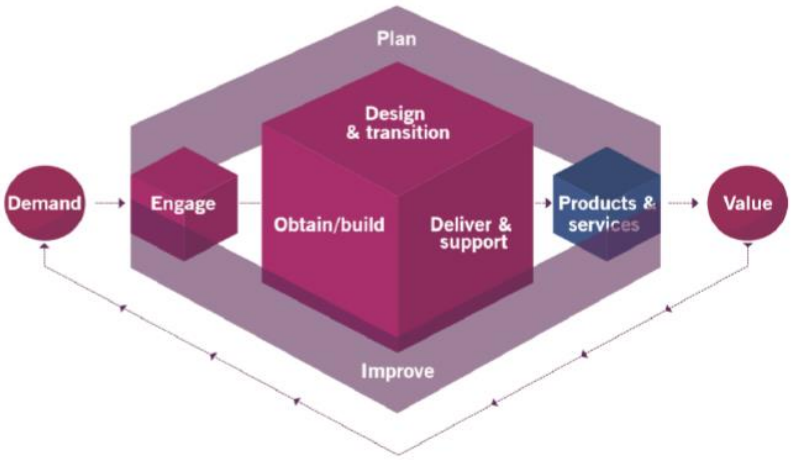
Nota: El gráfico representa los componentes del sistema de valor de servicio. Tomado de *Marcos de gestión de tecnologías de información, análisis del marco de gestión V4* (p. 21), por Remache Maritza (2022), biblioteca digital de la EPN.

Cadena de valor de Servicio. ITIL V4 indica las actividades de la cadena de valor de servicio de la siguiente manera, según IT Service (2019):

- **Plan**
    - La meta es asegurar que haya un entendimiento compartido de la visión, el estado actual y la dirección de mejora para las cuatro dimensiones de la gestión de servicios, así como para todos los productos y servicios en toda la organización.
- **Mejora**
    - Garantizar la mejora constante de los productos, servicios y prácticas en todas las actividades de la cadena de valor y en las cuatro dimensiones de la gestión de servicios.
- **Participación**
    - Ofrecer una comprensión sólida de las necesidades de las partes interesadas, promover la transparencia y el compromiso continuo, y establecer buenas relaciones con todas las partes interesadas involucradas.
- **Diseño y Transición**
    - Esta actividad de la cadena de valor se enfoca en garantizar que los productos y servicios cumplan con las expectativas de calidad, costos y tiempo de comercialización de las partes interesadas.
- **Obtener/Construir**
    - Asegurar que los componentes del servicio estén disponibles en el momento y lugar necesarios, y que cumplan con las especificaciones acordadas.
- **Entrega y Soporte**
    - Asegurar que los servicios se entreguen y soporten de acuerdo con las especificaciones acordadas y las expectativas de las partes interesadas.

Figura 6

Gráfico cadena de valor de servicio ITIL V4



Nota: El gráfico representa las actividades a realizar en la cadena da valor de servicio. Tomado de *Capacitación de ITIL V4 Foundation* (p. 43), por IT Service (2019).

En la **Tabla 4** se puede observar una comparativa entre las fases del ciclo de vida de ITIL V3 con las actividades de la cadena de valor de servicio de ITIL V4.

Tabla 4

Comparación de ITIL V3 con ITIL V4

ITIL V3 (Ciclo de vida)	**ITIL V4 (Cadena de valor de servicio)**
Estrategia del servicio	Plan
Diseño del servicio	Diseño y Transición
Transición del servicio	
Operación del servicio	Entrega y Soporte
Mejora continua	Mejora

Nota. Recuperado de *ITIL Service Lifecycle. In: Become ITIL Foundation Certified in 7 Days*.

Prácticas de ITIL V4. Son un grupo de recursos organizacionales que se han diseñado para realizar el trabajo y ayudar a la organización a proporcionar servicios de TI exitosos, estas se conocen como prácticas de ITIL. El objetivo de estas prácticas es mejorar el rendimiento de los servicios y cumplir con los contratos y acuerdos establecidos por la organización. (Remache Típan, 2022)

Las practicas utilizadas se pueden visualizar en la **Tabla 5.**

Tabla 5

Prácticas de ITIL V4

Practicas generales de gestión	**Prácticas de gestión de servicio de servicio**	**Practica de gestión técnica**
Mejora Continua	Gestión de la disponibilidad	Gestión de la implementación
Gestión de la seguridad de la información	Gestión de capacidad y rendimiento	Desarrollo y gestión de software
Gestión del portafolio	Seguimiento y gestión de eventos	
Servicio de gestión financiera	Gestión de lanzamiento	
Gestión de la estrategia	Gestión del catálogo de servicio	
Gestión de proveedores	Gestión de la configuración del servicio	
Mano de obra y gestión del talento	Diseño del servicio	
	Gestión del nivel de servicio	
	Servicio de validación y pruebas	

- **Gestión de la estrategia**

Esta es una práctica que asegura la alineación de los servicios de TI con los objetivos estratégicos de la institución. Incluye la identificación de necesidades de los servicios de TI, evaluación de opciones de servicios, y planificación y creación de una estrategia a largo plazo para proveer servicios de TI de alta calidad. Además, se monitorea y revisa periódicamente la estrategia para garantizar su relevancia y eficacia.

- **Servicio de gestión financiera**

Su objetivo principal consiste en evaluar y controlar los costes que están asociados a los servicios de TI de tal forma que se brinde un servicio de calidad a los clientes junto a un uso eficiente de los recursos.

Una actividad que ayuda a la gestión financiera es la realización de un inventario actualizado de los equipos que se encuentran en el área de TI, esto es proporcionado por el coordinador o encargado del área. Se debe tener en cuenta que en cuanto mayor sea la calidad de los servicios, mayor va a ser su costo, por lo que es muy de vital importancia evaluar cuidadosamente las necesidades del cliente y obtener un buen balance entre la calidad y el precio.

- **Gestión de la demanda**

La gestión de la solicitud del servicio tiene como objetivo primordial gestionar las solicitudes de los usuarios de manera eficiente y efectiva, brindando los servicios solicitados de manera oportuna y adecuada, y asegurando que los usuarios estén satisfechos con el resultado.

Entre las actividades que se llevan a cabo en la gestión de la solicitud se encuentran:

  - Registro y seguimiento de las solicitudes que entran al área.
  - Evaluación de la solicitud para comprobar que cumpla con los requisitos y políticas establecidas por el área.

- Priorización de las solicitudes de servicio en función de la importancia y urgencia.
- Escalamiento de las solicitudes de servicio cuando sea necesario.
- Coordinación con otros procesos de gestión de servicios para asegurarse de que las solicitudes se resuelvan de manera efectiva y eficiente.

- **Gestión del portafolio**

Esta es una práctica donde se muestran todos los servicios de TI con los que cuenta la organización, para el caso del presente proyecto el área ESPE-CERT, esto se lo hace con la finalidad de que el plan del servicio se adecúe y genere el máximo valor, mientras se administra los riesgos, costos y se gestión las inversiones de nuevos servicios y actualizaciones de servicios ya existentes.

La Gestión del Portafolio se vincula directamente con las siguientes prácticas del ciclo de vida:

- La gestión de financiera, que nos ayuda entender los costes del servicio que se está ofertando.
- La gestión del catálogo de servicios, la cual se encarga de presentar por completo el portafolio de servicios en una versión enfocada a los clientes.

- **Coordinación de diseño**

Esta práctica se encarga de organizar todas las tareas relacionadas con el diseño de servicios de TI. Es responsable de administrar el cronograma, los recursos y los problemas potenciales. También establece las normas y los procedimientos para el trabajo. El objetivo final es garantizar que el diseño se lleve a cabo de manera eficiente y se alcancen los objetivos establecidos.

- **Gestión del catálogo de servicios**

En esta actividad, el catálogo de servicios es visible para los clientes y es esencial para la empresa o institución, ya que ayuda a identificar los servicios proporcionados por el área, en el presente proyecto el área del ESPE-CERT. El ESPE-CERT se encargará de mostrar

los diferentes servicios disponibles y destacar su capacidad mediante la creación de un catálogo de servicios.

El catálogo de servicios ofrece una visión general de los servicios suministrados, cómo son entregados y utilizados, para qué finalidad y con qué nivel de calidad. El proceso es fácil, intuitivo y completamente claro.

- **Gestión del nivel de servicio**

La definición de los objetivos y la calidad de los servicios prestados, así como la documentación de estos, es el proceso mediante el cual se busca establecer un compromiso realista entre las necesidades y expectativas del cliente, mediante acuerdos necesarios con los clientes y proveedores para ofrecer los servicios requeridos (SLA) y alcanzar el nivel de servicio acordado.

- **Administración de suministros**

La administración de suministros se encarga de gestionar los proveedores y los servicios externos necesarios para el funcionamiento de una organización, incluyendo la identificación, selección, negociación, contratación y gestión de proveedores y servicios externos utilizados por la organización, con el objetivo principal de garantizar que los servicios externos cumplan con los requisitos de la organización y contribuyen al logro de los objetivos de negocio.

- **Gestión de la disponibilidad**

Esta es la práctica responsable de asegurar la continuidad e integridad de los servicios TI, cumpliendo con los niveles de disponibilidad establecidos en los acuerdos de nivel de servicio (SLA) y garantizando que los objetivos de disponibilidad de los servicios TI se cumplan de manera consistente.

- **Gestión de la capacidad y rendimiento**

En ITIL V4, la gestión de la capacidad y rendimiento se enfocan en asegurar que los servicios de TI sean capaces y tengan un rendimiento adecuado para satisfacer tanto las necesidades actuales como futuras del negocio y los usuarios.

- **Mano de obra y gestión del talento**

Se centra en la gestión del personal de TI dentro de una organización de servicios de TI. El propósito principal de este proceso es garantizar que la organización tenga suficiente personal con la capacitación y experiencia adecuadas para cumplir con los objetivos del negocio y las demandas de los usuarios.

- **Gestión de la continuidad del servicio**

Administrar la continuidad de los servicios de TI nos permita planificar y ejecutar los activos tecnológicos, esto con la finalidad de garantizar la disponibilidad de la información y que se cumplan los objetivos del área. Esta práctica también abarca la habilidad de mantener el funcionamiento del negocio en situaciones de emergencia o desastre.

- **Gestión de la seguridad de la información**

Esta práctica se trata de proteger la información que es necesaria para que la organización pueda llevar a cabo su negocio. Se relaciona en concreto con los daños resultantes de las fallas de confidencialidad, integridad y disponibilidad.

- **Plan de transición**

En esta etapa se describe cómo se va a realizar la transición de un servicio o su modificación, se toma en cuenta aspectos vistos en la planificación y diseño hasta su puesta en implementación y operación. El plan de transición incluye: las metas; las estrategias; los recursos y los procedimientos necesarios para ofrecer un servicio de la manera más eficaz. También se abarcan mecanismos para monitorear el progreso y asegurar que se cumplan los objetivos. Además, cuenta con procedimientos para la gestión de cambios y riesgos, y es esencial para garantizar una transición bien planificada y controlada.

- **Implantación**

En esta fase se pone en marcha los servicios, infraestructura, herramientas y procesos necesarios para cumplir con los objetivos establecidos en la estrategia de servicios TI. Incluye tanto la transición de los servicios existentes como la introducción de nuevos servicios. El proceso de implantación en ITIL se divide en varios subprocesos, que

incluyen planificación, diseño, construcción, pruebas, implementación y aceptación. Cada subproceso es esencial para garantizar que los servicios se entreguen de manera adecuada y se cumplan los objetivos establecidos.

- **Ejecución del lanzamiento**

Este el proceso en el cual se realizan actividades específicas descritas en el plan de implantación para implementar el nuevo servicio, infraestructura, herramienta. Se incluyen también la asignación de recursos, la supervisión del progreso, la realización de pruebas y la validación de los resultados. La ejecución del plan de implantación es responsabilidad del equipo de implantación y se lleva a cabo en colaboración con otros equipos y proveedores de servicios, como el equipo de operaciones, seguridad y soporte. La ejecución del plan debe ser monitoreada y evaluada para asegurar que se cumplan los objetivos de implantación y que se mantengan los estándares de calidad requeridos.

- **Procedimiento para la operación del servicio**

En esta primera etapa, se realiza la definición de cómo se va a operar el nuevo servicio por medio de procesos. Si ya se tiene una definición anterior, se utilizará dicha definición si tiene relación con el nuevo servicio, caso contrario, será necesario definirla para tener una guía estándar de cómo se debe operar el servicio.

- **Operación del servicio**

Se realiza la verificación del correcto funcionamiento del servicio, por medio de revisión de cada una de las funcionalidades prevista y definidas.

Es importante definir una bitácora en donde se tenga un registro de las pruebas que se han realizado y su respectivo resultado.

- **Evaluación del Servicio**

Se procede a realizar la evaluación del servicio por medio de instrumentos que permiten definir objetivos, preguntas y observaciones relacionadas a si se está obteniendo el comportamiento deseado de las funcionalidades del servicio. Los instrumentos utilizados

son el plan de investigación de campo, la evaluación técnica del servicio y el informe de evaluación.

- **Mejora continua**

Garantiza que los productos, servicios y prácticas de la organización sean flexibles ante las necesidades en constante cambio, y esto se logra al asegurar que los servicios de la organización estén alineados y mejorados en todas las fases de su prestación.

Estado del Arte

En el presente proyecto y con la finalidad de respaldar la instalación de un servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM), se realiza la búsqueda de información relevante, considerando las siguientes etapas, definición de preguntas de investigación, establecer estrategias de búsqueda, selección de estudios primarios o trabajos relevantes, evaluación de calidad y estrategia de selección. (Petersen, Feldt, Mujtaba, & Mattsson, 2008)

Planteamiento de la Revisión de Literatura Preliminar

Dentro de esta etapa para la revisión de literatura se debe realizar las siguientes actividades para determinar los parámetros adecuados para conocer el estado del arte: (1) definir la pregunta de investigación, (2) establecer la estrategia de búsqueda, (3) seleccionar los estudios primarios y evaluar su calidad, (4) definir la estrategia de extracción de datos. (Fernzandez, Insfran, & Abrahão, 2011)

Definir la Pregunta de Investigación

El objetivo del presente proyecto consiste en identificar información sobre cómo implantar un servicio de monitoreo (SIEM), por ello se plantean la siguiente pregunta de investigación: ¿Qué tan importante es contar con un servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en una institución académica? Debido a

que la pregunta de investigación es extensa, se propuso descomponerla en tres preguntas. La **Tabla 6** muestra las subpreguntas de investigación junto a su motivación.

Tabla 6

Subpreguntas de investigación

Ord	Subpregunta	Motivación
1	Q1. Problemas ocasionados por incidentes de seguridad relacionados a ataques informáticos.	Conocer los problemas que se pueden presentar tras sufrir un incidente de seguridad relacionados a ataques informáticos y como afectan estos a la prestación de servicios y la infraestructura en sí.
2	Q2. Cuáles son los requerimientos o requisitos técnicos y funcionales para la implementación de un SIEM.	Conocer cuáles son los requerimientos técnicos y funcionales (reglas y/o criterios) que se necesita para implementar de forma correcta un SIEM.
3	Q3. Soluciones Open Source de herramientas con capacidad de recolección de eventos y respuesta ante incidentes informáticos.	Descubrir las diferentes soluciones que existen para realizar el monitoreo de amenazas, recolección de eventos y brindar una respuesta apropiada.

Estrategia de Búsqueda

Las bibliotecas digitales que se usaron para la búsqueda de estudios primarios fueron: Google Scholar, IEEEXplorer y Science Direct, debido a su gran oferta de documentos de calidad enfocados al área de ingeniería y tecnología.

Para realizar una búsqueda en las bibliotecas digitales seleccionadas, se utilizaron cadenas de búsqueda, los detalles de la misma se encuentran en la **Tabla 7**. Se agruparon los términos de búsqueda en cuatro conjuntos y se consideró sus sinónimos, palabras

alternativas o relacionadas para formular una cadena de búsqueda, se puede evidenciar a detalle en la **Tabla 8**.

Conjunto 1: Definimos el alcance de la búsqueda institución o empresa

Conjunto 2: Términos relacionados con correlacionadores de eventos (SIEM), ITIL.

Conjunto 3: Términos de búsqueda relacionados con incidentes informáticos.

Conjunto 4: Terminamos relacionados a la implementación de un SIEM.

Tabla 7

Términos para las cadenas de búsqueda

Conjunto	Palabras	Palabras alternativas y/o relacionadas
1	Universidad	(CERT O empresa O institución)
2	Correlacionador de eventos	(SIEM O correlación de eventos)
3	Incidentes informáticos	(ataques O amenazas informáticas)
4	Soluciones	(Implementaciones open source)

Los conjuntos de búsqueda se aplicarán para las bases de datos de *Google Scholar*, *IEEExplorer* y *Science Direct.* Se han contemplado los estudios desde el año 2017 hasta el 2022.

Tabla 8

Cadenas de búsqueda

Base de datos	Cadena de búsqueda en español	Cadena de búsqueda en inglés
Google	("universidad") AND (“correlacionador de eventos” OR “SIEM") AND (“incidentes informáticos” OR “ataques	(“CERT” OR "university") AND (“event correlation” OR “SIEM") AND (“computer incidents OR

Base de datos	Cadena de búsqueda en español	Cadena de búsqueda en inglés
	informáticos”) AND (“solución” OR “open source” OR "software libre")	“computer attacks”) AND (“solution” OR “open source”)
IEEE	("Full Text & Metadata":universidad) AND ("Full Text & Metadata":correlacionador de eventos) OR ("Full Text & Metadata":SIEM) AND ("Full Text & Metadata":incidentes informáticos) OR ("Full Text & Metadata":ataques informáticos) AND ("Full Text & Metadata":solución)	("Full Text & Metadata":CERT) OR ("Full Text & Metadata":university) AND ("Full Text & Metadata":event correlation) OR ("Full Text & Metadata":SIEM) AND ("Full Text & Metadata":computer incidents) OR ("Full Text & Metadata":computer attacks) AND ("Full Text & Metadata":solution)
Sciense Direct	(“CERT” OR "universidad”) AND (“correlacionador de eventos” OR “SIEM") AND (“incidentes informáticos” OR “ataques informáticos”) AND (“solución” OR “open source” OR "software libre")	(“CERT” OR "university”) AND (“event correlation” OR “SIEM") AND (“computer incidents OR “computer attacks”) AND (“solution”)

Selección de Estudios Primarios y Evaluación de Calidad

Para la selección de los estudios primarios se utilizaron criterios de inclusión y exclusión que se presentan en la **Tabla 9**. Los estudios deben cumplir con al menos uno de los criterios.

Tabla 9

Criterios para la selección de estudios primarios

Ord.	Criterio	Descripción
1	Inclusión	Estudios que contienen información sobre amenazas de seguridad de la información.
2	Inclusión	Estudios que muestran información acerca de cómo implementar un SIEM o muestren la creación de reglas de un SIEM para una institución o empresa.
3	Inclusión	Estudios que presenten soluciones para mejorar el servicio de monitoreo de amenazas.
4	Exclusión	Artículos que no contengan temáticas de seguridad de la información.
5	Exclusión	Artículos que muestren únicamente recomendaciones.

Durante el proceso de inclusión y exclusión aparecen artículos dudosos que se pueden considerar como relevantes según el título y el *abstract*, posteriormente con la ayuda de los otros autores, se procede a revisar por completo los estudios descartados e identificar cuáles pueden ser añadidos como estudios primarios.

Estrategia de Extracción de Datos

La estrategia de extracción de datos se basa en proporcionar un conjunto de posibles respuestas a cada subpregunta de investigación planteada en la **Tabla 10**. Permite asegurar la aplicación de los mismos criterios de extracción de datos a todos los trabajos previamente seleccionados, facilitando su clasificación y evidenciando las posibles respuestas a cada subpregunta.

Tabla 10

Respuestas a cada subpregunta de investigación

Ord.	Subpregunta	Respuestas
1	Q1. Problemas ocasionados por incidentes de seguridad relacionados a ataques informáticos.	(a) Incidentes: si el documento explica cuáles son los incidentes más comunes que se dan en la organización, ya sea una institución o empresa. (b) Ataques informáticos: si se prestan las amenazas que pueden atacar el negocio.
2	Q2. Cuáles son los requerimientos o requisitos técnicos y funcionales para la implementación de un SIEM.	(a) SIEM: si el artículo indica: que es un correlacionador de eventos; cómo funciona; cuales son las distintas alternativas; como se establecen las reglas y cuales son requerimientos.
3	Q3. Soluciones *Open Source* de herramientas con capacidad de recolección de eventos y respuesta ante incidentes informáticos.	(a) Herramientas: si el documento presenta la implementación de un correlacionador de eventos SIEM y otras herramientas ayudan al monitoreo de amenazas. (b) Soluciones: si el artículo presenta un correlacionador de eventos SIEM en específico o muestra las distintas opciones disponibles en el mercado.

Resumen de Estudios Primarios

Implementación de un sistema de correlación de eventos basado en software libre para la empresa sistemas integrales de informática SISA S.A enfocado al área de SOC SISAMAX. (Becerra Acosta & Paramo Calderón, 2021)

En este trabajo de investigación, se identificó en el área de SISAMAX la ausencia de una herramienta que realice la recolección de eventos, que permita dar una respuesta acertada y oportuna con el fin de generar una reacción oportuna ante los incidentes de seguridad para así, minimizar los daños ante de este tipo de incidentes sin que se vean afectadas o amenazadas las operaciones del negocio. Se implementó el correlacionador de eventos Wazuh que es *Open Source* en un sistema operativo *Red Hat Enterprise* 8.4, además el trabajo presenta un anexo correspondiente a las especificaciones técnicas y de implementación necesarias para que Wazuh pueda ejecutarse de manera óptima. Con la implementación de la solución Wazuh, la institución pudo dar alcance a uno de los controles estipulados en su análisis de riesgos, de la misma forma pudo tener mayor visibilidad de los eventos en tiempo real de los activos más críticos para la compañía, permitiendo tomar decisiones más oportunas para generar acciones preventivas en caso de presentarse comportamientos anómalos.

Implementación de un correlacionador de eventos basado en software libre para la detección de ataques informáticos en la empresa eléctrica. (Pazmiño Gómez & Pazmiño Gómez, 2018)

En este trabajo de investigación, se llevó a cabo la implantación de un correlacionador de eventos basado en software libre para detectar ataques informáticos en la compañía eléctrica Riobamba S.A., ya que carecían de una solución centralizada para recopilar, almacenar y administrar los registros provenientes de los recursos de información. Se llevó a cabo un análisis comparativo entre diversas plataformas y se concluyó que la opción más adecuada es el sistema operativo *Security Onion*. Los resultados obtenidos consistieron en el total de ataques informáticos detectados por el correlacionador de

eventos, lo que permitió determinar que los principales tipos de ataques son la denegación de servicio y los ataques de fuerza bruta.

Plan de mejoramiento SIEM o Correlacionador de eventos de seguridad para el ministerio de educación nacional. (García Arias & Rodríguez Duarte, 2021)

En esta investigación se presenta la problemática que enfrenta el Ministerio de Educación Nacional en cuanto al manejo y administración de su SIEM. Se observan los principales inconvenientes en esta plataforma, como la definición limitada de los parámetros para la correlación de eventos de seguridad, la falta de auditabilidad, retención y parametrización de logs, lo que ocasiona una gestión ineficiente de las respuestas a los eventos e incidentes de seguridad. A través del levantamiento y clasificación de toda la red de infraestructura y de los recursos de información, se determinó la prioridad de correlacionar estos factores y se identificaron los dispositivos que proporcionan la mejor información de logs de seguridad, lo que hace que la SIEM sea más fácil de comprender y permite al analista aprender con mayor facilidad de la interfaz. El SIEM elegido para ser implementado en esta institución es FORTISIEM, una solución enfocada en la seguridad de la información que busca ofrecer un panel único de control para el centro de seguridad y operaciones de red.

Implementación de una solución "*Security Information and Event Mangement*" escalable y accesible basada en open source. (Bernal Barzallo & Mejía Broncano, 2021)

En el presente trabajo se realiza la implementación de una herramienta SIEM basada en *Open Source* para la gestión de incidentes de seguridad en PYMES. Como metodología para el desarrollo se utilizó el marco de trabajo Scrum y se estableció la metodología de investigación experimental por los procesos comparativos requeridos en entorno con y sin la solución planteada. Durante el desarrollo de la solución se utilizaron tecnologías como docker, docker compose, java, spring boot, elasticsearch, logstash, kibana, miro, gitlab entre otras. Como resultado se obtiene una herramienta *Open Source,* más asequible que las existentes en el mercado actual, capaz de detectar y notificar en menos de 60 segundos a partir del incidente el 100% de las anomalías en el

comportamiento de los servidores, así como identificar también posibles incidentes de seguridad basados en los comportamientos correlacionados de los diferentes orígenes de datos.

Implementación de un SIEM para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar ISO 27032. (Carrón Jumbo & Jumbo Vivanco, 2019)

Se llevó a cabo una investigación para el Comando de Ciberdefensa de las FF.AA. bajo las directrices del estándar ISO 27032, que busca mejorar la seguridad de las redes de sistemas. Para ello, se realizó un levantamiento de información que permitió evaluar los riesgos de la red, identificando los puntos vulnerables en la misma. Las especificaciones técnicas requeridas por el sistema SIEM implementado fueron evaluadas de acuerdo con las características basadas en la norma ISO 25000 de evaluación de calidad del software, en donde se determinó que el SIEM que mejor se ajusta a las necesidades es OSSIM. La implementación del SIEM permitió comprobar la hipótesis planteada, la cual establece que el sistema SIEM permite la detección automática y respuesta oportuna de las amenazas tecnológicas en tiempo real.

Implementación de un *security information and event management* –SIEM– en el comando de la armada nacional. Dirección de tecnologías de la información y las comunicaciones. (Fernández Granados, Herrera Kairuz, & Camilo García, 2017)

En este trabajo de investigación, se identificó que se requiere de un mecanismo de seguridad para la dirección de tecnologías de la información y las comunicaciones del Comando de la Armada Nacional, con el fin de correlacionar eventos de las diferentes plataformas y así tener una mayor visibilidad para proteger la información de los sistemas de comunicación e informáticos que se manejan al interior del comando. Se realizó una comparativa entre SIEM que sean *Open Source* en donde el que se ajustó más a los requerimientos fue MOZDEF, la cual incluye tres componentes dentro de su infraestructura ELASTIC SEARCH, LOGSTASH Y KIBANA. Con la herramienta implementada, se le facilitó a la Armada contar con un panel o *Dashboard* que presenta gráficamente los eventos que

les permiten a los administradores tomar datos estadísticos para tomar decisiones frente ataques informáticos.

Afinación de reglas en un SIEM para correlacionar los eventos de seguridad del laboratorio de redes convergentes del ITM. (Rivera Montoya & Perez Cataño, 2018)

En este proyecto lo que se busca es implementar un correlacionador de eventos SIEM apoyándose la infraestructura ya establecida con la que cuenta el laboratorio de redes convergentes del ITIM. Con el propósito de brindar un mecanismo de monitoreo eficaz de las distintas amenazas que pueden ocurrir en las instalaciones y equipos tanto físico como virtuales del laboratorio, el proyecto utiliza la herramienta OSSIM, ya que cuenta con una licencia *Open Source* y cumple con varios de los requisitos necesarios para gestión eventos de seguridad de los dispositivos que se encuentran conectados a la red; permite la recolección de logs, posee alertas sobres posibles vulnerabilidades, se puede configurar las reglas, entre otras funcionalidades. En este proyecto lo que se busca es implementar un correlacionador de eventos SIEM apoyándose la infraestructura ya establecida con la que cuenta el laboratorio de redes convergentes del ITIM. Con el propósito de brindar un mecanismo de monitoreo eficaz de las distintas amenazas que pueden ocurrir en las instalaciones y equipos tanto físico como virtuales del laboratorio, el proyecto utiliza la herramienta OSSIM, ya que cuenta con una licencia *Open Source* y cumple con varios de los requisitos necesarios para gestión eventos de seguridad de los dispositivos que se encuentran conectados a la red; permite la recolección de logs, posee alertas sobres posibles vulnerabilidades, se puede configurar las reglas, entre otras funcionalidades.

Implementación de un security information and event management -SIEM- en el comando de la Armada Nacional. Dirección de tecnologías de la información y las comunicaciones. (Herrera Kairul, Fernández Granados, & García Ruíz, 2017)

Este trabajo tiene como objetivo general la implementación de un SIEM (*Security Information and Event Management*) para la dirección de tecnologías de la información y comunicaciones del Comando de la Armada Nacional (“DITEL”), para esto se hará uso de herramientas de software libre o bajo costo que brinden un monitoreo en tiempo real de los

ataques a la infraestructura tecnológica, permitiendo advertir sobre su impacto y favorecer a la toma de decisiones por parte del área de ciberseguridad. También se determinarán los requerimientos técnicos necesarios para la implementación de un SIEM y se presentarán el nivel de impacto que tienen los ataques, esto por a través de categorías o aletas, bajas, medias y altas.

Implementación de un gestor de información y eventos de seguridad (SIEM) para la prevención y detección de ciber amenazas en una entidad gubernamental. (Játiva Alvarez & Muñoz Alvarez, 2022)

En esta investigación, se realiza un análisis preliminar del estado actual del sistema de información de la organización para luego realizar la implementación de un SIEM. La herramienta *Open Source* que se utiliza es OSSIM *AlienVault* que permite apoyar a la aplicación de lineamientos, directrices, procedimientos de control y seguimiento ante los incidentes informáticos que puedan ocurrir, también permite la detección de a través de medidas de monitoreo.

Capítulo III:

Fase 1: Plan, Diseño y Transición

Plan

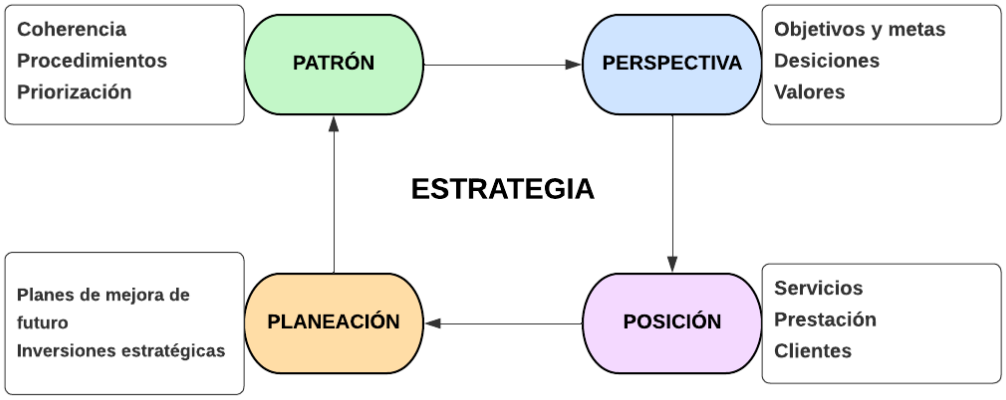
El plan del servicio es esencial para garantizar el éxito de un servicio, debido a que esta proporciona una estructura sólida y bien definida. Un buen plan es crucial, ya que es la base para las actividades posteriores de diseño y transición, entrega y soporte y mejora. En esta primera fase, lo que se busca es transformar el servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en un activo estratégico para el ESPE-CERT. Para lograr esto, es importante considerar varios aspectos clave: identificar las necesidades de negocio, evaluar las opciones de tecnologías disponibles, analizar el impacto en los procesos de negocio, definir indicadores de rendimiento, diseñar un plan de transición, capacitar al personal y monitorear y mejorar continuamente el servicio.

Gestión de la Estrategia

Para una eficiente estrategia del servicio a implementar, es importante contar con una perspectiva que determine correctamente los objetivos y decisiones que se deben adoptar, por lo cual es recomendable basarse en la 4P mostradas en la **Figura 7** debido a que de esta fase depende tener una base sólida para los siguientes procesos del ciclo de vida de ITIL.

Figura 7

Las 4P de Mintzberg



Perspectivas. Se requiere de una perspectiva en donde se definan claramente cuáles son las metas y valores, para lo cual se ha definido lo siguiente:

- Tener un monitor centralizado para la visualización de eventos de seguridad;
- Ayudar a reducir el tiempo de solución de incidentes de seguridad;
- Definir los SLA (acuerdos de nivel de servicio) para ofrecer un servicio más confiable y actuar en base a los tiempos establecidos con el cliente en caso de que no se cumpla un SLA;
- Capacitar al personal para que realice un manejo correcto del nuevo servicio.
- Brindar alertas en tiempo real para que el equipo de respuesta ante incidentes Informáticos actúe de manera oportuna y eficaz;
- Realizar la implementación del nuevo servicio de una manera estructura y correcta con el fin de poder brindarlo a otras instituciones educativas.

Planificación.

Promoción de los Servicios de Monitoreo de Amenazas Para el ESPE-CERT. El servicio de monitoreo de amenazas se encuentra orientado a aportar a los miembros trabajadores del ESPE-CERT que necesiten establecer alertas, recopilar logs para el correcto el funcionamiento de los sistemas y equipos informáticos.

Para esto es importante que el personal del área del ESPE-CERT se encuentre correctamente capacitadas para poder ayudar y solventar cualquier inquietud o eventualidad que ocurra con la implementación o funcionamiento.

Estrategias e iniciativas.

Tabla 11

Estrategias e Iniciativas

Estrategias	**Iniciativas**
Provisión de recursos	• Adquisición e instalación de la herramienta para brindar el servicio de monitoreo. • Reestructuración del portafolio de servicios del ESPE-CERT.
Aumentar eficiencia	• Automatizar los procesos manuales. • Plataforma central para la visualización de eventos de ciberseguridad.
Operación recursos	• Capacitaciones al personal encargado del área del ESPE-CERT. • Ahorro de recursos financieros al utilizar una herramienta de software libre.
Mejora de servicio	• Establecer y cumplir con los SLA • Reducción de tiempos en la solución de incidentes.

Reporte de estadísticas. En base a los reportes que se pueden generar con el nuevo servicio a implementar, las estadísticas más importantes que se van a mostrar por medio de reportes son los siguientes:

- Cantidad de eventos enviados al servicio para ser analizados
- Cantidad de eventos procesados y descartados
- Colas usadas
- Evolución de la cantidad de alertas
- Cantidad de eventos basados en Syscheck, Syscollector y Rootcheck.
- Agentes más activos

Ubicación de los recursos. Se utilizarán los recursos otorgados por el ESPE-CERT, en donde se realizará la instalación del nuevo servicio. A continuación, se describen los aspectos más importantes a considerar:

- El servicio de monitoreo se instalará en el servidor CentOS 7, el cual está conectado a la red del ESPE-CERT;
- La persona que opere en el área del ESPE-CERT será la encargada de visualizar la información centralizada proporcionada por el SIEM una vez que se termine de implementar, mientras tanto, los encargados de instalar el servicio, serán los que deban visualizar la información generada;
- El acceso al monitor para la visualización de los eventos de seguridad y parámetros establecidos, se realizará mediante acceso a navegadores web.

Posición. El ESPE-CERT es un equipo de respuesta ante incidentes informáticos de carácter académico y de investigación en ciberseguridad y ciberdefensa, orientado al dominio principal de la Universidad de las Fuerzas Armadas ESPE, que busca satisfacer con calidad, excelencia y ética científica los requerimientos de su comunidad objetivo, con base en tecnología de avanzada, autonomía financiera y personal técnico altamente calificado y especializado en ciberseguridad. Se proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que mejora la seguridad de estos sistemas.

Patrón. Para establecer el patrón de priorización de atención a los sensores en base a un servicio, se utiliza la siguiente formula: $P = I \times U$

- P= prioridad
- I= Impacto (determina la importancia de la incidencia dependiendo de cómo ésta afecta a los procesos de negocio y/o del número de usuarios afectados).
- U= Urgencia (rapidez con la que el negocio necesita una solución).

Tabla 12

Patrón de priorización de atención a los sensores

	Urgencia	**Impacto**	**Prioridad**
Registro de incidente se seguridad	Alta	Critico	1
Intrusiones detectadas	Alta	Alto	2
Vulnerabilidades detectadas	Media	Alto	3

Servicio de Gestión Financiera

La gestión financiera para proyectos de investigación desarrollados dentro del ESPE-CERT es una responsabilidad clave del director del proyecto. En este proceso, el docente o investigador encargado elabora una propuesta con un presupuesto detallado de los recursos necesarios para llevar a cabo el proyecto. La propuesta, una vez finalizada, es presentada al consejo del departamento para su aprobación. Luego, la propuesta es enviada a la Unidad de Gestión de la Investigación (UGIN) para ser evaluada por expertos y, finalmente, una vez recibida todas las aprobaciones necesarias, se le asigna el presupuesto solicitado al proyecto para su ejecución. Es importante mencionar que este proceso de gestión financiera es un ciclo continuo, ya que se revisa y se adapta según las necesidades del proyecto.

Gestión de la Solicitud de Servicio

Para conocer cómo se gestiona la solicitud de un servicio y realizar esta tarea se lleva a cabo una consulta con el personal encargado del área de ESPE-CERT y gracias a la colaboración de ingeniero Marco Bonilla se logró determinar que la gestión de la demanda se la realiza de la siguiente manera:

a. El departamento de UTIC recibe la solicitud, por ejemplo: realizar un análisis de vulnerabilidades. Esta solicitud puede ser enviada de diferentes áreas, inclusive desde diferentes sedes de la universidad.
b. Las UTIC solicitan al área del ESPE-CERT que realice un “análisis de vulnerabilidades”
c. El ingeniero encargado recibe la solicitud, confirma los datos del pedido y realiza una prueba de conexión mediante comandos en terminal. En caso de que no exista conexión, se pone en contacto con el responsable del equipo para comprobar lo sucedido.
d. En caso de que el equipo se encuentre en otra sede universitaria, el ingeniero encargado se pondrá en contacto con el personal de UTIC para solicitar un permiso temporal y tener acceso a una IP que se encuentra fuera de la sede principal.
e. Comprobada la conexión con el equipo se procede a realizar el análisis de vulnerabilidades.
f. Se redacta un reporte de las vulnerabilidades encontradas junto con su posible solución.

Gestión del Portafolio

El área del ESPE-CERT posee el siguiente portafolio de servicios:

Tabla 13

Servicios ofertados por el ESPE-CERT

Ord.	Servicio	Estado Actual	Definición
1	Gestión de incidentes	En implementación	Se encarga de restablecer los servicios lo más pronto posible para minimizar el daño que pueda tener la institución o empresa.
2	Análisis de vulnerabilidades	Implementado	Se generan informes donde se identifican, clasifican y priorizan las debilidades o fallos de seguridad de la institución o empresa.
3	Monitoreo y alerta de primer nivel	Implementado	Consiste en un servicio de monitoreo que indica cuando un evento puede producirse y afectar al equipo.
4	Asesoramiento técnico y consultoría	En implementación	Ayuda a resolver procesos relacionados con los aspectos técnicos de las TIC.
5	Firma electrónica	Implementado	Se encarga de garantizar la autenticidad e integridad y confidencialidad de los

Ord.	Servicio	Estado Actual	Definición
			documentos o transacciones en Internet.
6	Hacking ético	En implementación	Consiste en un servicio para realizar intrusiones de manera controlada sobre un sistema informático.

Diseño

Diseño del Servicio

Se coordinó con la Unidad de Seguridad Integrada (USIN) un acuerdo de confidencialidad sobre la información a la que se va a acceder, evitando así la fuga o el mal uso de la información y que se generen posibles brechas de seguridad. También se coordinó con el personal del ESPE-CERT una guía acerca de su infraestructura y servicios disponibles, esta información resulta de utilizada para poder seleccionar el equipo más adecuado en el cual se va a implementar el servicio de monitoreo de amenazas.

Gestión del Catálogo de Servicios

El catálogo de servicios tiene como finalidad mostrar información precisa a los usuarios acerca de los servicios activos con lo que se cuenta dentro del área del ESPE-CERT.

Propuesta del Catálogo de Servicios

El catálogo de servicios se encuentra organizado de la siguiente forma:

- Categoría: hace referencia a la clasificación del tipo de servicio que se está ofertando por parte del ESPE-CERT.

- Aplicación o servicio: son todos los servicios que ofrece el ESPE-CERT y esta relacionados al monitoreo de amenazas.
- Prioridad:
  - Alta (3): son aquellos requerimientos que cuya resolución no admite demoras y deben ser atendidos antes que otros.
  - Media (2): son aquellos requerimientos que se atienden en serie por orden de llegada.
  - Baja (1): son los requerimientos que tiene una baja prioridad y se atienden por orden de llegada. Se le puede asignar periodos de tiempo para ser solucionados.

En la **Tabla 14** se muestra el Catálogo de Servicios con el que se al disponer de un servicio de monitoreo de amenazas mediante un (SIEM):

Tabla 14

Catálogo de servicios - SIEM

Categoría	**Aplicación o servicio**	**Prioridad**
Software	Monitoreo de amenazas	3
	Gestión de incidentes	3
	Análisis de vulnerabilidades	2
	Alertas de intrusión	3
	Recopilación de Logs	1

Gestión de los Niveles de Servicio

El área del ESPE-CERT busca ofrecer servicios de buena calidad, y para llevar a buen término esta actividad, se debe considerar la infraestructura y redes con las que cuenta. Teniendo en cuenta que se pueden realizar reinicios programados en el servidor o

puede existir la posibilidad de que se corte la corriente eléctrica, además de fallos inesperados provocados por otros servicios o por un operador, se estableció que el servicio tendrá un SLA del 95%. En la **Tabla 15**, se puede visualizar cuanto tiempo puede estar fuera de servicio en un periodo de tiempo.

Tabla *15*

Periodos fuera de servicio en base al SLA establecido

Periodo	**Tiempo fuera de servicio**
Diariamente	1 hora 12 minutos
Semanalmente	8 horas 24 minutos
Mensualmente	1 día 12 horas
Anualmente	18 días 6 horas

Gestión de la Seguridad de la Información

El área del ESPE-CERT debe proteger los tres pilares de la seguridad, los cuales son: confidencialidad, integridad y disponibilidad. Debe velar por mantener la información segura, sin modificaciones de terceros y disponible para la organización con la finalidad de que sea utilizada únicamente por personas capacitas y autorizadas, es señal de un compromiso con la calidad y responsabilidad. Una manera de ayudar a la seguridad de la información es identificando las posibles vulnerabilidades que puedan manifestarse y afectar a la calidad del servicio. Esta información tiene que ser reserva y solo estar disponible para personas capacitadas y autorizadas. Los factores que el ESPE-CERT tiene que tener presente para la gestión de seguridad de la información se encuentran en la siguiente tabla.

Tabla 16

Factores de la seguridad de la información

Confidencialidad	Integridad	Disponibilidad
Proteger la información del acceso no autorizado y el uso indebido. La mayoría de los sistemas de información albergan información que tiene cierto grado de sensibilidad.	Proteger la información de alteraciones no autorizadas. Estas medidas garantizan la exactitud y la integridad de los datos.	La información debe estar disponible para los usuarios autorizados. Las medidas de disponibilidad protegen el acceso oportuno e ininterrumpido al sistema.

Gestión de Proovedores

El ESPE-CERT cuenta con los suplementos necesarios para realizar las pruebas o gestiones que se requieran, a continuación, se listan algunos de los sumisitos que se requieren para llevar a cabo de manera correcta la implementación del servicio:

- Se cuenta con papel suficiente para realizar las respectivas impresiones para el caso que se requieran imprimir informes o indicadores generados;
- Se cuentan con computadores en el laboratorio para realizar pruebas de conectividad y verificar si se puede acceder a la pantalla de monitorio por medio de la dirección IP;

Gestión de la Disponibilidad

El ESPE-CERT tiene como prioridad que sus servicios ofertados estén disponibles de manera ininterrumpida y de manera fiable, ya que estos están relacionados al monitoreo y aletas de seguridad dentro del área, por lo cual es primordial que los servicios estén funcionando las 24 horas del día.

En la **Tabla 17**, se puedo observar la administración de la disponibilidad para el nuevo servicio a ofertar:

Tabla 17

Administración de la disponibilidad

Servicio	**Disponibilidad**	**Usar cuando**
Monitoreo de amenazas	Para todos los servicios, 24/7 mientras el servidor esté en funcionamiento.	Se presenten alertas de seguridad en los sensores monitoreados
Gestión de incidentes		Se corta un servicio, se trata de reestablecerlo lo más pronto posible para que el daño sea mínimo
Análisis de vulnerabilidades		Se realizan actualizaciones en los activos, existen cambios de personal, se ingresan nuevos activos, si un equipo presenta error por malware, entre otros.
Alertas de intrusión		Se generan intrusiones en los sensores que están siendo monitoreados
Recopilación de Logs		Se requiere centralizar las alertas y actividad generadas por los sensores

Mano de Obra y Gestión de Talento Humano

El área del ESPE-CERT se encuentra orientado a un aspecto académico por lo que la mano de obra la proporcionan los miembros docentes del ESPE-CERT y los estudiantes de grado (pasantes de investigación y tesistas de pregrado). A continuación, se describen los aspectos más importantes de la gestión de talento humano:

- Recursos humanos: el ESPE-CERT cuenta con el suficiente personal para que el servicio pueda ser utilizado de manera eficiente, además de que se monitoreen las alertas e indicadores generados frecuentemente. En la **Tabla 18** se puede observar, tanto personal investigador como operador, que se encuentra activo, cabe mencionar que, en primera instancia, los estudiantes de grado serán los principales operadores del servicio, designando este rol a futuro al resto del personal una vez impartidas las respectivas capacitaciones:

Tabla 18

Personal del ESPE-CERT

Personal	**Departamento**
Walter Marcelo Fuertes Díaz	Ciencias de la Computación
Enrique Vinicio Enrique Carrera	Eléctrica y Electrónica
Freddy Mauricio Tapia León	Ciencias de la Computación
Luis Lenin Recalde Herrera	Seguridad y Defensa
Alberto Daniel Núñez Agurto	Ciencias de la Computación, Sede Santo domingo de los Sáchilas
Mario Bernabé Ron Egas	Ciencias de la Computación
Henry Omar Cruz Carrillo	Energía y Mecánica – Director UGI

Personal	Departamento
Mag. Andrés Castillo/ Mag. Rommel Asitimbay	Unidad de Tecnologías de la Información
Ing. Jonathan Benavides	Contrato Ocasional, Operador ESPE-CERT
CRNL. EM. Robert Vargas B.	COCIBER
Ing. Marco Antonio Bonilla Vergara	Ciencias de la Computación
Estudiantes de grado (pasantes de investigación y tesistas de pregrado)	Ciencias de la Computación

Gestión de la Capacidad y Rendimiento

Como parte de los recursos tecnológicos, el nuevo servicio va a ser implementado en un servidor Asus con las siguientes características tecnológicas: Asus Intel X79, 16 Gb RAM, 1Tb HDD - 120 Gb HDD. Como es notable, el servidor cuenta con una amplia gama de recursos, además de una gran cantidad de espacio de almacenamiento, en donde al momento de instalar el servicio, no se compromete el espacio en disco ni se satura el uso del resto de recursos. Es importante indicar que el espacio en disco utilizado por los demás servicios implementados previamente en el servidor es de 45 Gb, el uso de memoria RAM es de aproximadamente del 82% y de la memoria SWAP del 28%, y el uso del procesador oscila en un rango de 15 – 25%.

Gestión de la Continuidad del Servicio

Para la continuidad del nuevo servicio a implementar ante posibles siniestros, es necesario analizar los siguientes procedimientos:

- Proactivos: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.

- Reactivos: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

Para la recuperación del servicio en caso de que este sea interrumpido, se determinó la opción de *cold standby,* la cual determina que se requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas. Para el caso en que se presente una interrupción en la energía eléctrica, el piso en el que se encuentra el ESPE-CERT, que corresponde al H-402, cuenta con un UPS activo el cual proporcionará la energía eléctrica a los servidores para que estos puedan seguir funcionando sin problemas. Para el caso en el que el servidor presente algún error y su funcionamiento se vea comprometido, se deberá reiniciar el servicio mediante comandos haciendo uso de la terminal del servidor, si esto no fuese suficiente y el servicio dejase de funcionar por completo, se tiene un amplio conocimiento sobre los comandos y configuraciones necesarias para instalar lo más pronto posible el servicio y este vuelva a monitorear los sensores. Se estima que el volver a instalar el servicio, se requiere un periodo aproximado de 24 horas.

Transición

Gestión de Lanzamiento

Objetivos

- Preparar el servidor para la implantación del nuevo servicio
- Implantación del nuevo servicio siguiendo la guía de instalación de los componentes en base a la documentación oficial de Wazuh
- Enrolar los sensores al SIEM para que se pueda iniciar su monitoreo.
- Monitorear los eventos de seguridad que se presenten en los sensores conectados y tener una *dashboard* centralizado para visualizarlos.

Alcance

La implementación del servicio de monitoreo de amenazas mediante un correlacionador de eventos para el ESPE-CERT del DCCO, tiene un plazo aproximado de 2 semanas desde el comienzo de la transición para encontrarse en operación y estar listo para brindar servicio al área del ESPE-CERT. La fase transición estará finalizada cuando el servicio de monitoreo se encuentre correctamente instalado en el servidor CentOS y los demás equipos que funcionan como sensores.

Indicadores de cumplimiento

- Disponibilidad del servicio en términos de porcentaje.
- Puntualidad en la entrega.
- Cumplimiento de las condiciones establecidas en acuerdos previos.
- Tasa de errores o fallos.

Tareas a realizar

En la **Tabla 19,** se puede visualizar la planificación de las tareas a realizar para implementar el nuevo servicio.

Tabla 19

Tareas planificadas para la gestión de lanzamiento

Tarea	**Responsable**	**Duración**	**Inicio**	**Fin**
Preparación del servidor para la instalación	Bryan Meza Eduardo Cruz	1 día	11-01-2023	11-01-2023
Instalación del SIEM en el servidor del ESPE-CERT	Bryan Meza Eduardo Cruz	2 días	12-01-2023	13-01-2023

Tarea	Responsable	Duración	Inicio	Fin
Instalación de software necesario en los sensores del ESPE-CERT	Bryan Meza Eduardo Cruz	2 días	16-01-2023	17-01-2023
Evaluación del nuevo servicio	Bryan Meza Eduardo Cruz	2 día	18-01-2023	19-01-2023

Gestión de Implementación

Recursos

Equipo encargado del proyecto

- Bryan Meza – Estudiante
- Eduardo Cruz – Estudiante
- Ing. Mario Ron – Tutor

Materiales, equipos e instalaciones

- Servidor CentOS 7
- Memoria RAM de 16 Gb
- CPU con 16 núcleos (*cores)*
- Almacenamiento de 1Tb HDD - 120 Gb HDD
- Equipos del ESPE-CERT

Conocimiento

- Revisión de documentación oficial, foros oficiales y problemas reportados sobre el procedimiento de instalación y uso de Wazuh.
- Revisión de comandos básicos de CentOS 7.

Software requerido

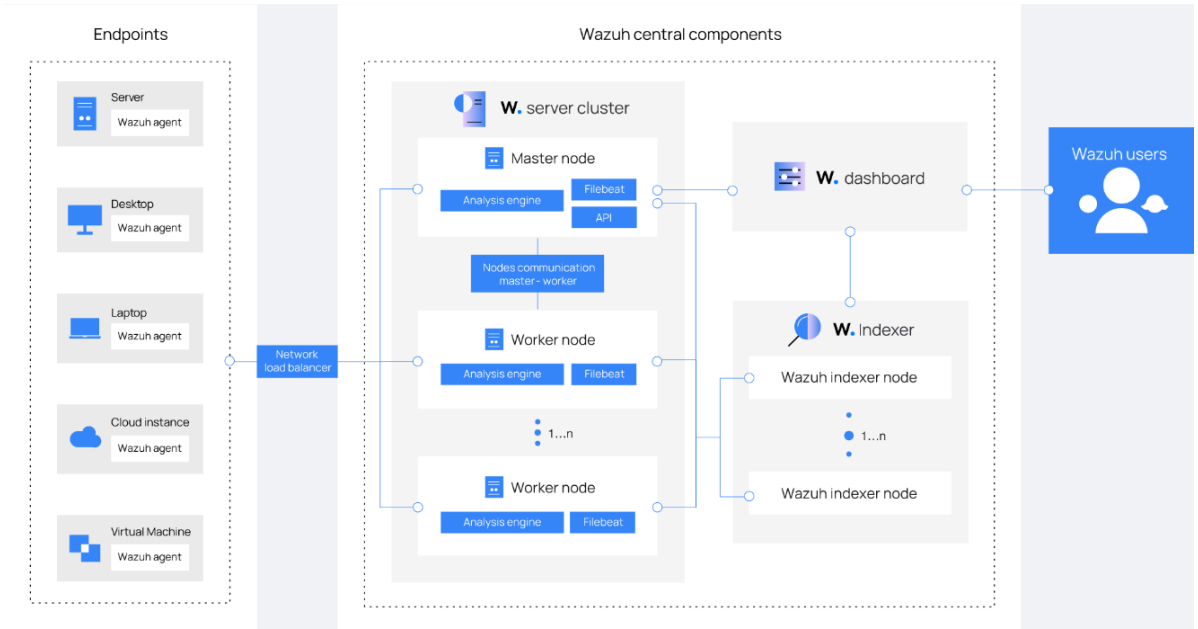
En la **Figura 8**, se presenta la arquitectura de Wazuh, la cual está conformada por tres componentes centrales los cuales serán instalados en el orden en que se presentan a continuación:

- *Wazuh indexer:* es un motor de análisis y búsqueda de texto, indexa y almacena las alertas generadas por el servidor Wazuh.
- *Wazuh server cluster:* analiza los datos generados por los agentes y los procesa a través de decodificadores y reglas, utilizando inteligencia de amenazas para buscar indicadores de compromiso (IOC) conocidos.
- *Wazuh dashboard*: interfaz de usuario web para la visualización y el análisis de datos.

También tenemos los *endpoints,* en donde ser realizara la instalación de *Wazuh Agent* para que se puedan enrolar con el servidor de Wazuh.

Figura 8

Arquitectura de Wazuh



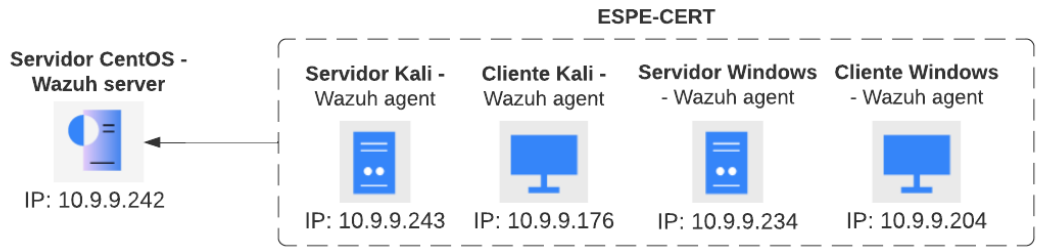
Nota. En el gráfico se presenta la arquitectura tradicional de Wazuh, en donde se visualizan sus componentes y *endpoints.* Tomado de *Wazuh architecture,* por Wazuh Inc., 2022.

Definición de topología

En la **Figura 9**, se definió la topología en donde constan los agentes (sensores) con sus respectivos sistemas operativos y direcciones IP, cabe indicar que todos estos equipos se encuentran dentro del ESPE-CERT y enviaran los datos al servidor CentOS, el cual contendrá al SIEM Wazuh.

Figura 9

Topología definida para el nuevo servicio



Ejecución del Lanzamiento

Verificación del hardware

La instalación de Wazuh posee ciertos requisitos para su correcto funcionamiento, uno de ellos es que su instalación se realice en un sistema operativo Amazon Linux 2 o CentOS 7 u 8. Para el hardware, se requieren las siguientes especificaciones:

- Mínimas: 4 Gb de memoria RAM y 2 cores de CPU
- Recomendadas: 16 Gb de memoria RAM y 8 cores de CPU

En cuanto al espacio de almacenamiento a utilizar, este se estima en base a las alertas generadas por segundo (APS) y cada 90 días:

- Servidores: con 0.25 de APS se generan 3.7 Gb
- Estaciones de trabajo: con 0.1 de APS se generan 1.5 Gb
- Dispositivos de red: con 0.5 de APS se generan 7.4 Gb

A manera de ejemplo para el almacenamiento, si se tuviera un entorno con 80 estaciones de trabajo, 10 servidores y 10 dispositivos de red, el almacenamiento necesario para 90 días es de 230 GB.

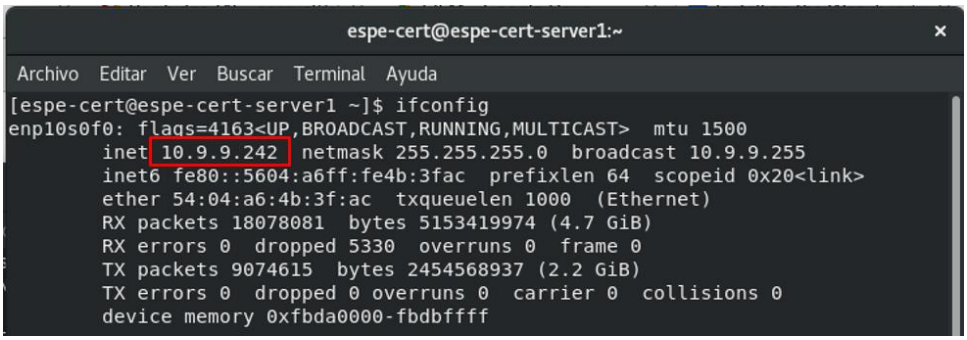
En base a los requisitos especificados anteriormente, se puede determinar que, si es factible realizar la instalación de Wazuh en el servidor, ya que como se describió en la fase diseño, este si posee las características necesarias para que se puede ejecutar eficientemente Wazuh.

Implantación de la herramienta en el servidor

Como primer paso, se realizó una verificación de que el servidor esté conectado adecuadamente a la red y que disponga una dirección IP, esto se logra haciendo uso del comando *ifconfig*. Además, es importante obtener la dirección IP para configuraciones posteriores.

Figura 10

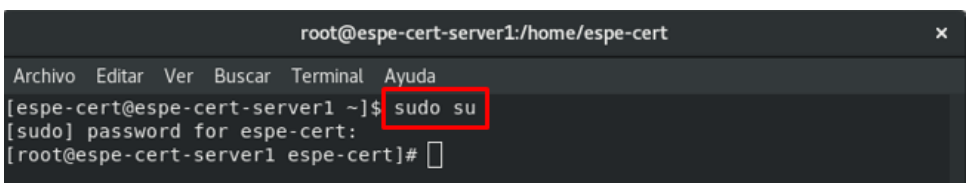
Obtención de la IP del servidor



Se debe ejecutar el comando sudo su para poder realizar la ejecución de los instaladores con privilegios y no tener problemas durante el procedimiento.

Figura 11

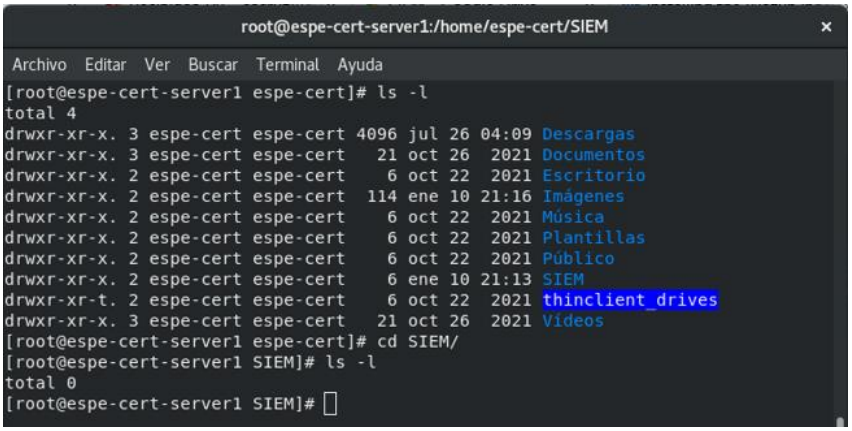
Comando sudo para ejecutar programas con los privilegios



Se creó un directorio dedicado a la instalación del nuevo servicio, el cual tiene como nombre SIEM, en la **Figura 12** se puede observar dicho directorio y el ingreso al mismo para realizar la descarga de los elementos necesarios.

Figura 12

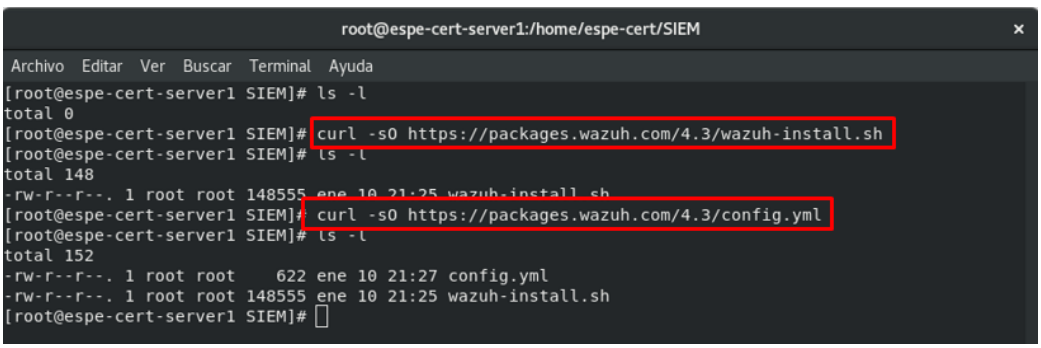
Creación de directorio SIEM



A continuación, se presenta el procedimiento de implantación de Wazuh, para lo cual se realizará primero la instalación de *Wazuh indexer*. Cabe mencionar que existen dos maneras de instalar los componentes, que son mediante el asistente de instalación de Wazuh o una instalación paso a paso. Para nuestro caso, se hizo uso del asistente de instalación ya que es una forma mucho más rápida y con menos configuraciones para realizar la instalación de todos los componentes. A continuación, se procede a descargar el asistente de instalación y el archivo de configuración haciendo uso de los comandos presentados a continuación.

Figura 13

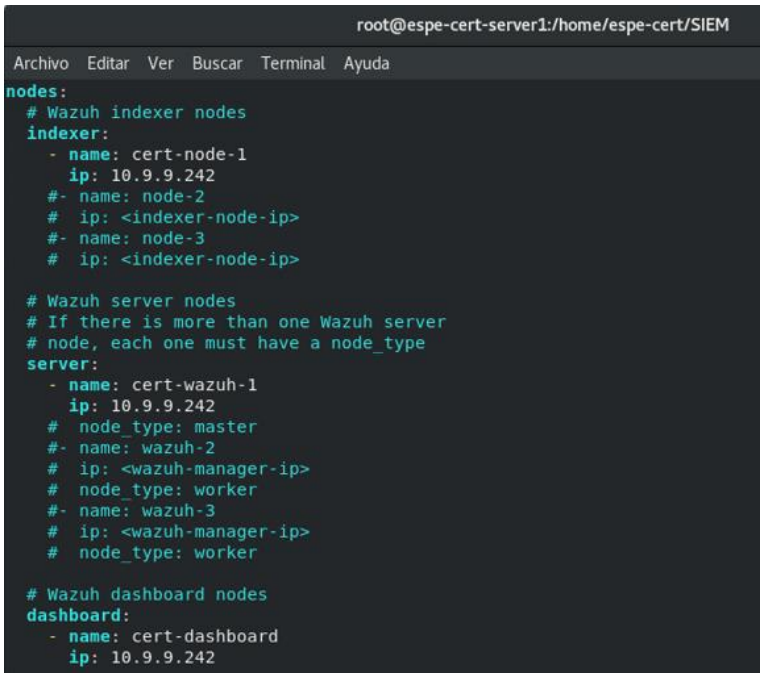
Uso de cURL para descargar el asistente y archivo de configuración



Se debe ingresar al archivo *config.yml* y se ingresa un nombre para el *indexer*, el servidor y el *dashboard.* Así mismo, se coloca la dirección IP en cada nodo, para este caso es la dirección IP de servidor CentOS obtenida en pasos anteriores. También es importante mencionar que, al no ser un entorno distribuido con múltiples nodos, es necesario ingresar el nombre e IP solamente de un nodo.

Figura 14

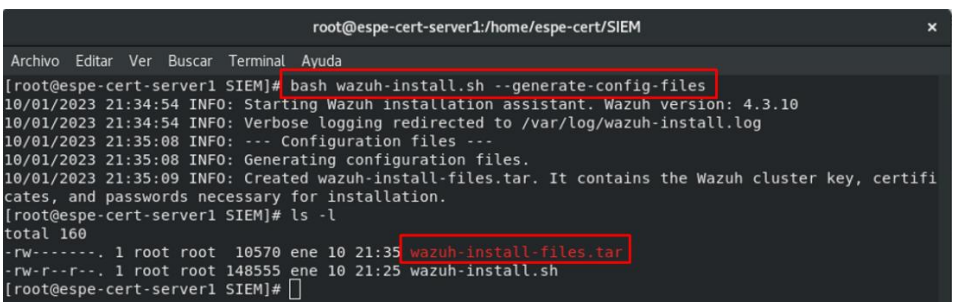
Configuración de config.yml



Se procede a ejecutar el asistente de instalación con la opción *--generate-config-files* para generar la llave de *cluster,* certificados y contraseñas necesarias para la instalación. Los archivos mencionados pueden ser encontrados en *wazuh-install-files.tar*.

Figura 15

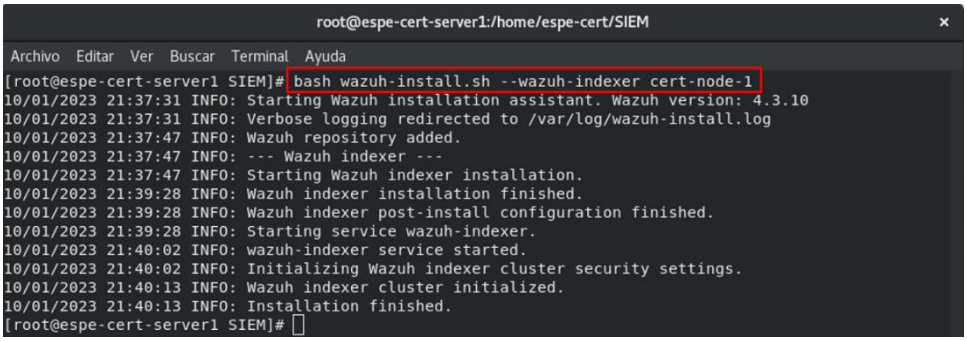
Generación de archivos de configuración



Se ejecuta el asistente con la opción *--wazuh-indexer* y el nombre de nodo establecido en el archivo *config.yml,* que para este caso será cert-node-1.

Figura 16

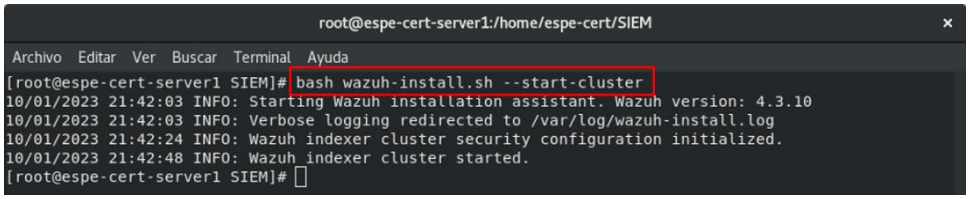
Instalación del nodo cert-node-1



Se ejecuta el asistente de instalación con la opción *--start-cluster* en el servidor para cargar los nuevos certificados de información e iniciar el *cluster*.

Figura 17

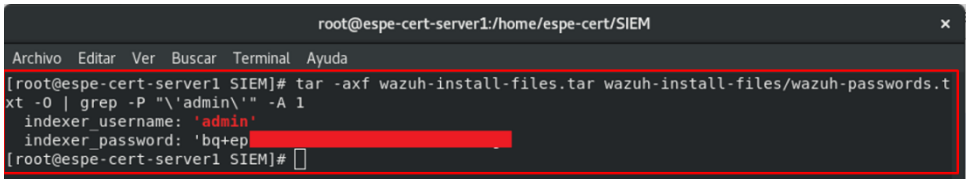
Inicialización del cluster



Una vez que se está en ejecución *Wazuh indexer*, se realizara un test para saber si se instaló de manera correcta. Para ello, se ejecuta el siguiente comando con el cual se obtiene la clave del usuario administrador.

Figura 18

Obtención de clave de admin

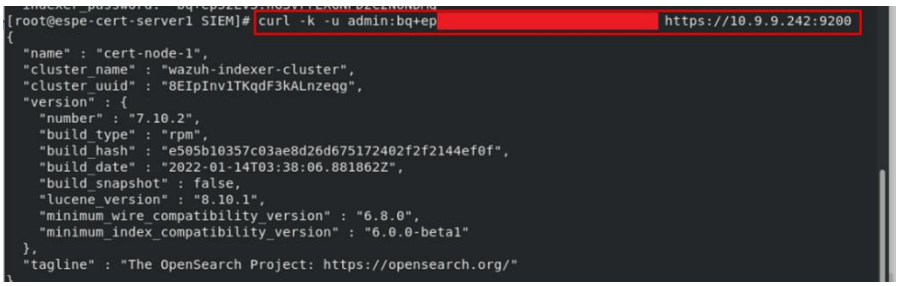


Se debe ejecutar el siguiente comando para confirmar que la instalación fue satisfactoria. Se agrega la IP del servidor y la clave obtenida en el paso anterior. Como se

observa en la **Figura 19**, se obtuvo una respuesta correcta, indicando que *Wazuh indexer* se está ejecutando.

Figura 19

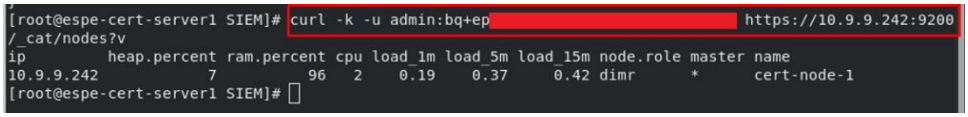
Verificación de instalación del indexador



Se procede a ejecutar el siguiente comando haciendo uso de la IP y clave para verificar si el *cluster* está trabajando adecuadamente.

Figura 20

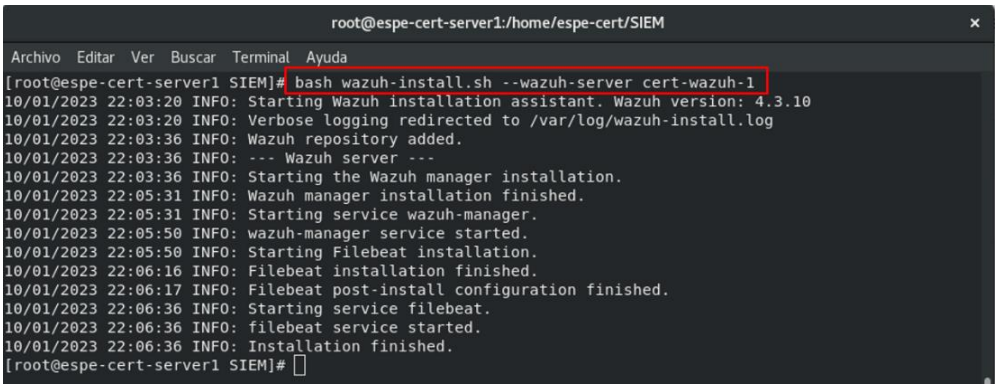
Verificación de ejecución



Una vez instalado y comprobado que está funcionando correctamente *Wazuh indexer*, se procede a realizar la instalación de *Wazuh server*. Para ello, se ejecuta el asistente con la opción *--wazuh-server* seguido del nombre del nodo establecido para el servidor, que para este caso es cert-wazuh-1.

Figura 21

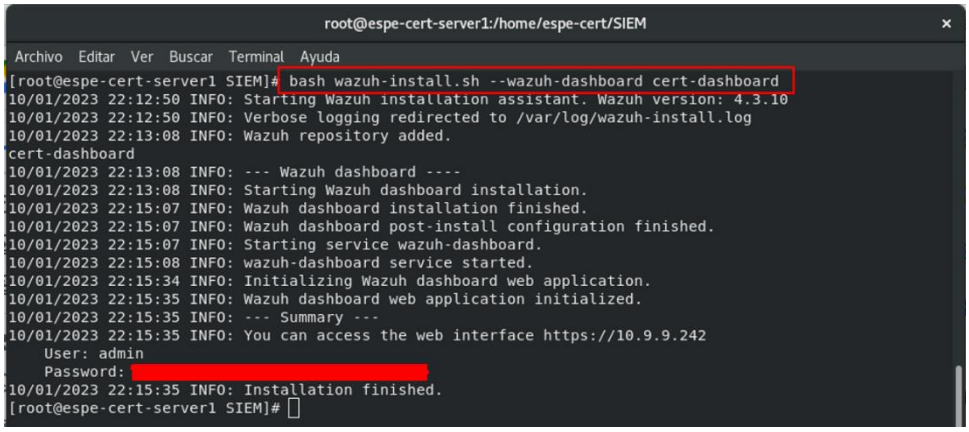
Instalación de Wazuh server



Con la instalación del indexador y el servidor, el ultimo componente a instalar será el *dashboard*, para lo cual se ejecuta el asistente con la opción *--wazuh-dashboard* y el nombre del nodo establecido, para este caso es *cert-dashboard.* Al ejecutar el comando, se obtiene la contraseña de administrador para poder ingresar por medio la interfaz web.

Figura 22

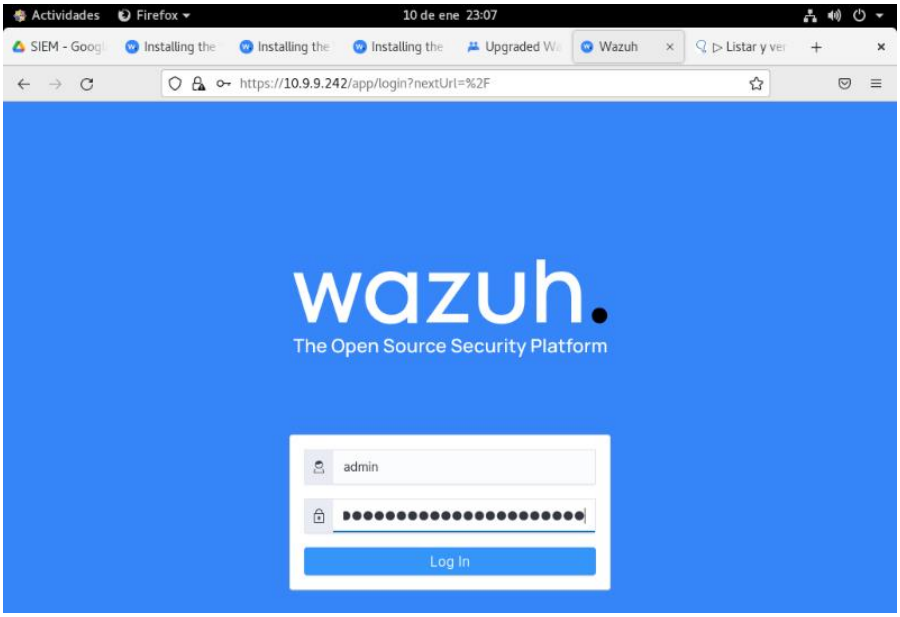
Instalación de Wazuh dashboard



Con el nombre de usuario y contraseña generadas en el paso anterior, ahora es posible acceder a la URL indicada para ingresar a la interfaz web de Wazuh, en donde pondremos los datos obtenidos para ingresar a la plataforma central.

Figura 23

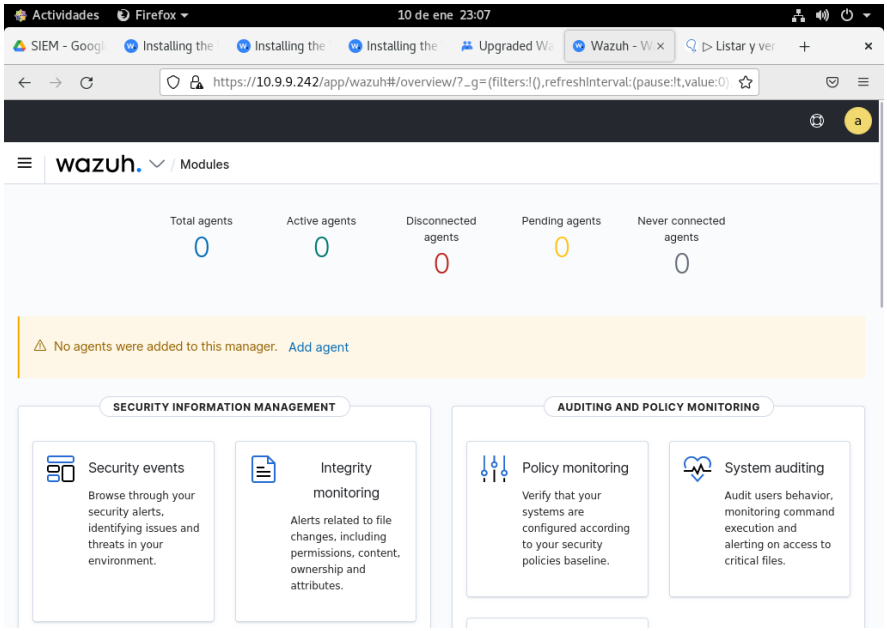
Interfaz web de Wazuh



Al dar clic en el botón de Log in, se pude observar que se ingresa a la pantalla principal de Wazuh, lo cual nos indica que todos los componentes están funcionando correctamente.

Figura 24

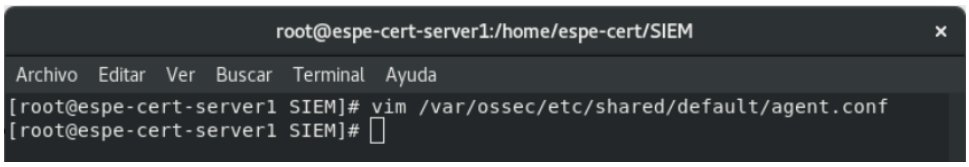
Interfaz web de Wazuh



Adicionalmente, se procede a habilitar el escaneo de vulnerabilidades antes de agregar los agentes al servidor. Para ello, se debe acceder al archivo de configuración de agentes compartido *ossec.conf.*

Figura 25

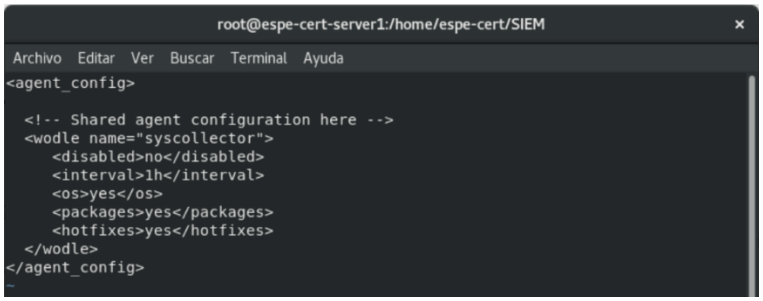
Configuración de agentes compartido



Se debe ingresar el siguiente bloque de configuraciones para que todos los agentes enrolados tomen las mismas y así, evitar el configurar manualmente cada uno de ellos. Realizado esto, se deben guardar los cambios y cerrar el archivo.

Figura 26

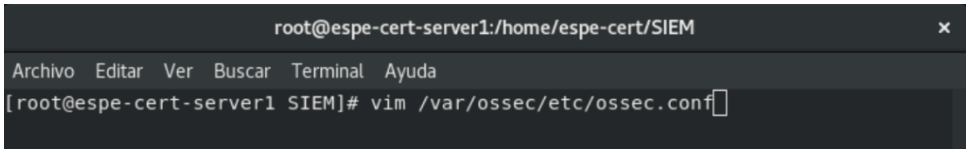
Bloque de configuraciones compartidas



Como siguiente paso, se procede a ingresar al archivo *ossec.conf* propio del servidor, en donde se va a habilitar el módulo de detección de vulnerabilidades.

Figura 27

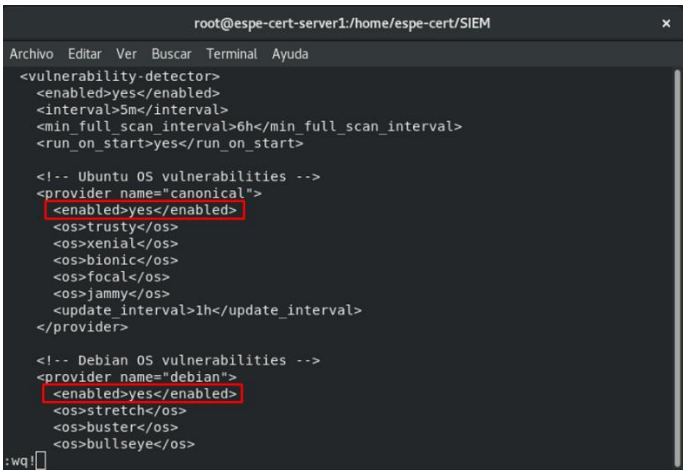
Ingreso al archivo ossec.conf



Se procede a cambiar el valor por defecto de “no” a “yes” en las etiquetas <*enabled*> dentro del bloque <*vulnerability-detector*> para habilitar la detección de vulnerabilidades hacia los sistemas operativos que se deseen analizar. Una vez realizado esto, se guardan los cambios.

Figura 28

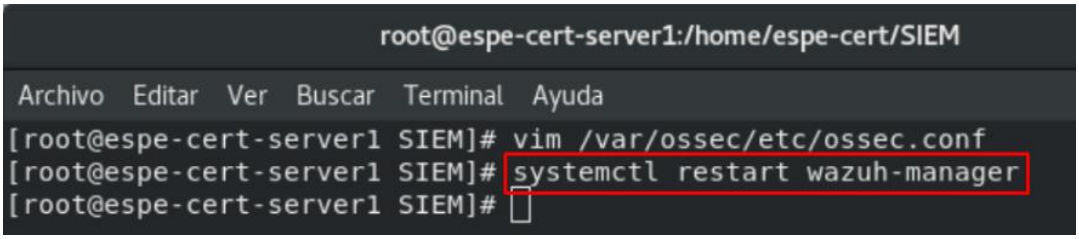
Habilitar el escaneo de vulnerabilidades para cada SO



Como paso final, es necesario reiniciar el servicio correspondiente al componente Wazuh manager para que los cambios se apliquen.

Figura 29

Reinicio de wazuh-manager



Implantación de la herramienta en los agentes

Para la instalación de los agentes, se consideró dividirlos en base el sistema operativo, que para este caso serán de tipo Linux y Windows ya que, los comandos y el procedimiento varía en base al SO que está siendo enrolado al servidor Wazuh.

Implantación en SO de tipo Linux

Para realizar la instalación del agente en sistemas operativos de tipo Linux, primero se creará un directorio de nombre SIEM-Wazuh que contenga los archivos descargados.

Luego, se procede a ejecutar el comando mostrado en la **Figura 30** el cual permite agregar el repositorio de Wazuh para descargar los paquetes oficiales y en primera instancia, instalar la llave GCP.

Figura 30

Instalación de la llave GPG

Se procede a ejecutar el siguiente comando para agregar el repositorio.

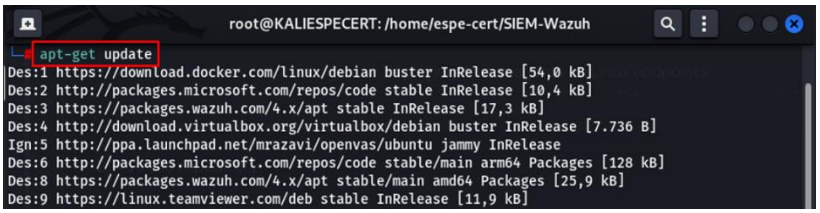
Figura 31

Agregar el repositorio de Wazuh

Por último, se realiza una actualización de los paquetes de información con el comando mostrado a continuación.

Figura 32

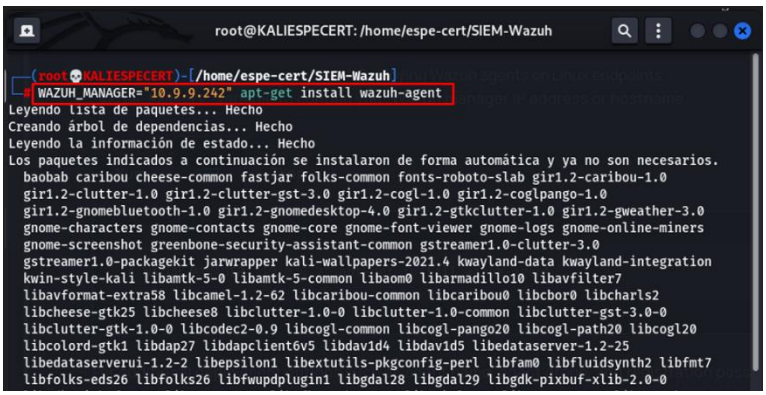
Actualización de los paquetes



Una vez agregado el repositorio de Wazuh, se procede a realizar el despliegue del agente. Para ello, se ejecuta el siguiente comando indicando la dirección IP del servidor Wazuh.

Figura 33

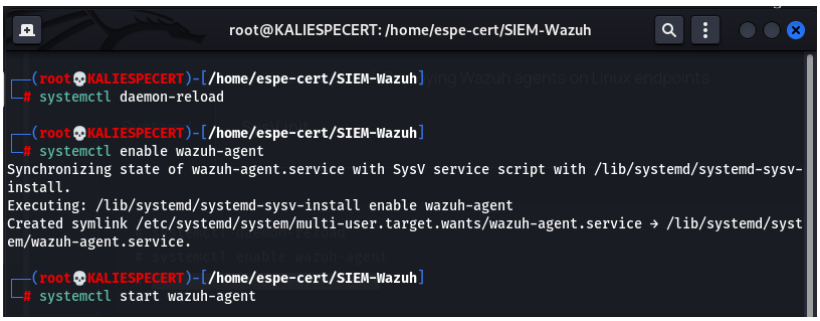
Instalación del agente de Wazuh



Se procede a habilitar e iniciar el servicio correspondiente al agente de Wazuh.

Figura *34*

Instalación del agente de Wazuh



Para verificar si se está ejecutando el agente, se ejecuta el siguiente comando mostrado en la **Figura 35.**

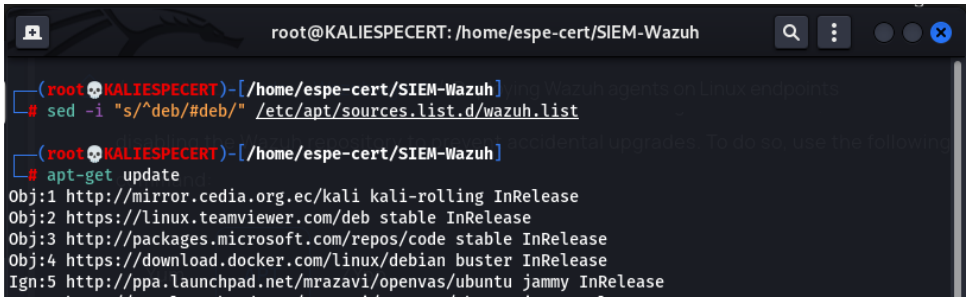
Figura 35

Verificación del agente de Wazuh

La documentación oficial, se recomienda deshabilitar las actualizaciones para Wazuh, ya que, si la versión del agente es mayor a la del servidor, se pueden presentar inconvenientes. Para prevenir esto, se ejecutan los siguientes comandos.

Figura 36

Deshabilitar actualizaciones de Wazuh

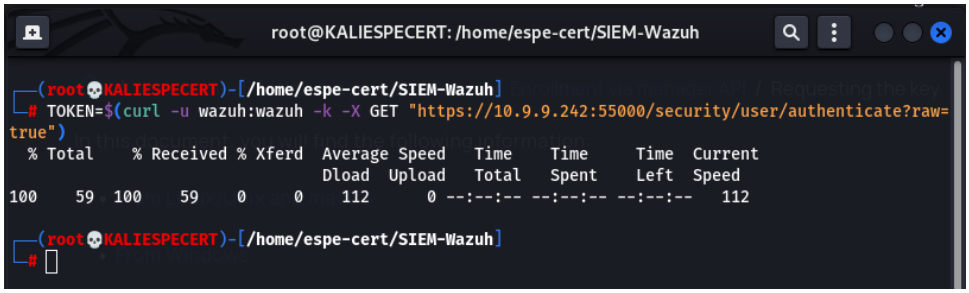


Enrolamiento del agente Linux

La clave del agente se puede solicitar desde cualquier sistema que tenga conectividad con la API del servidor, esto con el objetivo de enrolar el agente al servidor y pueda empezar a ser monitoreado. Para lograr esto, se procede a realizar la solicitud de un JSON Web Token (JWT) para autenticarse con el API, esto si logra con el siguiente comando en donde el las credenciales por defecto son wazuh:wazuh.

Figura 37

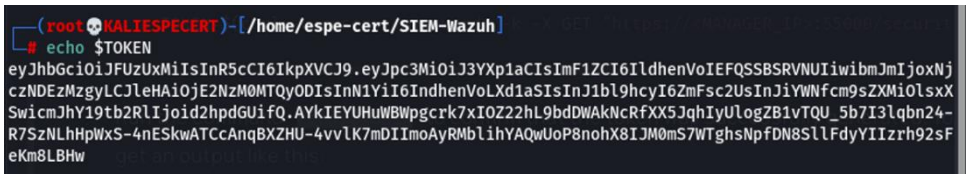
Obtención de JWT para autenticación



Se procede a ejecutar el siguiente comando para verificar que si se haya recibido un JWT para autenticarse más adelante.

Figura *38*

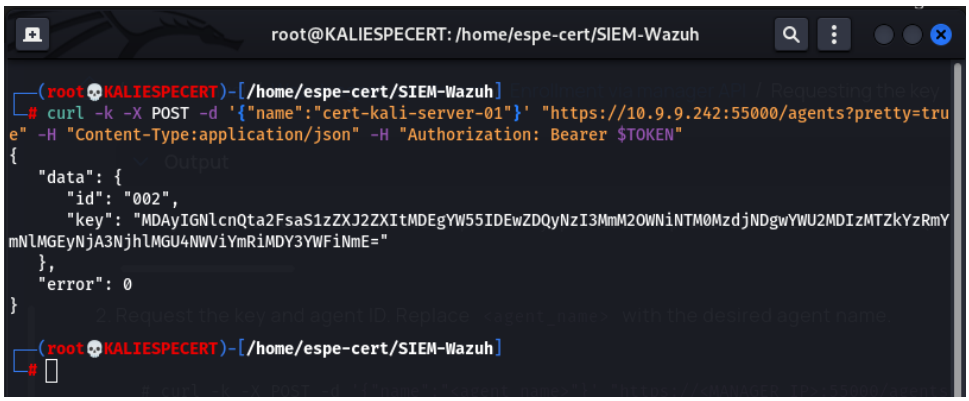
JWT de autenticación



Se debe solicitar la llave y el ID del agente al servidor, para ello, se hace eso del siguiente comando en donde se especifica en nombre que tendrá el agente, la dirección IP del servidor y el JWT de autenticación. Como se puede observar en la **Figura 39**, se obtuvo una respuesta exitosa con la llave que debe ser importada al agente.

Figura 39

Solicitud de llave de agente



Con la llave obtenida y desde el agente de Wazuh, se debe ingresar el siguiente comando para importar la llave al agente, en donde se ingresa la letra “y” para confirmar la acción.

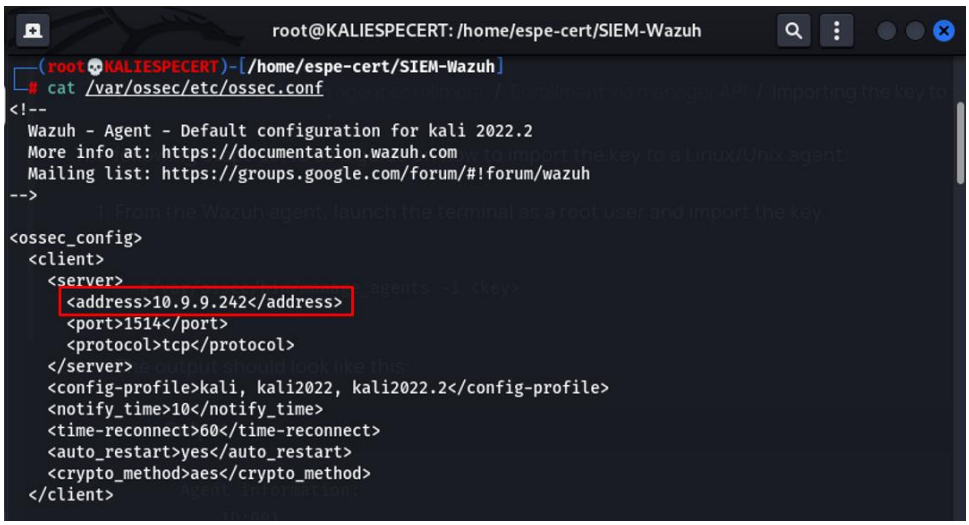
Figura 40

Importación de llave

Verificamos que en el archivo *ossec.conf,* se encuentre la dirección IP del servidor en el tag <*address*>, esto se puedo lograr con el siguiente comando.

Figura 41

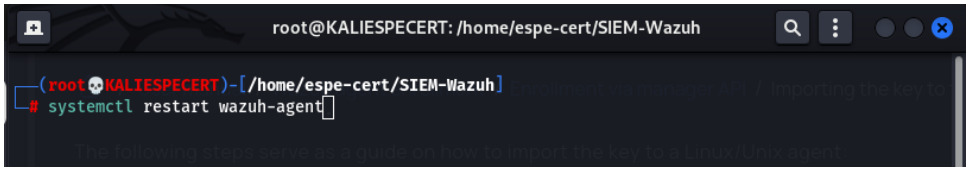
Verificación de dirección IP



Como último paso, se debe reiniciar el servicio correspondiente al agente para hacer los cambios efectivos.

Figura 42

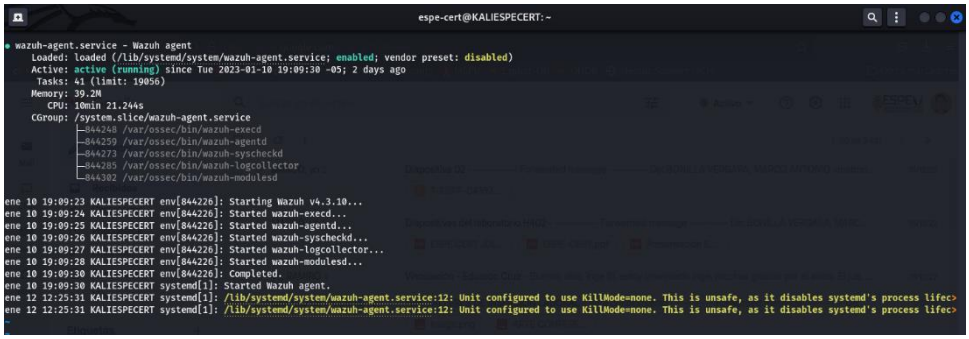
Reiniciar la ejecución del agente



A manera de verificación, se hacer uso del siguiente comando para ver si el servicio está ejecutándose de manera adecuada.

Figura 43

Verificación de la ejecución del agente

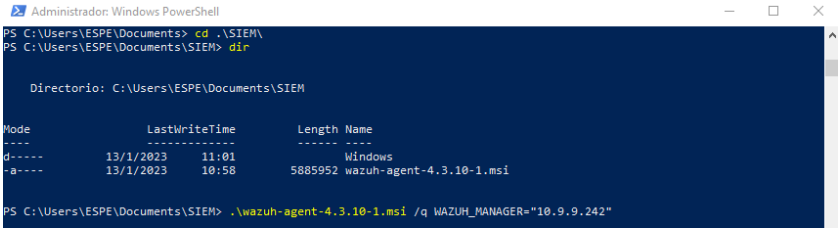


Implantación en SO de tipo Windows

Para realizar la instalación del agente en sistemas operativos de tipo Windows, primero se creará un directorio de nombre SIEM. Luego, se debe descargar el instalador del agente en dicho directorio desde la página oficial de Wazuh y posteriormente, ejecutar el siguiente comando.

Figura 44

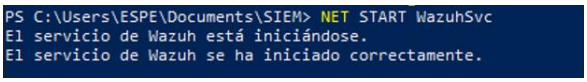
Creación de directorio e instalación del agente



Una vez instalado el agente, se procede a iniciar la ejecución del servicio correspondiente al agente.

Figura 45

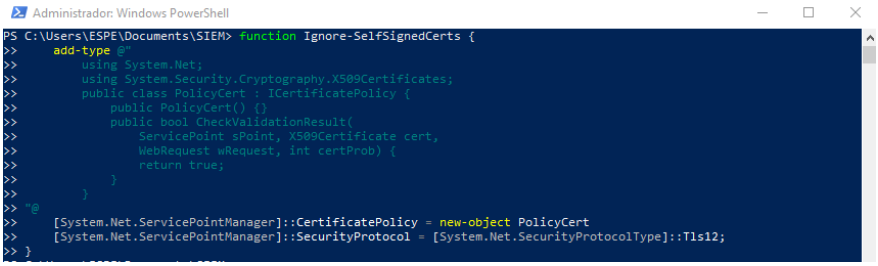
Ejecución del agente



Con la instalación finalizada, se procede a solicitar la llave para posteriormente, enrolar al agente al servidor. Para conseguir esto, se debe abrir el *PowerShell* de Windows con permisos de administrador y ejecutar la siguiente función si la API del servidor se ejecuta a través de HTTPS y usa un certificado auto firmado.

Figura 46

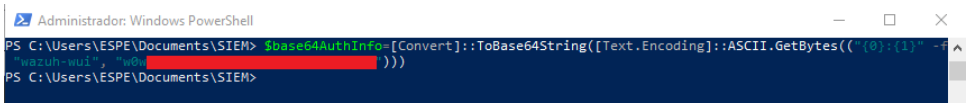
Función para API sobre HTTPS



Se procede a solicitar un JWT al servidor, para lo cual primero se codifican las credenciales como base64 y luego se hace uso del siguiente comando, en donde se especifica el usuario y clave de la API.

Figura 47

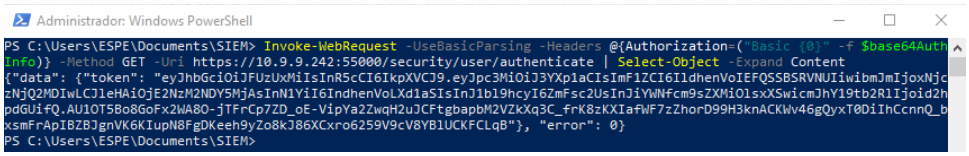
Codificación de credenciales



Se procede a realizar la solicitud del JWT para una posterior autenticación.

Figura 48

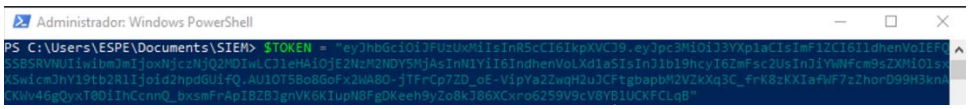
Solicitud de JWT



Con el JWT obtenido, se procede a guárdalo en una variable de entorno con el fin de utilizarla más adelante.

Figura 49

Variable de entorno $TOKEN



De la misma manera, se procede a crear una variable de entorno que almacene el nombre del agente a enrolar y se lo convierte a formato JSON para enviarlo al servidor.

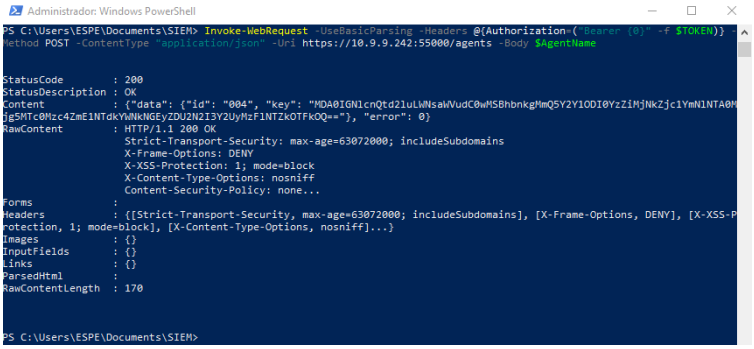
Figura 50

Variable de entorno $AgentName

Se procede a realizar la solicitud al servidor para obtener la llave y un ID con el siguiente comando, en donde se debe especificar la dirección IP del servidor, el *token* y el nombre que el agente va a tomar.

Figura 51

Solicitud de llave de agente

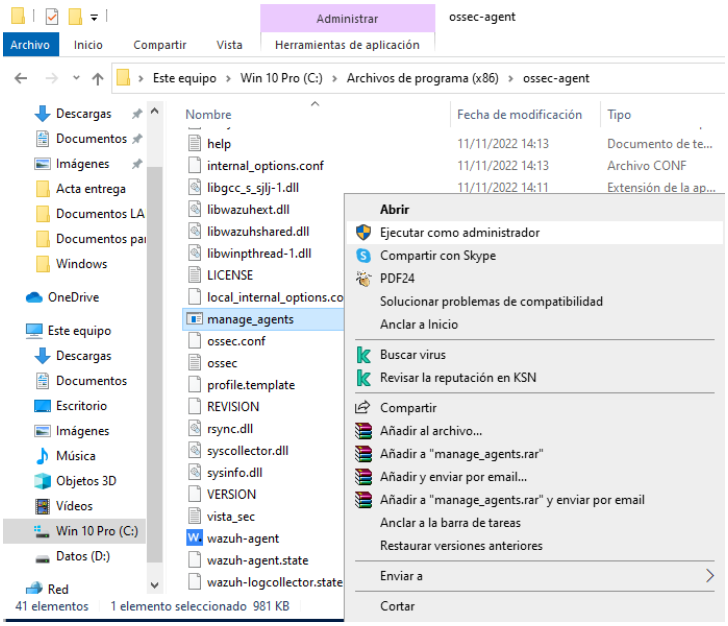


Enrolamiento del agente Windows

Para enrolar el nuevo agente Windows al servidor, ingresamos al directorio en donde se instaló por defecto el agente Wazuh, que para este caso es *C:\Program Files (x86)\ossec-agent* y en este directorio, se debe ejecutar como administrador el archivo *manage_agents*.

Figura 52

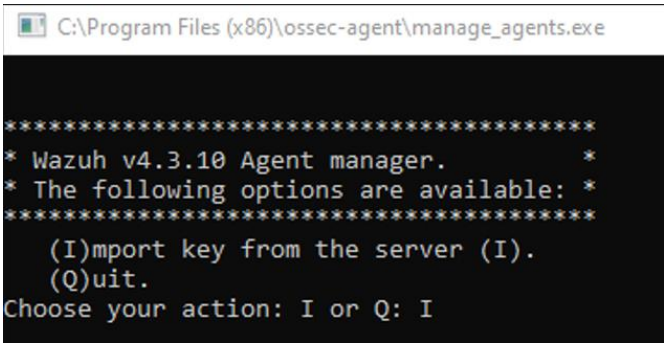
Ejecución de manage_agents



Se abrirá una nueva ventana en donde se presentar dos opciones, la primera es importar la llave obtenido anteriormente y la segunda para salir del asistente, para nuestro caso, se va a ingresar la tecla “I” para importar la llave y se presiona “Enter” para confirmar.

Figura 53

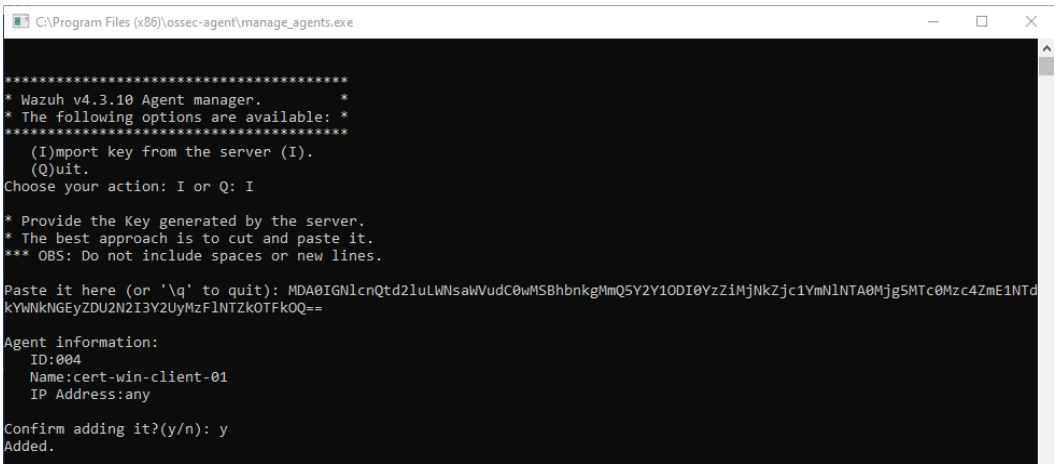
Importación de la llave mediante manage_agents



Se procede a pegar la llave obtenida en pasos anteriores y luego, se ingresa la tecla “y” para conformar la acción. Con esto, se muestra un mensaje indicando que se agregó la llave satisfactoriamente al agente.

Figura 54

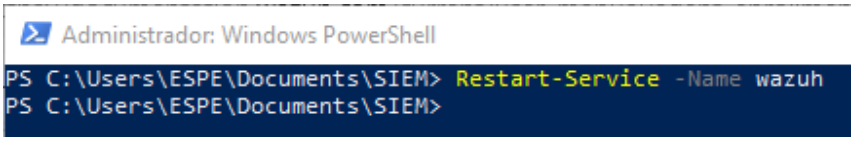
Llave agregada correctamente



Como último paso, se debe realizar el reinicio del servicio correspondiente al agente de Wazuh para que los cambios se vean reflejados.

Figura 55

Solicitud de llave de agente

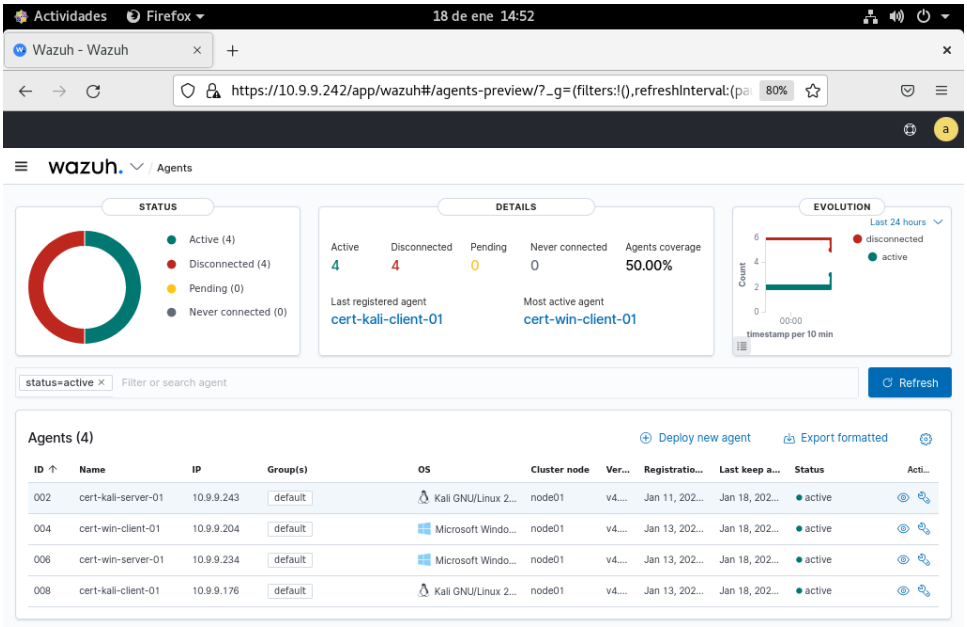


Verificación del servicio

Una vez que el nuevo servicio ha sido implantado correctamente en el servidor y los agentes han sido enrolados, se ingresa al apartado de agentes desde un navegar web como se observa en la **Figura 56** para verificar que, en este *dashboard*, aparezcan los agentes con sus respectivos nombres asignados, IDs y direcciones IP correspondientes. Con los agentes enrolados y siendo monitoreados correctamente, se puede proceder a visualizar vulnerabilidades, monitorear amenazas, entre otras funcionalidades prestadas por el SIEM.

Figura 56

Agentes enrolados al servidor Wazuh



Capítulo IV:

Fase 2: Entrega y Soporte, Mejora

Entrega y Soporte

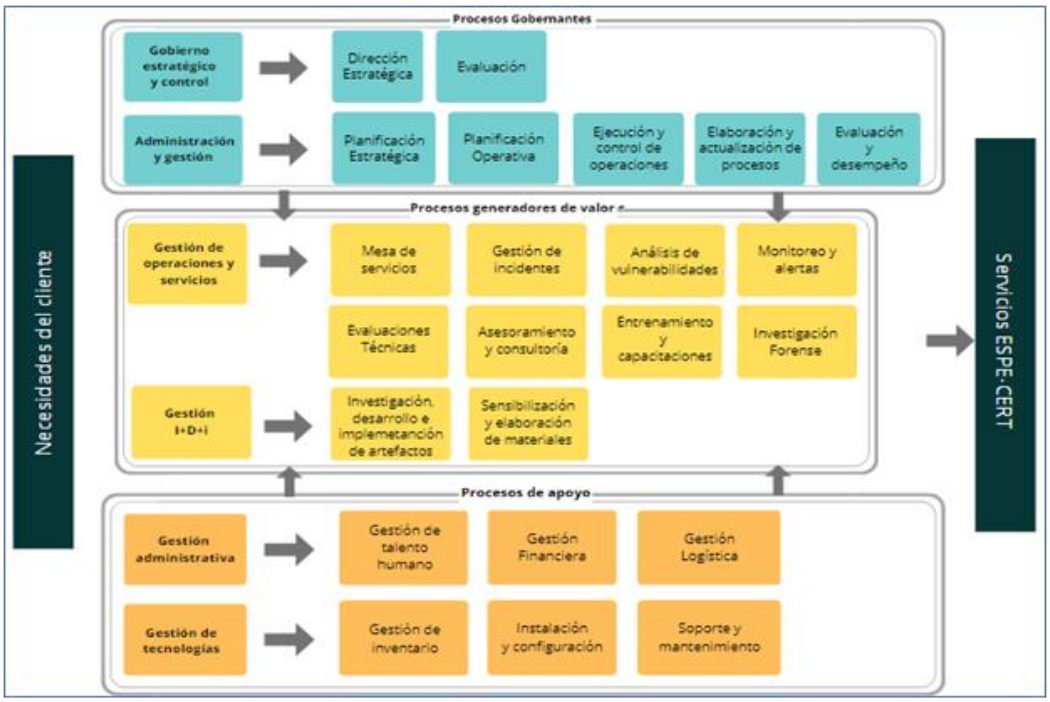
Con el servicio funcionando de manera adecuada tanto en el servidor como en los agentes, se procede a realizar las actividades de entrega y soporte, en donde se determinará cual será el procedimiento a seguir para entregar el servicio correctamente, en base a criterios ya establecidos. Luego se debe visualizar los resultados que está arrojando el SIEM y en base a estos realizar una evaluación para determinar qué tan efectivo es su funcionamiento.

Desarrollo y Gestión de Software

Mapa de Proceso General. En la **Figura 57**, se puede visualizar una perspectiva global sobre cómo está dada la organización, además de permitir visualizar los procedimientos, procesos y el cómo se interrelacionan.

Figura 57

Mapa de procesos ESPE-CERT



Nota: El gráfico fue tomado de *Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales* (p. 95), por Pacha Maycol & Ruiz Juan, repositorio institucional de la ESPE.

Proceso de monitoreo y alerta. Los procesos definidos en el procedimiento CERT-02.01.04 monitoreo y alerta de primer nivel por Pacha & Ruiz (2022), nos definen el cómo se debería tratar las amenazas detectadas por el nuevo servicio, a continuación, se define el procedimiento:

Objetivo:

Informar a los usuarios de las nuevas vulnerabilidades y técnicas de intrusión detectadas, por medio de alertas, y notificaciones para proteger los sistemas de información de los nuevos riesgos de seguridad antes de que se materialicen.

Alcance:

El proceso consiste en revisar los logs y eventos que sucedan dentro de la red del cliente, junto con un análisis de los activos que están involucrados dentro de las conexiones de la institución.

Responsables:

- Analista ESPE-CERT.
- Operadores ESPE-CERT.

Base legal:

La Norma Técnica NTE INEN-ISO/IEC 27002:2009 realizará las tareas de seguimiento y control del cumplimiento de la presente política, para lo cual se dará acceso a los registros de auditoría de las aplicaciones electrónicas, a la información contenida en los datos institucionales bases, y la información en poder de los funcionarios de la institución.

Políticas:

- ESPE-CERT acordará funciones y responsabilidades con los empleados encargados de monitorear y alertar dentro de la entidad.

- Es obligación de los operadores:
    - Realizar monitoreos diarios para cumplir con los estándares de seguridad establecidos.
    - Comunicar las alertas encontradas, máximo 2 horas después de haberlas detectado.

Definición:

- **Monitoreo:** La revisión y supervisión de todas las actividades realizadas a través de la infraestructura y el ecosistema de una organización constituye monitoreo.
- **Alerta:** El término "alerta" se refiere a los mensajes enviados a un usuario específico sobre eventos inminentes del sistema que requieren notificación. Lo mismo debe perdurar en todo el sistema hasta que se brinde una solución.

Desarrollo:

1. **Ingreso a la herramienta software. -** El operador o analista debe ingresar al portal *https://especare.freshdesk.com/support/home* para utilizar las herramientas instaladas para monitorear eventos, cada operador debe ingresar en su equipo y usuario designado.
2. **Revisión de eventos y logs. -** Para realizar la revisión, el operador debe determinar qué fuentes de registros están disponibles y qué herramientas automatizadas se pueden utilizar. Para ello, se realizará una copia de los registros y se trasladará a otra ubicación donde se puedan revisar sin cambiar el original, registros.
3. **Análisis de eventos. -** El operador realizará un análisis de los logs y eventos para identificar si se trata de un incidente. En el caso de ser positivo, pasa al procedimiento de gestión de incidente, en el caso contrario se cierra el monitoreo y se informa al cliente.
4. **Procedimiento de Gestión de Incidentes. –** Si se detecta algún incidente se realizan las respectivas actividades que corresponden al procedimiento denominado

Gestión de Incidentes, Código CERT-02.01.02 de lo contrario finaliza el procedimiento.

Nota: Cada uno de los pasos expuestos son extractos de la (NIST SP 800-61) Guía para el manejo de incidentes de seguridad informática, adaptados a las necesidades actuales del ESPE-CERT.

Indicadores de desempeño:

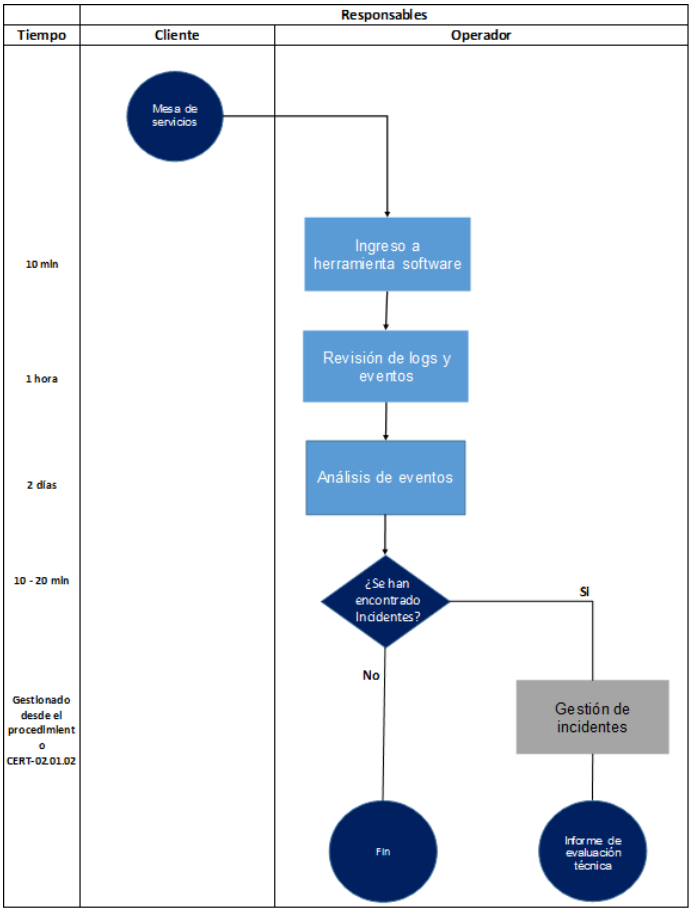
- Número de eventos que se identificaron y se lograron resolver con éxito en los tiempos establecidos.
- Número de vulnerabilidades conocidas por el ESPE – CERT.

Diagrama de flujo:

- Diagrama De Flujo Espe-Cert, Código CERT-02.01.04

Figura 58

CERT-02.01.04 Monitoreo y alerta de primer nivel



Nota: El diagrama de flujo fue tomado de *Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales* (p. 118), por Pacha Maycol & Ruiz Juan, repositorio institucional de la ESPE.

Monitoreo y Gestión de Eventos

Bitácora. En la **Tabla 20,** se puede visualizar un listado de los registros emitidos por el SIEM más relevantes, en donde se consideraron los análisis de vulnerabilidades, los registros de incidentes, las alarmas, alertas generadas y los eventos de seguridad.

Tabla 20

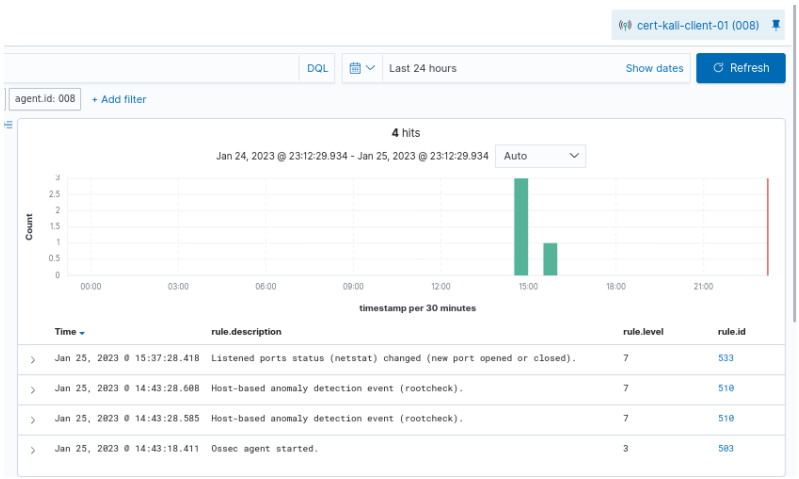
Bitácora de registros

#	Tipo de registro	Descripción	Fecha de registro
1	Alarmas y alertas	Detección de vulnerabilidades en los agentes	23-01-2023
2	Incidente de seguridad	Detección de posible archivo con virus troyano	25-01-2023
3	Alarmas y alertas	Evaluación de configuración de seguridad	25-01-2023
4	Eventos de seguridad	Fallo al ingresar al iniciar sesión	25-01-2023
5	Eventos de seguridad	Escalamiento de privilegios a usuario *root*	25-01-2023
6	Eventos de seguridad	Posible contenido oculto en archivos	25-01-2023

Registros de Incidentes. Por medio del servicio, se logró capturar un incidente de seguridad, el cual tiene como nombre "*Host-based anomaly detection event (rootcheck)*". Como se puede observar en la **Figura 59**, se tienen cuatro eventos registrados, de los cuales se va a analizar el mencionado anteriormente por su severidad y daños que podría causar a la infraestructura.

Figura 59

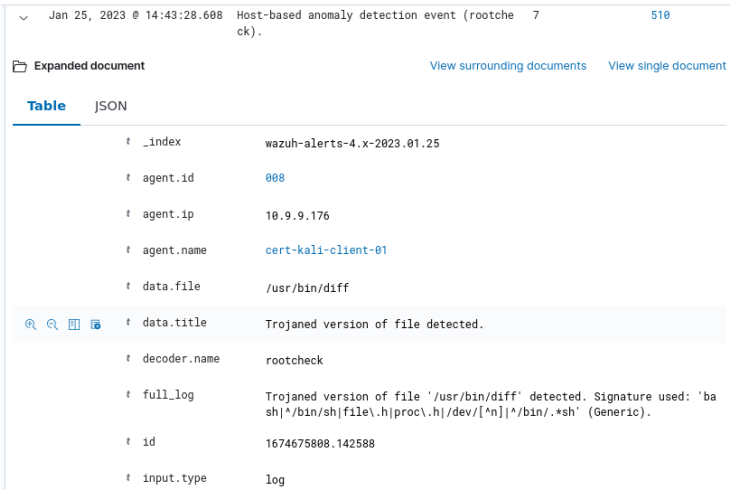
Incidente de seguridad registrado



Al desplegar la información de este incidente, se puede observar en la **Figura 60** que se trata de la detección de una versión troyana del archivo, lo cual nos indica que el archivo especificado, podría ser un virus troyano.

Figura 60

Detección de posible archivo con virus troyano



Alarmas y Alertas. Para esta funcionalidad del SIEM, se consideraron como prioridades la detección de vulnerabilidades y la evaluación de configuración de seguridad de los agentes.

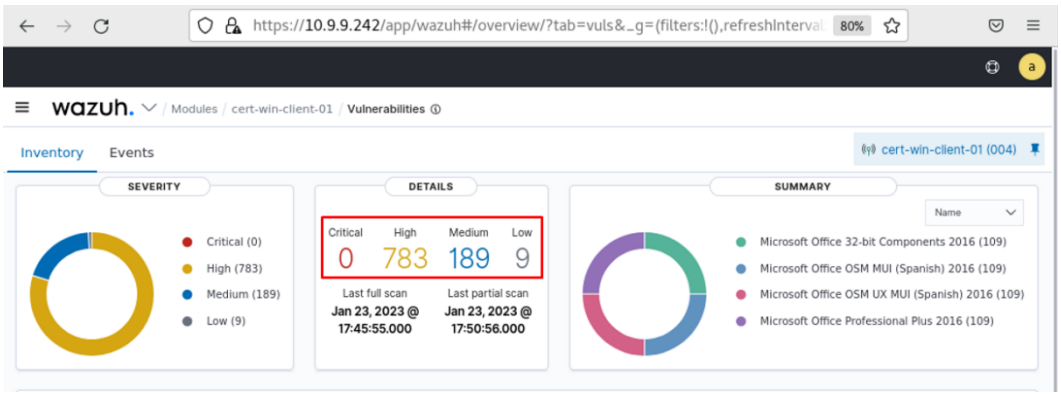
Detección de Vulnerabilidades. En la sección de implantación del nuevo servicio, se habilito el escaneo de vulnerabilidades de los agentes. A manera de demostración de esta funcionalidad, se tomó el agente cert-win-client-01, en donde cómo se puede visualizar en la **Figura 61**, se obtuvieron 981 vulnerabilidades, las cuales se desglosan de la siguiente manera:

- Altas: 783 vulnerabilidades
- Medias: 189 vulnerabilidades
- Bajas: 9 vulnerabilidades

También es importante destacar que se realizan escaneos parciales y completos en base a las configuraciones establecidas en pasos anteriores, el dashboard nos muestra la fecha y hora exacta en la que se realizaron los análisis.

Figura 61

Resumen de vulnerabilidades del agente cert-win-client-01



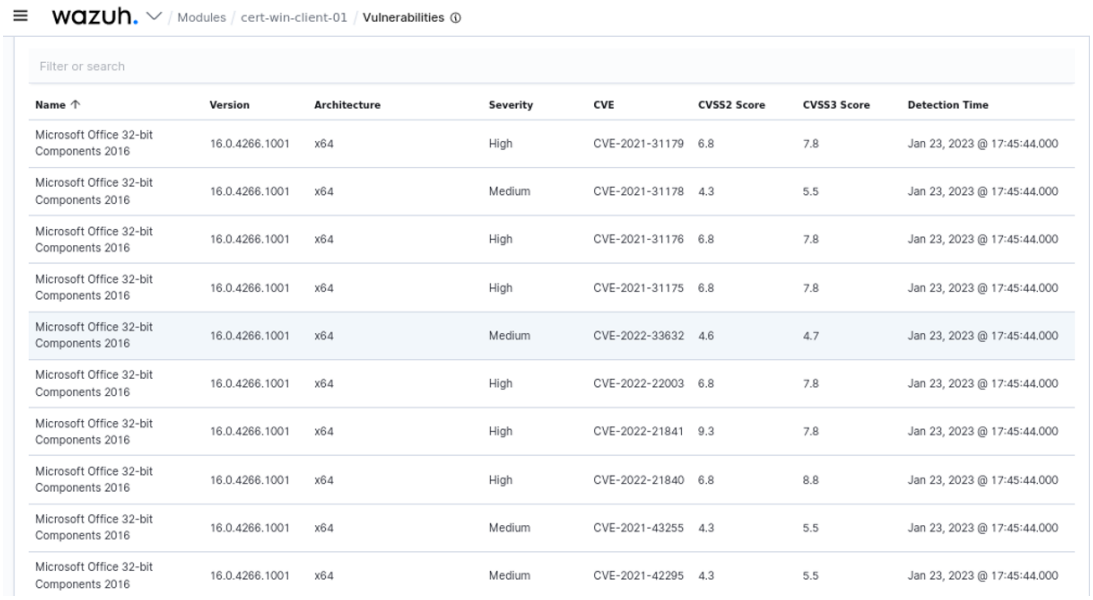
También se ofrece una vista más detallada de cada una de las vulnerabilidades analizadas como se puede observar en la **Figura 62,** en donde los parámetros establecidos nos indican lo siguiente:

- Name: nombre de la vulnerabilidad detectada
- *Severity*: grado de severidad detectada

- *CVE*: nombre estandarizado para la vulnerabilidad y otras exposiciones de seguridad de la información
- *CVSS2 Score*: sistema de puntuación que permite definir numéricamente el nivel de gravedad de un fallo de seguridad, su puntuación cualitativa es la siguiente:
    - Baja: 0.0 – 3.9
    - Media: 4,0 – 6,9
    - Alta: 7.0 – 10.0
- *CVSS3 Score*: sistema de puntuación que permite definir numéricamente el nivel de gravedad de un fallo de seguridad, su puntuación cualitativa es la siguiente:
    - Ninguna: 0.0
    - Bajo: 0.1 – 3.9
    - Medio: 4,0 – 6,9
    - Alta: 7.0 – 8.9
    - Crítico: 9.0 – 10.0
- *Detection Time*: hora y fecha en la cual se detectó la vulnerabilidad.

Figura 62

Detalle de vulnerabilidades del agente cert-win-client-01

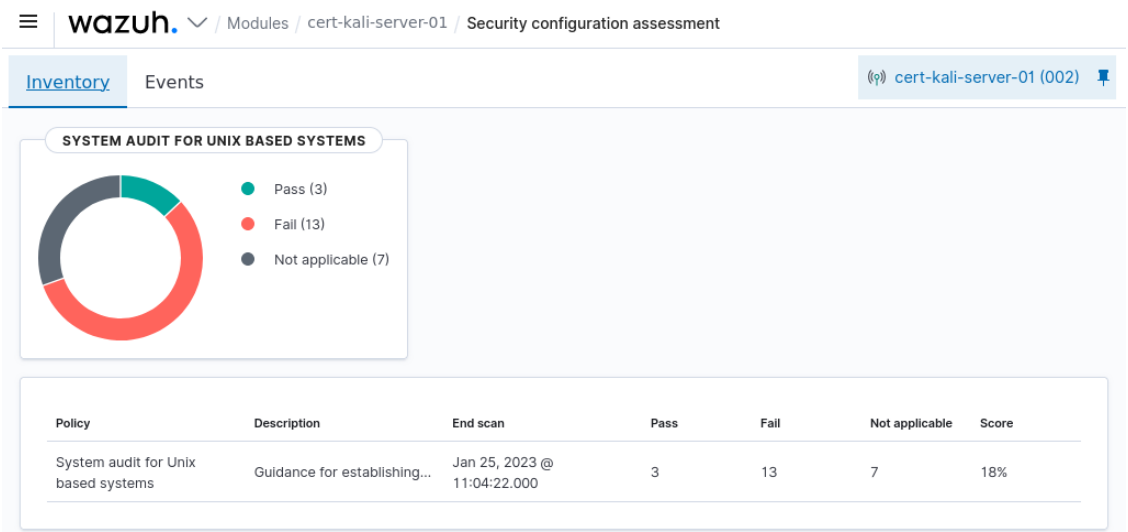


Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2021-31179	6.8	7.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	Medium	CVE-2021-31178	4.3	5.5	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2021-31176	6.8	7.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2021-31175	6.8	7.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	Medium	CVE-2022-33632	4.6	4.7	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2022-22003	6.8	7.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2022-21841	9.3	7.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	High	CVE-2022-21840	6.8	8.8	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	Medium	CVE-2021-43255	4.3	5.5	Jan 23, 2023 @ 17:45:44.000
Microsoft Office 32-bit Components 2016	16.0.4266.1001	x64	Medium	CVE-2021-42295	4.3	5.5	Jan 23, 2023 @ 17:45:44.000

Evaluación de Configuración de Seguridad. Uno de los módulos de la herramienta permite realizar evaluaciones de configuración de seguridad en base a una política, como por ejemplo una auditoria del sistema para sistemas basados en Unix. Con esto, es posible visualizar posibles alertas de seguridad en los agentes y una posible solución para las mismas. A manera de demostración, se escogió el servidor Kali para analizar su evaluación de configuración de seguridad.

Figura 63

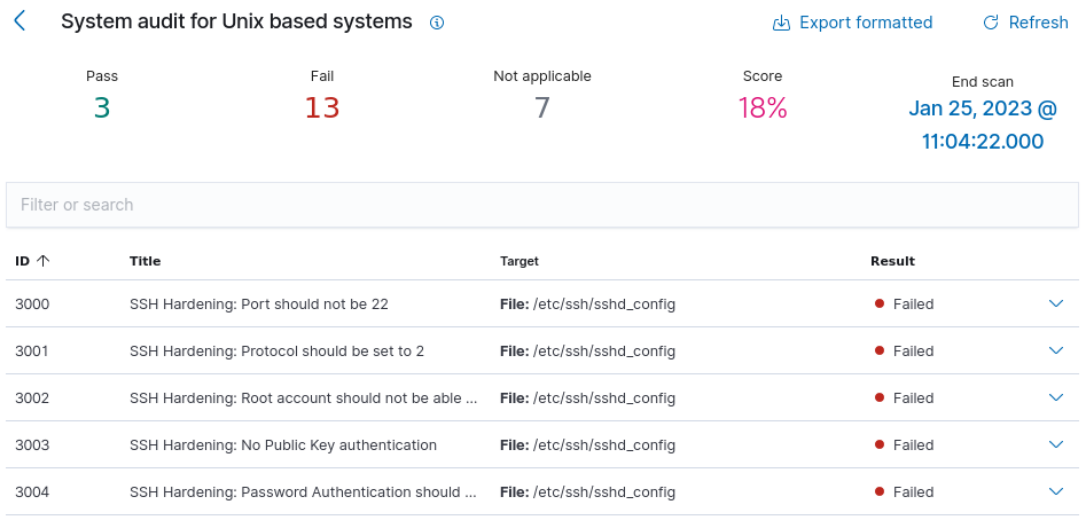
Evaluación de configuración de seguridad del agente cert-kali-server-01



Al ingresar a los detalles de la evaluación realizada, es posible observar que 13 de las evaluaciones no pasaron las pruebas, mientras que solamente tres si lo hicieron, y siete no aplicaron. En base a estos resultados, se le asigno un 18% como resultado de la evaluación, siendo un valor bastante bajo e indicando que se requieren realizar acciones sobre este servidor para mejorar su seguridad.

Figura 64

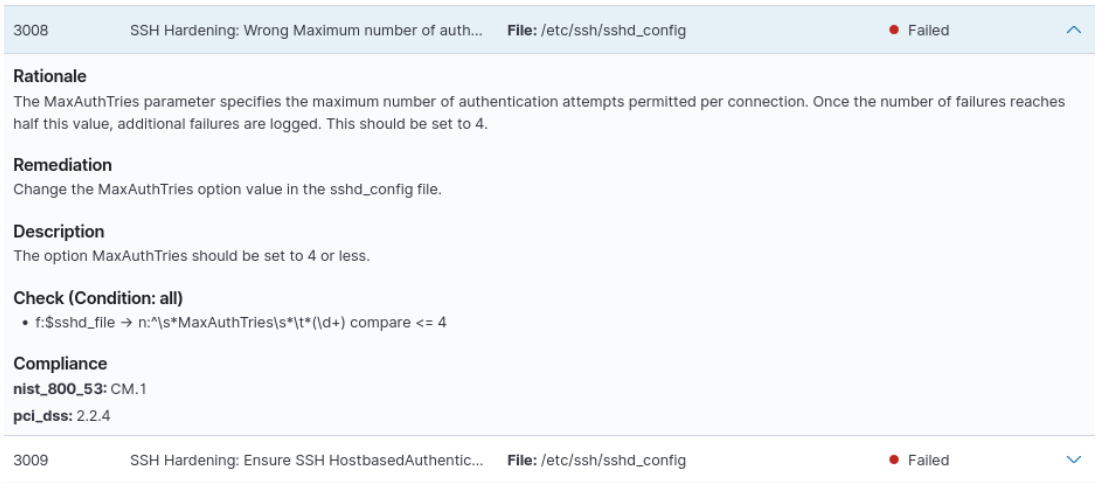
Detalles de la auditoria del sistema para sistemas basados en Unix



Si se visualiza el detalle de una de las evaluaciones, nos indica que la cantidad máxima para intentar conectarse al servidor, no está establecida en el valor recomendado que es de cuatro intentos. Una de las maneras de remediar esto, es modificar el valor de *MaxAuthTries* en el archivo *sshd_config* como se muestra en la **Figura 65**.

Figura 65

Número máximo de intentos permitidos para conectarse al servidor



Eventos de Seguridad. Wazuh posee varios módulos en donde se ubican las funcionalidades, uno de estos es el módulo de *Security events*, en donde se puede visualizar una serie de eventos registrados por cada agente, así como gráficos estadísticos

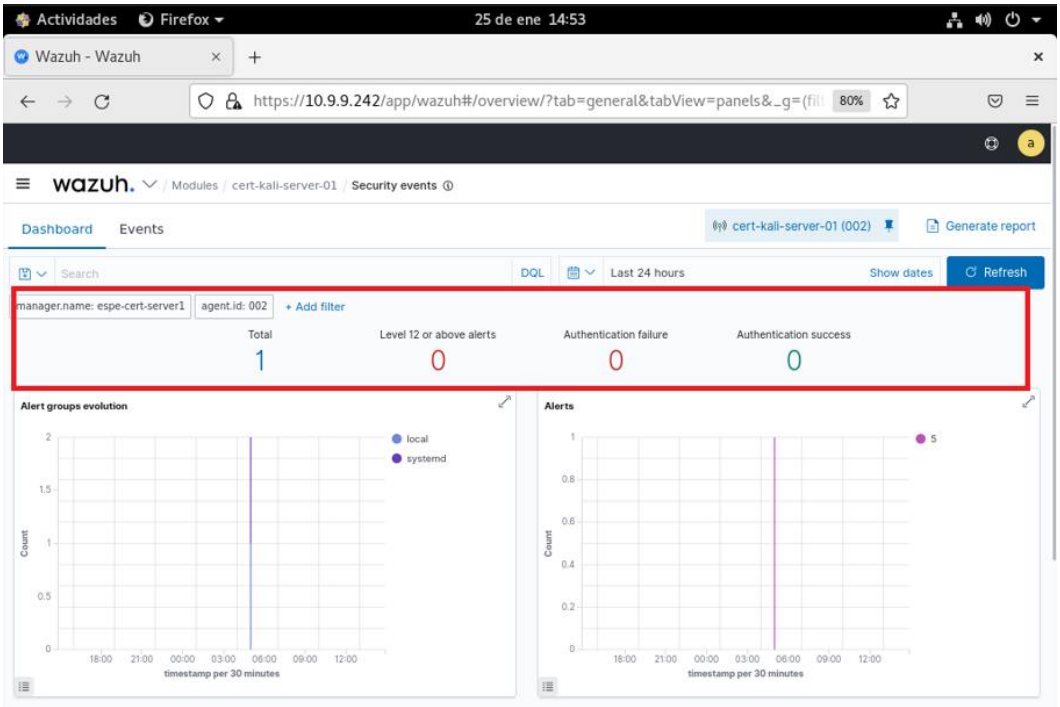
sobre los eventos que más han sucedido en un periodo de tiempo. En esta sección, se presenta una recopilación de los eventos más repetitivos.

Fallo al Ingresar a la Sesión. Uno de los eventos de seguridad que se logró visualizar con el nuevo servicio, fueron los intentos de autenticación fallidos cuando un usuario intenta iniciar sesión e ingresa una contraseña incorrecta.

En la **Figura 66**, se puede observar inicialmente que tanto el fallo de autenticación (*Autentication failure*) como éxito en la autenticación (*Autentication success*) se encuentran con el contador en cero, esto debido a que todavía no se ha ingresado a la sesión.

Figura 66

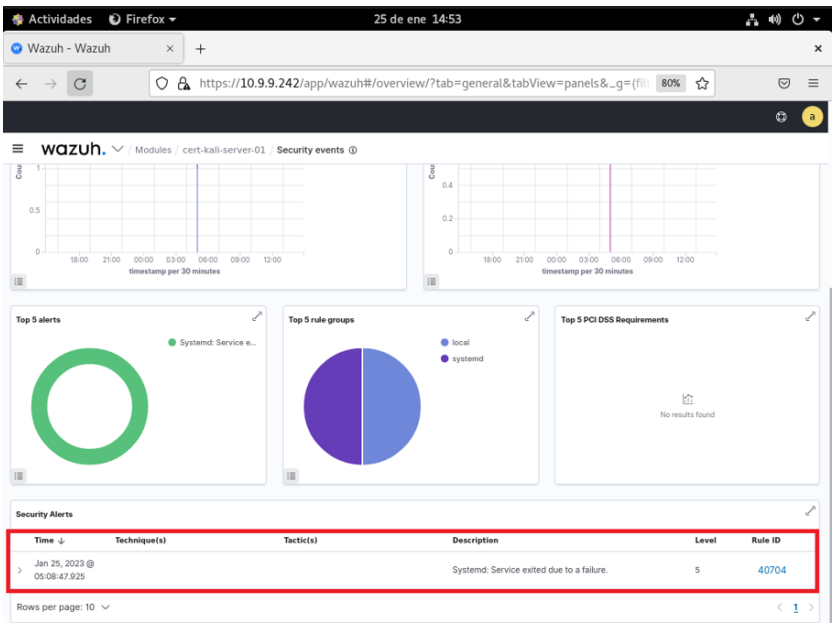
Dashboard de eventos de seguridad del agente cert-kali-server-01



En la parte inferior de esta misma página también se puede visualizar las Alertas de Seguridad (*Secutiry Alerts*), como está en la **Figura 67.**

Figura 67

Detalles de eventos de seguridad del agente cert-kali-server-01



Tras haber realizado cinco intentos fallidos de ingreso de sesión, se puede observar que estos quedan registrados abajo del fallo de autenticación, incrementando su contador de cero a cinco **Figura 68** y en las alertas de seguridad de la **Figura 69**.

Figura 68

Dashboard intentos fallidos de inicio de sesión del agente cert-kali-server-01

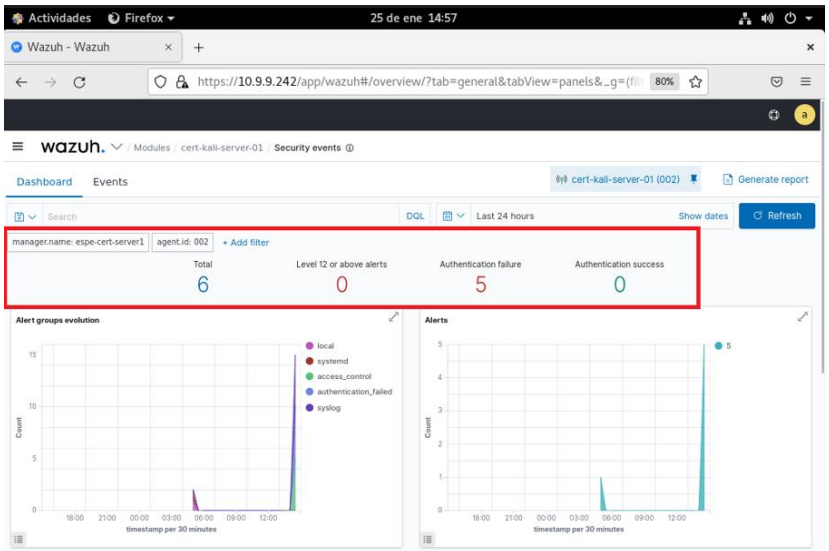
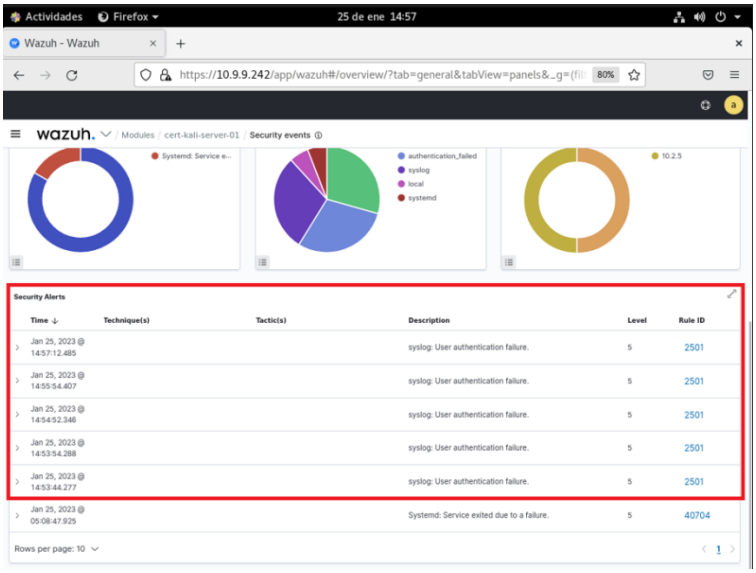


Figura 69

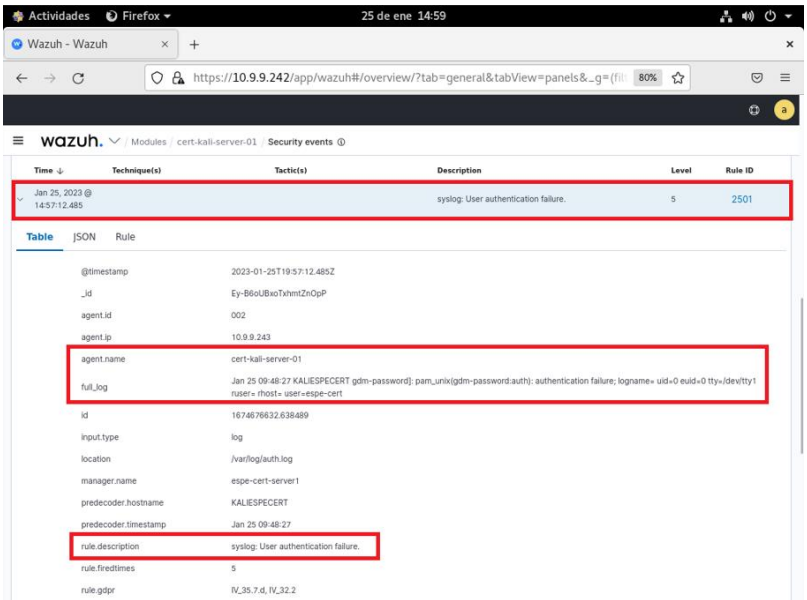
Detalles del agente cert-kali-server-01 tras intentos de inicio de sesión



Al dar clic sobre una de estas alertas de seguridad, se puede ver por completo la información del evento en cuestión **Figura 70**. Por ejemplo, en el fallo al ingresar a la sesión, se pude ver: el nombre del agente; la información completa del log, como la fecha, hora, usuario, id de usuario; la descripción de la regla a la que pertenece, entre otros atributos.

Figura 70

Intento fallido de inicio de sesión del agente cert-kali-server-01

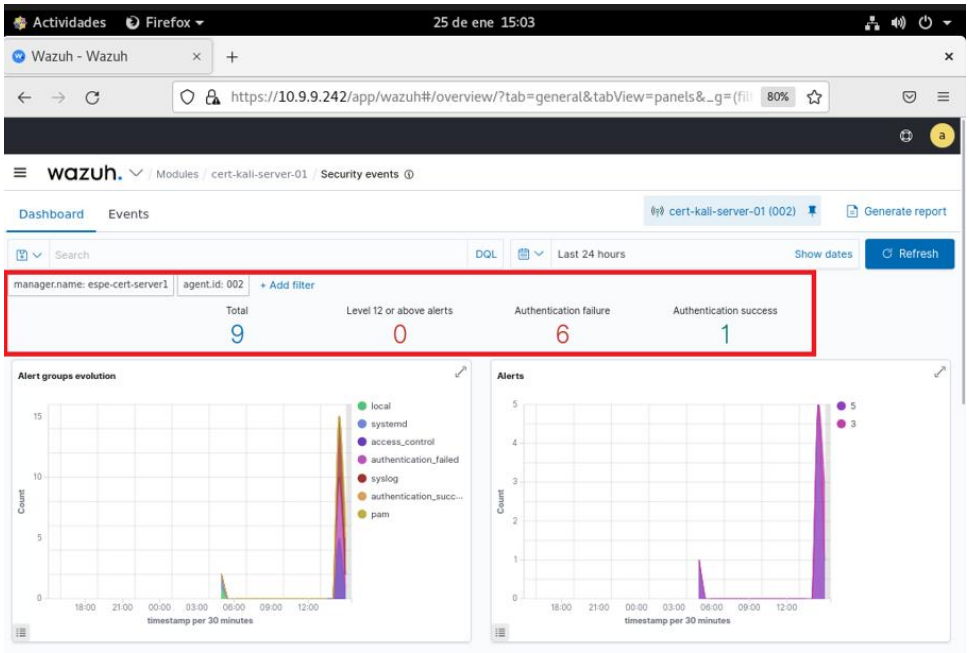


Ingreso Como Usuario ROOT en el Terminal de Kali Linux. En este evento de seguridad lo primero se ingresa al servidor Kali Linux, llamado cert-kali-server01, luego se abre una terminal y se ingresa siguiente comando: **sudo systemctl wazuh-agent.** El terminal pedirá que se ingrese la clave de super usuario. Una vez ingresada la clave de forma correcta, el comando se ejecutará.

De vuelta al servidor CentOS, se verifica la actividad en el *Dashboard* del agente cert-kali-server-01 en la **Figura 71**. Se puede ver que el contador de éxito en la autenticación incremento en uno.

Figura 71

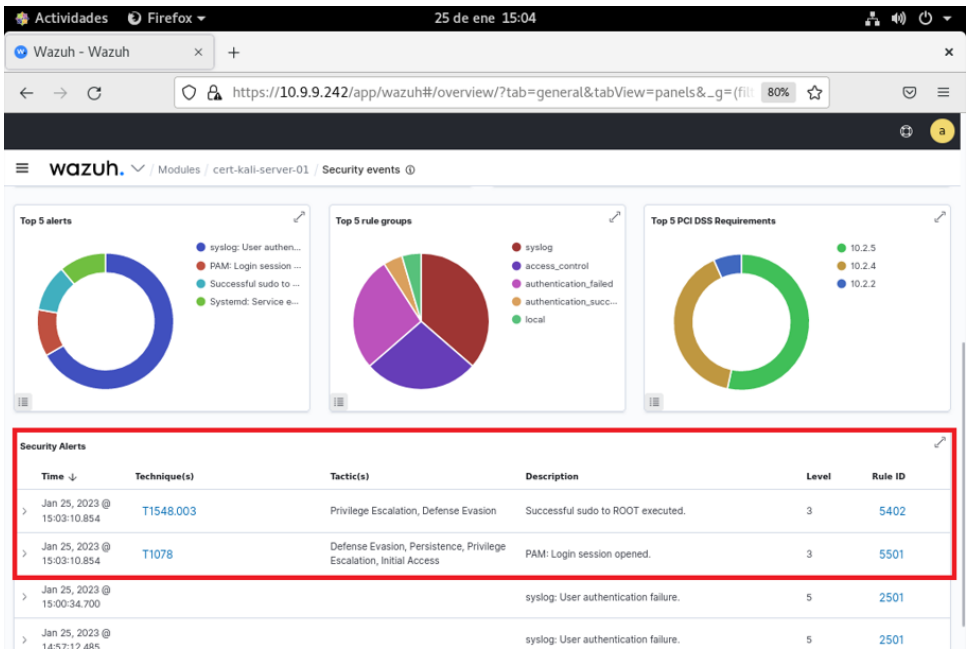
Vista del Dashboard tras un acceso de autenticación exitoso.



Bajando en el mismo *Dashboard* de eventos de seguridad se puede ver las alertas de seguridad **Figura 72**. Se ha registrado la actividad de escalar privilegios a super usuario (o usuario *ROOT*) de forma exitosa.

Figura 72

Eventos de seguridad en el agente cert-kali-server-01



Al dar clic sobre una de estas alertas de seguridad, se puede ver más información acerca del evento en cuestión **Figura 73**. Por ejemplo, al acceder como super usuario, se muestra: el nombre del agente; el comando utilizado; la forma de acceso e información completa del log. La **Figura 74** es una continuación de la **Figura 73**.

Figura 73

Detalles de autenticación exitosa del agente cert-kali-server-01 PARTE 1

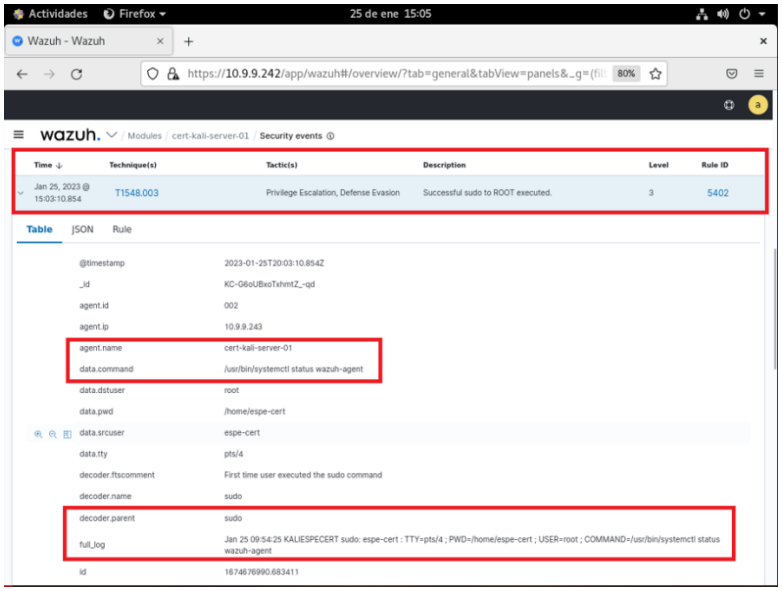
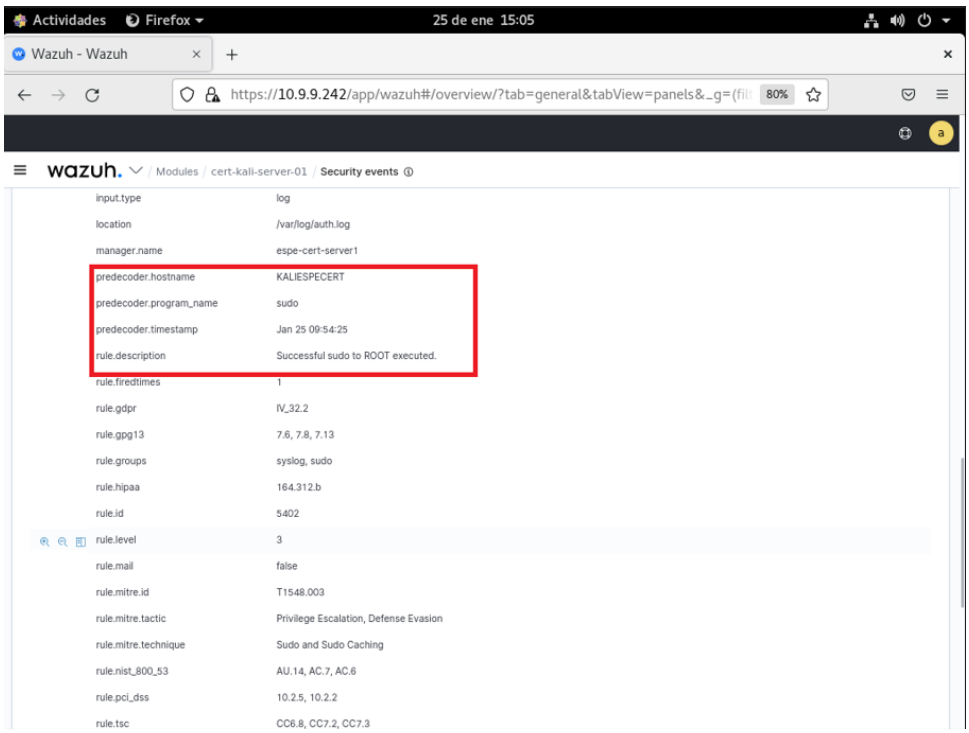


Figura 74

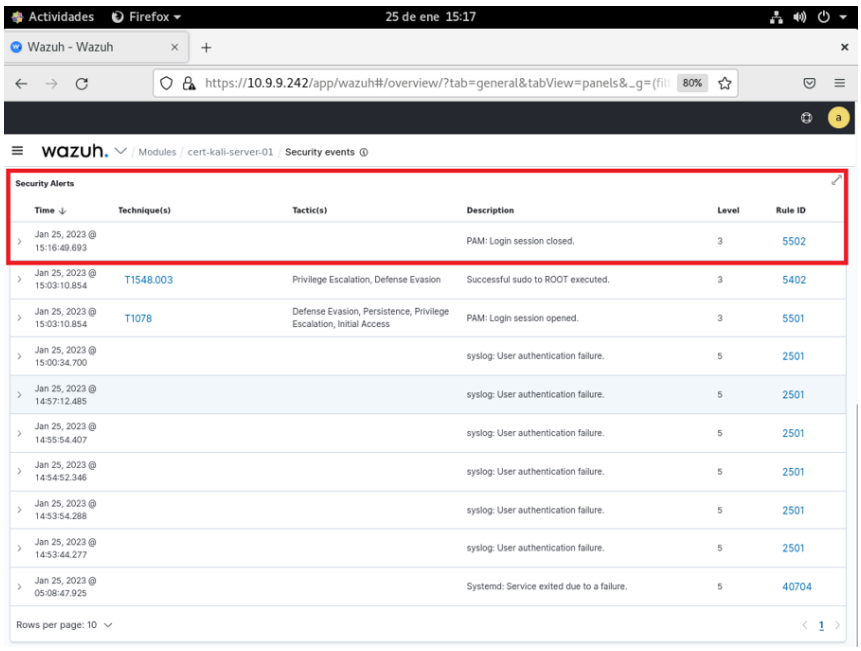
Detalles de autenticación exitosa del agente cert-kali-server-01 PARTE 2



Por último, se registra la actividad de cuando el usuario ha salido del modo de super usuario, como se pude ver el a **Figura 75**.

Figura 75

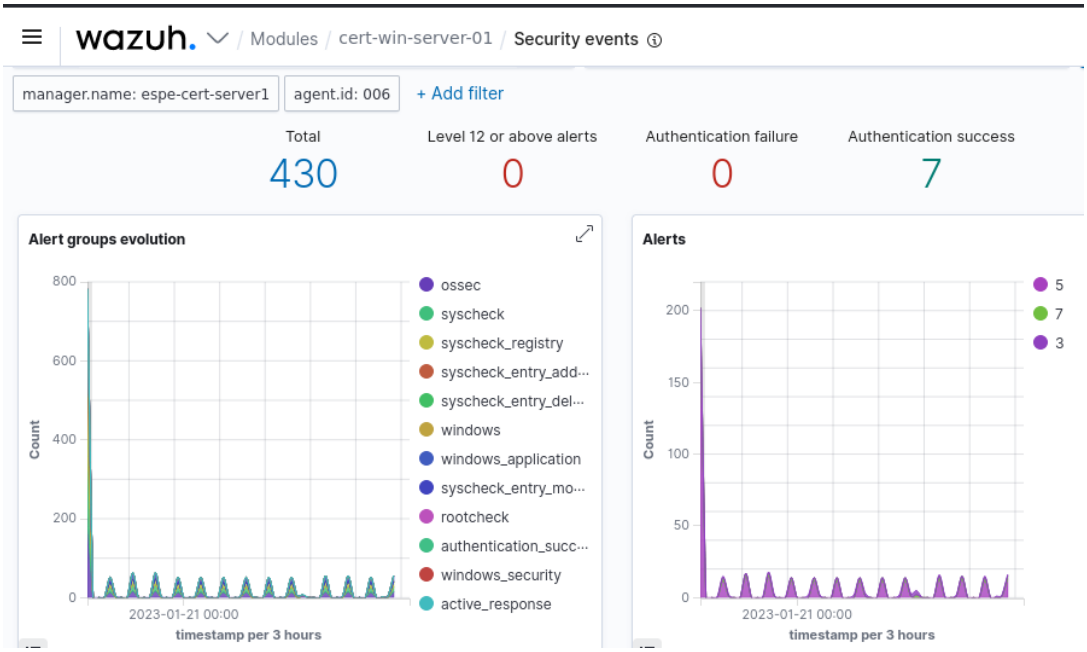
Salida del modo super usuario en el agente cert-kali-server-01



Posible Contenido Oculto en Archivos. Como se puede observar la **Figura 76**, en el agente correspondiente al servidor Windows, se tiene un registro de 430 eventos de seguridad, de las cuales se puede destacar en base al gráfico de alertas, que la gran parte tienen un nivel de impacto de cinco.

Figura 76

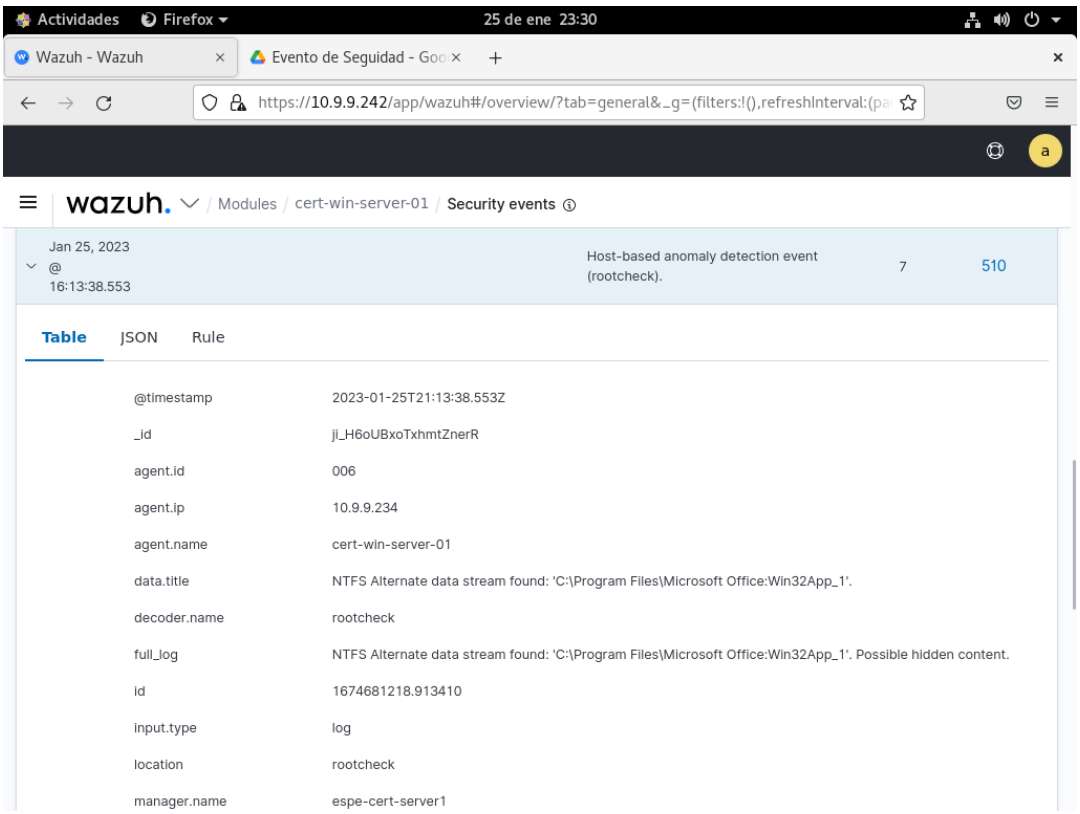
Número total de eventos de seguridad registrados en cert-win-server-01



Al ingresar a los detalles de estos eventos, se puede observar uno con un nivel de impacto 7, el cual se trata de un "*Host-based anomaly detection event (rootcheck)*". En su descripción, se puede visualizar de que uno de los archivos instalados de Microsoft Office, podría tener contenido oculto el cual podría ser de carácter malicioso.

Figura 77

Detección de posible contenido oculto en archivo de Microsoft Office

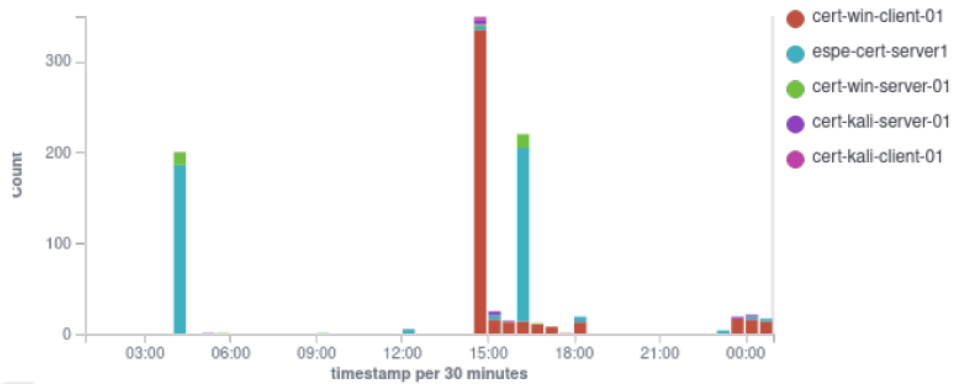


Informes y comunicados. Como parte fundamental en las funcionalidades de Wazuh, se espera poder obtener reportes variados en base a criterios establecidos por el usuario y que sea posible tener una vista general sobre que está sucediendo en los agentes. En esta sección, es posible visualizar algunos de los informes prestados por el SIEM y la información que nos presentan para tener un panorama claro sobre la actividad en los agentes.

Informe de Eventos de Seguridad. El informe de eventos de seguridad muestra un resumen de las alertas recopiladas por cada agente y también por el servidor, en periodos de treinta minutos. Como se puede ver en **la Figura 78**, el agente que presenta más aletas fue el cliente Windows (cert-win-client-01)

Figura 78

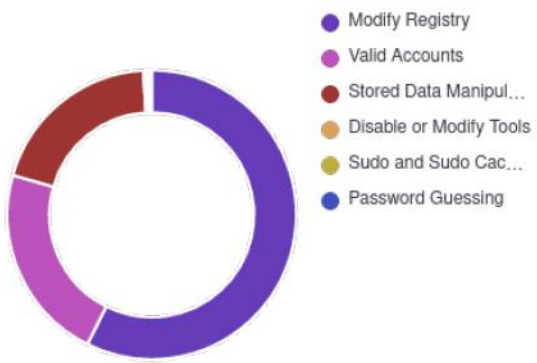
Evolución alertas de los cinco principales agentes



También nos muestra el tipo de alertas más frecuentes registradas, como en la **Figura 79**. Se puede ver que la alerta más frecuente fue la modificación de registros (*Modify Registry*), seguido por las cuentas validas (*Valid Accounts*) y, por último, la manipulación de datos almacenados (*Stored Data Manipulation*).

Figura 79

Alertas de los cinco principales agentes



El informe concluye con un resumen de las alertas **Figura 80**, donde se encuentra registrada la siguiente información:

- La ID de la regla a la que pertenecen;
- La descripción de la alerta;
- El nivel de impacto que tiene la alerta;
- La cantidad de veces que se emitió la alerta.

Figura 80

Resumen de alertas

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	374
752	Registry Value Entry Added to the System	5	205
60106	Windows logon success.	3	110
750	Registry Value Integrity Checksum Changed	5	68
594	Registry Key Integrity Checksum Changed	5	35
533	Listened ports status (netstat) changed (new port opened or closed).	7	22
61104	Service startup type was changed	3	20
60137	Windows User Logoff.	3	17
60642	Software protection service scheduled successfully.	3	10

Informe de Monitoreo de Integridad. Este informe nos proporciona una visión sobre alertas relacionadas con cambios de archivos, incluidos permisos, contenido, propiedad y atributos. Se puede observar las reglas establecidas sobre el monitoreo de integridad de archivos (FIM) que más generaron alertas, en el caso del informe mostrado en la **Figura 81**, las tres reglas son:

- *Registry Value Entry Added to the System* (Ingreso de Valor Registral Agregado al Sistema)
- *Registry Value Integrity Checksum Changed* (Modificación de la suma de verificación de integridad del valor del registro)
- *Registry Key Integrity Checksum Changed* (La suma de verificación de integridad de la clave de registro cambió)

Figura 81

Principales reglas que generan la mayoría de alertas

Top 3 FIM rules

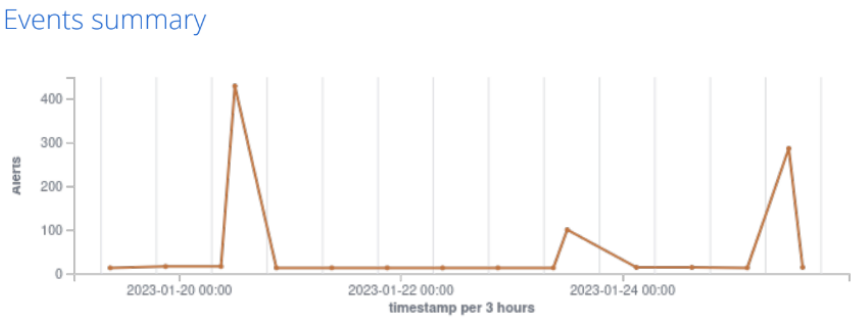
Top 3 rules that are generating most alerts.

Rule ID	Description
752	Registry Value Entry Added to the System
750	Registry Value Integrity Checksum Changed
594	Registry Key Integrity Checksum Changed

También es posible ver una gráfica que nos indica la cantidad de alarmas generadas a través del tiempo, como es posible observar en la **Figura 82**, se registró que aproximadamente el 21 de enero, existió un pico mayor a 400 alertas sobre el monitoreo de integridad de archivos.

Figura 82

Resumen de eventos registrados sobre FIM



De la misma manera, se presenta una tabla que nos indica los usuarios de cada agente, que más han realizado cambios en archivos y de esta manera, han afectado su integridad. Como se puede visualizar en la **Figura 83**, el usuario *SYSTEM* del agente cert-win-client-01, el cual es usado por el SO para la carga o precarga de servicios importantes en el inicio del sistema operativo, ha sido el que más cambios ha realizado en archivos, con un total de 76 cambios registrados.

Figura 83

Principales usuarios que han realizado cambios en archivos

Top users

Top user	Agent ID	Agent name	Count
SYSTEM	004	cert-win-client-01	76
Administradores	004	cert-win-client-01	60
SYSTEM	006	cert-win-server-01	28
root	000	espe-cert-server1	26
Administradores	006	cert-win-server-01	13
SERVICIO\ LOCAL	004	cert-win-client-01	5
Servicio\ de\ red	004	cert-win-client-01	5

Servicio de Validación y Prueba

Plan de Investigación de Campo e Instrumentos de Investigación de Campo.

Se planteo el plan de investigación de campo en donde los objetivos de control fueron la evaluación de la implantación del servicio y la evaluación de la operación del servicio con el fin de establecer una serie de preguntas básicas, las cuales fueron respondidas por medio de una guía de observación que fue establecida en base al instrumento seleccionado para evaluar este tipo de servicio, el cual es la observación. El plan de investigación completo puede ser visualizado en **Anexo 3**. En base a la recopilación de las alertas generadas, se generó una base de datos de las lecciones aprendidas, la cual se observa en la **Tabla 21**.

Tabla 21

Base de datos de lecciones aprendidas

ID de regla	Descripción del incidente	Nivel de amenaza	Conteo	Posible solución
510	Host-based anomaly detection event (rootcheck)	7	374	Verificar que el antivirus se encuentre actualizado y ejecutar un análisis del sistema. También se puede poner en cuarentena el archivo para realizar un análisis de su contenido y verificar si es un falso positivo.
752	Registry Value Entry Added to the System	5	205	La causa detrás de este error proviene del decodificador FIM que intenta extraer el value_type campo del json incorrecto. El decodificador intenta capturarlo en el mismo nivel que los campos arch y value_name. Se debe mover este campo

ID de regla	Descripción del incidente	Nivel de amenaza	Conteo	Posible solución
				para que se extraiga en fim_fetch_attributes_state.
2501	Syslog: User authentication failure	5	9	Configurar un número limitado de intentos para ingresar a la sesión.
533	Listened ports status (netstat) changed (new port opened or closed).	7	55	Identificar el puerto afectado y verificar si es necesario que esté abierto, o en caso de que haya sido cerrado, verificar cual fue la acción que lo provocó.
504	Ossec agent disconnected.	3	2	Esta alerta surge debido que el agente entra en modo de suspensión, ya que no se utilizado el equipo por más de 30 minutos. Lo que se recomienda hacer es incrementar el periodo de tiempo de espera del agente dentro de get_agent_status().
550	Integrity checksum changed.	7	4	En gran parte, se debe al prelinking, que es una utilidad para acelerar la vinculación dinámica de las librerías de las aplicaciones. Si no se desea recibir estas alarmas por esto, es posible

ID de regla	Descripción del incidente	Nivel de amenaza	Conteo	Posible solución
				deshabilitar esta funcionalidad, si se realiza esto y aun se siguen recibiendo alertas, existe la posibilidad de que el agente haya sido hackeado.
60602	Windows application error event	9	1	La solución consiste en actualizar a la última versión del programa. En caso de no querer actualizar se pude deshabilitar el mecanismo de sincronización del registro. Si el problema persiste informará al personal de soporte, ya que es un error que debe ser depurado por los desarrolladores.
61104	Service startup type was changed	3	40	Lo que se recomienda realizar en estos casos es ir a las propiedades del servicio y realizar un reinicio. También se debe verificar que el servicio este actualizado.
553	File deleted	7	86	Identificar si el archivo eliminado es parte crucial para la ejecución del sistema operativo o alguna aplicación crucial, y en base a este, realizar si es necesario su respectiva restauración en el directorio al que pertenece.

ID de regla	Descripción del incidente	Nivel de amenaza	Conteo	Posible solución
554	File added to the system	5	215	Identificar si a la ruta en la que fue agregado el nuevo archivo es un directorio de archivos de configuración del sistema operativo, ya que su contenido podría afectar al funcionamiento normal del agente o incluso podría ser un exploit.

Evaluación Técnica del Servicio. Mediante las preguntas planteadas en el plan de investigación de campo, en la **Tabla 22** se han puesto las mismas con sus respectivas respuestas. En el **Anexo 3**, se encuentra de forma detallada la guía de observación en donde se plantearon los objetivos, las preguntas básicas y sus respuestas.

Tabla 22

Preguntas del plan de investigación de campo

Preguntas básicas	Resultado
¿Cómo se procesan las solicitudes que entran al ESPE-CERT?	Haciendo uso de la observación, se pudo conocer cuál es el proceso que realiza el operador del ESPE-CERT para realizar las peticiones de los servicios.
¿Cómo se realizó el diseño del servicio de monitoreo mediante un correlacionador de	Se plantearon los procesos definidos por el marco de trabajo ITIL en su versión 4, en donde para un correcto diseño del servicio, se definió la coordinación del diseño, la gestión del catálogo de servicios, la gestión de los niveles de servicio, la gestión de seguridad de la información, la administración de

Preguntas básicas	Resultado
eventos (SIEM)?	suministros, la administración de disponibilidad, la gestión de la capacidad y la gestión de la continuidad del servicio.
¿Cuáles son los servicios que están implementados en el ESPE-CERT?	Los servicios implementados en el ESPE-SERT son los siguientes: - Análisis de vulnerabilidades - Monitoreo y alerta de primer nivel - Firma electrónica
¿Cuáles servicios se encuentran en proceso de implementación?	Los servicios en proceso de implementación en el ESPE-SERT son los siguientes: - Gestión de incidentes - Asesoramiento técnico y consultoría - Hacking ético
¿Cuál será el alcance y objetivos planteados en el plan de transición?	Los objetivos planteados se basarán en preparación del hardware, realizar la implantación del servicio tanto en el servidor como en los agentes y monitorear los eventos de seguridad. Para el alcance, se definió que se realizará el monitoreo de los equipos del ESPE-CERT, y el procedimiento de instalación tendrá un aproximado de dos semanas.
¿Cuál será el orden de la instalación de los componentes del SIEM?	En base a la arquitectura de los componentes de Wazuh, se debe realizar la instalación en el siguiente orden: 1. Wazuh indexer 2. Wazuh manager 3. Wazuh dashboard

Preguntas básicas	Resultado
¿En qué área se van a localizar los sensores?	Los sensores se van a localizar en el ESPE-CERT, en donde se encuentran dos servidores y dos clientes para monitorear. Lo adecuado sería tener más sensores ubicados en distintas áreas de la universidad.
¿Hubo problemas en la instalación y configuración del servidor SIEM?	No se dieron problemas al momento de instalar el servicio y su posterior configuración, ya que se tuvieron los permisos de red adecuados para poder descargar los componentes necesarios, además de que si existe conectividad entre los equipos del ESPE-CERT para acceder al *dashboard* desde otro ordenador y proceder con las configuraciones.
¿Hubo problemas en la instalación y configuración de los agentes (sensores) ubicados en el ESPE-CERT?	No existieron inconvenientes al momento de realizar la instalación en los agentes ya que estaban conectados a la red, y tenían conectividad con el servidor para realizar las solicitudes al API REST de Wazuh para enrolar los agentes.
¿Existe conectividad entre el servidor y los agentes?	Si existe conectividad entre los agentes y el servidor, con lo cual se realizó las solicitudes al API REST de Wazuh para enrolar los agentes.
¿Se están mostrando correctamente cada uno de los	Al usar los módulos de Wazuh, fue posible visualizar los incidentes registrados en los agentes, como el caso de los eventos de seguridad, en donde se detallaron cada uno de los eventos que estaban ocurriendo en los agentes. La visualización de los incidentes podría ser distinta si se

Preguntas básicas	Resultado
incidentes registrados?	implementaran nuevas reglas de correlación, en donde la información visualizada se personalizaría, además de que se tendrían incidentes en base a los criterios que se establezcan.
¿Qué funcionalidades se encuentran disponibles en el SIEM implementado?	Entre las funcionalidades de Wazuh se encuentra las siguientes: - Eventos de seguridad - File Monitoring Integrity (FIM) - Detección de vulnerabilidades - Evaluación de configuración de seguridad - Generación de informes Cabe mencionar que el SIEM también posee otras funcionalidades que no están siendo utilizadas por falta de capacitación y configuración sobre las mismas. Dichas funcionalidades podrían ayudar a tener un panorama más claro sobre los eventos ocurridos en los sensores además de permitir auditar de mejor manera a un agente.
¿Se están detectando incidentes de seguridad en los sensores?	Si se están detectando incidentes de seguridad, un ejemplo es la detección de un archivo troyano en uno de los sensores. Se desconoce si esta funcionalidad seguiría siendo efectiva en sensores que se encuentren en otra área que no sea el ESPE-CERT.
¿Los reportes muestran la	Se puede acceder a los detalles en cada uno de los registros generados sobre un incidente, en donde se pueden

Preguntas básicas	Resultado
información necesaria sobre un incidente registrado?	ver posibles acciones para remediarlo, además de más detalles sobre la naturaleza del mismo.
¿La información detallada de los incidentes es correcta y corresponde con el agente en cuestión?	La información mostrada si es la adecuada y esta puede ser visualizada en base a un registro dado en un agente, en donde se considera cual es sistema operativo base para emitir los detalles y posibles recomendaciones.
¿Se logró recopilar las distintas alertas y encontrar una solución?	Se realizó una recopilación de las diversas alertas, teniendo en consideración su nivel de impacto y su frecuencia, con esto, se planteó las posibles soluciones en base a sitios web oficiales.

Informe de Auditoría. En base a los resultados obtenidos en la evaluación técnica mediante la guía de observación, se realizó un informe de auditoría en base del formato de ITAF de ISACA, el cual se puede observar a detalle en el **Anexo 4**. En el informe, se establecieron observaciones y recomendaciones de los hallazgos encontrados los cuales pueden ser resumidos en los siguientes criterios:

Funcionalidad del Servicio

La implementación del servicio de monitoreo de amenazas mediante un SIEM proporciona una manera de tener una plataforma centralizada para visualizar los eventos que están ocurriendo en los sensores monitoreados. El SIEM implementado, Wazuh, posee una serie de funcionalidades que, al ser utilizadas, entregaron resultados satisfactorios en

base a criterios establecidos, como reportes en base a eventos de seguridad, análisis de vulnerabilidades, entre otros.

Sin embargo, Wazuh posee algunas funcionalidades que deben tener una configuración más profunda para funcionar adecuadamente y que proporcionarían información valiosa al momento de monitorear los sensores.

Las funcionalidades más llamativas y que no están siendo utilizadas son el cumplimiento normativo y monitoreo de políticas, las cuales poseen sus respectivas sub funcionalidades.

Procedimiento de instalación

La instalación del nuevo servicio se siguió en base al orden establecido por la documentación oficial de Wazuh, donde el orden de instalación fue el indexer, el servidor y por último, el dashboard. Posterior a esto, se procedió a enrolar a los sensores para que puedan ser monitoreados, en donde se enrolaron dos servidores y dos equipos cliente localizados en el ESPE-CERT.

Con estos cuatro sensores, fue posible verificar el funcionamiento de ciertas características del SIEM, sin embargo, no se tiene claro si los resultados fueran los mismos en el escenario en donde se tengan sensores ubicados fuera de la red del ESPE-CERT, además no se conoce si el rendimiento se vería afectado al momento de la generación de reportes o al visualizar los eventos registrados si se tuviera una cantidad más extensa de agentes enrolados al SIEM.

Mejora y creación de reglas

Al momento de la instalación de Wazuh, este viene con una serie de reglas de correlación predefinidas por los creadores. Se puede evidenciar el funcionamiento de las mismas al momento de revisar los eventos de seguridad, alarmas y alertas, entre otros, ya que al ingresar al dashboard de una de las funcionalidades, se puede observar que se tiene un registro detallado lo que está ocurriendo de manera individual o grupal en los agentes.

Sin embargo, si se implementaran reglas adicionales y si se realizaría una mejora de las reglas ya existentes, se podrían capturar eventos más detallados en base a criterios

establecidos por el personal que opera el servicio, además de que se tendría alguna información adicional sobre un evento en particular.

Mejora

En esta última actividad, se realiza el planteamiento del plan de mejora para que sea considerado y desarrollado a futuro en base a las conclusiones establecidas en el informe de auditoría, las cuales están basadas en los criterios de funcionalidad, procedimiento de instalación y mejora y creación de reglas:

- Se debe realizar un uso más a profundidad del SIEM Wazuh, el cual cuenta con una serie de funcionalidades que no están siendo explotadas al máximo, esto debido a la falta de capacitación sobre cómo usarlas y configurarlas. Es importante señar que, si se usaran estas funcionalidades, se tendría una mejor visión sobre las posibles mejoras en el aspecto de políticas y cumplimiento normativo de los agentes.
- En al procedimiento de instalación, se puede señalar que se requieren agregar más agentes para que sean monitoreados con el SIEM, esto con el objetivo de poder determinar si el rendimiento se vería afectado y visualizar si existen inconvenientes al momento de tener agentes externos al área del ESPE-CERT con respecto a la captura de eventos de seguridad.
- De la misma manera, el hacer uso solamente de las reglas establecidas por Wazuh, si permite tener un registro adecuado de lo que sucede en cada agente, sin embargo, al implementar reglas adicionales, se podría tener un control más personalizado en base a experiencias previas sobre eventos antes ocurridos en el área de ESPE-CERT.

Mejora Continua

Objetivo

Tomar las acciones necesarias en base a las recomendaciones emitidas en el informe de auditoría mediante una capacitación más profunda sobre Wazuh y la instalación

de agentes adicionales para mejorar el funcionamiento del servicio y hacer uso de todas sus capacidades.

Alcance

Realizar mejoras en el servicio de monitoreo de amenazas mediante un SIEM por medio del uso completo de todas las funcionalidades ofrecidas por la herramienta, además de agregar nuevos agentes que no pertenezcan al área del ESPE-CERT e implementar nuevas reglas de correlación para tener una visión más personalizada sobre los eventos que ocurren los agentes.

Indicadores de cumplimiento

- Uso de funcionalidades adicionales.
- Agregación de nuevos agentes.
- Mejora o agregación de reglas.

Recursos

- Personal operador del ESPE-CERT
- Servidor CentOS donde se ejecuta el servicio
- Sensores pertenecientes a otras áreas
- Acceso a los distintos segmentos de red de otras áreas

Acciones a realizar

En la **Tabla 23**, se plantearon las acciones que se deberían realizar para mejorar el servicio y el orden recomendado para no tener inconvenientes en el proceso.

Tabla 23

Acciones para el plan de mejora

Ord.	Criterio	Descripción
1	Uso de funcionalidades adicionales	Realizar una capacitación sobre el uso de las funcionalidades que no están siendo usadas de Wazuh, las cuales son el cumplimiento de normativa y el monitoreo de políticas.

Ord.	Criterio	Descripción
2	Uso de funcionalidades adicionales	Replicar lo aprendido en los agentes que se encuentran actualmente siendo monitoreados por Wazuh para realizar las configuraciones respectivas y verificar si las nuevas funcionalidades, están dando resultados.
3	Mejora o agregación de reglas	Realizar una capacitación sobre el funcionamiento de las reglas de correlación en Wazuh, en donde son configuradas y cuáles son las consideraciones para agregar nuevas reglas.
4	Mejora o agregación de reglas	Realizar un análisis de las reglas de correlación actuales y verificar si es necesario modificar alguna de estas para tener mejores resultados en los reportes.
5	Mejora o agregación de reglas	En base a la situación actual del ESPE-CERT, considerar si es necesario plantear y agregar nuevas reglas para obtener reportes más específicos.
6	Agregación de nuevos agentes	Realizar una planificación sobre en qué áreas se podrían localizar nuevos agentes para ser monitoreados por Wazuh para extender el servicio.
7	Agregación de nuevos agentes	Verificar que exista conectividad entre el servidor CentOS que contiene a Wazuh y los nuevos sensores, para así proceder a realizar la instalación del agente y su enrolamiento.
8	Agregación de nuevos agentes	Verificar en el *dashboard* de Wazuh que los agentes se hayan enrolado correctamente y realizar las configuraciones necesarias para tener un monitoreo más eficiente.

Capítulo V:

Conclusiones y Recomendaciones

Conclusiones

El servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) se implementó de manera satisfactoria en el área del ESPE-CERT, siguiendo el marco de trabajo establecido por ITIL V4, el cual sugiere una serie de actividades para una correcta gestión de un servicio. Se analizó la situación actual de los servicios del ESPE-CERT y su infraestructura tecnológica disponible. Es así que, siguiendo las actividades de plan, diseño y transición, entrega y soporte y mejora, se consiguió agregar de manera apropiada el nuevo servicio al portafolio de servicios del ESPE-CERT.

Se realizó la búsqueda de estudios primarios que estén estrechamente relacionados a la problemática del presente trabajo de titulación. Dichos estudios sirvieron de apoyo y guía para entender qué es y cómo funciona un correlacionador de eventos (SIEM) y los benéficos que pude traer el uso de esta herramienta a la institución. Los estudios primarios también fueron de ayuda al momento de realizar las actividades de ITIL V4.

El plan del servicio consistió primero en conocer cuáles son las necesidades del negocio, al saber que servicios se encuentran implementados y cuales están en proceso de implementación, nos permitió buscar una herramienta *Open Source* que sirva de apoyo y que no obstaculice con los demás servicios. También nos permitió distribuir los recursos con los que cuenta el ESPE-CERT.

Las actividades de diseño y transición fueron trascendentales para determinar en cuál de los servidores disponibles se iba a instalar el SIEM en base a sus capacidades tecnológicas debido a que se requirió de un equipo con una alta gama de características que pueda soportar y permitir que se ejecute de manera eficiente el SIEM. Además, se analizó las acciones que se deberían tomar en caso de que el servicio fallase y cuáles son los SLA ofertados.

Mediante la gestión de lanzamiento, se pudo realizar una correcta implantación del SIEM en el servidor designado gracias a que se realizó el planteamiento de objetivos y el alcance del plan, además de establecer las fechas para desarrollar cada tarea. Al realizar la implantación, no se presentó ningún inconveniente gracias a que existía conectividad entre los equipos y acceso libre al Internet.

En la entrega y soporte del servicio se realizaron diversas pruebas con las herramientas que ofrece el SIEM Wazuh, como son: la evaluación de configuración de seguridad; los eventos de seguridad; las alerta y alarmas; la generación de informes y comunicados. Para procesar toda esta información se hizo uso de una guía de observación como instrumento de investigación.

Finalmente, como parte de la mejora, se pudo determinar qué acciones se requieren y cual debería ser su orden para la implementación de mejoras en el servicio y que este sea utilizado en su totalidad, puesto que actualmente no se cuentan con muchos agentes además de que sus funcionalidades no están siendo usadas al máximo.

Recomendaciones

La instalación de los agentes se realizó solamente en los equipos pertenecientes al área del ESPE-CERT, por lo cual se recomienda extender el servicio de monitoreo a otras áreas de la universidad que cuenten con una serie de equipos que ejecuten procesos críticos de la institución, los cuales podrían también ser monitoreados por el nuevo servicio.

El SIEM Wazuh cuenta con una gran variedad de funcionalidades, de las cuales no pudieron ser explotadas en su totalidad debido a la falta de experiencia y conocimientos en algunos apartados. Por lo que, para mejorar en este aspecto se recomienda coordinar cursos de capacitación, estos pueden realizarse de manera individual por el área del ESPE-CERT o en cooperación junto con las UTIC, ya que cuentan con un el mismo servicio de monitoreo, pero a nivel de *outsourcing*.

Finalmente, se recomienda al personal que va a operar el nuevo servicio, tenga un amplio conocimiento sobre los manuales desarrollados que son el de usuario y el de

instalación para que puedan manejar de manera eficiente los módulos del SIEM, y también en caso de que sea necesaria la reinstalación del servicio, se tenga claro cuál es el procedimiento y los pasos a seguir para volver a tener el servicio lo más rápido posible en ejecución.

Bibliografía

Abhinav, K. K. (2016). ITIL Service Lifecycle. *Become ITIL Foundation Certified in 7 Days*, 33-44.

Ahmad, Z., Shahid, A., Wai, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans Emerging Tel Tech.*, 1-29.

Becerra Acosta, G., & Paramo Calderón, C. A. (2021, Diciembre 3). *Universidad Piloto de Colombia.* Retrieved from Implementación de un sistema de correlación de eventos basado en software libre para la empresa sistemas integrales de informática SISA S.A enfocado al área del SOC SISAMAX: http://repository.unipiloto.edu.co/handle/20.500.12277/11530

Bernal Barzallo, P. F., & Mejía Broncano, M. A. (2021, Septiembre). *Implementación de una solución "security information and event Mangement" escalable y accesible basada en open source.* Retrieved from https://repositorio.pucesa.edu.ec/handle/123456789/3291

Bickerstaffe, E. (2018). Data leakage prevention. *Information Security Forum, Tech. Rep.*

Calderón Arateco, L. L. (2015, Septiembre 10). *Seguridad informática y seguridad de la información.* Retrieved from http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Carrón Jumbo, J. L., & Jumbo Vivanco, P. L. (2019). *Implmetanción de un SIEM para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar ISO 27032.* Retrieved from http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf

Cestari Filho, F., Motta, A., & Boca Piccolini, J. D. (2022, Diciembre). *ITIL Information Technology Infraestructure Library.* Retrieved from https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI7.pdf

cisco.com. (2022, Noviembre). *¿Qué es el monitoreo de red?* Retrieved from https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

Falah Faiz, M., Arshad, J., Alazab, M., & Shalaignov, A. (2019, Noviembre 4). *Predicting likelihood of legitimate data loss in email DLP.* Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0167739X19314943#:~:text=Based%20on%20the%20outcomes%20of,true%20positive%20rate%20of%2090%25.

Fernández Granados, J. E., Herrera Kairuz, J. H., & Camilo García, J. C. (2017). *Implementación de un security information and event management –SIEM– en el comando de la armada nacional. Dirección de tecnologías de la información y las comunicaciones.* Retrieved from http://polux.unipiloto.edu.co:8080/00003801.pdf

Fernzandez, A., Insfran, E., & Abrahão, S. (2011). *Usability evaluation methods for the web: A systematic mapping study.* Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0950584911000607

García Arias, J., & Rodríguez Duarte, L. K. (2021). *Plan de mejoramiento SIEM o correlacionador de ebentos de seguiridad para el ministerio de educación nacional.* Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/10930/Proyecto%20Grado%20SIEM-MEN.pdf?sequence=12

González, G., González, S., & Diaz, R. (2021). *Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures.* Sensors.

Herrera Kairul, J. H., Fernández Granados, J. E., & García Ruíz, J. C. (2017, Abril 8). *Implementación de un security information and event management -SIEM- en el comando de la Armanda Nacional. Dirección de tecnologías de la información y las comunicaciones.* Retrieved from http://repository.unipiloto.edu.co/handle/20.500.12277/2657

Husham Ali, B., Adeeb Jalal, A., & Ibrahem Al-Obaydy Al-Obaydy, W. N. (2020, Enero 11). *Data loss prevention by using MRSH-v2 algorithm.* Retrieved from https://ijece.iaescore.com/index.php/IJECE/article/view/18663/14014

INCIBE. (2022, Dicembre 01). *Protecciónb de la infromación.* Retrieved from https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

iso27000.es. (2022). *Serie "27000"*. Retrieved from https://www.iso27000.es/iso27000.html

IT Service. (n.d.). *Capacitación de ITIL 4 Foundation.* Retrieved from https://itserviceuniversity.com/curso-itil-fundamentos/

Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices. *Intrusion Detection System for IoT Edge Devices*, 1-16.

Játiva Alvarez, J. X., & Muñoz Alvarez, L. D. (2022, Octubre). *Implementación de un gestor de información y eventos de seguridad (SIEM) para la prevención y detección de ciber amenazas en una entidad gubernamental.* Retrieved from https://repositorio.uisek.edu.ec/handle/123456789/4865

Kotenko, I., Kuleshov, A., & Ushakov, I. (2017). Aggregation of Elastic Stack Instruments for Collecting, Storing and Processing of Security Information and Events. *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*.

Lara, S. (2022). *Gestión de la Seguridad de Información ISO/IEC 27000 IT Service Management Principales preocupaciones empresariales.* Retrieved from https://www.academia.edu/30334406/Gestión_de_la_Seguridad_de_Información_ISO_IEC_27000_IT_Service_Management_Principales_preocupaciones_empresariales

Marrone, M., & Kolbe, L. (2011). Impact of IT Service Management Frameworks on the IT Organization. *Business & Information Systems Engineering*, 5-18.

Milajerdi, S., Gjomemo, R., Eshete, B., Sekar, R., & Venkatakrishnan, V. (2019). HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows. *2019 IEEE Symposium on Security and Privacy (SP)*, 1137-1152.

Neupane, K., Haddad, R., & Chen, L. (2018, Octubre 4). *Next Generation Firewall for Network Security: A Survey*. Retrieved from https://ieeexplore.ieee.org/document/8478973

ossec.net. (2022, Diciembre 4). *Host Intrusion Detection for Everyone*. Retrieved from https://www.ossec.net/about/

Pacha, M., & Ruiz, J. (2022). Desarrollo del manual de procesos operativos para el CERT académico de la ESPE utilizando estándares internacionales. *Repositorio institucional de la ESPE*.

Pazmiño Gómez, C. A., & Pazmiño Gómez, J. L. (2018). *Implementación de un correlacionador de eventos basado en software libre para la detección de ataques informaticos en la empresa eléctrica.* Retrieved from http://dspace.espoch.edu.ec/bitstream/123456789/8445/3/98T00191.pdf

Peffers, K., Tuunanen, T., & Rothenberger, M. A. (2007, Enero). *A design science research methodology for information systems research.* Retrieved from https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2014, Diciembre 8). *A Design Science Research Methodology for Information Systems Research.* Retrieved from https://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222240302#:~:text=The%20DS%20process%20includes%20six,demonstration%2C%20evaluation%2C%20and%20communication.

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008, Junio 26). Retrieved from https://dl.acm.org/doi/10.5555/2227115.2227123

Radoglou, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., . . . Ramos, F. (2021). *SPEAR SIEM: A Security Information and Event Management system for the Smart Grid.* Computer Networks.

RedHat. (2022, Noviembre). *Linux 4: Manual de seguridad*. Retrieved from https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-host.html

Remache Típan, M. L. (2022, Febrero). *BIBDIGITAL.* Retrieved from Marcos de gestión de tecnologías de información : análisis del marco de gestión ITIL v4.: https://bibdigital.epn.edu.ec/handle/15000/22414

Rivera Montoya, S., & Perez Cataño, C. A. (2018). *Afinación de reglas en un SIEM para correlacionar los eventos de seguridad del laboratorio de redes convergentes del ITM.* Retrieved from https://repositorio.itm.edu.co/handle/20.500.12622/488

Romero Castro, M. I., Figueroa Moran, G., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., & Murillo Quimiz, L. R. (2018, Octubre). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Retrieved from https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

Särelä, M., Kyöstilä, T., Kiravuo, T., & Manner, J. (2017). Evaluating intrusion prevention systems with evasions. *Department of Communications and , Aalto University*, 1-15.

Taylor, S. (2007). The official introduction to the ITIL service lifecycle. *London: The Stationary*.

Technopedia. (2015, Abril 8). *Security Event Management.* Retrieved from https://www.techopedia.com/definition/25763/security-event-management

Technopedia. (2022, aGOSTO 9). *Security Information Management (SIM).* Retrieved from https://www.techopedia.com/definition/4098/security-information-management

Voronkov, A., Horn Iwaya, L., Martucci, L. A., & Lindskog, S. (2017, Diciembre 6). *Systematic Literature Review on Usability of Firewall Configuration*. Retrieved from https://dl.acm.org/doi/10.1145/3130876

Wazuh Inc. (2022). *Architecture*. Retrieved from Wazuh: https://documentation.wazuh.com/current/getting-started/architecture.html

wazuh.com. (2022, Diciembre 4). *Wazuh Capabilities*. Retrieved from https://wazuh.com/platform/

Apéndices