ATMIRE

Title	Implementación de una solución SIEM basado en Open Source para la detección de vulnerabilidades y amenazas con el marco MITRE ATT&CK, para una BPO de Contact Center
Item Type	http://purl.org/coar/resource_type/c_7a1f
Authors	Guzmán Llontop, Lorena;Florencio Gutierrez, Miki Luiggi
Publisher	Universidad Peruana de Ciencias Aplicadas (UPC)
Rights	https://purl.org/coar/access_right/c_abf2
Download date	2026-11-27 00:25:22
Item License	https://creativecommons.org/licenses/by-nc-sa/4.0/
Link to Item	https://hdl.handle.net/10757/690705



UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y COMUNICACIONES

Implementación de una solución SIEM basado en Open Source para la detección de vulnerabilidades y amenazas con el marco MITRE ATT&CK, para una BPO de Contact Center

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR(ES)

Florencio Gutierrez, Miki Luiggi	0009-0001-4570-3653
Guzmán Llontop, Lorena	0009-0001-3886-5371

ASESOR(ES)

Seminario Garcia, Hernan Augusto	0000-0001-6971-355X

Lima, 24 de junio de 2026

DEDICATORIA

A mis padres, tíos, primos y familiares con quienes crecí y compartí cada etapa de mi vida.

Miki

A mis padres, abuelos y hermanas, por su esfuerzo constante, su apoyo incondicional y por enseñarme con su ejemplo, el valor de la perseverancia ante cada desafío.

Lorena

AGRADECIMIENTOS

Agradecemos a la universidad por brindarnos la oportunidad de acceder al conocimiento y contribuir a nuestra formación académica. Asimismo, expresamos nuestro agradecimiento a la empresa y, en especial, al área de Sistemas, por la apertura y las facilidades otorgadas en infraestructura y recursos tecnológicos, los cuales fueron fundamentales para la ejecución de este proyecto. De igual manera, agradecemos a nuestros compañeros de carrera por el apoyo mutuo y los consejos compartidos a lo largo del proceso académico. Finalmente, agradecemos a nuestro asesor por su orientación y acompañamiento durante la elaboración y culminación del presente trabajo.

RESUMEN

La presente investigación tiene como propósito implementar un sistema Security Information and Event Management (SIEM) basado en herramientas Open Source para fortalecer la detección de vulnerabilidades y amenazas mediante el marco MITRE ATT&CK en una empresa del sector servicios. El estudio aborda la problemática de la limitada visibilidad sobre eventos críticos de seguridad y la ausencia de una correlación estructurada frente a tácticas y técnicas empleadas por atacantes. Para ello, se identificaron los componentes críticos de la infraestructura y se evaluaron alternativas SIEM, seleccionándose ELK Stack como la solución más adecuada. Posteriormente, se diseñó una arquitectura que garantice la centralización de logs y se configuró un SIEM operativo con la integración de dos firewalls y dos servidores críticos. La validación del diseño se realizó mediante pruebas de disponibilidad, rendimiento y recepción de eventos. Asimismo, se implementaron casos de uso alineados a MITRE ATT&CK, orientados a ataques de fuerza bruta, intentos de acceso indebido y manipulación de cuentas administrativas, verificándose la detección exitosa de alertas y un tiempo medio de detección inferior a lo establecido inicialmente. Finalmente, se ejecutó un programa de capacitación para el personal de soporte TI, donde se alcanzó un nivel de asistencia y mejora superiores a los criterios establecidos. Los resultados obtenidos demostraron que el SIEM implementado cumple con los objetivos planteados, mejora significativamente la capacidad de monitoreo y fortalece la postura de seguridad de la organización.

Palabras clave**:** SIEM; ciberseguridad; MITRE ATT&CK; monitoreo de eventos; detección de amenazas; ELK Stack.

“Implementation of an Open-Source SIEM Solution for the Detection of Vulnerabilities and Threats Using the MITRE ATT&CK Framework in a Contact Center BPO”

ABSTRACT

The purpose of this research is to implement a Security Information and Event Management (SIEM) system based on Open Source tools to strengthen the detection of vulnerabilities and threats using the MITRE ATT&CK framework in a service sector company. The study addresses the issue of limited visibility over critical security events and the lack of structured correlation against tactics and techniques employed by attackers. To this end, critical infrastructure components were identified, and SIEM alternatives were evaluated, with the ELK Stack selected as the most suitable solution. Subsequently, an architecture was designed to ensure log centralization, and an operational SIEM was configured by integrating two firewalls and two critical servers. The proposed design was validated through availability, performance, and event ingestion tests. In addition, use cases aligned with the MITRE ATT&CK framework were implemented, focusing on brute-force attacks, unauthorized access attempts, and administrative account manipulation, verifying successful alert detection and a mean detection time lower than the initially established threshold. Finally, a training program was conducted for IT support staff, achieving attendance and improvement levels above the defined criteria. The results demonstrate that the implemented SIEM meets the proposed objectives, significantly enhances monitoring capabilities, and strengthens the organization’s security posture.

Keywords: SIEM; cybersecurity; MITRE ATT&CK; event monitoring; threat detection; ELK Stack.

5TSP_RC_202601-FlorencioMiki_GuzmanLorena

INFORME DE ORIGINALIDAD

8%	7%	1%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUD

FUENTES PRIMARIAS

1	repositorioacademico.upc.edu.pe	Fuente de Internet
2	Submitted to Universidad Peruana de Ciencias Aplicadas	Trabajo del estudiante
3	upc.aws.openrepository.com	Fuente de Internet
4	www.gruporecupera.com.pe	Fuente de Internet
5	Submitted to uide	Trabajo del estudiante
6	hdl.handle.net	Fuente de Internet
7	Submitted to Universitat Oberta de Catalunya	Trabajo del estudiante
8	www.dykinson.com	Fuente de Internet
9	www.elastic.co	Fuente de Internet
10	repository.unad.edu.co	Fuente de Internet
11	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC	Trabajo del estudiante
12	malaysia.tamilheritage.org	Fuente de Internet
13	Submitted to University of Winchester	Trabajo del estudiante
14	Submitted to Universidad Mariano Gálvez de Guatemala	Trabajo del estudiante
15	Submitted to Integración Blackboard	Trabajo del estudiante

16	openaccess.uoc.edu Fuente de Internet	
17	www.e3s-conferences.org Fuente de Internet	
18	www.scitel.es Fuente de Internet	
19	French, William. "Enhancing Threat Hunting Automation With Large Language Models." The University of North Carolina at Charlotte, 2024 Publicación	
20	jit.ndhu.edu.tw Fuente de Internet	
21	Submitted to Universitat Politècnica de València Trabajo del estudiante	
22	repositorio.espe.edu.ec Fuente de Internet	
23	repositorio.ucv.edu.pe Fuente de Internet	
24	repositorio.utc.edu.ec Fuente de Internet	
25	bibliotecaunapec.blob.core.windows.net Fuente de Internet	
26	doku.pub Fuente de Internet	
27	repositorio.uisek.edu.ec Fuente de Internet	
28	Submitted to Instituto Especializado de Estudios Superiores Loyola Trabajo del estudiante	
29	esdegrepositorio.edu.co Fuente de Internet	
30	juarez-nl.gob.mx Fuente de Internet	
31	repositorio.esan.edu.pe Fuente de Internet	
32	Submitted to Universidad de Lima Trabajo del estudiante	

33 www.fing.edu.uy
Fuente de Internet

34 Acosta Peña, Diana. "Modelo de Gestión a Incidentes de Seguridad en el Centro de Computación de Alto Desempeño (CECAD)", Universidad Distrital Francisco José de Cal (Colombia)
Publicación

35 Submitted to Unidades Tecnológicas de Santander
Trabajo del estudiante

36 Julio Armando Landázuri Castro, Renato M. Toasa, Maryory Urdaneta Herrera. "Detecti of Unauthorized Use in SIEM Through Behavioral Analysis and Adaptive Rules", International Journal of Advanced Computer Science and Applications, 2026
Publicación

37 pubmed.ncbi.nlm.nih.gov
Fuente de Internet

38 www.comie.org.mx
Fuente de Internet

39 www.ninjaone.com
Fuente de Internet

Excluir citas	Apagado	Exclude assignment template	Activo
Excluir bibliografía	Activo	Excluir coincidencias	< 20 words

TABLA DE CONTENIDOS

1 CAPÍTULO 1: DEFINICIÓN DEL PROYECTO 1

1.1 INTRODUCCIÓN 1

1.2 CASO DE ESTUDIO 2

1.2.1 Organización 2

1.2.2 Situación Problemática 6

1.2.3 Sector de Estudio 10

1.3 ANÁLISIS DEL PROBLEMA 12

1.3.1 Formulación del Problema 12

1.3.2 Análisis 13

1.4 OBJETIVOS 22

1.4.1 Objetivo General 22

1.4.2 Objetivos Específicos 22

1.4.3 Indicadores de Logro de los Objetivos 23

1.5 DESCRIPCIÓN DEL PROYECTO 25

1.5.1 Diagrama de Bloques 25

1.5.2 Estructura de Desglose de Tareas 32

1.5.3 Cronograma del proyecto 33

1.6 ALCANCE DEL PROYECTO 36

2 CAPÍTULO 2: MARCO TEÓRICO 38

2.1 SIEM 38

2.1.1 Arquitectura típica de un SIEM 39

2.1.2 Arquitectura modular de un SIEM 43

2.1.3 SIEMs Open Source 45

2.2 MITRE ATT&CK 57

2.2.1 Dominios tecnológicos 58

2.2.2 Tácticas 60

2.2.3 Técnicas 63

2.3 METODOLOGÍA DE CAPACITACIÓN 69
2.3.1 Método expositivo (lección magistral) 69
2.3.2 Otros métodos 70
3 CAPÍTULO 3: DESARROLLO DEL PROYECTO 73
3.1 IMPLEMENTACIÓN DE LA SOLUCIÓN 73
3.1.1 Identificación de Componentes Tecnológicos 77
3.1.2 Diseño de Arquitectura SIEM (ELK) 86
3.1.3 Implementación del sistema SIEM 91
3.1.4 Implementación de Casos de Uso con Mitre Attack 103
3.1.5 Desarrollo de la Capacitación en SIEM y MITRE ATT&CK 123
3.2 VALIDACIÓN DEL PROYECTO 129
3.2.1 Resultados del Plan de Prueba del Objetivo Específico N°1 130
3.2.2 Resultado del Plan de Prueba del Objetivo Específico N°2 134
3.2.3 Resultado del Plan Prueba del Objetivo Específico N°3 137
3.2.4 Resultado del Plan de Prueba del Objetivo Específico N°4 155
3.2.5 Resultado del Plan de Prueba del Objetivo Específico N°5 181
4 CONCLUSIONES Y RECOMENDACIONES 189
4.1 CONCLUSIONES 189
4.2 RECOMENDACIONES 191
5 REFERENCIAS 192
6 ANEXOS 202
6.1 ANEXO 1: CAPACITACIÓN SIEM Y MITRE ATT&CK. 202
6.2 ANEXO 2: CUESTIONARIO DE EVALUACIÓN: INTRODUCCIÓN AL SIEM Y AL MARCO MITRE ATT&CK 205
6.3 ANEXO 3: IDENTIFICACIÓN DE COMPONENTES CRÍTICOS DE LA INFRAESTRUCTURA 209
6.4 ANEXO 4: EVALUACIÓN DE SOLUCIONES SIEM OPEN SOURCE 214
6.5 ANEXO 5: DISEÑO DE ARQUITECTURA SIEM ELK 218

ÍNDICE DE TABLAS

Tabla 1 Registro de interesados 19
Tabla 2 Indicadores de Logro de los Objetivos 23
Tabla 3 Procedimiento de Actividades 28
Tabla 4 Procedimiento de Actividades 33
Tabla 5 Descripción de las principales técnicas del Marco Mitre Att&ck 65
Tabla 6 Matriz de Requerimientos 74
Tabla 7 Cuadro de componentes de Infraestructura 79
Tabla 8 Evaluación de Soluciones Open Source 82
Tabla 9 Resumen de lista de fuentes 96
Tabla 10 Cuadro de Casos de Uso con Mitre Attack 104
Tabla 11 Resumen de casos de uso y reglas implementadas 109
Tabla 12 Temario de Capacitación 124
Tabla 13 Objetivo específico 1, Definición y Alcance del Plan de Pruebas 130
Tabla 14 Objetivo específico 1, Ejecución del Plan de Pruebas 131
Tabla 15 Objetivo específico 2, Definición y Alcance del Plan de Pruebas 134
Tabla 16 Objetivo específico 2, Ejecución del Plan de Pruebas 135
Tabla 17 Objetivo específico 3, Definición y Alcance del Plan de Pruebas 137
Tabla 18 Objetivo específico 3, Ejecución del Plan de Pruebas 139
Tabla 19 Objetivo específico 4, Definición y Alcance del Plan de Pruebas 155
Tabla 20 Objetivo específico 4, Ejecución del Plan de Pruebas 156
Tabla 21 TTD de alertas generadas por Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1 162
Tabla 22 Listado de alertas generadas de ataque de Fuerza Bruta SSL VPN – Firewall 2 164
Tabla 23 Listado de alertas generadas de ataques de Fuerza Bruta hacia las cuentas de administrador -QNAP 168
Tabla 24 Listado de alertas generadas por cuenta eliminada de un grupo administrador – Active Directory 176
Tabla 25 Objetivo específico 5, Definición y Alcance del Plan de Pruebas 181
Tabla 26 Objetivo específico 5, Ejecución del Plan de Pruebas 182

Tabla 27 Listado de Asistencia de Capacitación 184
Tabla 28 Registro de Resultados del Pre-Test y Post-Test de los Participantes..... 186
Tabla 29 Cálculo del Porcentaje de Mejora de los Participantes..... 187

ÍNDICE DE FIGURAS

Figura 1 Organigrama referencial de la empresa 5
Figura 2 Incremento de Phishing en Perú 6
Figura 3 Incremento de malware en Perú 7
Figura 4 Sectores afectados por ciberataques en Perú 8
Figura 5 Sectores afectados por los grupos de ataque MITRE ATT&CK 9
Figura 6 Diagrama de red de la empresa 11
Figura 7 Árbol de problemas 14
Figura 8 Matriz de Interesados 21
Figura 9 Diagrama de bloque del diseño de la solución 26
Figura 10 Estructura de Desglose de Tareas (EDT) 32
Figura 11 Diagrama de Áreas Involucradas al proyecto 36
Figura 12 Sistema de procesos de un SIEM 39
Figura 13 Arquitectura básica de un SIEM 41
Figura 14 Arquitectura modular teórica de un SIEM 45
Figura 15 Arquitectura de clúster de un SIEM basada en Elastic Stack 47
Figura 16 Arquitectura de Logstash 48
Figura 17 Arquitectura modular teórica de un SIEM 49
Figura 18 Arquitectura de Wazuh 52
Figura 19 Arquitectura del USM Appliance 53
Figura 20 Matriz Enterprise MITRE ATT&CK 68
Figura 21 Diagrama de la solución propuesta 87
Figura 22 Arquitectura Lógica ELK Stack 89
Figura 23 Hardware asignado al equipo SIEM ELK Stack 92
Figura 24 Estatus Elasticsearch 93
Figura 25 Estatus Logstash 94
Figura 26 Estatus Kibana 95
Figura 27 Dashboard principal Elastic 95
Figura 28 Estatus Filebeat 96
Figura 29 Integración de Firewall Fortigate 98
Figura 30 Integración de Active Directory 99

Figura 31 Integración de QNAP 100
Figura 32 Mapa de casos de uso en Mitre Att&ck 108
Figura 33 Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1 111
Figura 34 Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 2 113
Figura 35 Caso de Uso de detección de múltiples intentos fallidos de inicio de sesión por parte de administradores 115
Figura 36 Caso de uso remoción de privilegios de grupos administrativos 118
Figura 37 Caso de uso B cuentas deshabilitadas o eliminadas 120
Figura 38 Caso de uso C Manipulación de credenciales (Cambio/Reset de contraseña) 122
Figura 39 Evidencia de reunión generada para la capacitación 126
Figura 40 Evidencia de Capacitación 127
Figura 41 Vista de Integración de Fuentes en SIEM ELK 140
Figura 42 Recepción de Logs Firewall 1 141
Figura 43 Detalle de Recepción de Log Firewall 1 142
Figura 44 Recepción de Logs Firewall 2 143
Figura 45 Detalle de Recepción de Log Firewall 2 144
Figura 46 Recepción de Logs Servidor NAS QNAP 146
Figura 47 Detalle de Recepción de Log Servidor NAS QNAP 147
Figura 48 Recepción de Logs Servidor Active Directory 148
Figura 49 Detalle de Recepción de Log Servidor Active Directory 149
Figura 50 Gráfica de Disponibilidad del SIEM 150
Figura 51 Tasa De Procesamiento EPS (Events Per Second) – Firewall 1 152
Figura 52 Tasa De Procesamiento EPS (Events Per Second) – Firewall 2 152
Figura 53 Tasa De Procesamiento EPS (Events Per Second) – Active Directory 153
Figura 54 Tasa De Procesamiento EPS (Events Per Second) – QNAP 153
Figura 55 Reglas de detección configuradas en el SIEM ELK Stack 159
Figura 56 Detección de Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1 160
Figura 57 Detección de Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 2 161
Figura 58 Evidencia de alerta generada por el caso de uso UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN 163

Figura 59 Evidencia de alerta generada por el caso de uso UC-REC-FW2-T1110.003 – Ataque de Fuerza Bruta SSL VPN 165
Figura 60 Detección de Caso de Uso Múltiples intentos fallidos de inicio de sesión por parte de administradores 166
Figura 61 Alertas de detección de Caso de Uso Múltiples intentos fallidos de inicio de sesión por parte de administradores 167
Figura 62 Evidencia de alerta 1 generada por el caso de uso UC-QNAP-T1110-BruteForce-Admins 169
Figura 63 Detección de Caso de Uso de Remoción de privilegios de grupos administrativos 170
Figura 64 Alertas de detección de Caso de Uso de Remoción de privilegios de grupos administrativos 171
Figura 65 Detección de Caso de Uso de cuentas deshabilitadas o eliminadas..... 172
Figura 66 Alertas de detección de Caso de Uso de cuentas deshabilitadas o eliminadas 173
Figura 67 Detección de Caso de Uso de manipulación de credenciales (Cambio/Reset de contraseña)..... 174
Figura 68 Alertas de detección de Caso de Uso de manipulación de credenciales (Cambio/Reset de contraseña)..... 175
Figura 69 Evidencia de Alerta 1 generada por el caso de uso A..... 177
Figura 70 Evidencia de Alerta 2 generada por el caso de uso B..... 178
Figura 71 Evidencia de Alerta 6 generada por el caso de uso C..... 179
Figura 72 Registro de Puntuaciones durante la Evaluación..... 183
Figura 73 Evidencia de respuestas de cuestionario..... 185

1 CAPÍTULO 1: DEFINICIÓN DEL PROYECTO

1.1 Introducción

En una sociedad cada vez más interconectada, la ciberseguridad se establece como un factor determinante para proteger la información y garantizar la continuidad operativa de las empresas. La sofisticación y frecuencia de los ataques cibernéticos han crecido exponencialmente, lo que ha impulsado la adopción de herramientas avanzadas para la detección y respuesta a amenazas. En este contexto, los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) han evolucionado como una solución esencial para el monitoreo y análisis de eventos en tiempo real, permitiendo detectar patrones anómalos y correlacionar incidentes de seguridad (Sheeraz et al., 2024).

Los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) se han convertido en una pieza fundamental para la monitorización centralizada, detección y respuesta ante amenazas cibernéticas. Tradicionalmente, el mercado ha estado dominado por soluciones comerciales como IBM QRadar y Splunk, que ofrecen capacidades avanzadas de análisis de eventos y correlación de datos. Sin embargo, el alto costo de licenciamiento y mantenimiento de estas herramientas dificulta su implementación en organizaciones con recursos financieros limitados, lo que ha impulsado la evaluación de soluciones SIEM de código abierto como una alternativa viable para garantizar la seguridad sin comprometer el presupuesto (Manzoor et al., 2024).

Ante esta problemática, Manzoor et al. (2024) señalan que las soluciones SIEM de código abierto han ganado popularidad, proporcionando alternativas escalables y accesibles sin comprometer la seguridad. Investigaciones recientes han evaluado la efectividad de estas herramientas en comparación con soluciones comerciales, destacando su viabilidad en la detección y gestión de amenazas.

Por otra parte, el marco MITRE ATT&CK se ha consolidado como una referencia clave en la clasificación de tácticas y técnicas de ataque, ofreciendo una base estructurada que permite optimizar las capacidades de identificación y reacción frente a incidentes (Al-Sada et al., 2024). Su integración en sistemas SIEM puede llegar a ser efectiva para la correlación de eventos y la mitigación de amenazas emergentes. A través de este enfoque, las organizaciones pueden fortalecer su postura de seguridad y anticiparse a posibles vulnerabilidades explotadas por actores maliciosos.

El presente proyecto se enfoca en la implementación de una solución SIEM basada en Open Source, alineada con el marco MITRE ATT&CK, para mejorar la detección de vulnerabilidades y amenazas dentro de un entorno empresarial. La implementación de esta solución permitirá reducir el tiempo de detección de incidentes y mejorar la capacidad de procesamiento de eventos para la detección temprana de amenazas mediante casos de uso, contribuyendo a una respuesta más eficaz ante posibles ataques.

Desde una perspectiva de ingeniería, la implementación de un SIEM de código abierto representa un aporte significativo en la automatización y optimización de procesos de ciberseguridad. La estandarización de técnicas de detección basadas en MITRE ATT&CK contribuirá a la formación de nuevas estrategias defensivas dentro de la organización, promoviendo el cumplimiento de normativas internacionales.

En conclusión, la creciente sofisticación de los ataques cibernéticos exige estrategias avanzadas de detección y respuesta. La combinación de herramientas SIEM de código abierto con el marco MITRE ATT&CK representa una solución viable para fortalecer la seguridad de la información y mitigar riesgos en entornos organizacionales.

1.2 Caso de Estudio

1.2.1 Organización

El Grupo Recupera es una empresa peruana especializada en servicios de outsourcing, cobranzas, dotación de capital humano, gestiones, inversiones y hunting. Con más de 20 años de experiencia, ofrece soluciones integrales orientadas a resultados.

El grupo es formado por 5 pilares:

a. Recupera Outsourcing: Administración de riesgo y recupero en todos los tramos de la gestión.

b. Recupera Ancoma: Soluciones tecnológicas y administrativas modeladas a medida para las diferentes industrias de Contact Center.

c. Recupera Inversiones: Evaluación de carteras y valorización para la compra de gestión interna. Cartera Propia.

d. Recupera Business Partner: Aliados estratégicos y especialistas en la consultoría de recursos humanos.

e. Abogados & Consultores: Servicios jurídicos, civiles, administrativos.

Recupera Outsourcing S.A.C. se formó como parte del Grupo Recupera, consolidándose como una empresa peruana con amplia trayectoria en servicios de Contact Center, especializada en cobranzas tercerizadas.

Razón Social: Recupera Outsourcing S.A.C.

Misión: Ofrecer a nuestros clientes servicios de cobranzas tercerizadas diseñados para cumplir con sus requisitos, respaldándonos de nuestra capacidad de innovación, amplia experiencia, talento humano y tecnología.

Visión: Ser la empresa líder en servicios de cobranzas tercerizadas en la región; innovando nuestros procesos apoyados con la transformación digital, demostrando una conducta corporativa responsable que promueva la satisfacción de nuestras partes interesadas.

Objetivos:

a. Brindar un servicio enfocado en la satisfacción del cliente y otras partes interesadas, a través de una atención rápida y servicios entregados en tiempos propuestos.

b. Apoyarse en personal competente y proveedores calificados que contribuyan al cumplimiento de los requisitos de calidad.

c. Asegurar el cumplimiento de todos los requisitos legales y otros aplicables a las actividades de la empresa.

d. Establecer y evaluar objetivos periódicamente, que permitan mejorar la calidad de los servicios entregados a sus clientes.

e. Proporcionar a sus colaboradores un ambiente laboral adecuado, que motive y propicie el desarrollo eficiente de sus actividades.

f. Comunicar, consultar y fomentar la participación activa de sus colaboradores en el sistema de gestión de calidad.

g. Asegurar la eficacia y la mejora continua del sistema de gestión de calidad, monitoreando adecuadamente el desempeño de los procesos involucrados.

Áreas de la Empresa:

- Servicios Jurídicos y Consultoría.
- Contact Center.
- Soluciones Tecnológicas.
- Gestión de Cartera Propia.
- Consultoría en Recursos Humanos.

Procesos Principales y Actividades:

- Gestión de cobranzas tercerizadas a través de Contact Center y canales alternos.
- Administración de operaciones de llamadas entrantes y salientes, con acceso a métricas, reportes e indicadores, supervisión en tiempo real de agentes y demás funcionalidades avanzadas de outbound e inbound.

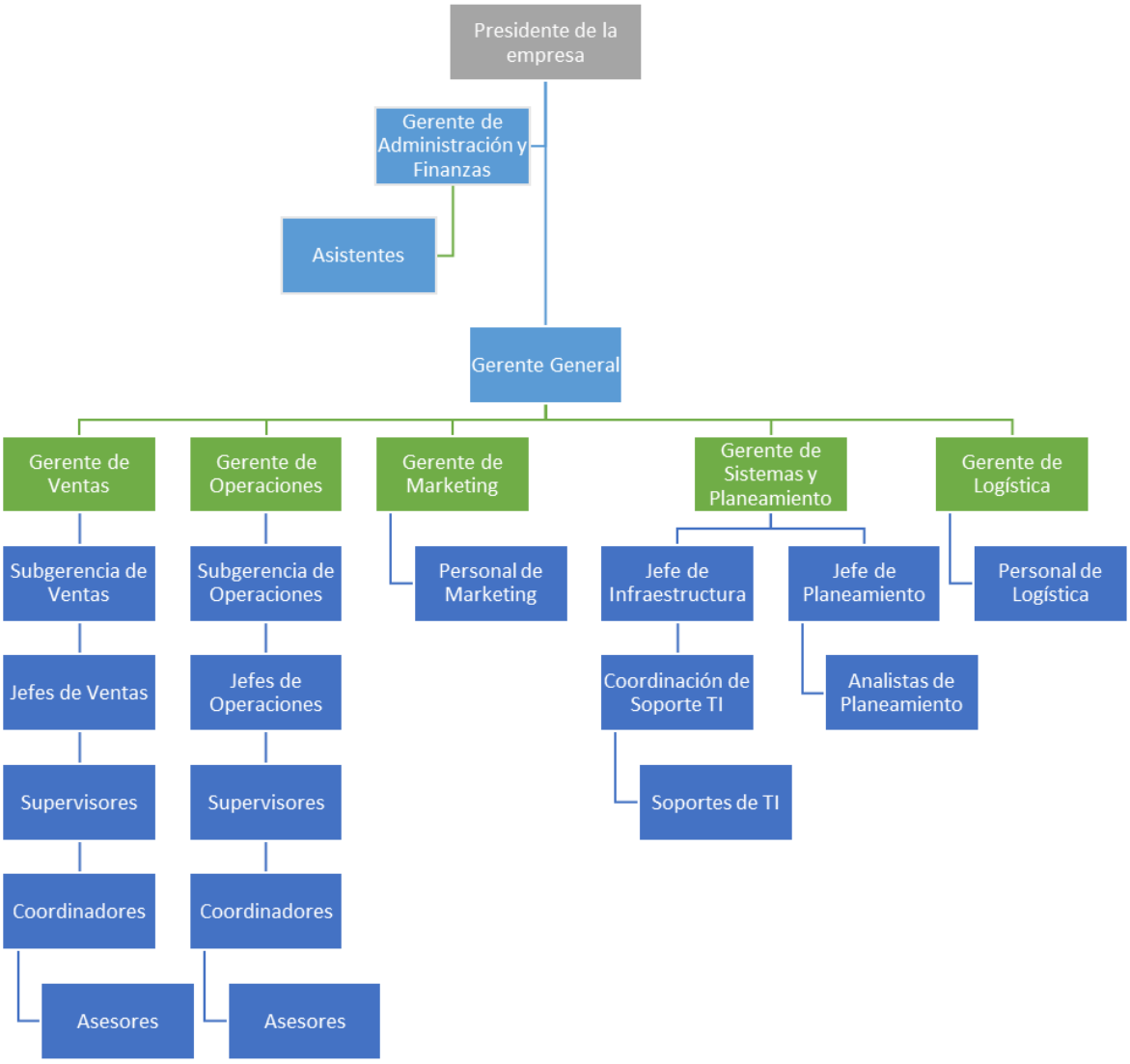
La empresa posee dos instalaciones propias en la ciudad de Lima, ubicadas en los distritos de Miraflores y Los Olivos. Ambas instalaciones están diseñadas para la atención al cliente y ventas, equipado con tecnología de punta para respaldar sus operaciones.

La empresa se destaca por su capacidad de innovación y adaptación a las necesidades de sus clientes, ofreciendo soluciones de valor en diversas industrias, incluyendo telecomunicaciones, bancos, aseguradoras, microfinanzas, sector automotriz, energía e hidrocarburos, retail, y venta directa.

A continuación, en la Figura 1 se presenta el organigrama referencial de la empresa.

Figura 1

Organigrama referencial de la empresa



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

1.2.2 Situación Problemática

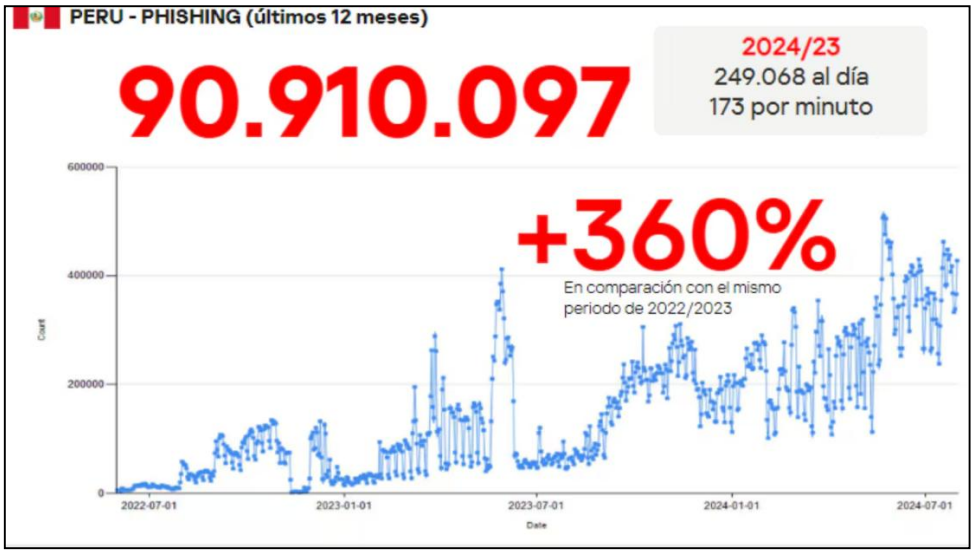
En la actualidad, Perú enfrenta desafíos significativos en ciberseguridad. Según el National Cyber Security Index (NCSI), el país ocupa el puesto 53 a nivel mundial con una puntuación de 62.34 %, lo que refleja la necesidad de fortalecer las políticas y medidas de seguridad cibernética (NCSI, 2024).

La falta de detección en tiempo real de las alertas de seguridad tiene consecuencias graves para las organizaciones. La ausencia de monitoreo proactivo permite que las amenazas persistan sin ser identificadas, aumentando el riesgo de brechas de seguridad, pérdida de datos sensibles y daños financieros. Adicionalmente, la reputación de las empresas se ve afectada, lo que genera desconfianza entre los clientes y socios comerciales (Infobae, 2025).

El incremento de ciberataques en Perú es alarmante. Durante 2024, se registraron más de un millón de detecciones únicas de phishing, la cifra más alta en los últimos años (Infobae, 2025). Así como se proyecta en la Figura 2.

Figura 2

Incremento de Phishing en Perú

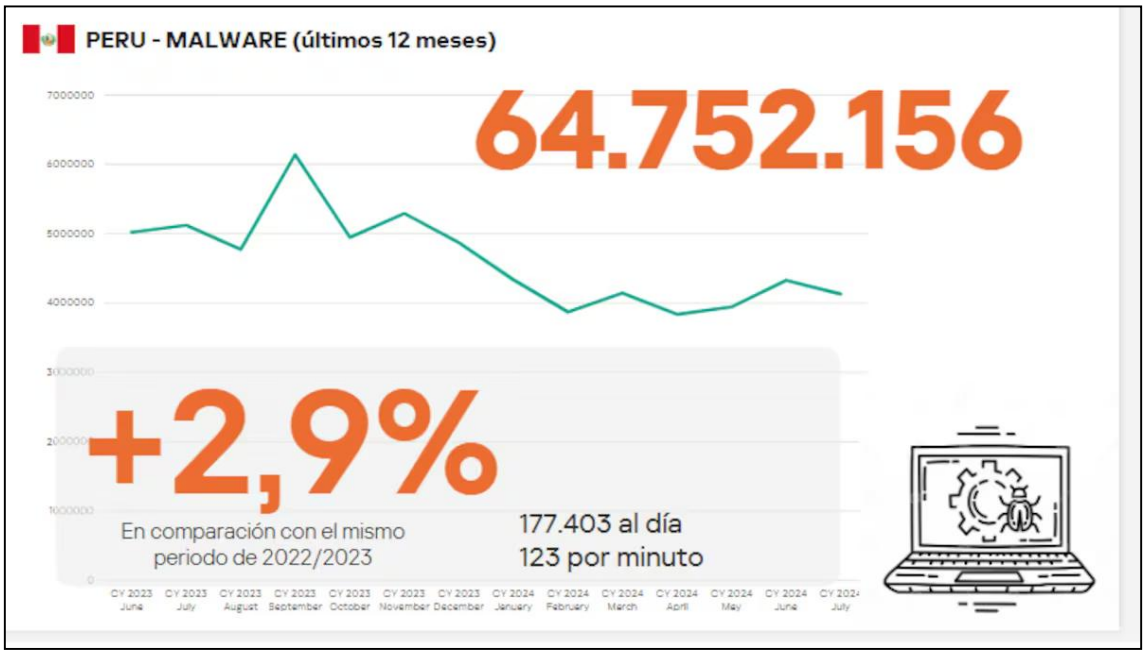


Nota. La figura evidencia el incremento de ataques phishing en el país a mediados del 2023 y 2024. Adaptado de "Perú se alza como un foco de ataques cibernéticos en Latinoamérica", por Redacción EC, 2024 (https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia/?ref=ecr)

Según datos de Kaspersky, Perú presenta una de las mayores tasas de incidencia en Latinoamérica, con más de 177,000 ataques de malware al día, destacando la creciente sofisticación y frecuencia de estas amenazas (Sociedad Telecom, 2025). Del mismo modo expuesto en la Figura 3.

Figura 3

Incremento de malware en Perú

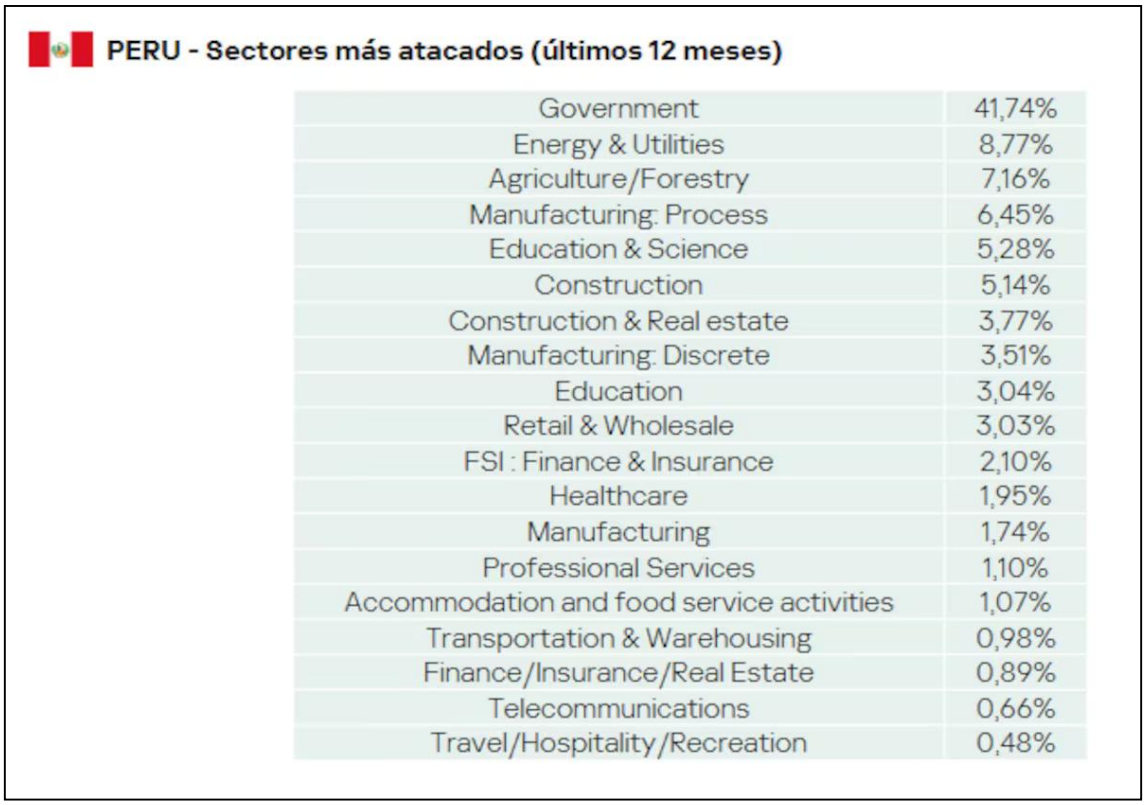


Nota. La figura muestra el incremento de los malware en el país a mediados del 2023 y 2024 comparado al periodo anterior. Adaptado de "Perú se alza como un foco de ataques cibernéticos en Latinoamérica", por Redacción EC, 2024 (https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia/?ref=ecr)

Así también se puede destacar en la siguiente Figura 4 los sectores más afectados por los ataques de malware en Perú en los últimos 12 meses.

Figura 4

Sectores afectados por ciberataques en Perú



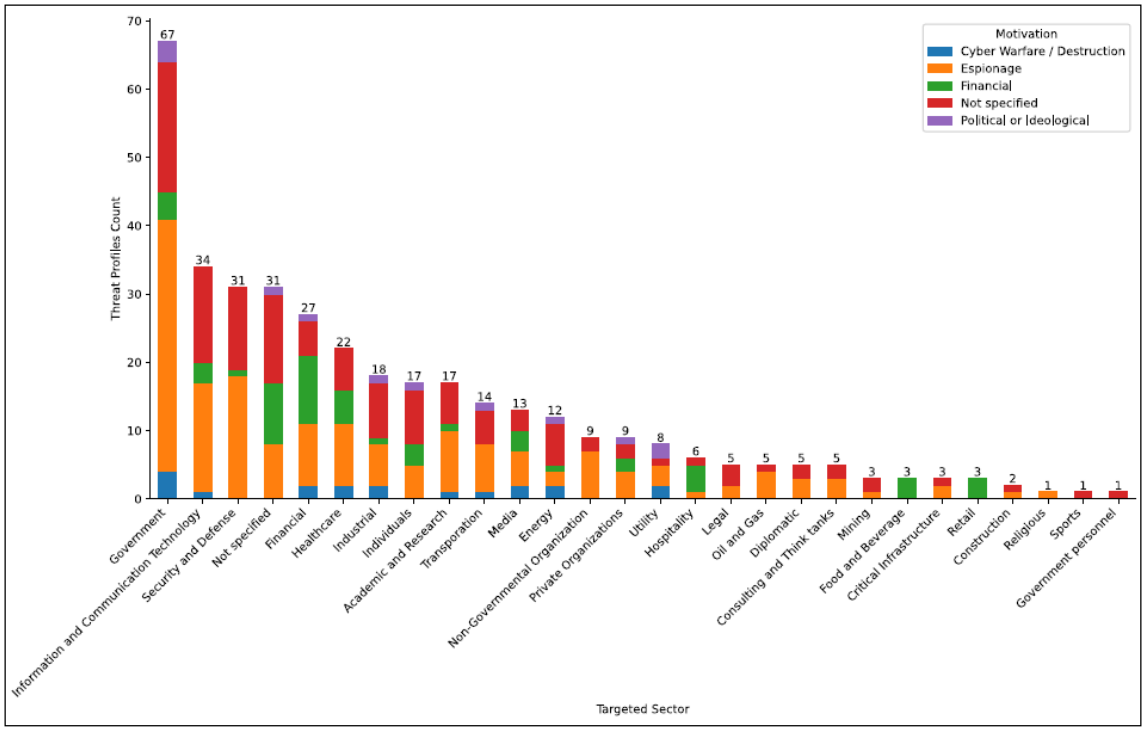
Nota. La figura muestra los sectores más atacados en el país a mediados del 2023 y 2024. Adaptado de "Perú se alza como un foco de ataques cibernéticos en Latinoamérica", por Redacción EC, 2024 (https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia/?ref=ecr)

La importancia de abordar estas amenazas es crucial para la sociedad peruana. Los ciberataques no solo afectan la economía, sino que también ponen en riesgo la privacidad y seguridad de los ciudadanos. La interrupción de servicios esenciales y la exposición de información personal tienen impactos duraderos en la confianza pública y en la estabilidad social (ESAN, 2024).

Como se muestra en la Figura 5, en el contexto de MITRE ATT&CK se puede señalar que los sectores más afectados por los ataques cibernéticos varían según las motivaciones de los grupos de amenazas, según Al-Sada et al. (2024), el sector gubernamental se posiciona como el principal objetivo, con un 50 % de los grupos de amenazas enfocados en espionaje y la obtención de información crítica. Asimismo, el sector de Tecnologías de la Información y Comunicación (TIC) también destaca, siendo atacado por casi el 50 % de estos grupos debido a su relevancia estratégica. Por otro lado, la motivación financiera se extiende a más de 15 sectores, afectando significativamente al sector financiero y a sectores críticos como salud, energía e industria, mientras que sectores como salud y servicios públicos también han sido atacados por motivaciones de guerra cibernética y destrucción.

Figura 5

Sectores afectados por los grupos de ataque MITRE ATT&CK



Nota. La figura muestra datos de los sectores atacados por grupo de ataque basado en MITRE ATT&CK. De "Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database.", por Al-Sada et al. 2024 (https://doi.org/10.1109/access.2023.3344680)

1.2.3 Sector de Estudio

La empresa, cuenta con clientes pertenecientes a los sectores bancario, retail, telecomunicaciones y cajas municipales, por consiguiente, trabaja en un entorno altamente expuesto a riesgos de ciberseguridad. Como se muestra en las Figuras 4 y 5, dichos sectores presentan una mayor exposición a amenazas cibernéticas debido al tratamiento de información sensible y a su alta dependencia de infraestructuras tecnológicas para la continuidad de sus operaciones.

Actualmente en la empresa, los eventos y registros generados por servidores, dispositivos de red, estaciones de trabajo y equipos de seguridad no se encuentran centralizados ni correlacionados de manera integral, lo que limita la visibilidad del estado real de la seguridad informática. Esta situación dificulta la detección oportuna de vulnerabilidades y amenazas, así como el análisis estructurado de posibles incidentes bajo un marco reconocido como MITRE ATT&CK.

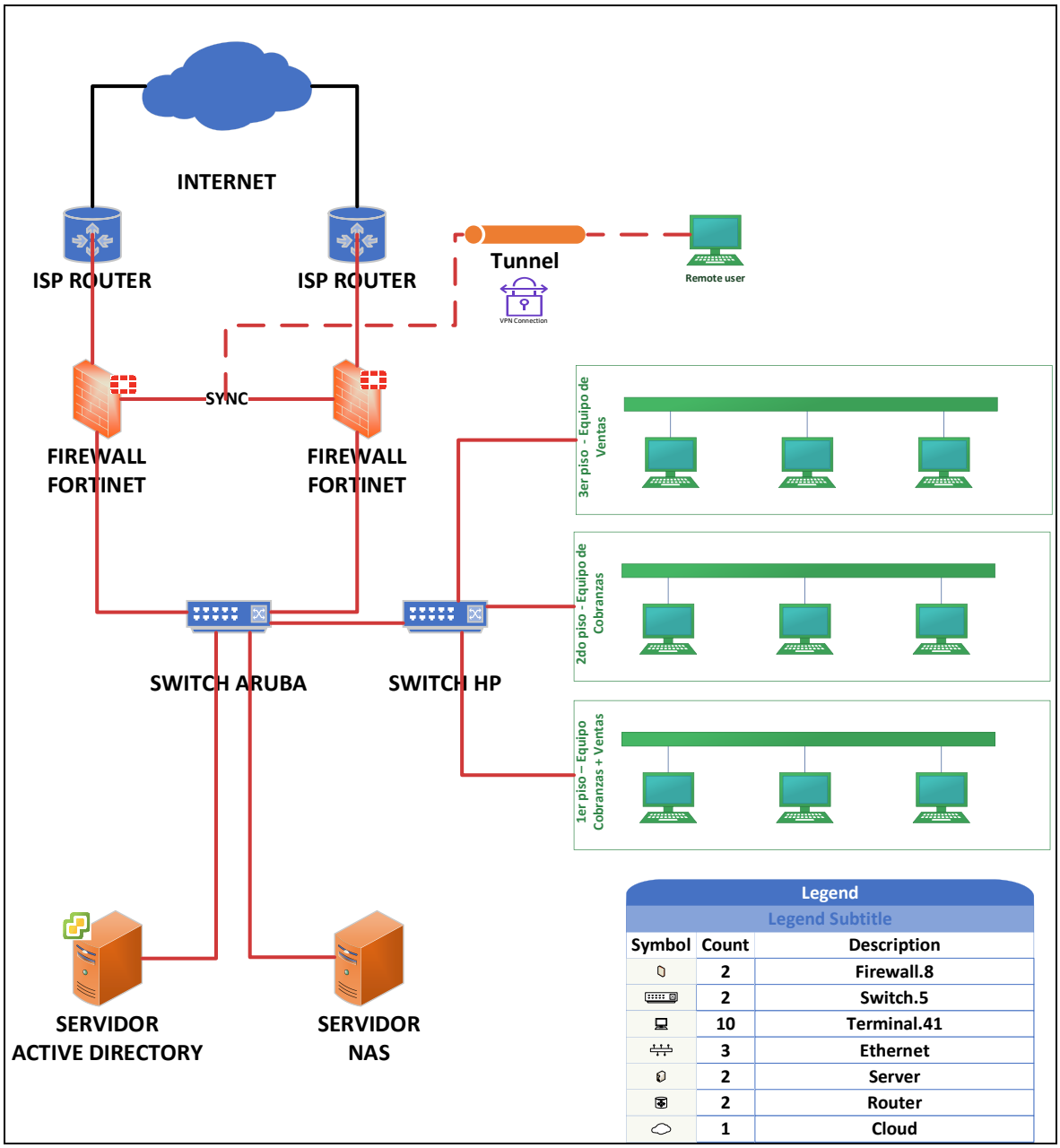
En consecuencia, la organización presenta una brecha en su capacidad de monitoreo y detección proactiva de amenazas, lo que podría comprometer la integridad, confidencialidad y disponibilidad de la información y los servicios críticos que soportan su operación.

A continuación, se presenta el diagrama de red de la infraestructura de la empresa, detallando sus principales componentes y la funcionalidad que cumplen dentro de la arquitectura tecnológica.

DIAGRAMA DE LA EMPRESA

Figura 6

Diagrama de red de la empresa



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

El diagrama de red representa la infraestructura de la empresa, enfocada en garantizar alta disponibilidad, seguridad y segmentación eficiente para soportar operaciones críticas. A continuación, se detalla la descripción de los componentes principales y su funcionalidad: La red cuenta con dos conexiones ISP (proveedores de servicios de Internet) configuradas para la redundancia. Estas conexiones están protegidas por dos firewalls Fortinet, configurados en un esquema activo-activo para optimizar el rendimiento y la continuidad operativa.

Los firewalls gestionan el tráfico entrante y saliente, se aplican políticas de seguridad y proporcionan conectividad segura para los usuarios remotos mediante túneles VPN. Este acceso remoto es esencial para los empleados que trabajan desde ubicaciones externas, garantizando la privacidad y la autenticidad de las conexiones.

En la capa de distribución, se encuentran dos switches de marcas Aruba y HP. Estos switches se conectan con dispositivos finales, servidores centrales y puntos de acceso. La red está segmentada en diferentes zonas de trabajo para los usuarios, lo que optimiza el rendimiento y limita la propagación de posibles amenazas.

Entre los servidores principales, se incluye un servidor de Active Directory, responsable de la autenticación de usuarios, la gestión centralizada y la aplicación de políticas de seguridad en el dominio. También se cuenta con un servidor NAS QNAP, que ofrece almacenamiento compartido para los datos de la empresa y facilita las copias de seguridad.

En resumen, la infraestructura está diseñada para cubrir las demandas de la empresa, priorizando la continuidad operativa, la conectividad segura y la protección de la información sensible de la empresa.

1.3 Análisis del Problema

1.3.1 Formulación del Problema

Limitada capacidad para detectar vulnerabilidades, amenazas y correlacionar eventos de ciberseguridad, lo que dificulta un monitoreo efectivo y en tiempo real de los riesgos tecnológicos en la organización.

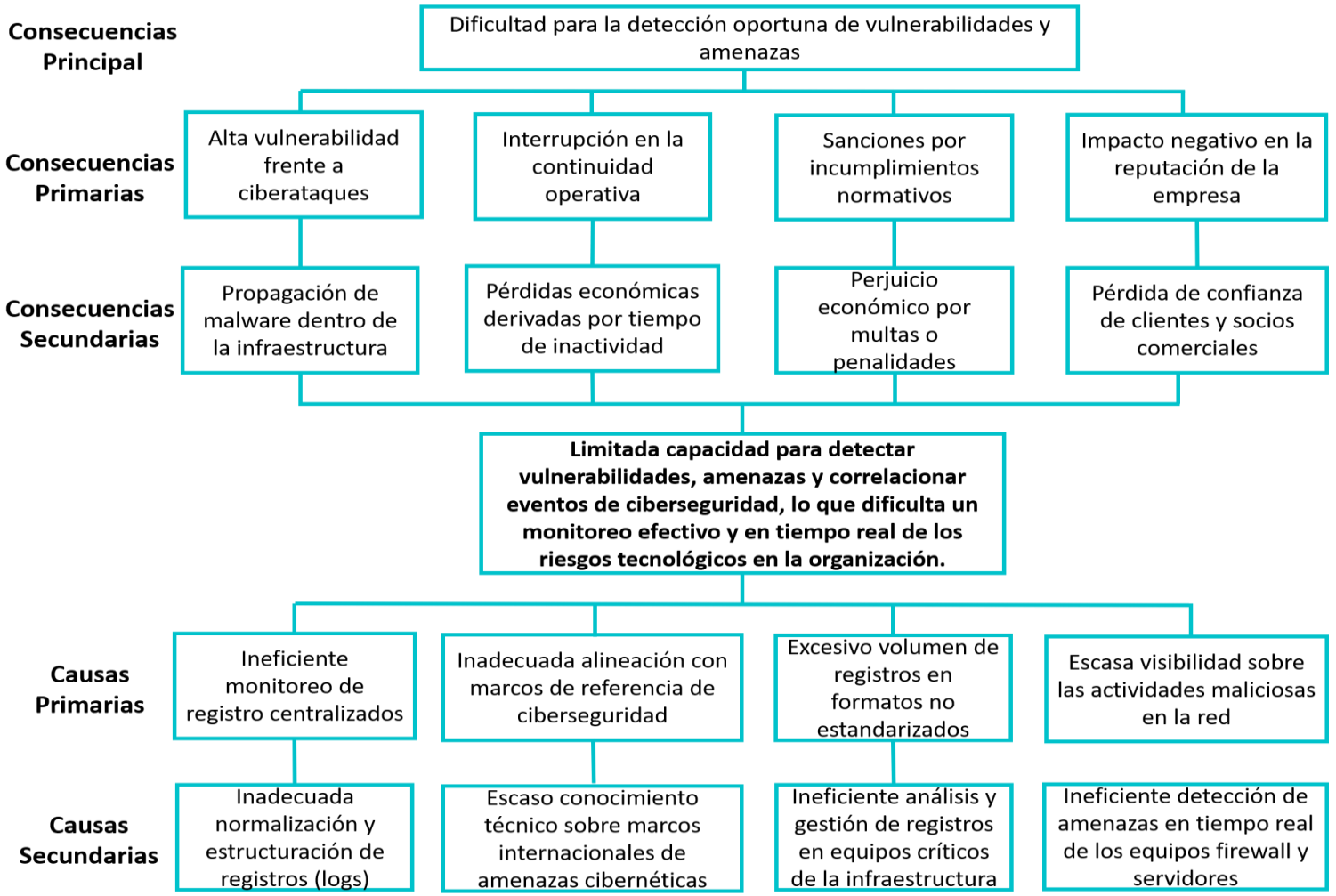
1.3.2 Análisis

El problema central radica en la necesidad de garantizar la ciberseguridad en un entorno tecnológico altamente dinámico y propenso a vulnerabilidades, como es el caso de las empresas de servicio del rubro de Contact Center. Estas organizaciones gestionan grandes volúmenes de datos sensibles de clientes y operaciones críticas en tiempo real, lo que las convierte en blancos frecuentes de ciberataques. No obstante, en muchas de estas empresas persisten carencias significativas que obstaculizan la implementación de estrategias de ciberseguridad robustas y efectivas, aumentando así su exposición a riesgos potenciales.

A continuación, se muestra el árbol de problemas:

Figura 7

Árbol de problemas



1.3.2.1 Alcance del problema

En el contexto de una empresa BPO de Contact Center, la capacidad limitada para detectar vulnerabilidades, amenazas y correlacionar eventos de ciberseguridad representa un riesgo crítico para la integridad, disponibilidad y confidencialidad de la información. Dado el volumen elevado de datos sensibles gestionados, tales como información de clientes, autenticaciones de usuarios y registros de actividad operativa, esta deficiencia repercute directamente en la eficacia del monitoreo y en la toma de decisiones ante incidentes tecnológicos.

La infraestructura tecnológica de estas organizaciones suele estar compuesta por múltiples equipos y plataformas interconectadas, como firewalls, servidores Active Directory y dispositivos de almacenamiento. Sin una herramienta capaz de consolidar y normalizar los eventos de seguridad provenientes de estas fuentes, la detección temprana de comportamientos maliciosos se ve comprometida. Esto conlleva a una alta dependencia de revisiones manuales, aumento en los tiempos de respuesta y dificultades para mantener una trazabilidad clara de los eventos que afectan la red.

El impacto de esta problemática abarca diversas dimensiones. En primer lugar, expone a la organización a la pérdida o filtración de información sensible, lo cual puede desencadenar consecuencias legales y regulatorias si se compromete información protegida. En segundo lugar, debilita la continuidad operativa ante la imposibilidad de actuar de forma oportuna frente a amenazas que afectan la disponibilidad de los servicios. Además, la falta de visibilidad sobre los eventos de seguridad incrementa el riesgo de que ataques como exfiltración de datos, movimientos laterales o accesos no autorizados permanezcan sin ser detectados, afectando no solo la infraestructura sino también la confianza de los clientes y socios estratégicos.

Asimismo, la carencia de correlación automatizada y de alineamiento con marcos de referencia como MITRE ATT&CK impide estructurar la detección de amenazas en función de tácticas y técnicas conocidas, lo que limita la profundidad del análisis de seguridad. Esto se traduce en una gestión fragmentada de los eventos, un incremento en la tasa de falsos positivos o negativos, y una sobrecarga para los analistas que deben interpretar los datos sin herramientas contextualizadas.

En consecuencia, el alcance del problema identificado no se restringe únicamente a la gestión técnica de eventos de seguridad, sino que se extiende a los ámbitos operativos,

reputacionales y normativos de la organización. Su persistencia impacta transversalmente en la capacidad de la empresa para prevenir, detectar y responder eficazmente a los riesgos tecnológicos, constituyéndose así en una amenaza constante para la estabilidad y sostenibilidad del servicio que presta.

1.3.2.2 Causas del problema

Causa 1: Ineficiente monitoreo de registro centralizados

Manzoor et al. (2024) enfatizan que la falta de soluciones SIEM centralizadas en pequeñas y medianas empresas (PYME) dificulta la recopilación y correlación efectiva de datos de seguridad, limitando la capacidad para identificar patrones y amenazas de manera oportuna.

Causa 2: Inadecuada normalización y estructuración de registros (logs)

La presencia de logs en formatos heterogéneos y sin estandarización dificulta su procesamiento y correlación, reduciendo la efectividad en la detección de incidentes de seguridad (Khairuddin et al., 2024).

Causa 3: Inadecuada alineación con marcos de referencia de ciberseguridad

Vazão et al. (2023) destacan la importancia de alinear los sistemas de seguridad con marcos regulatorios como el GDPR y estándares internacionales, señalando que su ausencia puede limitar la efectividad de las medidas de ciberseguridad implementadas.

Causa 4: Escaso conocimiento técnico sobre marcos internacionales de amenazas cibernéticas.

El escaso conocimiento técnico en ciberseguridad, incluyendo marcos y enfoques modernos para comprender amenazas, se relaciona con la falta de formación práctica y actualizada, ya que se requiere un proceso intensivo de educación y entrenamiento para desarrollar las competencias necesarias en equipos de seguridad y responder adecuadamente ante incidentes (Mohd Ariffin et al., 2022).

Causa 5: Excesivo volumen de registros en formatos no estandarizados

Khairuddin et al. (2024) identifican que el manejo de grandes volúmenes de logs heterogéneos puede generar inconsistencias en la correlación de datos, lo que reduce la efectividad en la detección de ciberataques.

Causa 6: Ineficiente análisis y gestión de registros en equipos críticos de la infraestructura.

Park (2024) menciona que la falta de estandarización y correlación de datos provenientes de dispositivos perimetrales y servidores limita la capacidad de las organizaciones para detectar amenazas y gestionar incidentes de manera eficiente.

Causa 7: Escasa visibilidad sobre las actividades maliciosas en la red

Ammi (2023) resalta que la falta de integración de plataformas de inteligencia de amenazas, como MISP, con sistemas de monitoreo limita la visibilidad sobre actividades maliciosas en la red.

Causa 8: Ineficiente detección de amenazas en tiempo real de los equipos firewall y servidores

Sheeraz et al. (2024) enfatizan que la ausencia de monitoreo en tiempo real de los equipos críticos, como firewalls y servidores, aumenta la probabilidad de que las amenazas no sean detectadas oportunamente.

1.3.2.3 Consecuencias del problema

Consecuencia 1: Alta vulnerabilidad frente a ciberataques

Manzoor et al. (2024) señalan que la falta de sistemas SIEM centralizados incrementa la exposición de las organizaciones a ciberataques debido a la incapacidad de identificar y mitigar amenazas de manera efectiva.

Consecuencia 2: Propagación de malware dentro de la infraestructura

Vazão et al. (2023) advierten que la ausencia de un monitoreo efectivo puede permitir la rápida propagación de malware o ransomware, comprometiendo datos sensibles y operaciones críticas.

Consecuencia 3: Interrupciones en la continuidad operativa

Según Park (2024), los incidentes no detectados a tiempo pueden causar interrupciones significativas en la continuidad operativa de una organización, afectando sus procesos esenciales.

Consecuencia 4: Pérdidas económicas derivadas por tiempo de inactividad

Khairuddin et al. (2024) destacan que los tiempos de inactividad generados por incidentes de seguridad no gestionados representan costos económicos significativos para las organizaciones.

Consecuencia 5: Sanciones por incumplimientos normativos

La falta de alineación con marcos normativos de ciberseguridad limita la efectividad de las medidas de protección y expone a la organización a incumplimientos regulatorios en el manejo de información sensible (Vazão et al., 2023).

Consecuencia 6: Perjuicio económico por multas o penalidades

Vazão et al. (2023) enfatizan que no cumplir con regulaciones como el GDPR puede llevar a sanciones económicas significativas, generando pérdidas financieras para la organización.

Consecuencia 7: Impacto negativo en la reputación de la empresa

Los incidentes de ciberseguridad no gestionados adecuadamente exponen vulnerabilidades y generan una percepción negativa sobre la capacidad de la organización para proteger sus activos, lo que puede deteriorar su reputación. Este tipo de implicación es coherente con los efectos discutidos por autores como Sheeraz et al. (2023), quienes enfatizan la importancia de la gestión proactiva de la ciberseguridad.

Consecuencia 8: Pérdida de confianza de clientes y socios comerciales

La falta de medidas adecuadas para proteger datos críticos genera incertidumbre sobre la capacidad de la empresa para manejar información sensible, debilitando relaciones comerciales clave.

1.3.2.4 Stakeholders

A continuación, se muestra el cuadro de interesados en el proyecto.

Tabla 1

Registro de interesados

Interesado	Categoría	Nivel de interés	Nivel de influencia	Descripción
Presidente de la empresa	Alta dirección	Medio	Medio	Tiene interés en la protección general de los activos de la empresa, pero delega decisiones técnicas. Su apoyo es importante para la sostenibilidad del proyecto.
Gerente General	Alta dirección	Alto	Medio	Interesado en los beneficios estratégicos del proyecto, como la continuidad operativa y reputación. Facilita los recursos y alineamiento organizacional.
Gerente de Sistemas y Planeamiento	Patrocinador	Alto	Alto	Promotor directo del proyecto, participa en la toma de decisiones clave y asegura que se alinee con la estrategia tecnológica de la empresa.
Jefe de Infraestructura	Socio	Alto	Alto	Responsable de la gestión técnica del entorno donde se implementará el SIEM. Su participación es clave para garantizar la viabilidad técnica del proyecto.
Coordinador de soporte	Socio	Medio	Medio	Participa en la operación diaria de TI. Interesado en cómo el SIEM facilitará la identificación de incidentes y mejorará los tiempos de respuesta.

Interesado	Categoría	Nivel de interés	Nivel de influencia	Descripción
Soporte TI	Socio	Bajo	Bajo	Ejecuta tareas técnicas asignadas. Afectado por cambios en los flujos de trabajo, pero con poca capacidad de decisión.
Gerente de Operaciones	Cliente	Medio	Bajo	Interesado en mantener la continuidad del servicio al cliente. Su influencia es baja, pero requiere que el sistema no afecte las operaciones.
Gerente de Marketing	Cliente	Bajo	Bajo	No tiene participación directa en el proyecto. Su interés se relaciona indirectamente con la imagen corporativa frente a incidentes de seguridad.

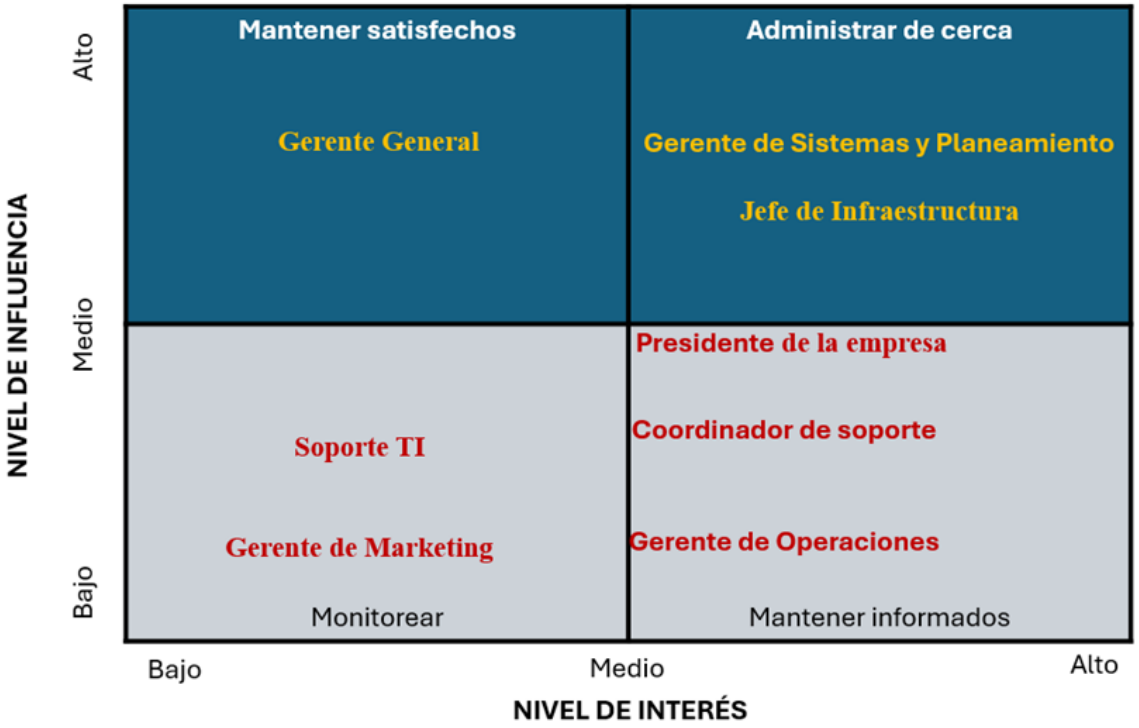
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

1.3.2.5 Matriz de Interesados

A continuación, se proyecta la matriz de interesados respecto al interés y el poder.

Figura 8

Matriz de Interesados



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

1.4 Objetivos

1.4.1 Objetivo General

Implementar un Security Information and Event Management (SIEM) basado en Open Source para la detección de vulnerabilidades y amenazas en el marco MITRE ATT&CK, para una BPO de Contact Center.

1.4.2 Objetivos Específicos

OE1: Identificar los componentes críticos de infraestructura tecnológica de la empresa para el diseño del sistema SIEM mediante un listado técnico y una evaluación comparativa de al menos tres soluciones Open Source.

OE2: Diseñar un diagrama de arquitectura SIEM basada en una herramienta Open Source aprobado por la gerencia de sistemas, asegurando que permita la centralización y gestión de eventos de seguridad.

OE3: Desplegar un SIEM operativo que registre los logs de dos firewalls y dos servidores críticos, garantizando una disponibilidad ≥ 99.5 %.

OE4: Desarrollar tres casos de uso basados en el marco MITRE ATT&CK para la detección de eventos de seguridad en un SIEM Open Source.

OE5: Capacitar al personal de soporte TI en el uso del SIEM y del marco MITRE ATT&CK para la gestión de eventos de seguridad, logrando una mejora del 40 % en las competencias adquiridas en los participantes.

1.4.3 Indicadores de Logro de los Objetivos

Tabla 2

Indicadores de Logro de los Objetivos

Objetivo Específico	Indicador de Logro	Métrica
Identificar los componentes críticos de infraestructura tecnológica de la empresa para el diseño del sistema SIEM mediante un listado técnico y una evaluación comparativa de al menos tres soluciones Open Source.	- Listado técnico que contiene los componentes críticos de la infraestructura tecnológica. - Evaluación comparativa de soluciones SIEM Open Source.	- Número de componentes identificados. - Puntuación en cuadro comparativo de soluciones SIEM Open Source
Diseñar un diagrama de arquitectura SIEM basada en una herramienta Open Source aprobado por la gerencia de sistemas, asegurando que permita la centralización y gestión de eventos de seguridad.	- Aprobación del diagrama de arquitectura por la gerencia de sistema y planeamiento < 5 días (desde la presentación)	- Número de días desde la presentación
Desplegar un SIEM operativo que registre los logs de dos firewalls y dos servidores críticos, garantizando una disponibilidad ≥ 99.5 %.	- 100% de los firewalls y servidores registrados en el SIEM. - Disponibilidad del SIEM ≥ 99.5% durante el monitoreo.	- Número de equipos integrados - Porcentaje de disponibilidad del SIEM durante el monitoreo

Objetivo Específico	Indicador de Logro	Métrica
	- Capacidad de procesamiento de eventos (LOG): EPS ≥ 155 eventos/segundo.	- Promedio de EPS durante el monitoreo.
Desarrollar tres casos de uso basados en el marco MITRE ATT&CK para la detección de eventos de seguridad en un SIEM Open Source.	- Tres casos de uso correlacionadas a TTPs de MITRE ATT&CK - Promedio de Tiempo de Detección (MTTD) ≤ 5 minutos. - Alertas detectadas ≥ 3.	- Número de caso de uso correlacionadas con TTPs del MITRE ATT&CK - MTTD (Promedio de TTD) durante el monitoreo. - Número de alertas detectados
Capacitar al personal de soporte TI en el uso del SIEM y del marco MITRE ATT&CK para la gestión de eventos de seguridad, logrando una mejora del 40 % en las competencias adquiridas en los participantes.	- Equipo de soporte TI capacitado en MITRE ATT&CK y en monitoreo del SIEM ≥ 80 % del personal citado. - Mejora del 40% en resultados de pruebas de conocimiento postcapacitación.	- Porcentaje de asistencia de capacitación del equipo de soporte de TI. - Porcentaje de mejora en los resultados postcapacitación

1.5 Descripción del Proyecto

A continuación, se desarrolla el diseño de la implementación de una solución SIEM basada en tecnología Open Source, con el objetivo de fortalecer las capacidades de detección y respuesta ante amenazas en la infraestructura tecnológica de la empresa. Mediante la integración de la plataforma ELK Stack (Elasticsearch, Logstash, Kibana), centralizando la recolección, procesamiento y análisis de registros (logs) generados por dispositivos y servicios críticos, tales como firewalls, servidores Active Directory y NAS.

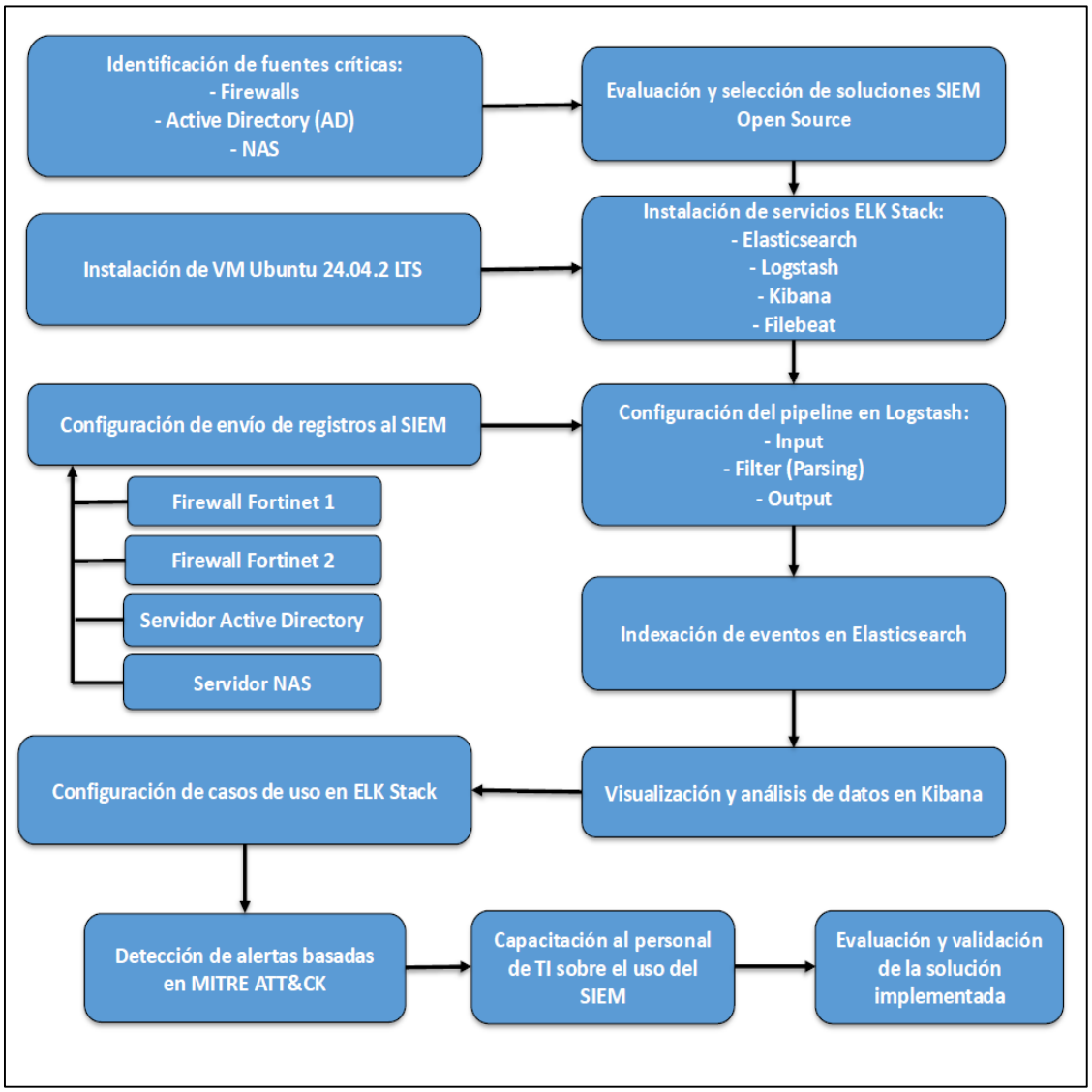
Asimismo, se incorpora el marco de referencia MITRE ATT&CK como elemento clave para el desarrollo de casos de uso orientados a la identificación de técnicas y tácticas empleadas por actores maliciosos.

1.5.1 Diagrama de Bloques

En la Figura 9, se estructura un diagrama de bloques que sintetiza las fases principales que componen el proceso de implementación, desde la identificación de las fuentes de datos hasta la validación de la solución desplegada.

Figura 9

Diagrama de bloque del diseño de la solución



El diseño expuesto permite representar de manera clara y estructurada las etapas fundamentales para la construcción de un SIEM Open Source alineado con los requerimientos de la empresa. Se considera algunos puntos que serán tratados más adelante en el capítulo 3 de diseño, desarrollo y validación de solución. Como los siguientes: La implementación del ELK Stack que proporciona una plataforma robusta, flexible y escalable para el análisis de eventos de seguridad, y la adopción del marco MITRE ATT&CK que garantiza un enfoque contextualizado frente a las amenazas contemporáneas.

Dicho esto, podemos mencionar que con esta arquitectura se busca no solo optimizar la detección y mitigación de vulnerabilidades en tiempo real, sino también brindar al equipo de TI herramientas analíticas avanzadas que permitan una gestión proactiva de la ciberseguridad y una toma de decisiones informada y oportuna.

A continuación, se detallan cada una de las actividades mencionadas en el flujograma anterior.

Tabla 3

Procedimiento de Actividades

Nº	Entrada	Actividad	Rol	Descripción	Herramientas	Salida
1	Inventario de activos tecnológicos	Identificación de fuentes críticas	Jefe de Infraestructura	Se realiza un levantamiento de activos críticos que generarán logs relevantes para la detección de amenazas: Firewalls, Active Directory y NAS. Se documentan los tipos de eventos generados y su criticidad.	Inventario de activos, hojas de cálculo	Cuadro de Fuentes Críticas
2	Cuadro de Fuentes Críticas	Evaluación y selección de soluciones SIEM Open Source	Coordinador de TI	Se analizan diferentes alternativas Open Source (Wazuh, ELK, Graylog) evaluando criterios de compatibilidad, escalabilidad, costo y comunidad de soporte.	Documentación técnica, fichas comparativas, lista de principales herramientas SIEM - Open Source	Solución SIEM seleccionada (ELK Stack)

Nº	Entrada	Actividad	Rol	Descripción	Herramientas	Salida
3	Solución SIEM seleccionada (ELK Stack)	Instalación de máquina virtual Ubuntu 24.04.2 LTS	Coordinador de TI	Se despliega la infraestructura base (VM) donde se alojará el SIEM. Se configura red, almacenamiento, usuarios y dependencias iniciales.	Proxmox, QEMU, Recursos de infraestructura (CPU, RAM, almacenamiento)	Servidor operativo y preparado para instalación
4	Servidor operativo y preparado para instalación	Instalación de servicios del ELK Stack	Coordinador de TI	Se instalan los componentes: Elasticsearch, Logstash, Kibana y Filebeat. Se validan versiones y dependencias.	CLI Ubuntu, documentación oficial Elastic	Servicios ELK instalados y en ejecución
5	Servicios ELK instalados y en ejecución	Configuración de fuentes para envío de registros	Coordinador de TI	Se configuran los dispositivos críticos para el envío de logs al SIEM: Firewalls Fortinet, Active Directory y NAS. Se prueban conectividades y formatos de logs.	Consola Fortigate, Winlogbeat, Filebeat	Logs enviados correctamente hacia Logstash
6	Logs enviados correctamente hacia Logstash	Configuración del pipeline en Logstash	Coordinador de TI / Analista de Cyberseguridad	Se establecen las fases del pipeline: Input, Filter (parsing y normalización) y Output hacia Elasticsearch.	Logstash, archivos .conf	Logs parseados correctamente hacia Elasticsearch

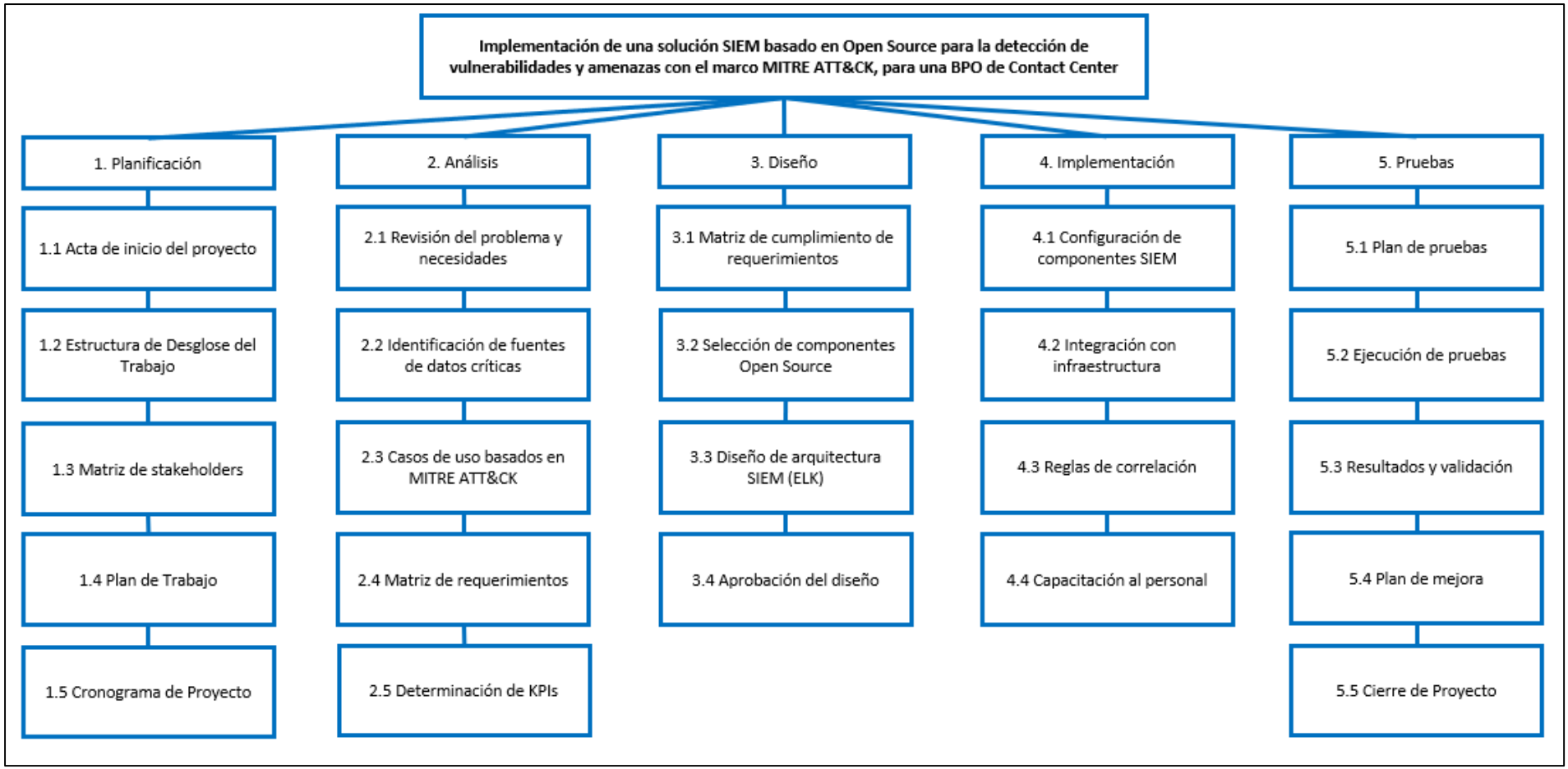
Nº	Entrada	Actividad	Rol	Descripción	Herramientas	Salida
7	Logs parseados correctamente hacia Elasticsearch	Indexación de eventos en Elasticsearch	Coordinador de TI / Analista de Cyberseguridad	Se verifica la correcta recepción, almacenamiento e indexación de logs en Elasticsearch.	Elasticsearch GUI, Dev Tools (Putty)	Índices de datos listos para consultar en Kibana
8	Índices de datos listos para consultar en Kibana	Visualización y análisis de datos en Kibana	Coordinador de TI / Analista de Cyberseguridad	Visualización de eventos de seguridad (LOG) para el monitoreo de alertas y correlaciones.	Kibana Analytics Discover	Eventos activos y visualizaciones de campos disponibles
9	Eventos activos y visualizaciones de campos disponibles	Configuración de casos de uso	Coordinador de TI / Analista de Cyberseguridad	Se desarrollan casos de uso de detección alineados al marco MITRE ATT&CK, configurando alertas y correlaciones.	Elastic Security, MITRE ATT&CK Navigator (matriz y requisitos)	Casos de uso activos y alertas configuradas
10	Casos de uso activos y alertas configuradas	Detección de alertas basadas en MITRE ATT&CK	Coordinador de TI / Analista de Cyberseguridad	Se elaboran alertas mediante dashboards que permiten visualizar las tácticas y técnicas MITRE asociadas a las detecciones.	Elastic Security Alerts, MITRE ATT&CK Navigator	Alertas operativas en base a los casos de uso

Nº	Entrada	Actividad	Rol	Descripción	Herramientas	Salida
11	Alertas operativas en base a los casos de uso	Capacitación al personal de TI	Coordinador de TI / Analista de Cyberseguridad	Se realiza la capacitación sobre gestión básica del SIEM y Mitre Att&ck	Manual del SIEM, diapositiva (Presentación PPT)	Personal capacitado y cuestionario de conocimientos

1.5.2 Estructura de Desglose de Tareas

Figura 10

Estructura de Desglose de Tareas (EDT)



1.5.3 Cronograma del proyecto

La siguiente tabla detalla el cronograma del proyecto, incluyendo las fases, actividades, responsables, fechas de inicio y fin, así como la duración estimada en días hábiles. Este cronograma fue elaborado con el fin de organizar y planificar de manera eficiente la implementación del SIEM basado en tecnología Open Source, alineado al marco MITRE ATT&CK.

Tabla 4

Cronograma del proyecto

Fase	Actividad	Responsable	Inicio	Fin	Duración (días)
Inicio	1.0 Inicio	Gerente de Sistemas	2/06/2025	2/06/2025	0
Planificación	1.1 Acta de inicio del proyecto	Gerente de Sistemas	2/06/2025	4/06/2025	3
	1.2 Estructura de Desglose del Trabajo (EDT)	Jefe de infraestructura	5/06/2025	6/06/2025	2
	1.3 Matriz de Stakeholders	Gerente de Sistemas	2/06/2025	6/06/2025	4
	1.4 Plan de trabajo	Jefe de infraestructura	9/06/2025	10/06/2025	2
	1.5 Cronograma de proyecto	Jefe de infraestructura	11/06/2025	12/06/2025	2
Análisis	2.1 Revisión del problema y necesidades	Jefe de infraestructura	13/06/2025	18/06/2025	4
	2.2 Identificación de fuentes de datos críticas	Jefe de infraestructura	19/06/2025	23/06/2025	3

Fase	Actividad	Responsable	Inicio	Fin	Duración (días)
	2.3 Casos de uso basados en MITRE ATT&CK	Coordinador de TI	24/06/2025	27/06/2025	4
	2.4 Matriz de requerimientos	Coordinador de TI	30/06/2025	1/07/2025	2
	2.5 Determinación de KPIs	Jefe de infraestructura	2/07/2025	3/07/2025	2
Diseño	3.1 Matriz de cumplimiento de requerimientos	Jefe de infraestructura	4/07/2025	7/07/2025	2
	3.3 Selección de componentes Open Source	Coordinador de TI	8/07/2025	10/07/2025	3
	3.2 Diseño de arquitectura SIEM	Coordinador de TI	11/07/2025	14/07/2025	2
	3.4 Diagrama técnico de arquitectura	Coordinador de TI	15/07/2025	16/07/2025	2
	3.5 Aprobación del diseño	Gerente de Sistemas	17/07/2025	18/07/2025	2
Implementación	4.1 Configuración de componentes SIEM	Coordinador de TI	21/07/2025	31/07/2025	7
	4.2 Integración con infraestructura	Coordinador de TI	1/08/2025	8/08/2025	6
	4.3 Reglas de correlación	Coordinador de TI	11/08/2025	29/08/2025	15
	4.4 Capacitación al personal	Coordinador de TI	1/09/2025	3/09/2025	3
Pruebas	5.1 Plan de pruebas	Coordinador de TI	4/09/2025	5/09/2025	2

Fase	Actividad	Responsable	Inicio	Fin	Duración (días)
	5.2 Ejecución de pruebas	Coordinador de TI	8/09/2025	19/09/2025	10
	5.3 Resultados y validación	Coordinador de TI	22/09/2025	26/09/2025	5
	5.4 Plan de mejora	Coordinador de TI	29/09/2025	30/09/2025	2
Cierre	5.5 Cierre del proyecto	Jefe de infraestructura	1/10/2025	1/10/2025	1
	5.6 Fin	Jefe de infraestructura	1/10/2025	1/10/2025	0

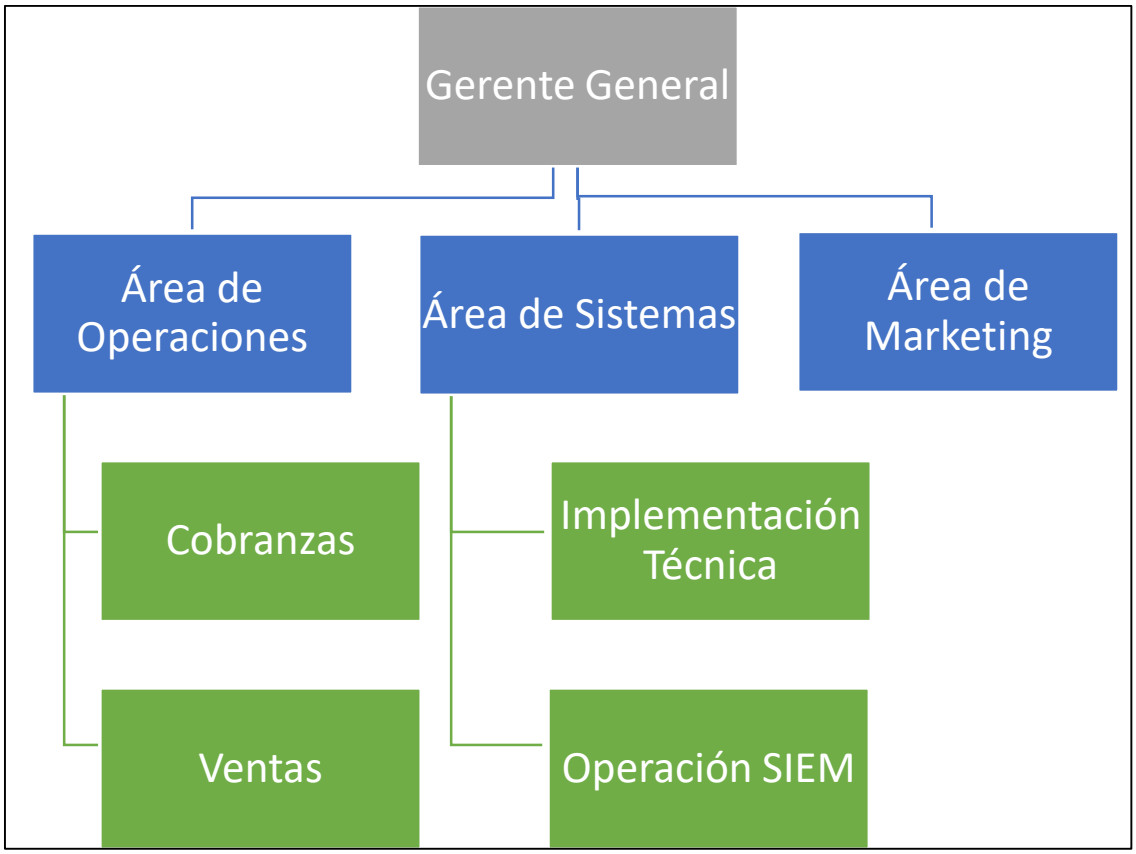
1.6 Alcance del Proyecto

El alcance del proyecto se centra principalmente en la sede del distrito de Los Olivos y está enfocado en el área de Sistemas, que será responsable de liderar y administrar la implementación técnica del SIEM, así como de su operación y monitoreo posterior. Además, se involucra de manera funcional al área de Operaciones, específicamente en los procesos de cobranzas y ventas, debido a que manejan información sensible relacionada con clientes y transacciones. También se considera, en menor medida, al área de Marketing y a Gerencia General, como usuarios indirectos que podrían requerir reportes de seguridad e indicadores para la toma de decisiones estratégicas.

Áreas involucradas en el alcance del proyecto:

Figura 11

Diagrama de Áreas Involucradas al proyecto



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

En cuanto a los procesos, el proyecto se enfoca en aquellos relacionados con la recolección, análisis y correlación de eventos de seguridad, utilizando como fuente principal los logs generados por dos firewalls y dos servidores identificados como críticos para la continuidad operativa de la empresa. Se abordarán exclusivamente tres casos de uso definidos, alineados con tácticas y técnicas del marco MITRE ATT&CK. Estos casos fueron seleccionados en función de su relevancia y factibilidad técnica, mientras que cualquier otro escenario adicional será considerado fuera del alcance.

La implementación se realizará utilizando recursos existentes de la organización, tales como servidores, almacenamiento y conectividad. No se contempla la adquisición de infraestructura adicional ni la incorporación de soluciones comerciales.

Desde una perspectiva de ingeniería, este proyecto representa un aporte valioso al demostrar que es posible implementar una solución de ciberseguridad avanzada, con capacidad de correlación y visibilidad sobre amenazas, utilizando únicamente tecnologías Open Source y marcos estandarizados como MITRE ATT&CK.

Por otro lado, este proyecto presenta ciertos límites que deben ser considerados. En primer lugar, solo se contemplan los tres casos de uso definidos; cualquier otro escenario será tratado en futuras fases. Del mismo modo, la correlación de eventos se limitará a dos firewalls y dos servidores, sin incluir otros dispositivos o plataformas internas. Además, la solución no integrará funcionalidades de respuesta automática (SOAR), ya que el enfoque está centrado en la detección y monitoreo de amenazas.

Finalmente, no se incluye la capacitación de todas las áreas de la empresa ni la implementación masiva en otras unidades organizacionales. El proyecto busca demostrar la viabilidad técnica de la solución SIEM con un alcance acotado, que pueda luego escalarse según las capacidades y prioridades futuras de la empresa.

2 CAPÍTULO 2: MARCO TEÓRICO

2.1 SIEM

Un Security Information and Event Management (SIEM) es una aplicación que permite recopilar datos de seguridad de los componentes de un sistema de información y presentarlos como información procesable a través de una única interfaz (National Institute of Standards and Technology [NIST], 2013).

En otras palabras, un Security Information and Event Management (SIEM) es una solución que centraliza la recolección, estandarización, análisis y correlación en tiempo real de registros (logs) provenientes de múltiples fuentes, y que expone tableros, reportes y alertas para apoyar la detección de amenazas y la respuesta a incidentes. Según Vazão et al. (2023) en esencia, una solución SIEM proporciona una visión amplia y detallada de la seguridad de una empresa, lo que permite a los analistas realizar análisis de seguridad en tiempo real. Además, por sus características, las soluciones SIEM permiten identificar con mayor antelación los ciberataques y posibles incidentes de seguridad, contribuyendo así al cumplimiento de normativas por parte de una empresa.

Las soluciones de gestión de eventos e información de seguridad, conocidas como SIEM, no operan de manera aislada. Su eficacia se potencia cuando se integran con otras capacidades de seguridad. Un claro ejemplo de esto es su combinación con sistemas de detección de intrusiones (IDS) y técnicas de aprendizaje automático, lo cual permite transformar el tráfico de red en eventos enriquecidos (JSON) que se visualizan y alertan en el SIEM. Esto facilita el análisis en vivo y la detección de ataques como los de denegación de servicio (DoS) (Muhammad et al., 2023).

Así también se puede señalar que la función del SIEM se extiende a contextos educativos y de laboratorio, donde su capacidad para procesar y correlacionar eventos provenientes de honeypots, firewalls u otros sensores ofrece experiencias cercanas a un SOC real y favorece la formación práctica en detección y análisis de amenazas (Ariffin et al., 2022).

2.1.1 Arquitectura típica de un SIEM

"La arquitectura de un SIEM se compone de un sistema de procesamiento de eventos/flujo, que incluye la formalización y el procesamiento de reglas, y luego se transfiere al sistema de análisis de correlación, donde se analizan los eventos recopilados" (Park J. S., 2024, p. 2).

Figura 12

Sistema de procesos de un SIEM



Nota. La figura muestra los procesos básicos de un sistema SIEM a alto nivel. Adaptado de "Efficient analysis and detection of intelligent security threats in cloud environment.", por Park, J. S. 2024 (https://doi.org/10.70003/160792642024072504013)

El diagrama anterior representa el ciclo mínimo de un SIEM desde la generación de registros hasta la detección de amenazas. Cada etapa transforma datos operacionales en evidencia analítica para apoyar la respuesta a incidentes. Esta estructura para el análisis y la detección de seguridad consta de cuatro pasos fundamentales:

a) **Generación de LOG:** en esta fase los activos de tecnología (firewalls, sistemas operativos, aplicaciones, nubes y endpoints) producen eventos que describen acciones, errores y cambios de estado. Para que esos eventos sean útiles, deben incluir atributos básicos como marca de tiempo confiable, origen/destino, identidad y resultado, y emitirse con mecanismos estandarizados (por ejemplo, Syslog) y controles de integridad y transporte seguro hacia un colector central.

b) **Parseo y análisis de LOG (correlación):** Los eventos crudos son normalizados para convertir formatos heterogéneos en un esquema común y enriquecidos con contexto (geolocalización, criticidad del activo, pertenencia a grupos, amenazas conocidas). A partir de ello se aplican correlaciones: agregaciones temporales, secuencias causales, coincidencias entre fuentes y detecciones de anomalías. Esta etapa crea la base semántica que permite comparar comportamientos entre tecnologías y mapearlos con marcos de conocimiento como MITRE ATT&CK para describir las técnicas y tácticas subyacentes observadas (MITRE Corporation, s.f.-a; NIST, 2006).

c) Creación de reglas personalizadas: Con los campos normalizados, se define la lógica de detección que refleja el riesgo del negocio: condiciones, umbrales y ventanas temporales; uniones por identidad (Identity Correlation), host o red; y excepciones para reducir falsos positivos. Cada regla debe declarar su objetivo, severidad esperada, fuentes requeridas y relación con técnicas ATT&CK para mantener trazabilidad analítica. El ajuste continuo (tuning) se guía por la relevancia de activos críticos y por métricas de desempeño operativo del SOC (MITRE Corporation, s.f.-a; NIST, 2011).

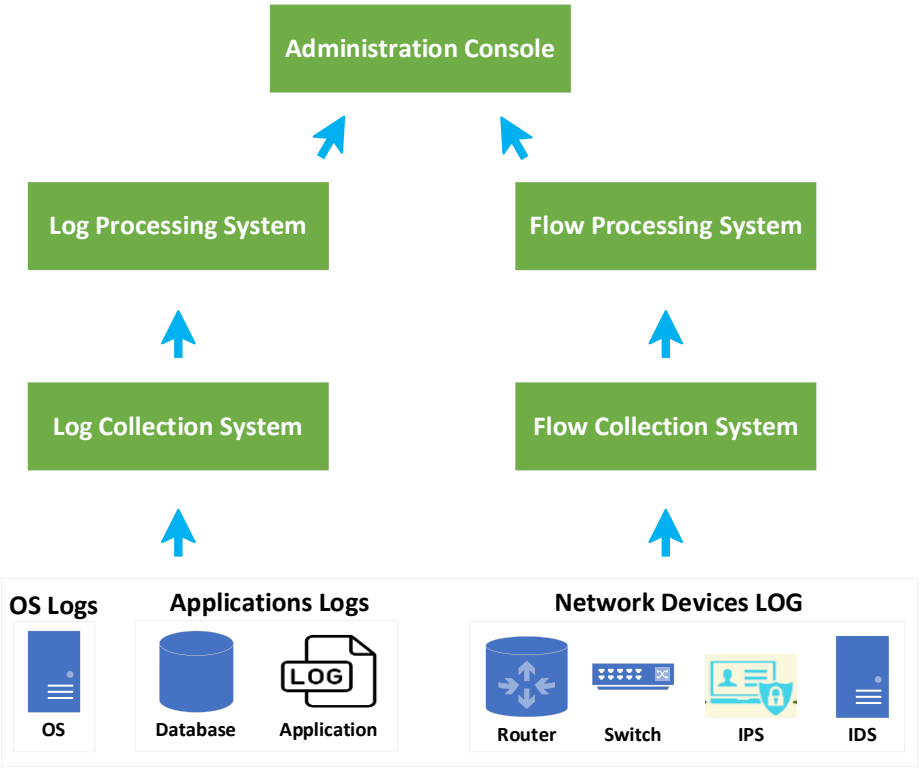
d) Detección de amenazas de seguridad: Cuando se cumplen las condiciones de una regla, el SIEM genera una alerta que inicia el flujo de gestión de incidentes: triage, investigación (pivotando por usuario, host y tiempo), contención, erradicación y recuperación. La documentación resultante fortalece la evidencia forense y alimenta la mejora del contenido de detección y de las políticas de registro. La integración de este ciclo con los procedimientos formales de manejo de incidentes y con la monitorización continua de seguridad es esencial para reducir el tiempo de detección y respuesta (NIST, 2011, 2012).

"El sistema SIEM monitorea el estado de seguridad de todos los dispositivos conectados en una red organizacional al analizar los registros enviados desde estos dispositivos" (Sheeraz et al., 2023, p. 16).

A continuación, se muestra la arquitectura básica de un SIEM.

Figura 13

Arquitectura básica de un SIEM



Nota. La figura muestra el funcionamiento de un sistema SIEM a alto nivel. Adaptado de "Efficient analysis and detection of intelligent security threats in cloud environment.", por Park, J. S. 2024 (https://doi.org/10.70003/160792642024072504013)

El gráfico representa una arquitectura de SIEM basada en dos canales de telemetría paralelos (eventos y flujos de red) que convergen en una consola de administración. En la base están las fuentes de datos (sistemas operativos, bases de datos y aplicaciones, así como equipos de red, IPS e IDS).

La arquitectura mencionada se puede dividir de la siguiente manera:

Fuentes de datos

Los sistemas y aplicaciones generan registros que describen actividades, errores y cambios de estado; los dispositivos de red aportan eventos propios y flujos que resumen comunicaciones (por ejemplo, bytes, paquetes, duración). En términos de estándares, los eventos suelen transportarse mediante Syslog u otros mecanismos de recolección, mientras que los flujos se exportan mediante NetFlow o IPFIX (IETF, 2009; IETF, 2004, 2013).

Log Collection System (sistema de colección de logs).

Es la infraestructura que recibe y transporta eventos desde las fuentes hacia el SIEM. Incluye agentes/forwarders, colecciones por API y receptores Syslog. Sus objetivos son: asegurar integridad y confidencialidad del transporte, preservar marcas de tiempo sincronizadas (NTP), desacoplar picos de EPS con colas/búferes y garantizar reintentos ante caídas (NIST, 2006; IETF, 2009).

Log Processing System (sistema de procesamiento de logs).

Transforma eventos heterogéneos en un esquema común y agrega contexto. Las funciones típicas son: parseo/normalización, deduplicación, enriquecimiento (GeoIP, inventario de activos, identidad), etiquetado por técnica/táctica, y persistencia indexada para búsquedas y correlaciones. Este nivel habilita consultas coherentes entre tecnologías y sienta las bases para la monitorización continua y la detección basada en reglas y comportamiento (NIST, 2006, 2011).

Flow Collection System (sistema de colección de flujos).

Recolecta resúmenes de tráfico generados por routers, switches, IPS/IDS u otros exportadores en formatos NetFlow/IPFIX. A diferencia de los logs de aplicación, los flujos no contienen carga útil; capturan metadatos esenciales para conocer patrones de comunicación y volumen, con bajos costos de almacenamiento y sin inspección profunda (IETF, 2004, 2013).

Flow Processing System (sistema de procesamiento de flujos).

Agrega, normaliza y aporta valor analítico a los registros de flujo: calcula tasas, identifica escaneos, tormentas de conexiones, variaciones de base, y correlaciona con activos y listas de reputación. Los resultados alimentan reglas que detectan descubrimiento, movimiento lateral o exfiltración, y complementan la evidencia de eventos de host/aplicación (NIST, 2011).

Administration Console (consola de administración).

Es la interfaz central para búsqueda, correlación, visualización, gestión de reglas y orquestación de respuesta. Desde aquí se ejecuta la clasificación, se abren casos, se sigue el ciclo de vida de incidentes y se generan reportes operativos y ejecutivos.

2.1.2 Arquitectura modular de un SIEM

Para tener una comprensión y una visión general del funcionamiento interno de un SIEM es necesario establecer una arquitectura teórica. De acuerdo con Sheeraz et al. (2023) propone la arquitectura modular de un sistema SIEM, basada en módulos para facilitar la comprensión de estos, esto debido a que según los autores no existe una arquitectura claramente definida que las organizaciones puedan seguir para desarrollar o implementar sus propios sistemas SIEM. Así pues, proponen 10 módulos los cuales se detallan a continuación:

1) **Módulo de Agregación de Datos:** Recibe logs, eventos y datos contextuales desde múltiples fuentes (servidores, redes, aplicaciones) y los introduce en el pipeline del SIEM. Debe soportar ráfagas a alta velocidad, por lo que los autores contemplan incluso aceleración de captura a "line rate" con tarjetas dedicadas (p. ej., Napatech) cuando las NIC estándar no alcanzan el caudal requerido. Su salida alimenta inmediatamente al módulo de normalización. (Sheeraz et al., 2023).

2) **Módulo de Normalización:** Convierte entradas heterogéneas a un formato uniforme (JSON) para que el resto de los módulos opere de forma consistente, usando paralelismo para acelerar el procesamiento. La sección de formatos de log contextualiza por qué normalizar (Syslog/rsyslog, IDMEF, CEF, GELF, etc.) antes de convertir a JSON. El resultado normalizado se persiste mediante el módulo de almacenamiento. (Sheeraz et al., 2023).

3) **Módulo de Correlación:** Aplica reglas sobre los datos normalizados para vincular eventos y generar alertas cuando se cumplen patrones. Se subrayan límites de esquemas puramente basados en umbrales (por ejemplo, eventos "near-miss" que quedan por debajo del umbral) y abre la puerta a mejorar con metaheurísticas/ML o enfoques híbridos para reducir falsos negativos. (Sheeraz et al., 2023).

4) **Módulo de Alerta en Tiempo Real:** Entrega las alertas de correlación al GUI de la forma más apropiada para la operación, habilitando notificación inmediata al analista y priorización según criticidad/urgencia. (Sheeraz et al., 2023).

5) **Módulo de Visualización:** Presenta alertas y contexto mediante dashboards. Un GUI eficiente ayuda a descubrir eventos "near-miss" que no activaron reglas por umbral, mejorando detección y análisis; como línea futura, proponen realidad aumentada

(AR) para enriquecer la percepción de ataques por parte del analista. (Sheeraz et al., 2023).

6) **Módulo de Reportes:** Genera informes personalizados sobre la base activa según filtros y búsquedas. Se listan cinco familias comunes: autenticaciones, accesos a archivos, cambios en usuarios/grupos/servicios, eventos de amenaza, y eventos de ataque; estos reportes apoyan auditoría, cumplimiento y mejora continua. (Sheeraz et al., 2023).

7) **Módulo de Almacenamiento:** Conserva datos normalizados y alertas de correlación en una base activa, idealmente con tecnologías de big data para ingestión y consulta en tiempo real. El diseño recomienda gestión centralizada e indexada, backups automáticos, soporte cloud (S3, Nextcloud, etc.), garantías CIA, y capacidades de escalado, filtrado, compresión y archivado, además de cumplimiento (PCI DSS, HIPAA, SOX, GDPR). (Sheeraz et al., 2023).

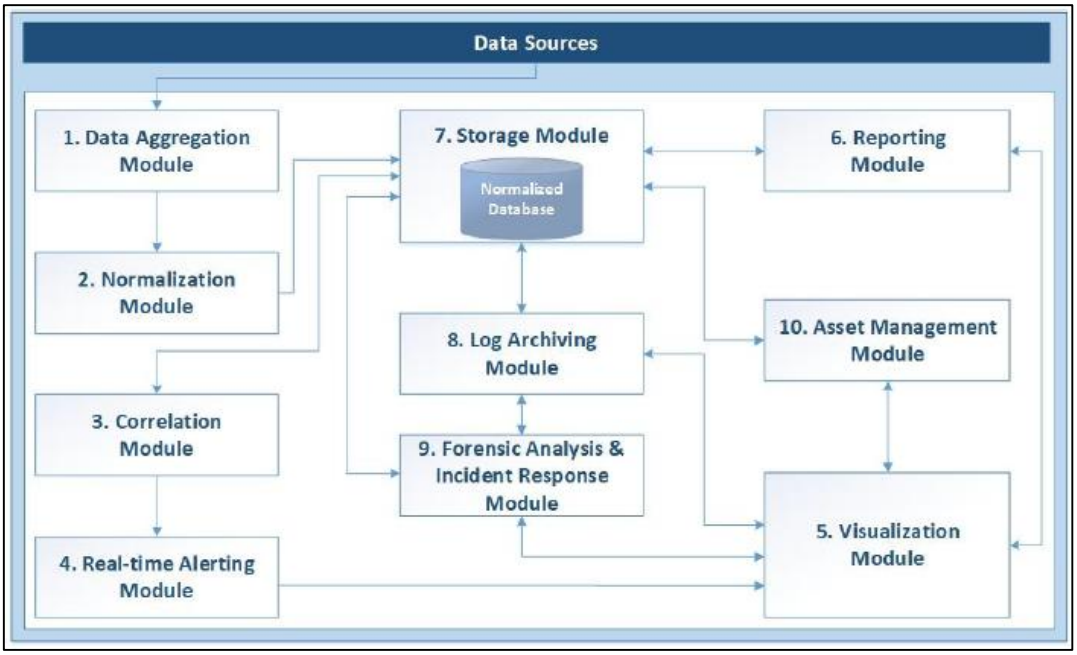
8) **Módulo de Archivado de logs:** Tras un período definido, migra datos desde la base activa a un repositorio en estado "dormant" para retención a largo plazo. La selección del medio (óptico, magnético, disco, cloud, etc.) valora tamaño, fiabilidad, velocidad y costo, en función de las necesidades de acceso y políticas de conservación. (Sheeraz et al., 2023).

9) **Módulo de Análisis Forense e Respuesta a Incidentes:** Aplica técnicas analíticas sobre registros históricos para reconstruir actividades, identificar rutas de compromiso y preparar evidencia técnica que alimente la respuesta y la mejora de controles. (Sheeraz et al., 2023).

10) **Módulo de Gestión de Activos:** Automatiza el inventario y la administración integral de los activos de la organización (tanto hardware como software), superando las limitaciones de la gestión manual y manteniendo una visión actualizada de todo elemento que habilita las operaciones del negocio; su información se integra con el resto de módulos para sostener las funciones centrales del sistema y, gracias al diseño modular y extensible, admite la incorporación de nuevas funcionalidades conforme surjan necesidades futuras (Sheeraz et al., 2023).

Figura 14

Arquitectura modular teórica de un SIEM



Nota. La figura muestra una propuesta de arquitectura de un SIEM basado en 10 módulos. De "Effective Security Monitoring using Efficient SIEM Architecture.", por Sheeraz et al. 2023 (https://doi.org/10.22967/hcis.2023.13.023)

Aunque esta es una propuesta conceptual, proporciona una visión clara del funcionamiento interno de un sistema SIEM. Cabe destacar que en el mercado existen diversos tipos de SIEM, tanto comerciales como de código abierto.

2.1.3 SIEMs Open Source

En cuanto al ecosistema de soluciones, los estudios comparativos recientes sobre herramientas abiertas y gratuitas señalan a Wazuh, SIEMonster, OSSIM y Elastic Stack entre las opciones más difundidas, destacando que su elección exige ponderar características de seguridad, rendimiento y facilidad de despliegue, especialmente en pymes con restricciones presupuestarias (Manzoor et al., 2024).

2.1.3.1 Elastic Stack (ELK Stack)

El ELK Stack es un conjunto de tecnologías open source desarrollado por Elastic que ha evolucionado como una de las soluciones más adoptadas para la gestión centralizada de datos, logs y métricas en entornos empresariales y de seguridad informática. El acrónimo ELK hace referencia a sus tres componentes principales: Elasticsearch, Logstash y Kibana, los cuales, en conjunto, proporcionan un flujo completo para la ingesta, almacenamiento, análisis y visualización de datos (Elastic, s. f.-a).

A continuación, se detalla los componentes que forman esta tecnología:

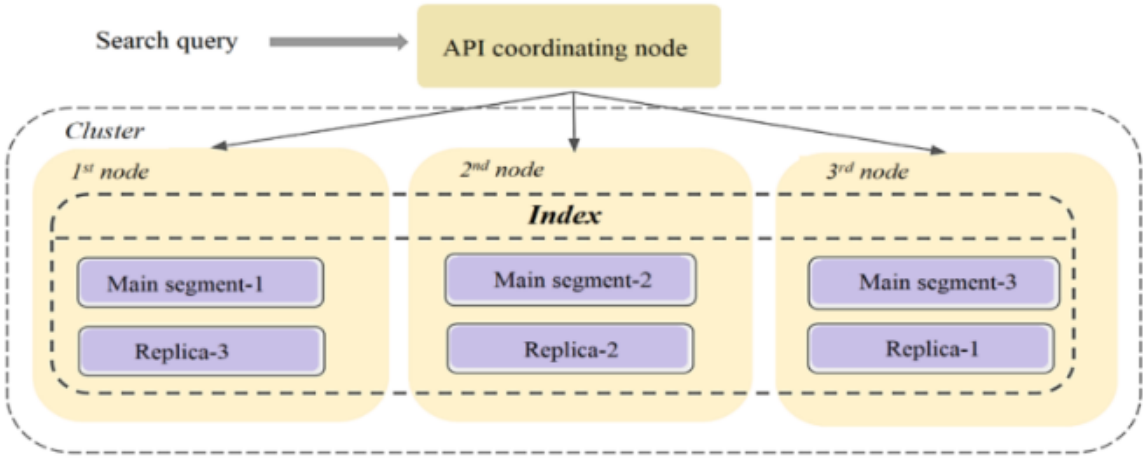
Elasticsearch

Es un motor de búsqueda y análisis distribuido, basado en Apache Lucene, que permite realizar consultas en tiempo real sobre volúmenes masivos de datos estructurados y no estructurados. Su arquitectura distribuida permite el escalamiento horizontal mediante nodos y clústeres, asegurando disponibilidad y tolerancia a fallos, lo que lo convierte en el núcleo de indexación dentro del stack.

Elasticsearch actúa como núcleo de almacenamiento, búsqueda y analítica del stack: organiza la información como documentos JSON dentro de índices (análogos a bases/tablas/filas en relacionales), distribuye los datos en segmentos (shards) entre nodos de un clúster y garantiza alta disponibilidad mediante réplicas; un nodo coordinador recibe las consultas y las distribuye a los nodos que contienen los shards relevantes para resolverlas eficientemente (Nezhmetdinov et al., 2023).

Figura 15

Arquitectura de clúster de un SIEM basada en Elastic Stack



Nota. La figura muestra una propuesta de arquitectura de un SIEM basada en la organización de nodos, segmentos y réplicas para la gestión de índices. De Automating log analysis for industrial equipment maintenance using elastic stack, por Nezhmetdinov, R., Kotyrova, S., Nezhmetdinova, R., & Kovalev, I., 2023, E3S Web of Conferences, 389, 01064 (https://doi.org/10.1051/e3sconf/202338901064).

Asimismo, es importante considerar que Elasticsearch incorpora el Elastic Common Schema (ECS) como mecanismo de estandarización para la gestión de datos. Y al respecto se presenta la siguiente definición.

El Elastic Common Schema (ECS) es una especificación de código abierto, impulsada por la comunidad, que define un conjunto común de campos, sus tipos de datos en Elasticsearch, valores permitidos y una jerarquía de uso para los datos ingestados en Elasticsearch. Unifica todos los modos de análisis disponibles en Elastic, incluyendo búsqueda, exploración detallada, pivoteo, visualización de datos, detección de anomalías basada en machine learning, reglas de detección y alertas (Elastic, s.f.-b).

Una de sus principales ventajas es que reduce el tiempo dedicado al desarrollo de contenido analítico: en lugar de crear nuevas búsquedas y dashboards cada vez que la organización incorpora una nueva fuente de datos, es posible continuar aprovechando los existentes. Asimismo, las integraciones nativas de Elastic garantizan que los datos ingestados ya estén mapeados a ECS, por lo que basta con habilitar la integración e ingestar los datos para comenzar a trabajar con ellos en formato ECS dentro de soluciones como Elastic Security y Observability (Elastic, s.f.-b).

Logstash

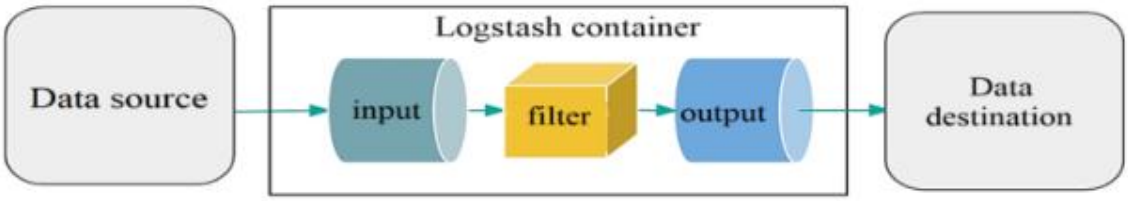
Es un motor de procesamiento de datos que recolecta información de múltiples fuentes heterogéneas (archivos de log, bases de datos, servicios de red, APIs, entre otros). Permite aplicar transformaciones, filtrados y enriquecimiento de datos mediante un sistema de "pipelines" compuesto por inputs, filters y outputs, enviando finalmente la información normalizada hacia Elasticsearch u otros destinos compatibles.

Un pipeline de datos es un proceso sistemático y automatizado para el movimiento, transformación y gestión eficiente y confiable de datos de un punto a otro dentro de un entorno informático. Está compuesto por una serie de pasos de procesamiento encadenados, donde cada paso genera una salida que sirve como entrada para el siguiente, hasta completar el flujo. (Hazelcast, 2025).

Según Nezhmetdinov et al. (2023), Logstash cumple el rol de agregador y preprocesador: implementa un pipeline de tres etapas —input{} (genera eventos), filter{} (los transforma; opcional) y output{} (los envía al destino)—, todo definido en un archivo de configuración con plugins para entradas, filtros y salidas. Esta arquitectura permite normalizar y enriquecer datos heterogéneos (línea única, XML, JSON) antes de su indexación en Elasticsearch.

Figura 16

Arquitectura de Logstash



Nota. La figura muestra la arquitectura de Logstah, en la cual los datos son procesados a través de fases de entrada (input), filtrado (filter) y salida (output) dentro de un contenedor antes de llegar a su destino. De Automating log analysis for industrial equipment maintenance using elastic stack, por Nezhmetdinov, R., Kotyrova, S., Nezhmetdinova, R., & Kovalev, I., 2023, E3S Web of Conferences, 389, 01064 (https://doi.org/10.1051/e3sconf/202338901064).

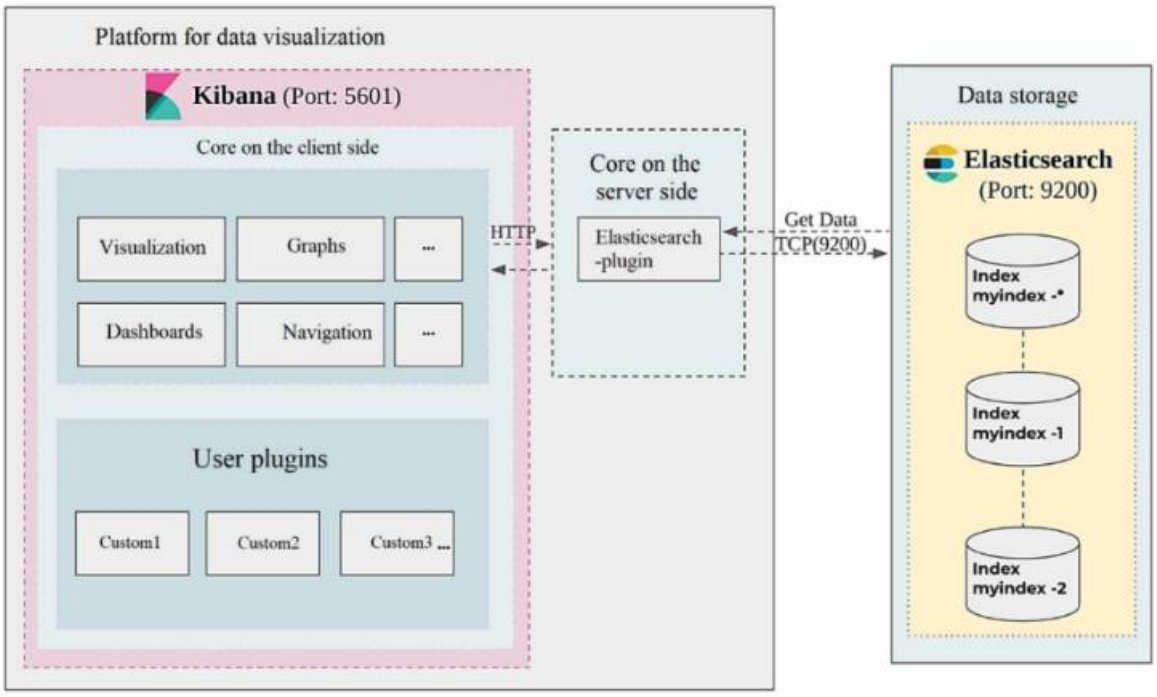
Kibana

Constituye la interfaz de visualización y exploración de datos, ofreciendo dashboards personalizables, gráficos dinámicos, mapas interactivos y herramientas de análisis. En el ámbito de la ciberseguridad, Kibana se utiliza para construir paneles de Security Operations Centers (SOC), facilitando la supervisión de alertas, tendencias de ataque y análisis forense.

Kibana constituye la capa de visualización sobre Elasticsearch y se divide en dos módulos: (1) el módulo de interfaz de usuario, que carga los plugins con la lógica funcional necesaria (dashboards, búsquedas, paneles), y (2) el módulo servidor, que se enlaza al clúster de Elasticsearch y expone un API interno para servir datos a la interfaz. Este diseño modular habilita análisis visual y exploración de datos en tiempo real dentro del SIEM (Nezhmetdinov et al., 2023).

Figura 17

Arquitectura de Kibana



Nota. La figura muestra la arquitectura de Kibana, destacando los módulos de visualización, paneles, navegación y complementos de usuario, así como su integración con Elasticsearch para la consulta y visualización de datos. De Automating log analysis for industrial equipment maintenance using elastic stack, por Nezhmetdinov, R., Kotyrova, S., Nezhmetdinova, R., & Kovalev, I., 2023, E3S Web of Conferences, 389, 01064 (https://doi.org/10.1051/e3sconf/202338901064).

A partir de 2015, Elastic expandió el stack mediante la incorporación de Beats, agentes ligeros diseñados para recolectar datos en tiempo real desde sistemas operativos, servidores y aplicaciones (por ejemplo: Filebeat para logs, Metricbeat para métricas de sistemas, Packetbeat para tráfico de red, entre otros). Con esta adición, el término Elastic Stack (o "ELK + Beats") se consolidó para referirse al ecosistema completo.

En el contexto de la ciberseguridad y SIEM, el ELK Stack es ampliamente utilizado como base tecnológica para construir soluciones de detección de amenazas, correlación de eventos y cumplimiento normativo. Diversos proyectos open source, como Wazuh o SIEMonster, integran ELK como motor de indexación y visualización, aprovechando su capacidad de correlacionar logs provenientes de firewalls, sistemas operativos, aplicaciones en la nube y dispositivos de red. Asimismo, su flexibilidad permite desarrollar casos de uso de seguridad alineados con marcos de referencia como MITRE ATT&CK, fortaleciendo las operaciones de monitoreo, investigación y respuesta a incidentes en un SOC.

En conclusión, el ELK Stack no solo representa un conjunto de herramientas para la gestión de logs, sino un ecosistema modular y escalable que posibilita construir soluciones avanzadas de seguridad y análisis de datos. Su combinación de recolección, procesamiento, indexación y visualización lo posiciona como un estándar de facto en el ámbito de la ciberseguridad empresarial y en el diseño de arquitecturas SIEM modernas.enes de datos de manera eficiente.

2.1.3.2 Wazuh

Wazuh es un SIEM de código abierto con arquitectura cliente-servidor: agentes en los endpoints envían eventos hacia un clúster compuesto por Indexer (almacenamiento/consulta), Server (análisis y alertado) y Dashboard (gestión y visualización). Sus capacidades incluyen análisis de logs, monitoreo de integridad de archivos (FIM), detección de intrusiones, respuestas activas y paneles personalizables; además ofrece control de acceso basado en roles (dos modos de RBAC) y plantillas de cumplimiento (PCI DSS, GDPR, HIPAA, GPG13). En las comparativas del estudio, también dispone de despliegues con alta disponibilidad. (Manzoor et al., 2024)

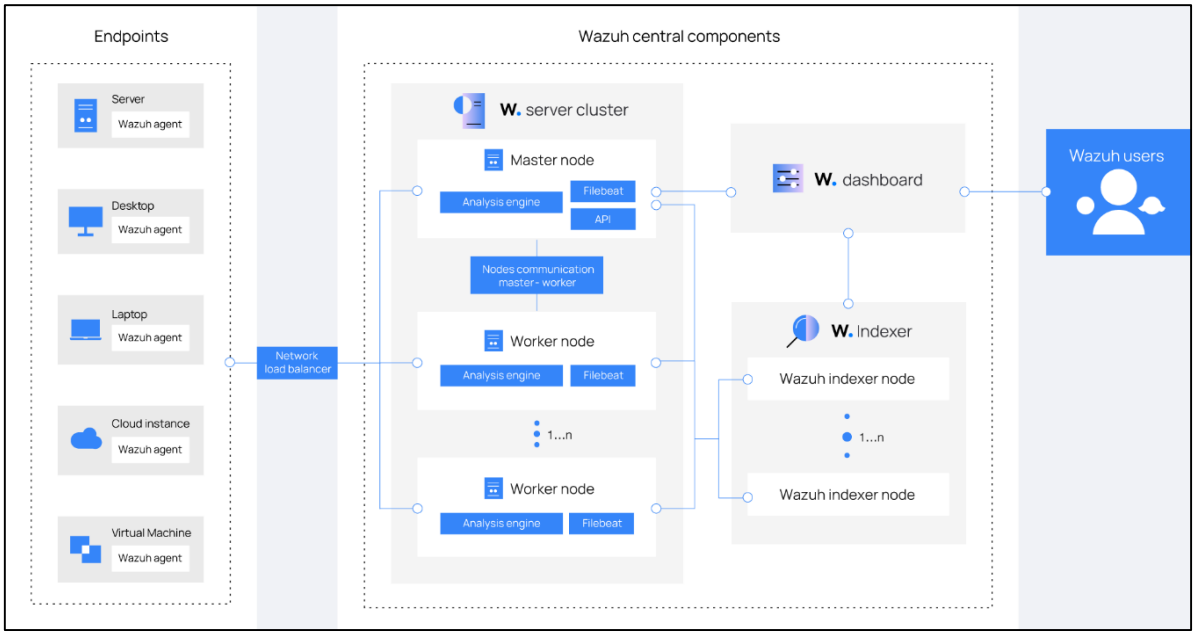
Wazuh adopta una arquitectura modular compuesta por un agente multiplataforma y tres componentes centrales: Wazuh Server, Wazuh Indexer y Wazuh Dashboard. El agente se instala en los endpoints para recolectar telemetría y eventos de seguridad y los envía al Server para su decodificación, correlación y detección. Los datos analizados se indexan y almacenan en el Indexer, y finalmente se consultan y visualizan en el Dashboard para alertamiento y análisis. Además, Wazuh admite monitoreo sin agente (agentless) para dispositivos en los que no se puede instalar el agente (p. ej., firewalls, routers, switches) mediante Syslog y SSH.

En despliegue, Wazuh es flexible y escalable:

a) All-in-one (todos los componentes en un único servidor) para laboratorios o entornos pequeños.
b) Single-node (server, indexer y dashboard en servidores separados) para cargas medias.
c) Multi-node con clustering del Server y del Indexer, y un Dashboard dedicado, recomendado para alta disponibilidad, tolerancia a fallos y alto throughput de eventos. El diagrama oficial de despliegue ilustra estos clústeres y su balanceo de carga.

Figura 18

Arquitectura de Wazuh



Nota. La figura muestra la arquitectura de Wazuh, incluyendo los agentes instalados en los diferentes endpoints, el clúster de servidores con nodos maestro y de trabajo, el componente de indexación y el panel de control para los usuarios. Tomado de Architecture, por Wazuh, s.f.-a (https://documentation.wazuh.com/current/getting-started/architecture.html).

La comunicación entre componentes está definida y cifrada por defecto. El agente se conecta al Server (por defecto TCP 1514) usando el protocolo de mensajes de Wazuh con AES (128-bit blocks, keys de 256 bits; Blowfish opcional). El Server envía alertas y eventos al Indexer mediante Filebeat con TLS (el Indexer escucha por defecto en TCP 9200). El Dashboard consulta el API REST del Server (por defecto TCP 55000 con TLS) para estado y configuración, y visualiza datos desde el Indexer. La documentación lista los puertos por defecto (por ejemplo: Server 1514/TCP-UDP, 1515/TCP, 1516/TCP, 514/UDP/TCP opcional; Indexer 9200/TCP y 9300-9400/TCP; Dashboard 443/TCP).

Finalmente, Wazuh integra un servicio de Cyber Threat Intelligence (CTI) público que agrega y normaliza información sobre vulnerabilidades (CVEs, severidad, explotabilidad y mitigaciones) y que se conecta directamente con el módulo de Vulnerability Detection de la plataforma.

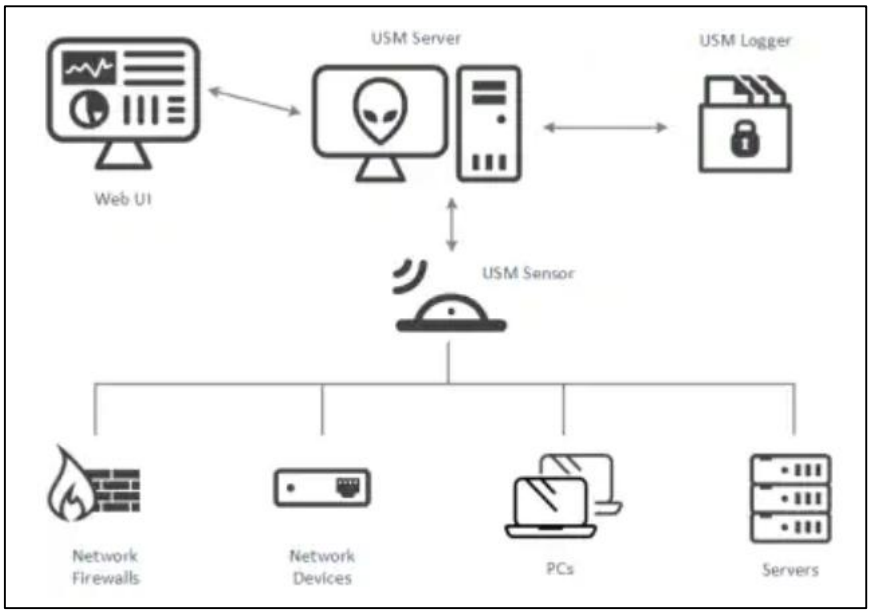
2.1.3.3 AlienVault OSSIM

OSSIM es el SIEM abierto de AT&T/AlienVault. Implementa RBAC con tres roles (Read-Only, Analyst, Manager) y admite personalización mediante “plugins” para nuevas fuentes; en la evaluación reporta uso de AES-128 para integridad de logs y retención por 5 días. Sus limitaciones en la edición comunitaria incluyen ausencia de alta disponibilidad y de plantillas de cumplimiento. (Manzoor et al., 2024).

OSSIM (Open Source Security Information Management) es una plataforma SIEM de código abierto que unifica en una sola solución varias funciones de seguridad: gestión y correlación de eventos (SIEM), descubrimiento de activos, detección de intrusiones (NIDS/HIDS), evaluación de vulnerabilidades, monitorización de comportamiento y amenazas externas (Threat Intelligence). Su diseño se basa en una arquitectura modular con sensores y un servidor SIEM que recolectan, normalizan y correlacionan eventos provenientes de múltiples fuentes para generar alertas y facilitar la investigación. En despliegues típicos, los sensores capturan logs/tráfico y los envían al servidor, donde se almacenan y correlacionan; esta separación permite escalar horizontalmente según el volumen de eventos y las redes a cubrir (AT&T Cybersecurity, s.f.-a).

Figura 19

Arquitectura del USM Appliance



Nota. La figura muestra la arquitectura del USM Appliance y sus componentes principales. De About USM Appliance system architecture and components, por AT&T Cybersecurity, s.f.-b, (Recuperado el 14 de septiembre de 2025, de https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm).

OSSIM integra de forma nativa varios proyectos open source para cubrir los distintos dominios de monitoreo:

a) HIDS (Host IDS): OSSEC para monitoreo de logs, FIM (file integrity) y detección en host.
b) NIDS (Network IDS): Snort y/o Suricata para inspección profunda de tráfico y firmas de ataque.
c) Vulnerabilidades: OpenVAS (Greenbone) para escaneo y correlación con eventos de IDS.
d) Descubrimiento/flujo/monitoreo: PRADS, FProbe/NFDump-NfSen (NetFlow), Nagios/Munin, TCPTrack, entre otros.

Esta combinación provee telemetría amplia (host, red, vulnerabilidades, servicios), que el SIEM normaliza y correlaciona mediante directivas para detectar comportamientos maliciosos con mayor contexto.

Un diferenciador histórico de OSSIM es su integración con OTX (Open Threat Exchange), plataforma colaborativa de inteligencia de amenazas. Mediante pulses (colecciones de IoCs como IPs, dominios, URLs, hashes), OSSIM/USM puede enriquecer eventos y disparar alarmas cuando un activo se comunica con indicadores maliciosos; en entornos distribuidos, los IoCs se replican desde el servidor hacia sensores para mantener la detección actualizada (AT&T Cybersecurity, s. f.-c).

En términos de despliegue, la lógica de sensor/servidor facilita: (1) instalaciones todo-en-uno para entornos pequeños; (2) despliegues distribuidos con varios sensores para segmentar por redes/zonas y aumentar capacidad; y (3) alta disponibilidad al separar funciones (captura, correlación, almacenamiento). La documentación oficial de AT&T/LevelBlue para USM (la edición comercial basada en OSSIM) describe estos componentes y flujos, que son equivalentes conceptualmente en OSSIM: el Sensor recolecta y normaliza, y el Server correlaciona, almacena y presenta eventos/alertas (AT&T Cybersecurity, s. f.-d).

2.1.3.4 SIEMonster

SIEMonster (edición comunitaria) es un SIEM open-source que utiliza Kibana para visualización y ofrece RBAC de grano fino; incorpora autenticación en dos factores. La edición gratuita no provee alta disponibilidad y su escalabilidad está limitada (un servidor, hasta 100 endpoints), aunque la plataforma comercial amplía estas capacidades; sí ofrece reportes de cumplimiento (NIST/HIPAA). (Manzoor et al., 2024).

SIEMonster es una plataforma SIEM/XDR basada en software open source y una arquitectura modular pensada para escalar horizontal y verticalmente. Su diseño típico organiza el flujo en cuatro capas: ingesta, procesamiento/correlación, almacenamiento/búsqueda y visualización/orquestación. En ingesta, SIEMonster admite agentes y fuentes heterogéneas (por ejemplo, Wazuh/OSSEC para HIDS y FIM; Suricata para NIDS), más entradas vía Syslog y colectores; esta telemetría se normaliza y enruta hacia procesadores/event pipelines.

En procesamiento y correlación, versiones recientes han incorporado componentes open-source de alto rendimiento y orquestación (históricamente Apache Kafka y Apache NiFi para flujos; Cortex y TheHive para respuesta e IR), además de integraciones de Threat Intelligence (MISP, OpenCTI) para enriquecer eventos y activar casos de uso. Estas piezas permiten construir pipelines con reglas, enriquecimiento y priorización antes del almacenamiento.

Para almacenamiento y búsqueda, SIEMonster ha utilizado Open Distro for Elasticsearch (hoy OpenSearch) como motor de índices y consultas, soportando altos EPS y permitiendo retención flexible y análisis interactivo. La visualización se apoya en dashboards personalizables y paneles de mando listos para cumplimiento y operaciones SOC.

En orquestación y automatización (SOAR), la plataforma integra Shuffle SOAR, lo que habilita workflows de respuesta (notificaciones a correo/SMS/Slack, contención, tickets en TheHive, etc.) y playbooks reutilizables para acortar MTTR.

En cuanto a despliegue, SIEMonster ofrece desde instalaciones “single” hasta arquitecturas distribuidas con múltiples nodos/componentes y opciones en cloud (AWS Marketplace). La documentación y materiales de V5 resaltan un rediseño modular para despliegues rápidos, auto-escalabilidad y personalización por MSSP/empresas.

En síntesis, SIEMonster combina proyectos OSS (por ejemplo, Wazuh/OSSEC, Suricata, MISP, OpenCTI, Cortex, TheHive, Kafka/NiFi, OpenSearch) bajo un marco unificado de colección-correlación-visualización-respuesta, con arquitectura abierta y automatización integrada para SOCs que requieren alto rendimiento, escalabilidad y coste contenido.

2.1.3.5 Otros

Graylog:

Es una plataforma open source de gestión de logs y SIEM que permite recolectar, indexar y analizar grandes volúmenes de datos en tiempo real. Basada en arquitecturas distribuidas (con MongoDB y OpenSearch/Elasticsearch), ofrece funcionalidades de normalización, correlación de eventos, dashboards personalizables y alertamiento, siendo utilizada ampliamente en entornos de monitoreo y respuesta a incidentes de seguridad.

OpenSearch como SIEM:

Es un motor de búsqueda y análisis open source derivado de Elasticsearch, desarrollado por Amazon y la comunidad. Su arquitectura distribuida permite almacenar, consultar y visualizar grandes volúmenes de datos, y se integra con herramientas de seguridad (como Wazuh o SIEMonster) para el procesamiento de logs, métricas y trazas, constituyendo el núcleo de indexación en muchas soluciones SIEM modernas.

Prelude:

Es un SIEM híbrido open source enfocado en la correlación de eventos de seguridad provenientes de diversas fuentes (HIDS, NIDS, firewalls, aplicaciones). Diseñado bajo estándares como IDMEF (Intrusion Detection Message Exchange Format), permite integración flexible, correlación avanzada de alertas y escalabilidad, siendo utilizado tanto en entornos de investigación como en operaciones de ciberseguridad empresariales.

2.2 MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es una base de conocimientos accesible globalmente que documenta las tácticas, técnicas y procedimientos (TTP) utilizados por adversarios en ciberseguridad. Este marco se desarrolla a partir de observaciones del mundo real y se utiliza ampliamente para diseñar modelos de amenazas y fortalecer las estrategias de ciberseguridad de las organizaciones (MITRE Corporation, s.f.-b).

La estructura del MITRE ATT&CK se presenta como una matriz que incluye 14 categorías de tácticas, cada una de las cuales representa un objetivo técnico específico del atacante. Estas tácticas abarcan desde el reconocimiento inicial hasta la exfiltración de datos y el impacto en los sistemas de las víctimas. Además, cada táctica se desglosa en técnicas específicas y subtécnicas que describen en detalle los métodos utilizados por los atacantes (MITRE Corporation, s.f.-a).

Este marco es fundamental en la ciberseguridad, ya que ofrece un lenguaje común que facilita la colaboración y el intercambio de información entre organizaciones y profesionales. Muchas herramientas de seguridad, como los sistemas de gestión de eventos e información de seguridad (SIEM) y las soluciones de detección y respuesta extendida (XDR), incorporan MITRE ATT&CK para mejorar su capacidad de detección y respuesta ante amenazas (MITRE Corporation, s.f.-b).

MITRE ATT&CK está estructurado en una matriz que organiza las tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios en ciberataques.

Además, la matriz organiza tácticas (objetivos del atacante) en columnas y técnicas (cómo se logran esos objetivos) en filas; su creación se remonta al experimento de Fort Meade (2013), y hoy abarca dominios Enterprise, Mobile e ICS, con relaciones hacia CVE y CAPEC para análisis más rico.

La estructura se puede desglosar de la siguiente manera:

a) **Tácticas:** Estas son las metas de alto nivel que los adversarios intentan lograr durante un ataque. Las tácticas están organizadas en columnas en la matriz y representan las fases del ataque, como la inicialización, la ejecución, la persistencia, la escalada de privilegios, la exfiltración de datos, entre otras.

b) **Técnicas:** Cada táctica se descompone en técnicas específicas que describen cómo los adversarios logran sus objetivos. Las técnicas están organizadas en filas y proporcionan descripciones detalladas de los métodos utilizados por los atacantes.
c) **Subtécnicas:** Algunas técnicas pueden tener subtécnicas que ofrecen un nivel adicional de detalle sobre cómo se implementan las técnicas en situaciones específicas.
d) **Dominios tecnológicos:** MITRE ATT&CK abarca tres dominios principales:
    - Enterprise: Incluye técnicas aplicables a entornos de TI tradicionales, como sistemas operativos de escritorio y servidores.
    - Mobile: Se centra en las técnicas que afectan a dispositivos móviles.
    - Industrial Control Systems (ICS): Se refiere a las técnicas que impactan en sistemas de control industrial.
e) Grupos de amenazas: MITRE ATT&CK también clasifica los grupos de amenazas (APT) que utilizan estas tácticas y técnicas, proporcionando información sobre sus motivaciones, objetivos y comportamientos.
f) Mitigaciones y detección: Cada técnica en la matriz incluye recomendaciones sobre cómo mitigar el riesgo y detectar la actividad maliciosa asociada.

2.2.1 Dominios tecnológicos

El marco MITRE ATT&CK se estructura a partir de matrices que organizan tácticas y técnicas de adversarios en función de diferentes contextos tecnológicos. Dichos contextos se denominan dominios y representan entornos donde las amenazas pueden desarrollarse con particularidades propias. Los dominios principales son tres: Enterprise, Mobile e Industrial Control Systems (ICS), cada uno con características, técnicas y fuentes de evidencia específicas. Esta organización permite a los equipos de seguridad y a los Centros de Operaciones de Seguridad (SOC) orientar sus capacidades de detección y respuesta de manera más precisa (MITRE Corporation, s.f.-a).

Enterprise

El dominio Enterprise comprende los ambientes tradicionales y modernos de tecnologías de la información. Incluye plataformas como Windows, Linux y macOS, así como Active Directory, servicios en la nube (AWS, Azure, GCP), aplicaciones SaaS y entornos de

contenedores. La matriz cubre tácticas que van desde el Reconocimiento y el Desarrollo de Recursos hasta el Impacto, incorporando además lo que antes era el marco PRE-ATT&CK. Entre las técnicas más relevantes se encuentran el Brute Force (T1110), el uso de Command and Scripting Interpreter (T1059) y el abuso de Valid Accounts (T1078). La aplicación práctica de este dominio es particularmente significativa en los SOC corporativos, ya que es el que ofrece mayor cobertura de incidentes y fuentes de datos como registros de seguridad de Windows, Sysmon, EDR, servicios de autenticación en la nube, firewalls e IDS/IPS. (MITRE Corporation, s.f.-a).

Mobile

El dominio Mobile se centra en los sistemas operativos móviles Android e iOS, considerando tanto la capa de aplicaciones como el sistema operativo y las comunicaciones asociadas. Este dominio contempla tácticas y técnicas adaptadas al ecosistema móvil, entre las cuales destacan la entrega de aplicaciones maliciosas fuera de las tiendas oficiales (T1476), la captura de entradas de usuario como contraseñas o gestos (T1418) y el uso de puertos comúnmente permitidos para evadir detecciones (T1437). Para su monitoreo, resultan relevantes las fuentes de datos provenientes de plataformas de gestión de dispositivos móviles (MDM/MAM), soluciones EDR específicas, registros de pasarelas VPN o Wi-Fi, y servicios de seguridad en la nube como CASB. Aunque su adopción suele ser menor en entornos corporativos centrados en TI tradicional, este dominio cobra importancia en organizaciones con modelos de Bring Your Own Device (BYOD) o con flotas móviles corporativas (MITRE Corporation, s.f.-a).

Industrial Control Systems (ICS)

El dominio Industrial Control Systems (ICS) responde a las necesidades de entornos de tecnología operacional (OT), tales como sistemas SCADA, DCS, PLC, interfaces hombre-máquina (HMI) e historiadores. Su matriz incluye tácticas similares a las del dominio Enterprise, pero adaptadas a las particularidades del ámbito industrial, con énfasis en técnicas que buscan manipular la lógica de control, interrumpir la comunicación con dispositivos de campo o evadir mecanismos de seguridad industrial. Ejemplos de técnicas incluyen la modificación de tareas en controladores (T0809), el bloqueo de mensajes de comando (T0814) o la explotación de vulnerabilidades en protocolos industriales para evadir detecciones (T0803). En este ámbito, las fuentes de evidencia provienen de registros de

sistemas de ingeniería, firewalls industriales, IDS para OT y capturas de tráfico en redes industriales. A diferencia de los entornos corporativos, aquí la respuesta debe priorizar la continuidad operacional y la seguridad funcional, lo que hace de este dominio un componente crítico para sectores como energía, manufactura o transporte (MITRE Corporation, s.f.-a).

2.2.2 Tácticas

En Enterprise se reconocen 14 tácticas; además, en ICS se añaden tácticas específicas del entorno operacional (por ejemplo, Impair Process Control y Inhibit Response Function). A continuación, una síntesis técnica (objetivo y lógica operativa) de las tácticas:

1) **Reconnaissance.** Búsqueda y recolección de información sobre el entorno objetivo (por ejemplo, sitios abiertos, huella de la víctima) para planear el ataque. Agrupa las actividades y técnicas que los adversarios emplean para recopilar información acerca de un objetivo antes de iniciar una intrusión operativa; esto incluye búsquedas en internet, escaneos de red, enumeración de personal y recopilación de anotaciones públicas o internas que faciliten el diseño del ataque. (MITRE Corporation, s.f.-a).
2) **Resource Development.** Preparación de capacidades, infraestructura o artefactos (por ejemplo, dominios, herramientas) antes de operar contra la víctima. Engloba la preparación por parte del atacante de las capacidades necesarias para llevar a cabo operaciones maliciosas, tales como la adquisición de infraestructura (servidores, dominios), la creación o compra de cuentas, y el desarrollo o adquisición de malware y herramientas. En la práctica de defensa, la detección de esta táctica puede apoyarse en monitoreo de dominios registrados recientemente, detección de conexiones a servicios de hosting anómalos y análisis de reputación de artefactos binarios; estos indicadores ayudan a anticipar campañas antes de que alcancen una fase de acceso inicial. (MITRE Corporation, s.f.-a).
3) **Initial Access.** Obtención del primer punto de apoyo en el sistema o red objetivo (frecuentemente vía phishing, explotación o credenciales). En otras palabras, se refiere a las técnicas mediante las cuales un adversario consigue entrar por primera vez en el entorno objetivo, por ejemplo, mediante phishing con archivos adjuntos, explotación de aplicaciones expuestas, uso de credenciales robadas o acceso a través de proveedores de terceros. (MITRE Corporation, s.f.-a).

4) **Execution.** Ejecución de código malicioso tras el acceso (CLI, GUI o binarios activados por el usuario). Comprende las técnicas que permiten la ejecución de código o comandos dentro del entorno comprometido (por ejemplo, ejecución de macros, uso de intérpretes de comandos (PowerShell, Bash) o ejecución de binarios maliciosos). (MITRE Corporation, s.f.-a).
5) **Persistence.** Mantenimiento del acceso pese a contramedidas (secuestro de código legítimo, autostart, etc.). Es decir, agrupa las técnicas que permiten a un adversario mantener acceso a un entorno tras un reinicio, pérdida de conexión o cambio de credenciales; ejemplos típicos son la creación de cuentas locales, servicios o tareas programadas que re-lanzan código malicioso. (MITRE Corporation, s.f.-a).
6) **Privilege Escalation.** Elevación de privilegios explotando vulnerabilidades o configuraciones para ampliar control. Cubre las técnicas utilizadas para obtener niveles mayores de acceso (convertirse en administrador), como explotación de vulnerabilidades locales, abuso de servicios con privilegios o manipulación de tokens. (MITRE Corporation, s.f.-a).
7) **Defense Evasion.** Evasión de defensas y borrado de rastros para evitar detección y continuidad operativa. Describe las técnicas que adversarios usan para evitar la detección o interferencia por mecanismos de seguridad, tales como ofuscación de código, borrado de rastros, modificación de timestamps o desactivación de soluciones de protección. Por ejemplo, en un SIEM esto se manifiesta mediante ausencia o anomalías en logs esperados (por ejemplo, vacíos de telemetría), cambios en la configuración de soluciones de seguridad, y patrones de ejecución que intentan evadir firmas; detectar evasión exige correlación entre pérdida de visibilidad y actividad sospechosa en otros vectores. (MITRE Corporation, s.f.-a).
8) **Credential Access.** El acceso a credenciales agrupa los métodos empleados para obtener datos de autenticación, como nombres de usuario y contraseñas. Esto puede lograrse mediante técnicas como la captura de pulsaciones de teclado o la extracción directa de credenciales almacenadas. Una vez obtenidas, estas credenciales permiten a los atacantes infiltrarse en los sistemas de forma encubierta, reduciendo las posibilidades de ser detectados y facilitando la creación de nuevas cuentas con las que avanzar en sus objetivos maliciosos (MITRE Corporation, s.f.-a).

9) **Discovery.** Reconocimiento interno tras el acceso para perfilar servicios, datos y recursos de red. Agrupa técnicas que los atacantes emplean para explorar la red y sistemas internos una vez dentro del entorno objetivo, como el listado de recursos compartidos, enumeración de cuentas y servicios, o reconocimiento de topología de red. Fuentes claves para detectar descubrimiento incluyen logs de consultas SMB/NFS, comandos de descubrimiento registrados por EDR/Sysmon, registros de escaneo interno y actividad de consultas a Active Directory; identificar ráfagas de descubrimiento ayuda a priorizar contención antes de movimientos laterales (MITRE Corporation, s.f.-a).
10) **Lateral Movement.** Desplazamiento entre cuentas/equipos comprometidos (aprovechando confianza interna). Se refiere a las técnicas que permiten a un adversario trasladarse desde el punto de compromiso inicial hacia otros sistemas dentro de la red, mediante herramientas remotas (RDP, WinRM, SSH), explotación de servicios o reutilización de credenciales (MITRE Corporation, s.f.-a). En el contexto de un SIEM, la detección de movimiento lateral suele apoyarse en correlación de eventos de autenticación entre hosts, detección de sesiones remotas inusuales, y telemetría de EDR que muestre ejecución remota; la identificación rápida de patrones de movimiento reduce la superficie de impacto.
11) **Collection.** Recolección de información (por ejemplo, desde medios removibles) previa a la exfiltración. Agrupa técnicas por las cuales un adversario recolecta datos de interés dentro del ambiente comprometido, como archivos relevantes, capturas de pantalla o extracción de datos de bases. Los artefactos de colección suelen dejar rastros en accesos a ficheros, lecturas masivas en bases de datos, actividad de procesos asociados y transferencias temporales a ubicaciones intermedias; correlacionar eventos de acceso a datos sensibles con contexto de usuario y procesos facilita la detección de exfiltración inminente (MITRE Corporation, s.f.-a).
12) **Command and Control (C2).** Comprende los métodos mediante los cuales los atacantes mantienen comunicación con los sistemas que han logrado comprometer dentro de la red objetivo. Para pasar desapercibidos, estos suelen enmascarar su actividad imitando el tráfico legítimo de la red. Las formas de establecer este canal de comunicación son variadas, y su nivel de ocultamiento dependerá tanto de la arquitectura de la red como de los mecanismos de defensa que tenga implementados la organización afectada. (MITRE Corporation, s.f.-a).

13) **Exfiltration.** Extracción de datos (a menudo comprimidos/ofuscados para evadir controles). Es decir, se describe las técnicas usadas para extraer datos del entorno objetivo hacia ubicaciones controladas por el atacante; puede realizarse por canales directos (SFTP, HTTPS) o por métodos encubiertos (steganografía, fragmentación por múltiples canales). (MITRE Corporation, s.f.-a). En un SIEM, por ejemplo, señales de exfiltración incluyen transferencias inusuales de volumen hacia destinos externos, uso atípico de servicios legítimos para movimiento de datos, y correlaciones entre accesos a datos sensibles y conexiones salientes; implementar alertas basadas en perfilamiento de tráfico y detección de anomalías de volumen ayuda a identificar exfiltración en curso.
14) **Impact.** Degradación de la confidencialidad, integridad o disponibilidad (por ejemplo, destrucción o cifrado de datos). En otras palabras, agrupa las técnicas mediante las cuales un adversario busca degradar, destruir o negar la integridad y disponibilidad de sistemas y datos, incluyendo cifrado masivo (ransomware), sabotaje de sistemas de control o eliminación de registros de auditoría. En entornos empresariales y OT, las evidencias incluyen modificaciones masivas de archivos, ejecuciones de rutinas de cifrado, cambios en configuraciones críticas y señales de interrupción del servicio (MITRE Corporation, s.f.-a).

2.2.3 Técnicas

Las técnicas son los métodos concretos que implementa el adversario para alcanzar cada táctica; organizan procedimientos detallados (procedures) y se mapean a plataformas (Windows, Linux, macOS, nube, contenedores, etc.). En Enterprise, el marco recoge del orden de centenares de técnicas y sub-técnicas, según Al-Sada et al. (2024), 14 tácticas, 193 técnicas, 401 sub-técnicas y 3 897 relaciones, lo que evidencia la complejidad del espacio y la necesidad de correlación con otras fuentes (CVE, CAPEC, NIST) y con telemetría SIEM.

Identificadores (ID) en MITRE ATT&CK

Dentro del marco MITRE ATT&CK, cada táctica, técnica y sub-técnica está asociada a un identificador único (ID) que facilita su referencia, documentación y uso en investigaciones de ciberseguridad. Estos IDs siguen una nomenclatura estándar que inicia con la letra T (de technique), seguida de una secuencia numérica. En el caso de las sub-técnicas, se añade un

sufijo decimal que las vincula directamente con la técnica principal. Por ejemplo, el ID T1110 corresponde a la técnica Brute Force, mientras que T1110.001 hace referencia a la sub-técnica Password Guessing.

La clasificación de los IDs responde a tres niveles jerárquicos dentro del marco ATT&CK. En primer lugar, las tácticas se conciben como las fases u objetivos estratégicos de un adversario durante el ciclo de ataque, y cada táctica agrupa múltiples técnicas asociadas. En segundo lugar, las técnicas describen cómo los adversarios logran cada objetivo táctico, contando cada una con un ID específico. Finalmente, las sub-técnicas ofrecen un nivel adicional de granularidad, describiendo variantes particulares de una técnica y compartiendo la misma raíz de identificador numérico. Esta estructura jerárquica permite a los analistas de seguridad, a los SOC y a los investigadores mantener un lenguaje común y estandarizado para la detección, mitigación y documentación de amenazas (MITRE Corporation, s.f.-a).

Por consiguiente, los IDs de ATT&CK cumplen una función crítica tanto en la práctica operativa como en la investigación académica. Su uso permite la trazabilidad en reportes de incidentes, la correlación de reglas en sistemas de gestión de eventos de seguridad y la alineación con controles normativos y estándares internacionales. Asimismo, facilitan la interoperabilidad entre herramientas de seguridad, bases de conocimiento y comunidades de intercambio de inteligencia de amenazas, consolidando su valor como un sistema de referencia universal en ciberseguridad (MITRE Corporation, s.f.-a).

A continuación, se presenta las principales técnicas del marco.

Tabla 5

Descripción de las principales técnicas del Marco Mitre Att&ck

Técnica	ID	Táctica	Descripción corta
Active Scanning	T1595	Reconnaissance	Escaneo activo de puertos y servicios para mapear la superficie de ataque.
Search Open-Source Information (OSINT)	T1593	Reconnaissance	Recolección de información pública (redes, dominios, repositorios) sobre objetivos.
Acquire Infrastructure	T1583	Resource Development	Adquisición de dominios, servidores o servicios de hosting para operaciones maliciosas.
Develop Capabilities	T1587	Resource Development	Creación o personalización de malware y herramientas.
Phishing	T1566	Initial Access	Envío de correos/mensajes con enlaces o adjuntos maliciosos para obtener acceso o credenciales.
Exploit Public-Facing Application	T1190	Initial Access	Explotación de vulnerabilidades en aplicaciones o servicios expuestos al público.
Valid Accounts	T1078	Initial Access	Uso de cuentas válidas (robadas o compradas) para acceder a sistemas.
Command and Scripting Interpreter	T1059	Execution	Uso de intérpretes (PowerShell, Bash, cmd) para ejecutar comandos o scripts.
User Execution	T1204	Execution	Ejecución que requiere la acción del usuario (macros, ejecución manual de binarios).
Boot or Logon Autostart Execution	T1547	Persistence	Configuraciones que permiten ejecutar código en el arranque o inicio de sesión.
Create or Modify System Process	T1543	Persistence	Creación o modificación de servicios/procesos del sistema para mantener persistencia.
Exploitation for Privilege Escalation	T1068	Privilege Escalation	Aprovechamiento de vulnerabilidades locales para obtener mayores privilegios.

Técnica	ID	Táctica	Descripción corta
Abuse Elevation Control Mechanism	T1548	Privilege Escalation	Abuso de mecanismos de elevación (por ejemplo, bypass de UAC).
Obfuscated Files or Information	T1027	Defense Evasion	Ofuscación o empaquetado de código/artefactos para dificultar el análisis.
Indicator Removal on Host	T1070	Defense Evasion	Eliminación o alteración de logs y artefactos que evidencien la intrusión.
Disable or Modify Tools	T1562	Defense Evasion	Desactivación o manipulación de soluciones de seguridad para evitar detección.
Credential Dumping	T1003	Credential Access	Extracción de hashes, contraseñas u otros credenciales desde memoria o ficheros del sistema.
Brute Force	T1110	Credential Access	Intentos reiterados de adivinar credenciales (incluye password spraying).
Account Discovery	T1087	Discovery	Enumeración de cuentas, grupos y permisos dentro del dominio/AD.
Network Service Scanning	T1046	Discovery	Descubrimiento de servicios y topología de red interna mediante escaneos.
Remote Services	T1021	Lateral Movement	Abuso de servicios remotos (RDP, SSH, WinRM) para moverse entre hosts.
Exploitation of Remote Services	T1210	Lateral Movement	Explotación de servicios remotos para acceder y moverse lateralmente.
Data from Local System	T1005	Collection	Acceso y agregación de archivos y datos locales de interés.
Screen Capture	T1113	Collection	Captura de pantallas para obtener información visual sensible.
Application Layer Protocol	T1071	Command and Control	Uso de protocolos de aplicación (HTTP/S, SMTP, etc.) para comunicaciones C2.
Exfiltration Over C2 Channel	T1041	Exfiltration	Transferencia de datos a través de canales de comando y control existentes.
Exfiltration Over Web Service	T1567	Exfiltration	Subida de datos a servicios web o almacenamiento en la nube para exfiltrar información.

Técnica	ID	Táctica	Descripción corta
Data Encrypted for Impact	T1486	Impact	Cifrado masivo de datos (ransomware) para degradar disponibilidad o exigir rescate.
Inhibit System Recovery	T1490	Impact	Acciones que impiden la recuperación del sistema. Por ejemplo, eliminación de backups.
Endpoint Denial of Service	T1499	Impact	Acciones destinadas a degradar o negar la disponibilidad de servicios en endpoints.

Nota. Adaptado de Techniques – Enterprise, por MITRE Corporation, s.f.-c (https://attack.mitre.org/techniques/enterprise/).

Esta estructura nos permitirá modelar, evaluar y responder a las amenazas de manera más efectiva, utilizando un enfoque basado en el conocimiento acumulado de ataques reales.

Figura 20

Matriz Enterprise MITRE ATT&CK



Nota. Adaptado de MITRE ATT&CK® enterprise matrix, por MITRE Corporation, s.f.-c (https://attack.mitre.org/matrices/enterprise/).

Por último, podemos señalar que se han establecido los fundamentos teóricos esenciales para la implementación de una solución SIEM basada en herramientas de código abierto y alineada con el marco MITRE ATT&CK.

A lo largo del capítulo se han abordado conceptos clave como el funcionamiento general de un sistema SIEM, su arquitectura modular propuesta, la funcionalidad del ELK Stack como plataforma tecnológica y la utilidad estratégica del marco MITRE ATT&CK en la identificación y análisis de amenazas reales.

Cada componente teórico presentado no solo describe una tecnología o metodología aislada, sino que ha sido cuidadosamente seleccionado por su aplicabilidad directa en el desarrollo del proyecto.

2.3 METODOLOGÍA DE CAPACITACIÓN

La metodología de capacitación se entiende como el conjunto de principios, enfoques y procedimientos pedagógicos orientados a organizar el proceso de enseñanza–aprendizaje con el fin de desarrollar conocimientos, habilidades y actitudes en los participantes (Noe, 2020). Su función principal es establecer las estrategias didácticas más adecuadas según los objetivos de formación, el perfil de los aprendices y el contexto en el cual se imparte la instrucción. Una metodología de capacitación no se limita únicamente a transmitir información, sino que también contempla mecanismos de evaluación y retroalimentación que permitan verificar la efectividad del proceso (Blanchard & Thacker, 2019). En este marco, se van a identificar diferentes métodos de capacitación que han sido ampliamente documentados y que se aplican de manera flexible según la naturaleza de los contenidos y las necesidades formativas. A continuación, se describen los principales métodos que se relacionan con esta metodología:

2.3.1 Método expositivo (lección magistral)

El método expositivo es una de las metodologías tradicionales más utilizadas en la enseñanza. Se centra en la transmisión organizada y secuenciada del conocimiento desde el docente hacia el estudiante, quien asume un rol principalmente receptivo (Bligh, 2000). Este método resulta eficiente para presentar grandes volúmenes de información en un tiempo limitado y garantizar la uniformidad de contenidos impartidos. Sin embargo, suele criticarse que fomenta un aprendizaje memorístico y pasivo si no se acompaña de mecanismos de

verificación de la comprensión (Universidad de Navarra, s. f.). La evaluación en este enfoque se realiza comúnmente a través de pruebas objetivas, cuestionarios escritos o resúmenes de los contenidos expuestos.

2.3.2 Otros métodos

2.3.2.1 Método demostrativo

El método demostrativo consiste en que el formador muestra la forma correcta de ejecutar una tarea o procedimiento, mientras los estudiantes observan y posteriormente reproducen la acción bajo supervisión. Este enfoque es adecuado para la enseñanza de destrezas prácticas, ya que facilita la imitación y el perfeccionamiento a través de la práctica guiada (Noe, 2020). El proceso de aprendizaje se consolida mediante la observación, la repetición y la retroalimentación inmediata. La evaluación se realiza generalmente a través de listas de cotejo o rúbricas que verifican la correcta ejecución de los pasos establecidos.

2.3.2.2 Aprendizaje activo

El aprendizaje activo se basa en la participación activa del estudiante en el proceso formativo, incorporando actividades que promuevan la reflexión, la discusión y la resolución de problemas. A diferencia de la enseñanza pasiva, este método busca una mayor implicación cognitiva del estudiante en la construcción del conocimiento (Prince, 2004). Se fundamenta en la idea de que el aprendizaje significativo ocurre cuando el estudiante interactúa activamente con los contenidos. La evaluación suele contemplar cuestionarios de aplicación inmediata, breves productos escritos y participación en actividades en clase.

2.3.2.3 Estudio de caso

El estudio de caso constituye un método de enseñanza que emplea narrativas o situaciones realistas para que los estudiantes analicen, discutan y propongan soluciones fundamentadas. Esta estrategia fomenta el pensamiento crítico y el desarrollo de la capacidad analítica, ya que los casos suelen presentar información incompleta y múltiples vías de resolución (Herreid, 1994). Su fortaleza radica en la contextualización del aprendizaje en situaciones concretas. La evaluación en este método se lleva a cabo mediante informes escritos,

discusiones grupales y presentaciones, valoradas con rúbricas que consideran la coherencia, la argumentación y la pertinencia de las conclusiones.

2.3.2.4 Aprendizaje Basado en Problemas (ABP)

El aprendizaje basado en problemas (ABP) organiza la enseñanza en torno a un problema abierto que los estudiantes deben analizar y resolver con la guía de un facilitador. Esta metodología fomenta la autonomía, el trabajo colaborativo y la integración de conocimientos, al tiempo que promueve el desarrollo de competencias de investigación y pensamiento crítico (Hmelo-Silver, 2004). A diferencia del estudio de caso, en el ABP el estudiante debe indagar activamente para construir las bases conceptuales necesarias para resolver el problema. La evaluación se centra en la calidad de las soluciones propuestas, los procesos de indagación y la reflexión sobre los aprendizajes alcanzados.

2.3.2.5 Simulaciones y role-play

Las simulaciones y el role-play constituyen métodos que reproducen situaciones reales o ficticias en entornos controlados para que los estudiantes puedan experimentar procesos de toma de decisiones y aplicación de conocimientos en un contexto seguro. Estos enfoques permiten desarrollar habilidades prácticas y sociales, a la vez que generan retroalimentación inmediata sobre el desempeño (Sitzmann, 2011). Las evaluaciones suelen realizarse a través de rúbricas de desempeño, análisis posterior de la actividad (after-action review) y métricas de precisión o efectividad.

2.3.2.6 Capacitación en el puesto (OJT), coaching y mentoring

La capacitación en el puesto de trabajo (On-the-Job Training, OJT), junto con estrategias de coaching y mentoring, son métodos que trasladan el aprendizaje directamente al entorno laboral. Bajo la supervisión de un experto, los participantes observan, replican y perfeccionan sus habilidades en situaciones reales de trabajo, recibiendo retroalimentación inmediata (Noe, 2020). Estos métodos favorecen la transferencia directa del aprendizaje a la práctica profesional. La evaluación suele basarse en la evidencia de desempeño, indicadores de calidad y tiempos de resolución en las tareas ejecutadas.

2.3.2.7 E-learning y microlearning

El e-learning se refiere al proceso de enseñanza-aprendizaje mediado por plataformas digitales, que permite flexibilidad en el acceso a contenidos y la autogestión del ritmo de estudio. Por su parte, el microlearning consiste en fragmentar los contenidos en unidades breves y específicas que facilitan la asimilación progresiva del conocimiento (Monib et al., 2024). Ambos métodos han demostrado ser efectivos en la formación continua y en contextos donde se requiere aprendizaje rápido y puntual. La evaluación se realiza comúnmente mediante cuestionarios automatizados, seguimiento del progreso en plataformas y micro-tareas aplicadas.

2.3.2.8 Blended learning (formación mixta)

El blended learning o aprendizaje combinado integra sesiones presenciales o virtuales con actividades asincrónicas en línea. Su propósito es aprovechar las ventajas de cada modalidad, optimizando los tiempos de formación y adaptando los contenidos a distintos estilos de aprendizaje (Graham, 2013). Este método se ha consolidado como una práctica frecuente en educación superior y formación corporativa. La evaluación incluye pruebas escritas, actividades en línea y la integración de evidencias prácticas desarrolladas en ambos entornos.

2.3.2.9 Aula invertida (flipped classroom)

El aula invertida plantea un modelo en el cual los estudiantes acceden a los contenidos teóricos de forma previa a la clase, mediante videos, lecturas u otros recursos, y el tiempo en aula se dedica a la aplicación de los conocimientos a través de actividades prácticas y colaborativas (Bishop & Verleger, 2013). Este método incrementa la participación activa durante las sesiones sincrónicas y favorece el aprendizaje significativo. La evaluación se realiza mediante cuestionarios previos de verificación y la valoración de las actividades desarrolladas en clase.

3 CAPÍTULO 3: DESARROLLO DEL PROYECTO

3.1 Implementación de la Solución

En esta sección se describe la implementación basada en el diseño y desarrollo de la solución propuesta, tomando como referencia el árbol de problemas, causas y consecuencias presentado en el Capítulo 1, el cual permitió identificar las deficiencias en el monitoreo de registros.

A partir de este análisis, se elaboró una matriz de requerimientos, en el cual se definieron las necesidades del sistema en función de los objetivos específicos del proyecto. Cada requerimiento fue descrito y asociado a dichos objetivos, asegurando la trazabilidad entre el problema identificado y la solución planteada.

A continuación, se presenta la Matriz de requerimientos según objetivos específicos.

Matriz de requerimientos según objetivos específicos

Tabla 6

Matriz de Requerimientos

N°	Objetivos Específicos	Requerimiento	Descripción
OE1	Identificar los componentes críticos de infraestructura tecnológica de la empresa para el diseño del sistema SIEM mediante un listado técnico y una evaluación comparativa de al menos tres soluciones Open Source.	- Requerimiento de listado de fuentes criticas tecnológicas - Requerimiento de evaluación tecnológica	- Identificar Fuentes Críticas de la infraestructura tecnológica actual de la organización. - Evaluar 4 soluciones SIEM Open Source para seleccionar la solución más adecuada.
OE2	Diseñar un diagrama de arquitectura SIEM basada en una herramienta Open Source aprobado por la gerencia de sistemas, asegurando que permita la centralización y gestión de eventos de seguridad.	- Requerimiento de diseño técnico - Requerimiento de buenas prácticas alineado a un framework de seguridad	- Elaborar un diagrama de arquitectura SIEM Open Source para definir componentes, flujos de datos. - Incluir controles detectivos alineados al marco MITRE ATT&CK, como Credential Access e Impact, dentro del diseño de la arquitectura SIEM para el monitoreo y detección de eventos de seguridad.

N°	Objetivos Específicos	Requerimiento	Descripción
OE3	Desplegar un SIEM operativo que registre los logs de dos firewalls y dos servidores críticos, garantizando una disponibilidad ≥ 99.5 %.	- Requerimiento funcional: recolección y análisis - Requerimiento técnico: integración de fuentes de datos	- Asegurar la recolección y procesamiento de eventos mediante Beats (Winlogbeat) y Logstash, utilizando pipelines de logs para su captura y normalización hacia el Elasticsearch. - Integrar de 2 firewalls Fortinet y 2 servidores (AD y NAS) en el SIEM, asegurando la ingesta y disponibilidad de logs normalizados
OE4	Desarrollar tres casos de uso basados en el marco MITRE ATT&CK para la detección de eventos de seguridad en un SIEM Open Source.	- Requerimiento de correlación: reglas personalizadas para detectar eventos maliciosos - Requerimiento visual para el análisis y visualización de eventos correlacionados.	- Implementar 3 reglas de correlación alineadas al marco MITRE ATT&CK, para la identificación de técnicas asociadas a amenazas reales, como parte de un control de detección en el SIEM. **Para el caso de uso 1:** Detección de Ataque de fuerza bruta SSL VPN Táctica: Credential Access Técnica (ID / Nombre): T1110.003 - Brute Force: Password Spraying

N°	Objetivos Específicos	Requerimiento	Descripción
			Para el caso de uso 2: Detección de Múltiples intentos fallidos de inicio de sesión por parte de administradores Táctica: Credential Access Técnica (ID / Nombre): T1110.001 - Brute Force: Password Guessing **Para el caso de uso 3:** Detección de Cuenta eliminada o modificada de un grupo administrador Táctica: Impact Técnica (ID / Nombre): T1531 – Account Access Removal
OE5	Capacitar al personal de soporte TI en el uso del SIEM y del marco MITRE ATT&CK para la gestión de eventos de seguridad, logrando una mejora del 40 % en las competencias adquiridas en los participantes.	- Requerimiento de formación	- Capacitar al equipo técnico mediante sesiones teóricas, con registro de asistencia y evaluación de aprendizaje.

3.1.1 Identificación de Componentes Tecnológicos

3.1.1.1 Identificación de Fuentes Críticas

En esta etapa se realizó el levantamiento y análisis de los activos tecnológicos que conforman la infraestructura crítica de la organización, con el objetivo de identificar las principales fuentes de eventos y registros necesarias para la implementación de la solución SIEM Open Source. Este proceso permitió reconocer dispositivos y sistemas relevantes dentro de la operación de la empresa, tales como firewalls, servidores, dispositivos de red y sistemas de almacenamiento, los cuales participan directamente en la gestión, protección y disponibilidad de la información.

Dicho análisis incluyó parámetros como el modelo y versión de cada dispositivo, su función específica dentro de la arquitectura tecnológica, la capacidad de procesamiento o velocidad, ubicación física dentro de la organización y la asignación de responsabilidades o propietarios. Toda esta información es esencial para evaluar las capacidades técnicas actuales y definir los requerimientos de integración con la plataforma SIEM Open Source elegida.

Como resultado de este levantamiento, se identificaron siete activos considerados críticos para la operación de la empresa, los cuales se presentan en el cuadro general de infraestructura crítica. Sin embargo, no todos los dispositivos identificados forman parte del alcance de integración del presente proyecto. Esto se debe a que algunos equipos corresponden a infraestructura administrada por proveedores externos, por lo que cualquier intervención técnica o configuración sobre dichos activos se encuentra fuera del alcance operativo de la organización.

En este contexto, la implementación del SIEM consideró únicamente aquellos activos que son administrados directamente por la empresa y que, además, representan fuentes relevantes de eventos de seguridad. Bajo este criterio, se seleccionaron dos firewalls perimetrales, debido a que gestionan las conexiones VPN utilizadas para la comunicación con los distintos clientes y usuarios internos de la empresa, constituyendo un punto clave para el monitoreo de accesos, tráfico y eventos de seguridad.

Asimismo, se consideró el servidor Active Directory, debido a que la organización aplica políticas de dominio orientadas al cumplimiento de requerimientos establecidos por sus clientes, tales como restricciones de instalación y ejecución de aplicaciones, así como controles asociados a la seguridad de la información y gestión de usuarios. Del mismo modo, se incluyó el servidor NAS QNAP, ya que almacena información crítica para la operación de la empresa, incluyendo audios de llamadas y documentación relacionada con la gestión administrativa y operativa. La conservación de esta información responde a requerimientos contractuales y procesos de auditoría establecidos por los clientes, quienes exigen mantener la disponibilidad y resguardo de los datos durante periodos prolongados.

Por otro lado, las plataformas CRM utilizadas por la organización no fueron consideradas dentro de este proceso de identificación, debido a que son software administradas por terceros o proporcionadas directamente por los clientes. En consecuencia, cualquier monitoreo o intervención sobre dichas plataformas se encuentra fuera del alcance técnico y administrativo del presente proyecto.

A continuación, se presenta el cuadro general de los componentes de la infraestructura crítica identificados en el data center de la empresa.

Tabla 7

Cuadro de componentes de Infraestructura Critica

SERVICIOS DE INFRAESTRUCTURA					
Componente	**Modelo/Versión**	**Función**	**Velocidad**	**Ubicación Física**	**Propietario**
FortiGate	FG200E [redacted]	Firewall perimetral [redacted]	-	Rack2 Data center	La Empresa
FortiGate	FG200D [redacted]	Firewall perimetral [redacted]	-	Rack2 Data center	La Empresa
QNAP NAS	Modelo: [redacted] Version: [redacted] RAM: [redacted] CPU: [redacted]	Almacenamiento [redacted]	RAID1: [redacted] TB / RAID2: [redacted] TB	Rack1 Data center	La Empresa
Servidor AD	Windows Server [redacted] CPU [redacted]	Almacenamiento [redacted]	Ram: [redacted]GB / Disco: [redacted] GB	Rack1 Data center	La Empresa

SERVICIOS DE INFRAESTRUCTURA					
Componente	**Modelo/Versión**	**Función**	**Velocidad**	**Ubicación Física**	**Propietario**
		[redacted]			
Router [redacted] (ISP 1)	Cisco [redacted]	Conectividad Internet	[redacted] Mbps simétrico	Rack2 Data center	Proveedor
Router [redacted] (ISP 2)	Fortinet [redacted]	Conectividad Internet	[redacted] Mbps simétrico	Rack2 Data center	Proveedor
Router [redacted] RPV	Huawei [redacted]	Conectividad a la red [redacted]	[redacted] Mbps	Rack2 Data center	Proveedor

Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

3.1.1.2 Evaluación de soluciones SIEM Open Source

Se evalúa diversas herramientas Open Source disponibles para cada componente del sistema SIEM como recolección de logs, procesamiento, almacenamiento, y visualización, a fin de seleccionar aquellas que cumplan con los criterios funcionales de rendimiento y facilidad de integración con la infraestructura tecnológica actual de la organización.

Considerando lo mencionado, para la elección más adecuada de una solución SIEM open source, se consideró un análisis comparativo basado en el estudio de Manzoor et al. (2024), el cual evalúa distintas herramientas mediante una metodología de puntuación centrada en diversas características técnicas y de funcionalidad. En síntesis, Cada característica se valora con base en su nivel de implementación, asignándole una puntuación según la siguiente escala:

0: No implementada

2: Implementación básica

4: Implementación avanzada

Esta metodología permite establecer un criterio uniforme y objetivo al momento de comparar herramientas como Wazuh, OSSEM, SIEMonster y Elastic Stack, considerando aspectos como correlación de eventos, autenticación de usuarios, escalabilidad, soporte de comunidad, entre otros.

A continuación, se presenta la tabla de evaluación que incluye los parámetros y sus puntajes respectivos.

Tabla 8

Evaluación de Soluciones Open Source

N°	Parámetro	Puntuación			
		Wazuh	**OSSIM**	**SIEMonster**	**ELK Stack**
1	EPS	4	2	4	2
2	Reglas de correlación	4	2	4	2
3	Personalización de reglas	4	4	0	4
4	Integridad de los registros	4	2	4	4
5	Conservación de registros	4	2	4	4
6	Autenticación de usuarios	2	2	4	2
7	Control de acceso	4	4	4	4
8	Tolerancia a fallos	4	0	0	4
9	Visualización	4	2	4	4
10	Conformidad	4	0	4	4
11	Fuentes de datos personalizadas	2	2	0	2
12	Escalabilidad	2	0	0	2
13	Exploración de vulnerabilidades	2	2	2	0
14	Inteligencia sobre amenazas	1	1	2	2
15	Comunidad y apoyo	2	1	1	2
16	**Madurez de la solución Open Source**	**2**	**0**	**2**	**4**
17	**Flexibilidad para adaptarse a casos de uso personalizados**	**2**	**0**	**2**	**4**

N°	Parámetro	Puntuación			
		Wazuh	OSSIM	SIEMonster	ELK Stack
18	**Abundancia de recursos de aprendizaje y documentación en línea**	**2**	**0**	**2**	**4**
Puntuación SIEM:		**53**	**26**	**43**	**54**

Nota. Adaptado de Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs, por Manzoor et al., 2024, PLOS ONE, 19(3), e0301183 (https://doi.org/10.1371/journal.pone.0301183). CC BY 4.0.

El estudio original identificó a Wazuh como la solución con mayor puntuación dentro de los criterios evaluados. No obstante, para el presente proyecto se consideró pertinente complementar la evaluación incorporando criterios adicionales relacionados con aspectos de implementación, aprendizaje y adaptabilidad de la solución, debido a su relevancia en entornos donde se requiere flexibilidad operativa y facilidad de adopción de herramientas open source.

La incorporación de estos criterios mantiene el enfoque de evaluación propuesto por Manzoor et al. (2024), complementando el análisis con factores relevantes para el despliegue y gestión de la solución en entornos reales.

Por lo que a continuación, se justifica la elección de los 3 parámetros agregados:

1. **Madurez de la solución Open Source**

ELK Stack (Elasticsearch, Logstash y Kibana) ha sido ampliamente adoptado en entornos empresariales debido a su madurez tecnológica y una comunidad activa que respalda su evolución constante. Su desarrollo es mantenido por Elastic N.V., y complementado por miles de colaboradores en foros, GitHub y comunidades como Stack Overflow. Según Horovits (2023), el ELK Stack es una de las plataformas de gestión de logs más populares a nivel mundial, con millones de descargas de sus componentes y una amplia adopción en entornos empresariales.

En comparación, herramientas como OSSIM y SIEMonster poseen comunidades más pequeñas y menor frecuencia de actualización, lo que puede limitar su evolución tecnológica. Aunque Wazuh también cuenta con una comunidad activa y es una bifurcación de OSSEC (Open Source HIDS SECurity), su madurez como SIEM completo aún está en consolidación.

2. **Flexibilidad para adaptarse a casos de uso personalizados**

El ELK Stack presenta una arquitectura modular que permite la recolección, procesamiento y análisis de datos provenientes de múltiples fuentes, facilitando su adaptación a distintos escenarios de monitoreo de seguridad. En este sentido, según Stoleriu, Puncioiu y Bica (2021), el ELK Stack puede integrarse con diversas herramientas externas, como VirusTotal y la plataforma MISP, permitiendo la correlación y enriquecimiento de información para la detección de amenazas avanzadas basadas en el marco MITRE ATT&CK. Asimismo, el estudio destaca el uso de mecanismos de enriquecimiento de logs, como GeoIP, y la aplicación de algoritmos de aprendizaje automático en Elasticsearch para la detección de anomalías en el tráfico de red. Estos elementos demuestran la capacidad del ELK Stack para adaptarse a diferentes casos de uso mediante la integración y configuración de sus componentes.

En comparación con las demás soluciones evaluadas por Manzoor et al. (2024), el ELK Stack presenta una mayor flexibilidad para integrar y adaptar componentes según las necesidades del entorno de monitoreo. Bajo este enfoque, OSSIM, aunque integrado con herramientas como OpenVAS y Snort, presenta limitaciones para manejar flujos personalizados, mientras que SIEMonster requiere una arquitectura más orientada a integraciones específicas. Y Wazuh se centra principalmente en el monitoreo de hosts y el uso de reglas predefinidas.

3. **Abundancia de recursos de aprendizaje y documentación en línea**

La disponibilidad de documentación y material de formación constituye un factor determinante en la adopción de soluciones open source, especialmente en entornos donde no se dispone de soporte comercial. En este contexto, el ELK Stack destaca ampliamente debido a la gran cantidad de recursos disponibles, incluyendo documentación técnica

oficial, guías paso a paso, ejemplos prácticos, material de capacitación y contenido multimedia, lo que facilita significativamente su implementación, aprendizaje y escalabilidad (Elastic, s.f.-c).

Además, la documentación del Elastic Stack se caracteriza por ofrecer guías estructuradas, referencias técnicas detalladas y buenas prácticas para su despliegue y operación, permitiendo a los usuarios implementar soluciones de análisis y visualización de datos de manera eficiente. Por ejemplo, herramientas como Kibana permiten la creación flexible de dashboards personalizados para la exploración y visualización de datos, lo que incrementa su aplicabilidad en distintos contextos organizacionales (Elastic, s.f.-d).

En contraste, Wazuh presenta una documentación completa pero principalmente orientada a guías de instalación, configuración y casos de uso específicos en ciberseguridad, como monitoreo de endpoints, cumplimiento normativo y detección de amenazas, lo que enfoca su uso hacia escenarios más definidos (Wazuh, s.f.-b).

Si bien esta documentación es sólida, su enfoque puede resultar menos flexible en etapas iniciales de aprendizaje en comparación con el ecosistema más amplio y diverso de recursos disponibles para ELK Stack. En el caso de las otras soluciones como OSSIM y SIEMonster, la documentación disponible es menos centralizada y puede requerir la consulta de múltiples fuentes, lo que podría incrementar la complejidad durante las etapas iniciales de implementación.

En conclusión, la incorporación de criterios subjetivos como los detallados en los puntos 1,2 y 3 han permitido complementar el análisis técnico de las soluciones SIEM open source con factores estratégicos relevantes para entornos reales de implementación. Estos criterios permiten valorar no solo el rendimiento de las herramientas, sino también su escalabilidad, facilidad de adopción y sostenibilidad operativa a largo plazo. A partir de esta evaluación integral, ELK Stack se posiciona como la opción más adecuada para el presente proyecto, al ofrecer un equilibrio entre capacidad técnica, adaptabilidad y soporte comunitario, aspectos fundamentales para asegurar una implementación eficiente y alineado con los objetivos planteados.

3.1.2 Diseño de Arquitectura SIEM (ELK)

3.1.2.1 Esquema General de la solución SIEM propuesta

La presente propuesta plantea la implementación de un sistema de Security Information and Event Management (SIEM) basado en la plataforma open source ELK (Elasticsearch, Logstash y Kibana), definida en la evaluación previa de soluciones. Este SIEM está diseñado para recolectar, procesar y analizar los registros de eventos (Log) generados por dispositivos críticos de la infraestructura de la empresa, cuyo objetivo principal es detectar amenazas y vulnerabilidades en tiempo real, además el proyecto va a utilizar el marco de referencia MITRE ATT&CK como base para el diseño de los casos de uso.

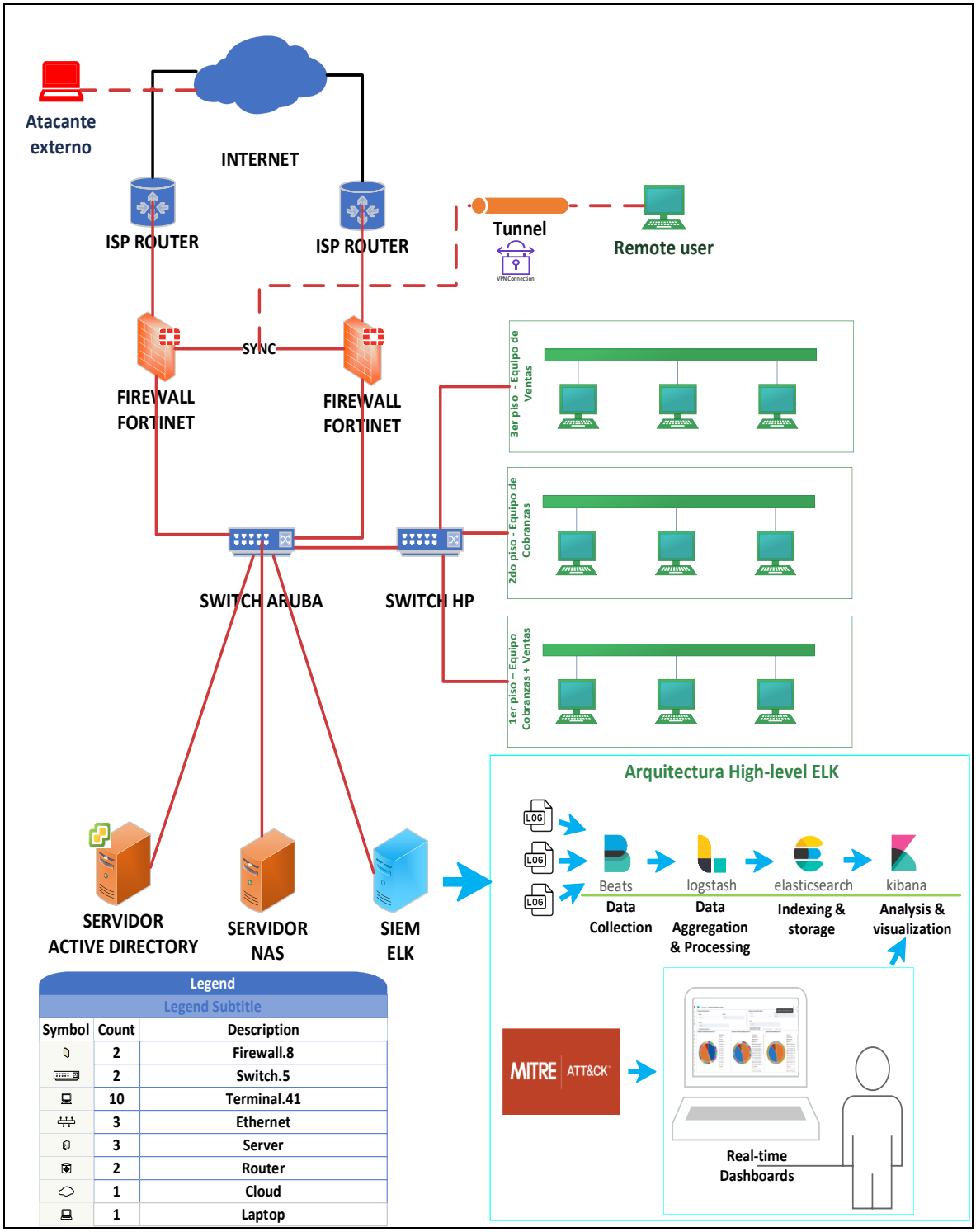
Según la previa identificación de las fuentes críticas, la infraestructura actual de la organización incluye dispositivos clave como dos firewalls Fortinet, configurados en un esquema activo-activo para garantizar un rendimiento y disponibilidad óptimo. Estos firewalls generan registros relacionados con la seguridad perimetral, como intentos de intrusión, conexiones sospechosas y accesos remotos. Además, se incluyen el servidor Active Directory, que aporta registros vinculados a autenticación y gestión de usuarios, y el servidor NAS, que centraliza el almacenamiento y proporciona eventos relacionados con accesos a archivos. Estos equipos serán los principales generadores de logs que se recolectarán mediante el SIEM.

En cuanto al funcionamiento del SIEM, se desplegará una máquina virtual dedicada, donde se instalarán los servicios que conforman ELK Stack. Esta máquina será ubicada en el entorno de la red de servidores de la empresa, permitiendo una integración segura y eficiente con los equipos que generan los registros. El despliegue en un entorno virtualizado facilitará su gestión, escalabilidad y mantenimiento, conservando los recursos controlados y centralizados.

Como se muestra a continuación, la arquitectura está diseñada para asegurar una integración clara entre los dispositivos Firewalls, los servidores internos y la solución SIEM:

Figura 21

Diagrama de la solución propuesta



Nota. Elaborado a partir de Yeminyi (2020) e información extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

3.1.2.2 Arquitectura Lógica

La arquitectura lógica del procesamiento de logs muestra el flujo de información desde los equipos monitoreados hacia el sistema SIEM. Para el presente proyecto, la recolección de logs desde las distintas fuentes se realiza de la siguiente manera:

- Servidores (Active Directory): Para la recolección de eventos en los servidores se utiliza Beats, un agente ligero diseñado específicamente para entornos de servidor. Este componente permite la captura eficiente de eventos relevantes del sistema, tales como autenticaciones de usuarios, bloqueos de cuentas y actividades administrativas. La información recolectada es enviada a la plataforma central de análisis para su procesamiento y correlación.
- Servidor (NAS) y Firewalls Fortinet: Los dispositivos de seguridad perimetral Fortinet están configurados para utilizar el protocolo Syslog, así también como el servidor QNAP, este protocolo tiene como función la transmisión en tiempo real de los registros generados hacia un servidor central. Dichos registros son recibidos por Logstash, una herramienta capaz de procesar, transformar y normalizar los datos provenientes de dispositivos de red y seguridad.

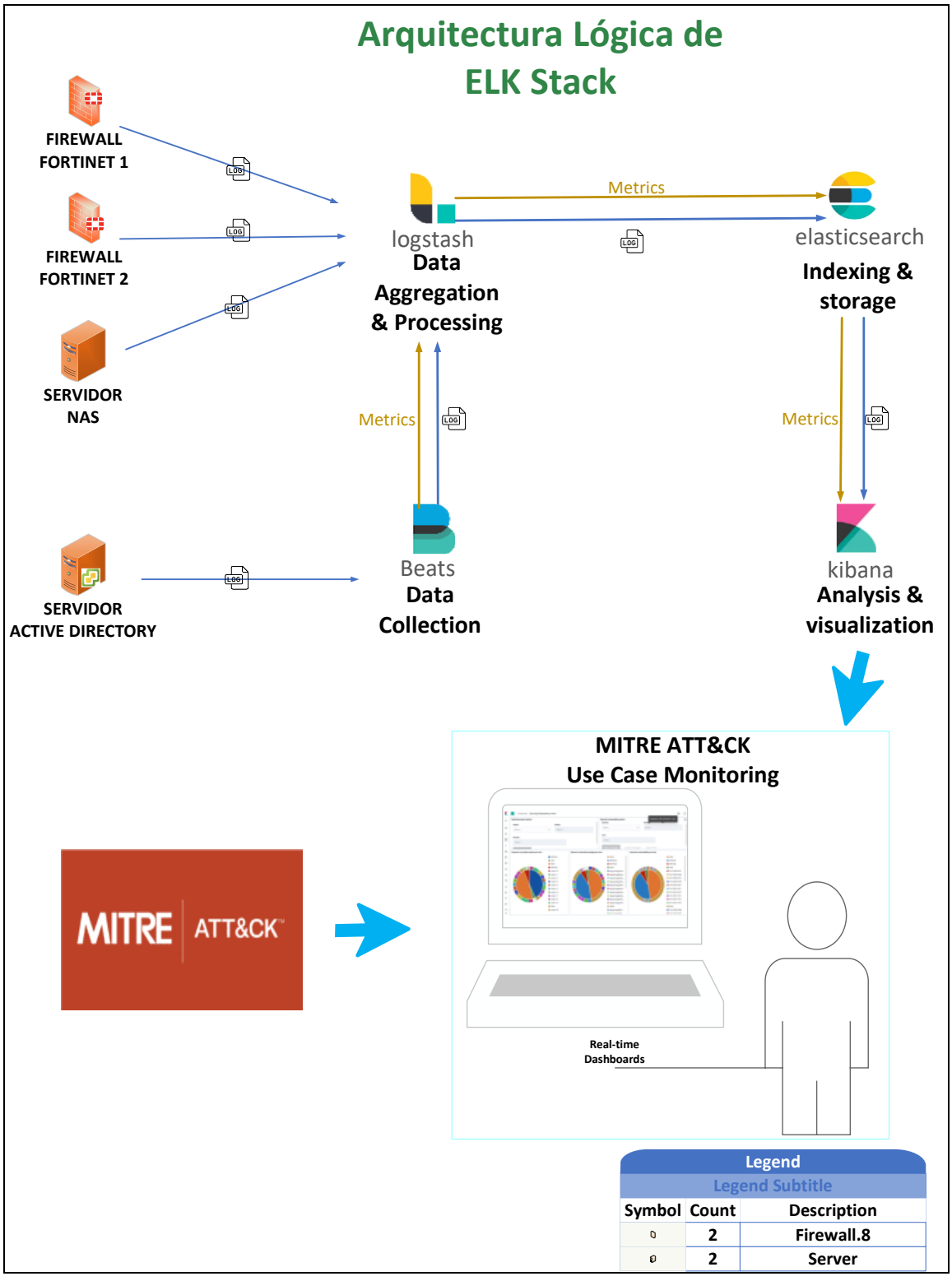
Así, desde todos los dispositivos monitoreados se realiza la recolección de registros y se envían los datos hacia Logstash, componente que se encarga de procesar, filtrar y enriquecer la información antes de su almacenamiento. Posteriormente, los logs son enviados a Elasticsearch, que permite su indexación y facilita búsquedas rápidas y eficientes.

Por último, la interfaz Kibana será utilizada para el análisis visual. A través de esta herramienta, se podrán diseñar visualizaciones que representen los eventos de seguridad según las tácticas y técnicas del marco MITRE ATT&CK, permitiendo al área de sistemas verificar los eventos de seguridad en tiempo real mediante los casos de uso configurados, los cuales se detallarán más adelante.

Conforme a lo expuesto, se presenta la propuesta de la arquitectura lógica ELK Stack:

Figura 22

Arquitectura Lógica ELK Stack



Nota. Elaborado a partir de Ammi (2023), Vazão et al. (2023) y Yeminyi (2020).

Este diseño de arquitectura lógica proyecta el flujo del camino del evento (log), desde las fuentes de origen hasta la visualización final, pasando por los servicios como agentes

Beats, Logstash, Elasticsearch y Kibana; facilitando así la detección de patrones de comportamiento anómalos o posibles ataques.

Asimismo, la arquitectura propuesta está preparada para escalar y adaptarse a nuevas necesidades, permitiendo integrar más fuentes de logs en el futuro, manteniendo la trazabilidad y la centralización de eventos (log).

Finalmente, para esta sección se concluye que el diseño de arquitectura SIEM propuesto representa una solución tecnológica sólida orientada a fortalecer las capacidades de monitoreo y detección de amenazas en tiempo real para la organización. Adicionalmente la incorporación de controles detectivos alineados al marco Mitre Attack, como Credential Access e Impact, dentro del diseño de la arquitectura SIEM, permitirá orientar la construcción de casos de uso y reglas de correlación alineadas a técnicas reales utilizadas por los atacantes, contribuyendo a una mejor capacidad de análisis y respuesta antes incidentes de seguridad.

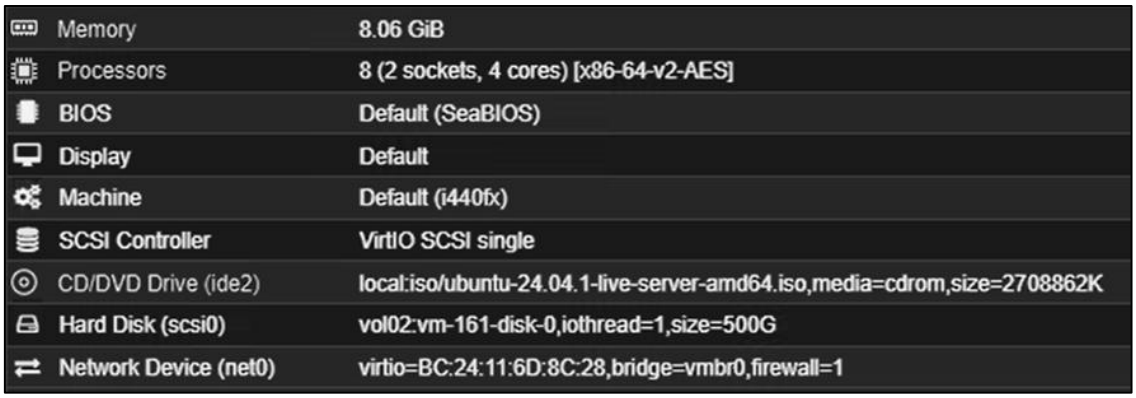
3.1.3 Implementación del sistema SIEM

3.1.3.1 Configuraciones de la Máquina Virtual

Una vez seleccionado el sistema SIEM Open Source a utilizar y definida su respectiva arquitectura, se presentan los recursos necesarios para el despliegue del mismo. Por consiguiente, en la Figura 23 se muestran los parámetros de configuración inicial de la máquina virtual utilizada para su implementación. Se detallan los recursos asignados, como memoria RAM, cantidad de núcleos de CPU, disco duro, adaptador de red y la imagen ISO empleada para la instalación del sistema operativo Ubuntu Server 24.04. Estas configuraciones aseguran un entorno adecuado para el correcto funcionamiento de los servicios del ELK Stack.

Figura 23

Hardware asignado al equipo SIEM ELK Stack



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

3.1.3.2 Despliegue de Servicios de ELK Stack

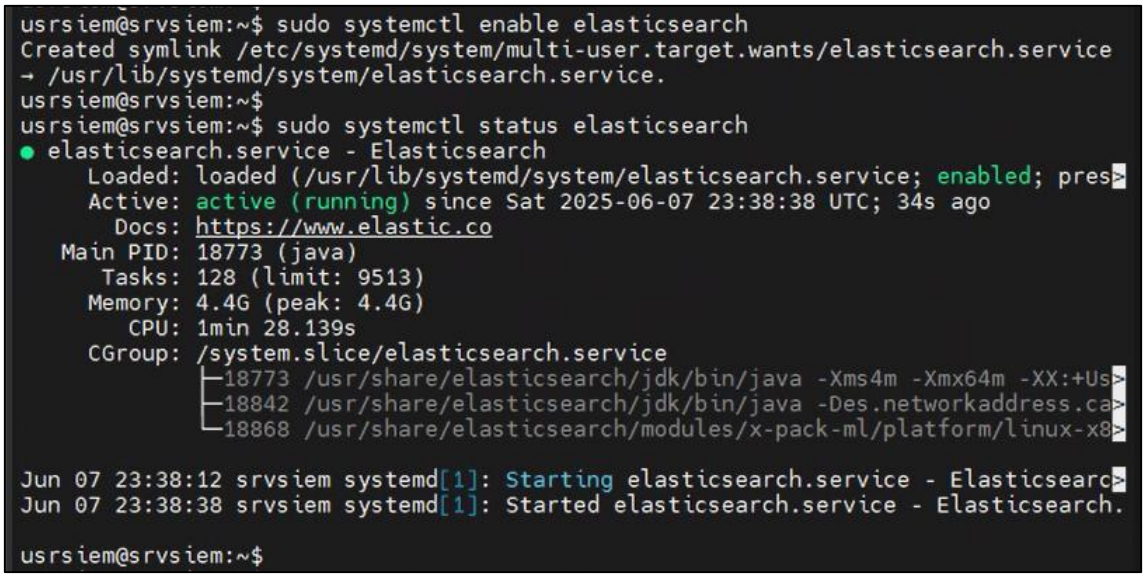
Luego de completarse los recursos para la máquina virtual del SIEM (servidor Ubuntu), seguidamente, se expone la correcta ejecución de los servicios necesarios para la implementación propuesta. Con el propósito de asegurar el correcto despliegue.

Servicio Elasticsearch

Una vez instalado los paquetes del servicio Elasticsearch, en la Figura 24, se visualiza el estado final del servicio, evidenciando que se encuentra activo y funcionando correctamente. Este servicio es fundamental para el almacenamiento y búsqueda de logs dentro del SIEM ELK Stack.

Figura 24

Estatus Elasticsearch



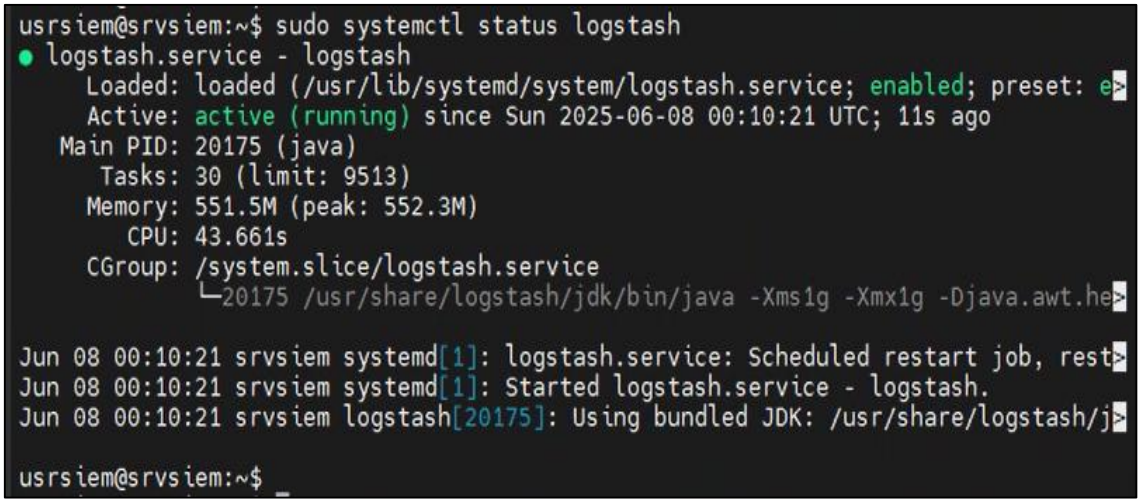
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Servicio Logstash

Una vez finalizado con Elasticsearch, se procedió con la instalación de Logstash. En la Figura 25 se muestra el estado operativo del servicio, evidenciando que se encuentra activo y funcionando correctamente. Este componente cumple la función de recibir, procesar y canalizar los logs hacia Elasticsearch como parte del flujo de procesamiento del SIEM.

Figura 25

Estatus Logstash



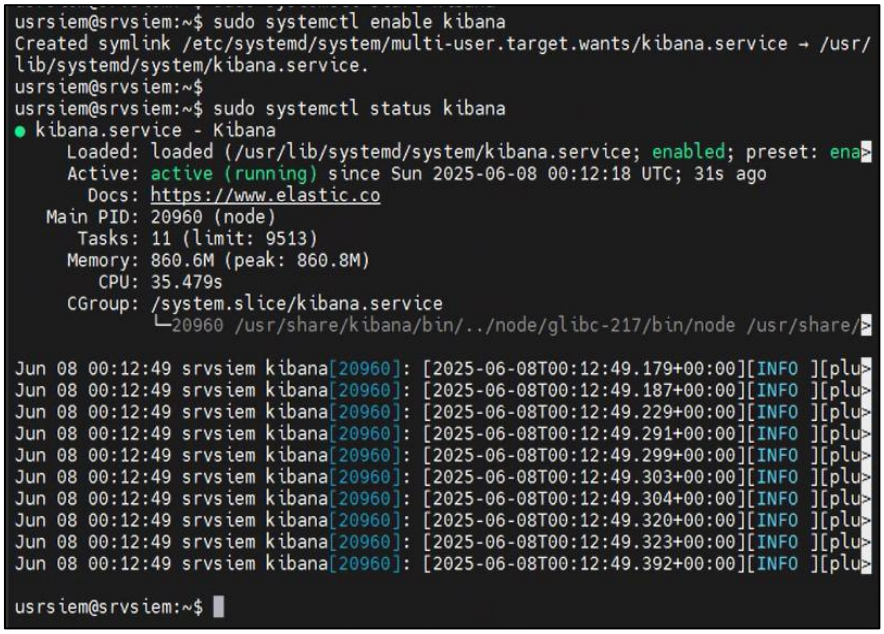
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Servicio Kibana

Luego de finalizar con Logstash, se continuo con la instalación de Kibana. En la Figura 26 se confirma que el servicio se encuentra activo, garantizando el acceso a las visualizaciones e interfaces necesarias para analizar los eventos de seguridad recopilados por los agentes y Logstash. Asimismo, en la Figura 27, se muestra la pantalla de bienvenida del portal principal Elastic, cuya disponibilidad es posible gracias al funcionamiento del servicio Kibana.

Figura 26

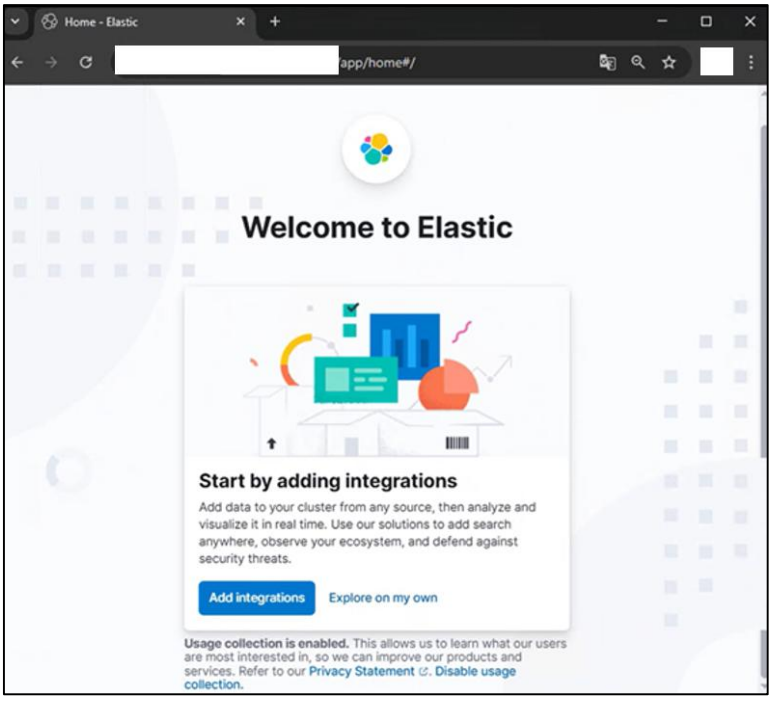
Estatus Kibana



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Figura 27

Dashboard principal Elastic



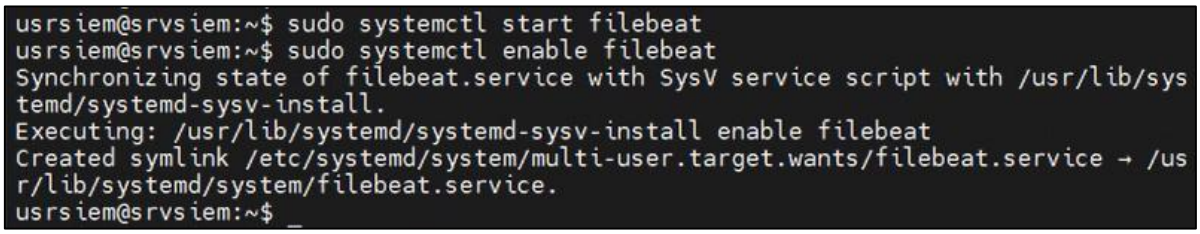
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Servicio Filebeat

Por último, se realizó la instalación de Filebeat. En la Figura 28, se puede verificar que el servicio se encuentra activo y funcionando correctamente. Este componente se encarga de recolectar los logs desde las diferentes fuentes.

Figura 28

Estatus Filebeat



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

3.1.3.3 Integración de Fuentes

Una vez instalado todos los servicios base para el funcionamiento del sistema SIEM ELK Stack, se procedió con la integración de las fuentes, facilitando la centralización y correlación de los registros de eventos en el sistema para un monitoreo más eficiente.

A continuación, se proyecta lista resumida de fuentes:

Tabla 9

Resumen de lista de fuentes

Ítem	Solución	Marca/Modelo	Observación	Propietario
1	Firewall	Fortinet	Firewall 1	La Empresa
2	Firewall	Fortinet	Firewall 2	La Empresa
3	NAS	QNAP	NAS QNAP	La Empresa
4	Servidor AD	HP	Active Directory	La Empresa

Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la recopilación y análisis de la empresa de estudio. Por Recupera, 2025.

En adelante para cada integración se muestra la interfaz de Kibana, herramienta de visualización incluida en el ELK Stack (Elasticsearch, Logstash, Kibana), en la que se evidencia los eventos generados por las fuentes de datos integrados en el SIEM. Cada evento se procesa y almacena de manera estructurada, permitiendo la exploración y filtrado mediante consultas KQL (Kibana Query Language).

Estos registros contienen información clave como el timestamp de la transacción, el tipo de evento, la acción tomada (permitir o denegar), el servicio involucrado (puertos UDP/TCP), las políticas aplicadas y datos de origen/destino de los paquetes. Esta visualización facilita la identificación de patrones anómalos y contribuye al diseño de casos de uso apoyados en el marco MITRE ATT&CK para detectar tácticas, técnicas y procedimientos (TTPs) utilizados por posibles actores maliciosos.

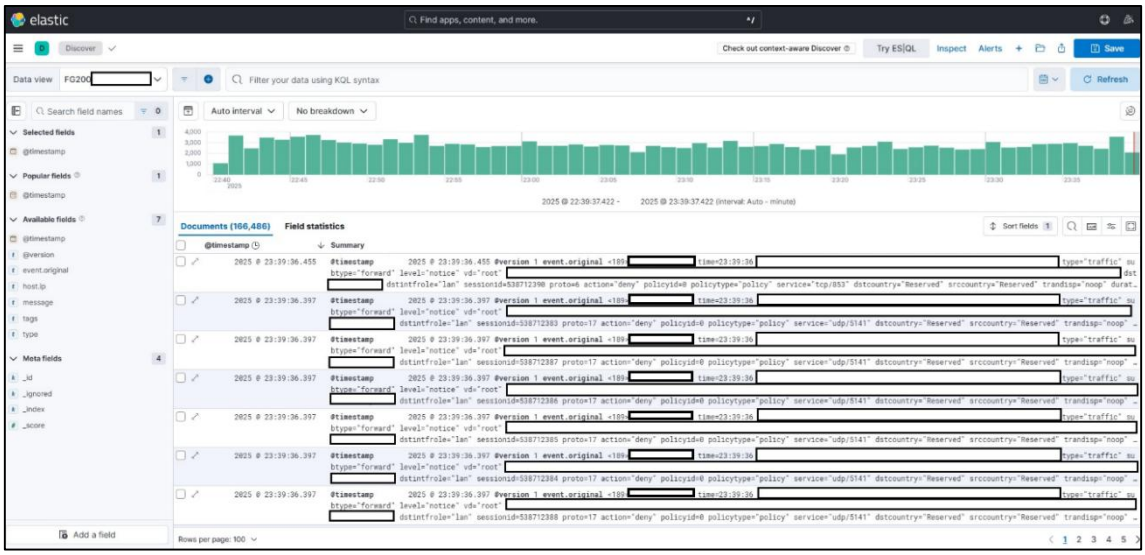
La integración de los datos en Kibana no solo centraliza la gestión de logs, sino que también optimiza el monitoreo en tiempo real y la capacidad de respuesta ante incidentes de seguridad en la infraestructura tecnológica de la empresa.

Integración del Firewall

Tal como se ilustra en la Figura 29, la interfaz de Kibana correspondiente al módulo Discover, donde se visualizan los registros de eventos (logs) captados desde los firewalls Fortigate. La vista refleja una muestra de eventos almacenados en Elasticsearch, los cuales se presentan en formato estructurado con campos como @timestamp, event.original, action, policyid, service, srcountry, entre otros. Estos registros permiten el análisis detallado de la actividad de red y la aplicación de políticas de seguridad configuradas en el dispositivo perimetral.

Figura 29

Integración de Firewall Fortigate



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Es importante señalar que, con fines de confidencialidad, se han anonimizado datos sensibles, tales como direcciones IP internas y otros identificadores, garantizando de esta manera la protección de la información local sin afectar la comprensión técnica del proceso. Asimismo, la gráfica superior de barras temporales (barras en color verde) muestra la distribución de eventos por intervalo de tiempo, lo cual facilita identificar patrones de tráfico y posibles anomalías en periodos específicos.

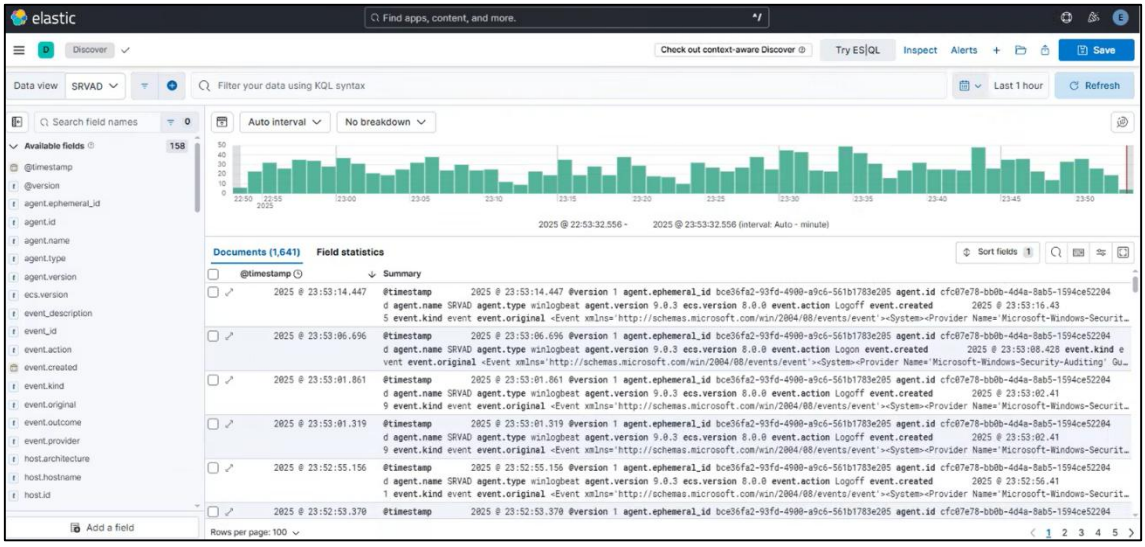
Integración del Active Directory

Por otro lado, para el proceso de implementación del SIEM, también se estableció la integración con el servidor Active Directory (AD) basado en Windows Server 2019, con el propósito de centralizar los eventos de seguridad generados en la infraestructura de autenticación y administración de usuarios.

La Figura 30, se presenta la interfaz de Kibana, donde se visualizan los logs recolectados mediante el agente Winlogbeat, encargado de enviar al SIEM los registros del visor de eventos de Windows.

Figura 30

Integración de Active Directory



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

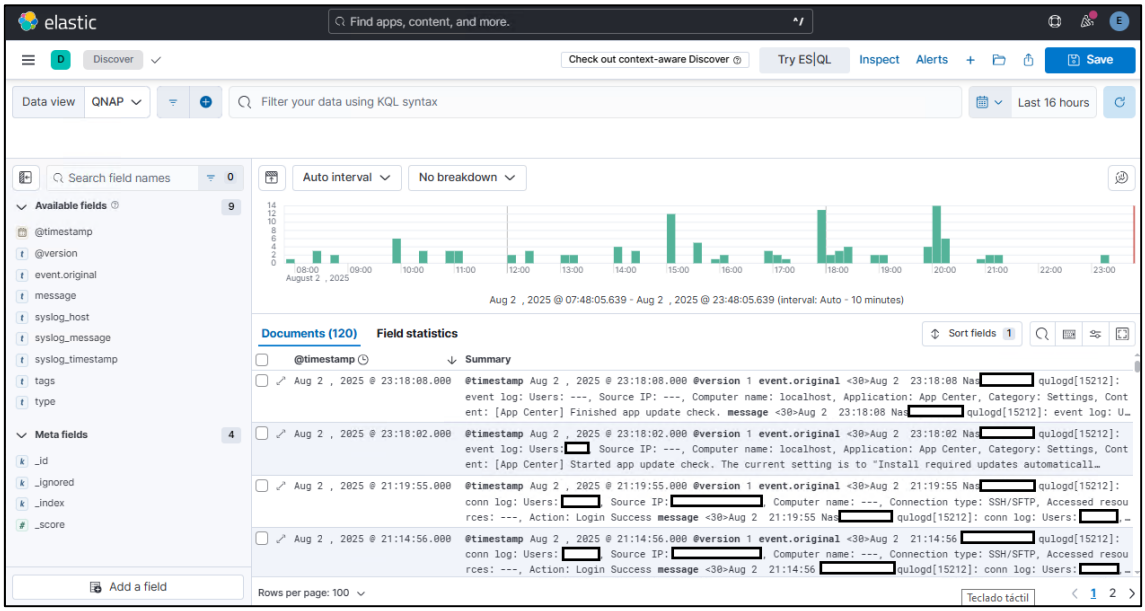
Estos eventos incluyen información relevante como la fecha y hora de ocurrencia (timestamp), el nombre del agente, el tipo y categoría del evento (inicio/cierre de sesión, creación/modificación de cuentas, entre otros) y el proveedor de origen (en este caso, Microsoft-Windows-Security-Auditing). Esta recopilación permite al equipo de ciberseguridad realizar un análisis detallado sobre las actividades críticas en el AD, identificar intentos de acceso no autorizados, movimientos laterales y otros indicadores de compromiso (IoC) asociados a las tácticas y técnicas descritas en el marco MITRE ATT&CK.

Integración del NAS

Asi también se ha establecido la integración con el Nas QNAP. En la Figura siguiente se presenta la visualización de logs provenientes de un dispositivo de almacenamiento en red (QNAP) a través de la interfaz de Kibana. La captura muestra el módulo Discover, en el cual se listan los eventos registrados por el sistema de archivos, incluyendo parámetros como @timestamp, event.original, syslog_message, syslog_host y categorías asociadas al funcionamiento de aplicaciones internas del NAS, tales como App Center, conexiones SSH/SFTP y procesos de autenticación de usuarios.

Figura 31

Integración de QNAP



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

La gráfica superior permite observar la distribución temporal de los eventos, facilitando la detección de picos de actividad en horarios determinados. Esta funcionalidad contribuye a identificar comportamientos inusuales en el acceso al sistema de almacenamiento, los cuales podrían representar intentos de acceso no autorizado o fallas en servicios críticos. Asimismo, se han anonimizado datos sensibles, tales como direcciones IP y otros identificadores.

Variables de indicadores de logro del OE3

Para el logro correcto del objetivo específico señalado se han establecido las siguientes variables, las cuales serán usadas más adelante en la ejecución del plan de pruebas.

Variable 1: Disponibilidad del Sistema SIEM

$$Disponibilidad = \frac{Tiempo\ Operativo}{Tiempo\ Total} \times 100$$

- Datos de medición:

Tiempo Operativo: Número de horas (o minutos) en que el SIEM estuvo funcionando sin interrupciones dentro del período de medición.

Tiempo Total: Período total de medición (por ejemplo, un mes = 30 días × 24 horas = 720 horas).

Ejemplo:

Supongamos que durante un mes (30 días), se monitoreó el funcionamiento del SIEM. El tiempo total del mes equivale a 720 horas. Se registraron dos interrupciones no planificadas:

- Una de 2 horas por mantenimiento.
- Otra de 1 hora por un fallo en el servidor.

Cálculo:

- Tiempo Operativo = 720 h - (2 h + 1 h) = 717 horas
- Tiempo Total = 720 horas

$$Disponibilidad = \frac{717}{720} \times 100 = 99.58\%$$

Esto significaría que el SIEM estuvo disponible el 99.58% del tiempo.

Variable 2: Capacidad de procesamiento de eventos del SIEM

La capacidad de procesamiento de eventos del SIEM se calcula mediante el promedio de EPS, una métrica de rendimiento que determina la capacidad de respuesta y la carga de trabajo de un sistema SIEM. Esta métrica representa la tasa promedio de eventos procesados por el sistema en un intervalo de tiempo específico. Su cálculo se realiza mediante la siguiente expresión:

$$EPS\ Promedio = \frac{Total\ de\ Eventos\ Procesados}{Total\ de\ Segundos}$$

- Datos de medición:

Total de Eventos Procesados: La cantidad total de eventos o logs recopilados y procesados por el SIEM en un periodo de tiempo determinado

Total de Segundos: El tiempo total, en segundos, correspondiente al periodo en el que se recopilaron los eventos.

Ejemplo:

Si consideramos que en un periodo de 1 hora (3600 segundos), el SIEM procesó un total de 5,400,000 eventos provenientes de los dos firewalls y dos servidores integrados.

Cálculo:

- Total de eventos procesados = 5,400,000
- Total de segundos = 3600 s

$$EPS\ Promedio = \frac{5{,}400{,}000}{3600} = 1{,}500\ EPS$$

Este resultado indica que el SIEM soporta un promedio de 1,500 eventos por segundo.

3.1.4 Implementación de Casos de Uso con Mitre Attack

En esta sección se presentan los casos de uso implementados con base en el marco MITRE ATT&CK, los cuales fueron seleccionados considerando la criticidad de los activos tecnológicos involucrados en los procesos clave de la organización. La finalidad de estos casos de uso es establecer mecanismos de detección ante tácticas y técnicas comúnmente empleadas por actores de amenazas, permitiendo una mejor visibilidad de los eventos de seguridad, así como una respuesta oportuna y eficaz frente a posibles incidentes.

De acuerdo con los requerimientos definidos para este objetivo, se establecieron los siguientes tres casos de uso:

Caso de uso 1: Detección de Ataque de fuerza bruta SSL VPN

Caso de uso 2: Detección de Múltiples intentos fallidos de inicio de sesión por parte de administradores

Caso de uso 3: Detección de Cuenta eliminada o modificada de un grupo administrador

En la siguiente tabla se detallan las tácticas de Credential Access e Impact, así como las técnicas asociadas a los casos de uso definidos. Es importante precisar que este cuadro clasifica dichas tácticas y técnicas limitándose la descripción y detección de las mismas. En cuanto a los casos de uso y sus detalles de configuración dentro del SIEM se expondrán en las secciones posteriores.

Tabla 10

Cuadro de Casos de Uso con Mitre Attack

Nombre del caso de Uso	Táctica	Técnica (ID)	Nombre	Descripción	Detección
Detección de ataque de fuerza bruta SSL VPN	Credential Access	T1110.003	Brute Force: Password Spraying	Técnica en la que el atacante prueba una o pocas contraseñas comunes contra muchas cuentas diferentes (en lugar de probar muchas contraseñas contra una sola cuenta). El objetivo es encontrar credenciales válidas evitando desencadenar bloqueos por intentos fallidos en una sola cuenta. Desde la vista del firewall, esto se manifiesta como múltiples fallos de autenticación hacia servicios que atraviesan el perímetro (VPN/SSL, portales web/SSO, acceso remoto), muchas veces originados desde una o pocas direcciones IP o desde una red	Monitorear los registros de autenticación del firewall (SSL-VPN, VPN, RADIUS/LDAP y portal cautivo) para detectar patrones de múltiples intentos fallidos de acceso a distintas cuentas donde se reutiliza la misma contraseña o un pequeño conjunto de contraseñas (comportamiento típico de password spraying). Monitorear indicadores en el firewall como: numerosos ssl-login-fail / vpn auth fail para diferentes usernames desde la misma IP de origen o desde un conjunto reducido de IPs en un intervalo corto; intentos fallidos contra el mismo servicio

				distribuida que busca pasar desapercibido o no llamar la atención.	(VPN o portal SSO), ausencia de bloqueos por intentos repetidos en una sola cuenta.
Detección de múltiples intentos fallidos de inicio de sesión por parte de administradores	Credential Access	T1110.001	Brute Force: Password Guessing	Esta técnica consiste en que un adversario intenta adivinar la contraseña de una cuenta mediante el uso manual o automatizado de múltiples contraseñas comunes o aleatorias. El objetivo es obtener acceso a una cuenta válida dentro del sistema o servicio atacado. A diferencia del "password spraying", donde se usa una misma contraseña sobre muchas cuentas, en el "password guessing" el atacante prueba muchas contraseñas sobre una sola cuenta o sobre un número limitado de ellas, normalmente cuentas con altos privilegios (como administradores o usuarios del sistema). Esta técnica puede aplicarse en diversos entornos y servicios, incluyendo	La detección de esta técnica se centra en identificar múltiples intentos de autenticación fallidos hacia una misma cuenta o conjunto reducido de cuentas dentro de un periodo corto. Es importante analizar los registros de inicio de sesión generados por sistemas operativos, servicios de autenticación (por ejemplo, Active Directory, Kerberos, SSH, RDP, o portales web), así como los logs de seguridad centralizados.

				autenticaciones locales, remotas o basadas en red (como SSH, RDP, SMB, HTTP, LDAP o servicios en la nube). Su éxito depende de la debilidad de las contraseñas y de la ausencia de mecanismos de defensa como bloqueo de cuentas tras varios intentos fallidos, autenticación multifactor (MFA) o políticas robustas de complejidad de contraseñas.	
Detección de Cuenta eliminada o modificada de un grupo administrador	Impact	T1531	Account Access Removal	Actores maliciosos pueden comprometer la disponibilidad de recursos del sistema y de la red obstruyendo el acceso legítimo de los usuarios a sus cuentas. Esta obstrucción se logra mediante la eliminación, bloqueo o manipulación de las credenciales de las cuentas. Además, los atacantes pueden iniciar cierres de sesión o apagados/reinicios del sistema para facilitar el despliegue de alteraciones maliciosas. Dentro de entornos Windows,	**Modificación o eliminación de cuentas:** Supervisar los eventos del sistema (ID 4723, 4724, 4725, 4726) que indiquen cambios o eliminaciones de cuentas.

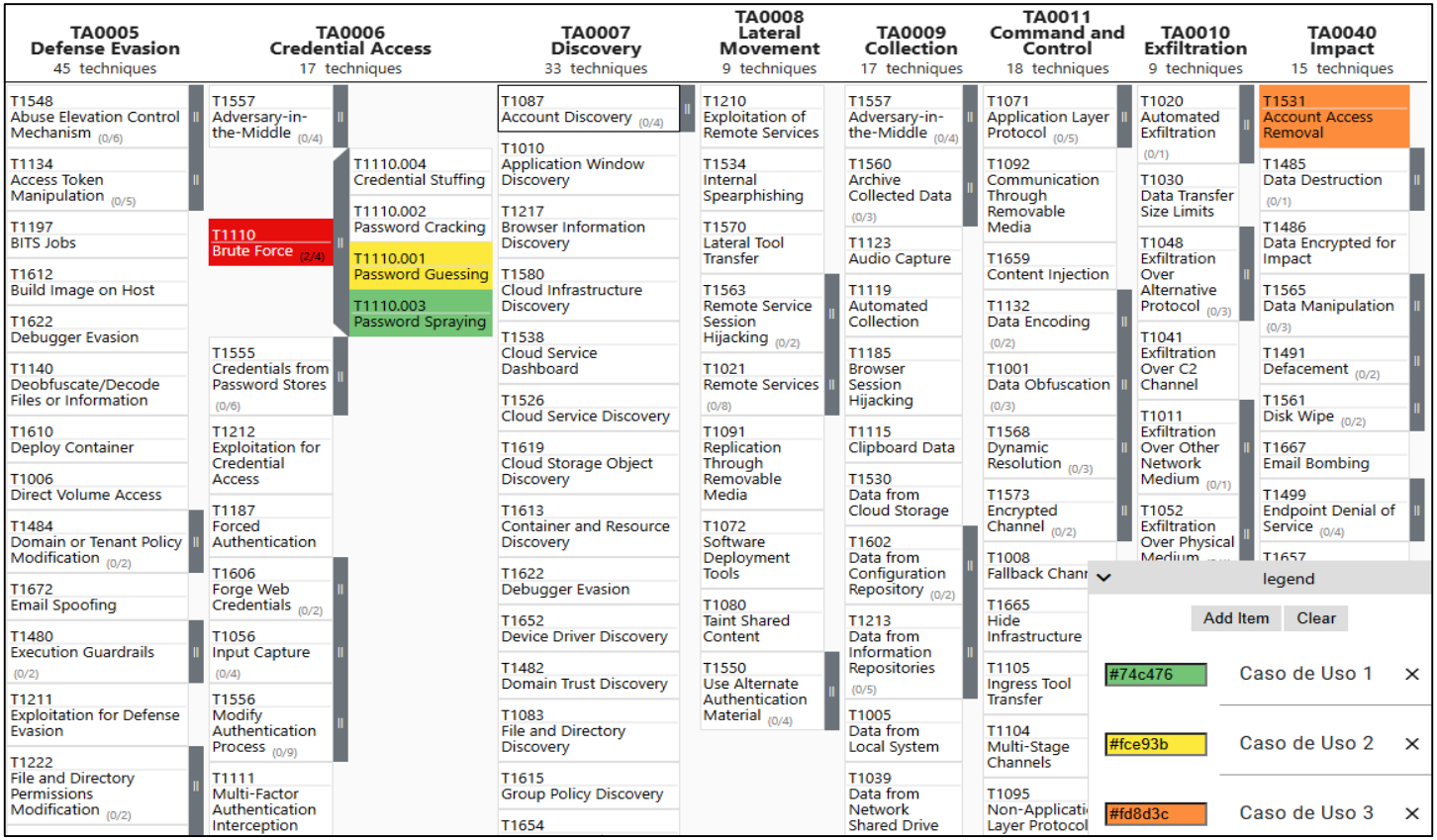
	los adversarios comúnmente emplean utilidades como Net Utility, Set-LocalUser, y cmdlets de PowerShell que incluyen Set-ADAccountPassword y passwd para modificar cuentas de usuario. Adicionalmente, la deshabilitación de cuentas puede realizarse a través de la Directiva de Grupo.	

Nota. Elaborado a partir de Techniques – Enterprise, por MITRE Corporation, s.f.-c (https://attack.mitre.org/techniques/enterprise/).

En la siguiente figura se presenta la Matriz Enterprise MITRE ATT&CK, donde se ubica las tácticas y técnicas asociadas a los casos de uso mencionados.

Figura 32

Mapa de casos de uso en Mitre Att&ck



Nota. Adaptado de ATT&CK Navigator, por MITRE Corporation, s.f.-e (https://mitre-attack.github.io/attack-navigator/).

Previo al desarrollo de los casos de uso, en la siguiente tabla se presenta un resumen de las reglas implementadas en el SIEM, incluyendo las soluciones monitoreadas, las tácticas y técnicas de la matriz MITRE ATT&CK asociadas, y los umbrales definidos para la generación de alertas.

Tabla 11

Resumen de casos de uso y reglas implementadas

Ítem	Solución	Marca	Nombre del caso de uso	Nombre de la regla	Táctica	Técnica	Umbral
1	Firewall	Fortinet	Detección de Ataque de fuerza bruta SSL VPN	UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN UC-REC-FW2-T1110.003-Ataque de Fuerza Bruta SSL VPN	Credential Access	T1110.003	Notificación por cada evento
2	NAS	QNAP	Detección de Múltiples intentos fallidos de inicio de sesión por parte de administradores	UC-QNAP-T1110-BruteForce-Admins	Credential Access	T1110.001	>= 2 eventos en <5min
3	AD	Windows Server	Detección de Cuenta eliminada o modificada de un grupo administrador	WIN-AD-T1531-A-Miembro removido de grupos admin WIN-AD-T1531-B-Cuentas deshabilitadas/eliminada WIN-AD-T1531-C-Cambio/Reset de contraseña (success)	Impact	T1531	Notificación por cada evento

A partir de las tácticas y técnicas identificadas, se realizó la implementación de los casos de uso en el sistema SIEM ELK Stack, definiendo las reglas de detección y criterios de correlación correspondientes, los cuales se describen en la siguiente sección:

3.1.4.1 Caso de uso 1: Detección de ataque de fuerza bruta SSL VPN

Alineación con Mitre Attack:

- Táctica: Credential Access
- Técnica (ID / Nombre): T1110.003 - Brute Force: Password Spraying
- Plataforma: Firewall – Fortinet1

Descripción del Caso de Uso:

Este caso de uso fue implementado para identificar múltiples intentos fallidos de autenticación en el servicio SSL VPN del Firewall 1, mediante una contraseña contra muchas cuentas diferentes. Este comportamiento se relaciona con la técnica T1110.003 – Password Spraying del marco MITRE ATT&CK, la cual describe escenarios donde el objetivo del atacante es encontrar credenciales válidas evitando desencadenar bloqueos por intentos fallidos en una sola cuenta. El propósito de la regla es fortalecer la capacidad de detección del SIEM frente a posibles accesos no autorizados a servicios de acceso remoto.

Configuración de la regla

La regla fue creada en Kibana utilizando registros provenientes del módulo Fortinet y empleando el patrón de índice correspondiente al Firewall 1. Para la detección se empleó una consulta KQL orientada a eventos de error en autenticaciones SSL VPN. Asimismo, se utilizaron campos normalizados bajo ECS (Elastic Common Schema), permitiendo mantener consistencia en el análisis y correlación de eventos dentro del SIEM. La regla fue configurada con severidad High y un umbral basado en múltiples intentos consecutivos de autenticación fallida.

A continuación, se detalla la configuración de la regla:

- Nombre de la regla: UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN
- Descripción: Detectar múltiples intentos de inicio de sesión fallidos hacia el servicio SSL VPN del Firewall 1.
- KQL / Query: subtype:"vpn" AND action:"ssl-exit-error"

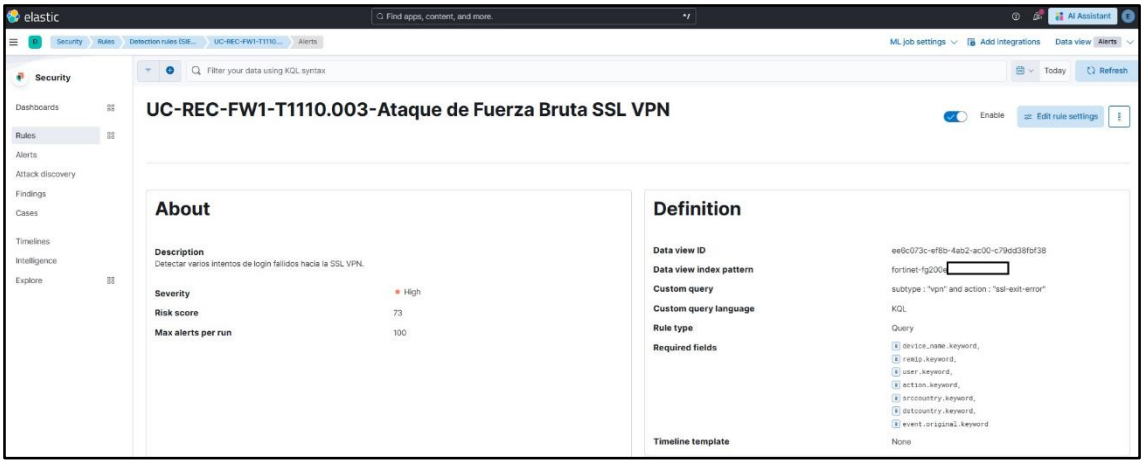
Lógica de detección:

Esta consulta permite identificar eventos del firewall donde se registra un error de salida del túnel SSL debido a intentos de autenticación no exitosos, los cuales son esenciales para detectar patrones compatibles con fuerza bruta del tipo password spraying.

En la Figura 33 se muestra la configuración de la regla implementada en Kibana.

Figura 33

Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Plataforma: Firewall – Fortinet2

Alineación con Mitre Attack:

- Táctica: Credential Access
- Técnica (ID / Nombre): T1110.003 - Brute Force: Password Spraying

Descripción del Caso de Uso:

Se muestra la regla de detección orientada a identificar actividades anómalas asociadas a intentos fallidos de autenticación sobre el servicio SSL VPN del Firewall 2. Este comportamiento se vincula con la técnica T1110.003 – Password Spraying del marco MITRE ATT&CK, en la cual un atacante intenta acceder mediante el uso repetitivo de contraseñas en distintas cuentas. A través de esta regla, se busca detectar oportunamente patrones de acceso sospechosos que puedan representar intentos de intrusión hacia la infraestructura monitoreada.

Configuración de la regla:

La implementación de la regla se realizó en Kibana tomando como fuente los eventos generados por el Firewall 2 relacionados con autenticaciones SSL VPN. Para ello, se empleó una consulta KQL que permite correlacionar múltiples eventos de acceso fallido desde un mismo origen. Adicionalmente, se utilizaron campos normalizados bajo ECS (Elastic Common Schema) para asegurar uniformidad en el procesamiento y análisis de los logs dentro del SIEM. La regla fue configurada con severidad High y un umbral orientado a evaluar intentos consecutivos de autenticación fallida.

A continuación, se describen los parámetros configurados en la regla:

- Nombre de la regla: UC-REC-FW2-T1110.003-Ataque de Fuerza Bruta SSL VPN
- Descripción: Detectar varios intentos de inicio de sesión fallidos hacia la SSL VPN del Firewall 2.
- KQL / Query utilizada: subtype:"vpn" AND action:"ssl-exit-error"

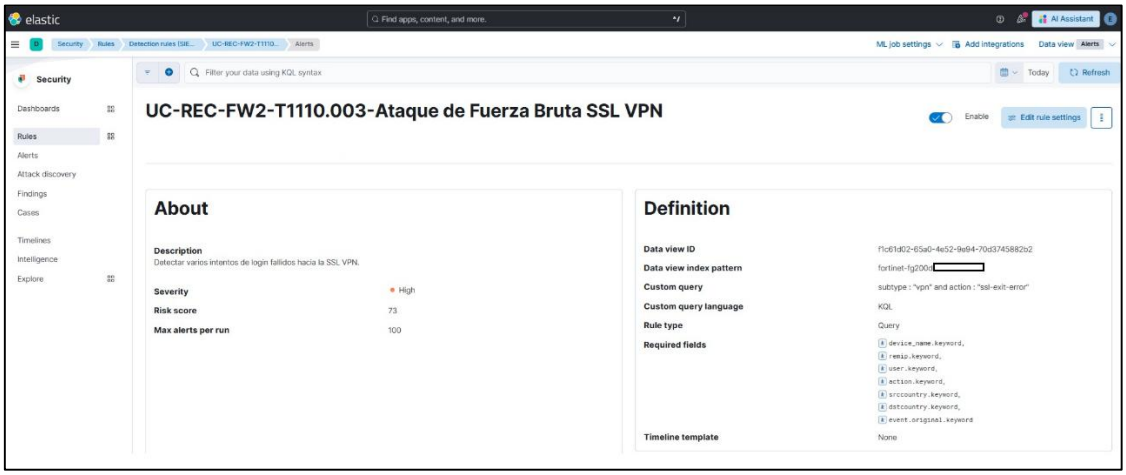
Lógica de detección:

Esta consulta filtra eventos de fallas de autenticación SSL VPN generados por el Firewall 2, permitiendo al SIEM identificar múltiples intentos fallidos provenientes de una misma IP de origen y detectar patrones de fuerza bruta compatibles con ataques de tipo password spraying.

En la Figura 34 se muestra la configuración de la regla implementada en Kibana.

Figura 34

Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 2



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

3.1.4.2 Caso de uso 2: Detección de múltiples intentos fallidos de inicio de sesión por parte de administradores

Alineación con Mitre Attack:

- Táctica: Credential Access
- Técnica (ID / Nombre): T1110.001 - Brute Force: Password Guessing
- Plataforma: NAS-QNAP

Descripción del Caso de Uso:

Para este caso de uso se implementó una regla de detección orientada a identificar múltiples intentos fallidos de inicio de sesión realizados por cuentas administrativas en el NAS QNAP. Este comportamiento es característico de posibles ataques de fuerza bruta, descritos en la técnica T1110.001 – Password Guessing del marco MITRE ATT&CK, donde un atacante intenta adivinar credenciales válidas mediante repetidos intentos de

autenticación contra una misma cuenta privilegiada. El objetivo de la regla es fortalecer la capacidad del SIEM para detectar actividades sospechosas dirigidas a credenciales con altos privilegios.

Configuración de la regla:

Con este fin, se configuró en el SIEM una regla específica sobre los eventos provenientes del módulo de logs del NAS QNAP, tomando como fuente el índice qnap-logs-*. Además, para el análisis y correlación de eventos, se emplearon filtros basados en campos normalizados bajo ECS (Elastic Common Schema), permitiendo mantener consistencia en el procesamiento de logs de autenticación dentro del SIEM. Asimismo, la regla fue configurada con severidad High y un umbral orientado a detectar múltiples intentos consecutivos de autenticación fallida desde una misma dirección IP hacia cuentas administrador.

A continuación, se detalla la configuración de la regla:

- Nombre de la regla: UC-QNAP-T1110-BruteForce-Admins
- Descripción: Detección de múltiples intentos fallidos de inicio de sesión contra cuentas privilegiadas en QNAP.
- KQL / Query: event.module:"qnap" and event.category:"authentication" and event.outcome:"failure" and labels.is_admin:"true"

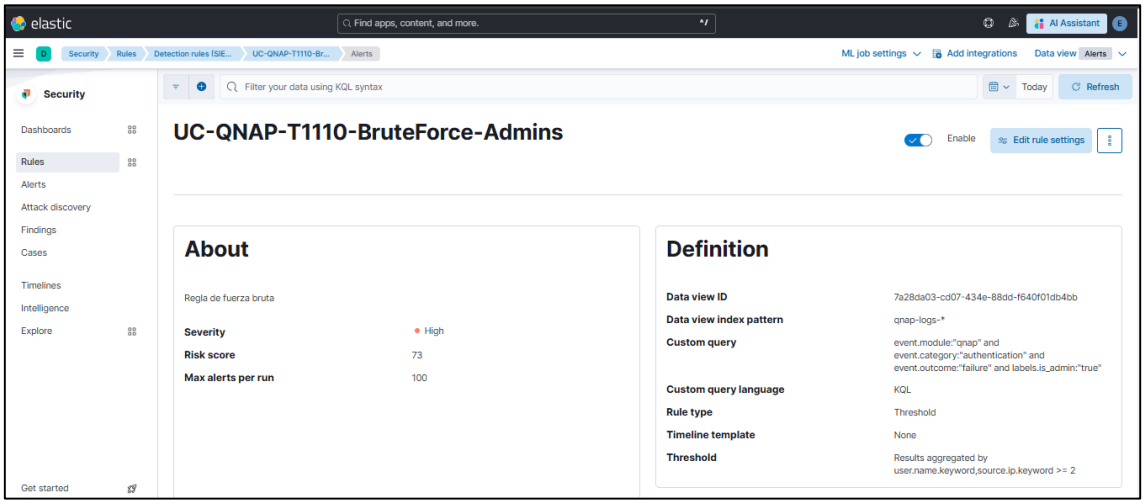
Lógica de detección:

Esta consulta permite filtrar eventos de autenticación fallida asociados a cuentas administrativas del NAS QNAP, asegurando que la alerta se genere únicamente cuando exista riesgo real sobre credenciales de alto privilegio, con el objetivo de detectar patrones asociados a ataques de password guessing.

En la Figura 35, se muestra la configuración de la regla implementada en Kibana.

Figura 35

Caso de Uso de detección de múltiples intentos fallidos de inicio de sesión por parte de administradores



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

3.1.4.3 Caso de uso 3: Detección de Cuenta eliminada o modificada de un grupo administrador

Alineación con Mitre Attack:

- Táctica: Impact
- Técnica (ID / Nombre): T1531 – Account Access Removal
- Plataforma: AD-Windows

Descripción del Caso de Uso:

Para este caso de uso se implementó un mecanismo de supervisión orientado a detectar modificaciones críticas realizadas sobre cuentas privilegiadas en el Active Directory. Las acciones como la eliminación de usuarios, la deshabilitación de cuentas, los cambios de contraseña o la remoción de privilegios administrativos representan actividades alineadas a la táctica Impact y la técnica T1531 – Account Access Removal del marco MITRE ATT&CK.

Es así que, con el fin de monitorear estas operaciones sensibles, se configuró la ingesta de eventos del servidor Windows mediante el agente Winlogbeat, permitiendo centralizar en el SIEM los eventos de seguridad asociados a la administración de cuentas (ID 4723, 4724, 4725, 4726) señalados en el marco MITRE ATT&CK y la gestión de grupos (ID 4729, 4733, 4757).

Por lo tanto, como parte del diseño para alinearse correctamente con la técnica señalada del marco MITRE ATT&CK se establecieron tres reglas independientes que cumplen con el monitoreo de los IDs señalados:

a. Remoción de privilegios de grupos administrativos: monitoreo de ID 4729, 4733 y 4757.
b. Cuentas deshabilitadas o eliminadas: monitoreo de ID 4725 y 4726.
c. Manipulación de credenciales: monitoreo de ID 4723 y 4724.

Establecido estos puntos, se procede a detallar cada uno de los elementos indicados.

a. Remoción de privilegios de grupos administrativos (Miembro removido de grupos admin)

Este caso de uso tiene como finalidad detectar la remoción de cuentas privilegiadas desde los grupos administrativos dentro del Active Directory. Este comportamiento se encuentra alineado con la técnica T1531 – Account Access Removal, perteneciente a la táctica Impact del marco MITRE ATT&CK, la cual describe acciones orientadas a deshabilitar, limitar o retirar accesos con el objetivo de afectar la capacidad de operación normal de la organización. A través de esta regla se busca identificar modificaciones no autorizadas sobre grupos críticos que puedan comprometer la administración y disponibilidad de los servicios.

Configuración de la regla

La regla fue configurada en Kibana utilizando los eventos de auditoría de seguridad de Windows provenientes de Microsoft-Windows-Security-Auditing, recolectados mediante Winlogbeat, específicamente los identificadores 4729, 4733 y 4757, asociados a la administración de grupos de seguridad. La consulta utilizada permite identificar la remoción de usuarios pertenecientes a grupos críticos como Administrators, Domain Admins, Enterprise Admins o Schema Admins. Asimismo, la regla fue configurada con

severidad High y con una frecuencia de ejecución de 1 minuto, considerando un período adicional de búsqueda de 5 minutos con el fin de asegurar una detección oportuna de este tipo de actividades.

A continuación, se describe los parámetros configurados:

- Nombre de la regla: WIN-AD-T1531-A-Miembro removido de grupos admin
- KQL / Query:

  event.provider:"Microsoft-Windows-Security-Auditing" and

  winlog.channel:"Security" and

  (winlog.event_id:4729 or winlog.event_id:4733 or winlog.event_id:4757) and

  (

  winlog.event_data.TargetSid:"S-1-5-32-544" or

  winlog.event_data.TargetSid:"*-512" or

  winlog.event_data.TargetSid:"*-518" or

  winlog.event_data.TargetSid:"*-519" or

  winlog.event_data.TargetUserName:("Administrators" or "Administradores" or "Domain Admins" or "Enterprise Admins" or "Schema Admins")

)

- Horarios de ejecución:
  - Runs every 1 minutos
  - Additional look-back time 5 minutos

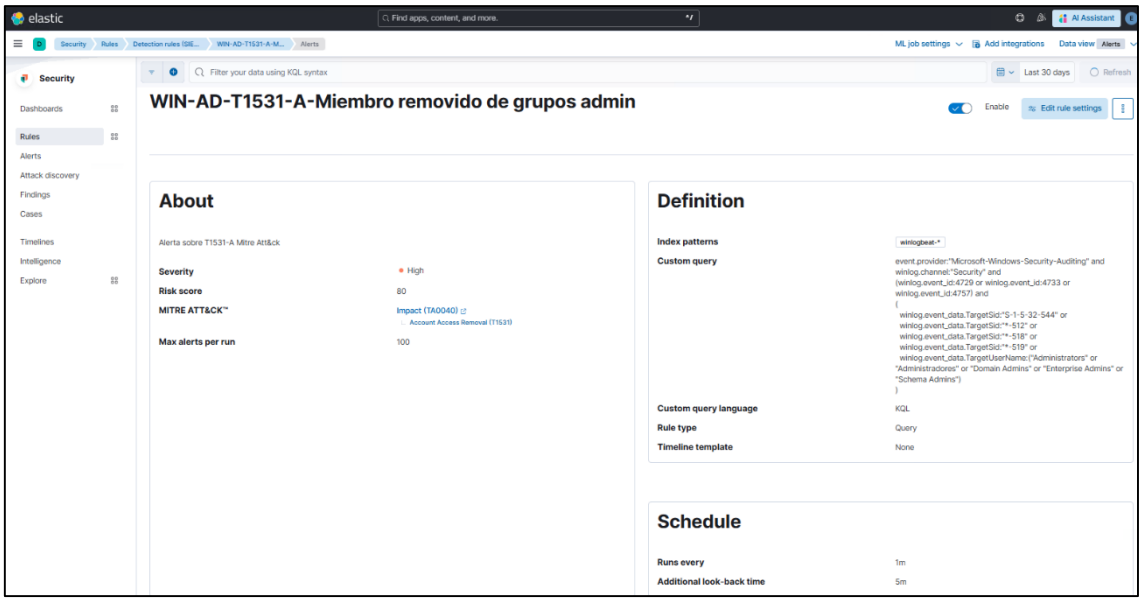
Lógica de detección:

La consulta permite identificar eventos relacionados con la remoción de miembros pertenecientes a grupos administrativos críticos del Active Directory, como son Administrators, Administradores, Domain Admins, Enterprise Admins o Schema Admins; facilitando la detección de actividades que puedan afectar privilegios elevados o comprometer el acceso administrativo dentro del entorno.

En la Figura 36, se muestra la configuración de la regla implementada en Kibana, y los parámetros indicados anteriormente, las cuales permiten asegurar la detección oportuna para este tipo de modificaciones en cuentas privilegiadas.

Figura 36

Caso de uso remoción de privilegios de grupos administrativos



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

b. Cuentas deshabilitadas o eliminadas

Este caso de uso tiene por objetivo identificar eventos relacionados con la deshabilitación o eliminación de cuentas de usuario en Active Directory. Este comportamiento se encuentra directamente alineado con la técnica T1531 – Account Access Removal del marco MITRE ATT&CK, la cual describe acciones orientadas a la eliminación, bloqueo o manipulación del acceso de cuentas legítimas con el fin de interrumpir procesos o afectar la continuidad operativa de la organización. La regla permite detectar modificaciones críticas sobre cuentas de usuario que podrían estar asociadas a actividades maliciosas o intentos de sabotaje.

Configuración de la regla

Para su implementación, se configuró en el SIEM una regla orientada a supervisar los eventos de auditoría de seguridad de Windows provenientes de Microsoft-Windows-Security-Auditing, recolectados mediante Winlogbeat, Para la detección de estos eventos, se consideraron los identificadores 4725 (cuenta deshabilitada) y 4726 (cuenta eliminada) dentro de Active Directory. Estos eventos permiten detectar de forma inmediata cualquier modificación crítica sobre la disponibilidad de cuentas de usuario, lo cual resulta relevante en escenarios donde la manipulación maliciosa de usuarios podría ser usada como mecanismo de sabotaje, evasión o impacto operacional. Asimismo, la regla fue configurada para monitorear eventos provenientes de los índices logs-* y winlogbeat-*, con severidad High, con una frecuencia de ejecución 1 minuto, con un período de retroceso de 5 minutos, permitiendo una supervisión continua y reduciendo el tiempo de detección frente a acciones críticas sobre cuentas de usuario. Esta configuración garantiza que el SIEM detecte de manera oportuna cualquier acción que impacte el acceso de usuarios en el Active Directory.

A continuación, se detalla la configuración de la regla:

- Nombre de la regla: WIN-AD-T1531-B-Cuentas deshabilitadas/eliminadas
- KQL / Query: event.provider:"Microsoft-Windows-Security-Auditing" and winlog.channel:"Security" and (winlog.event_id:4725 or winlog.event_id:4726)

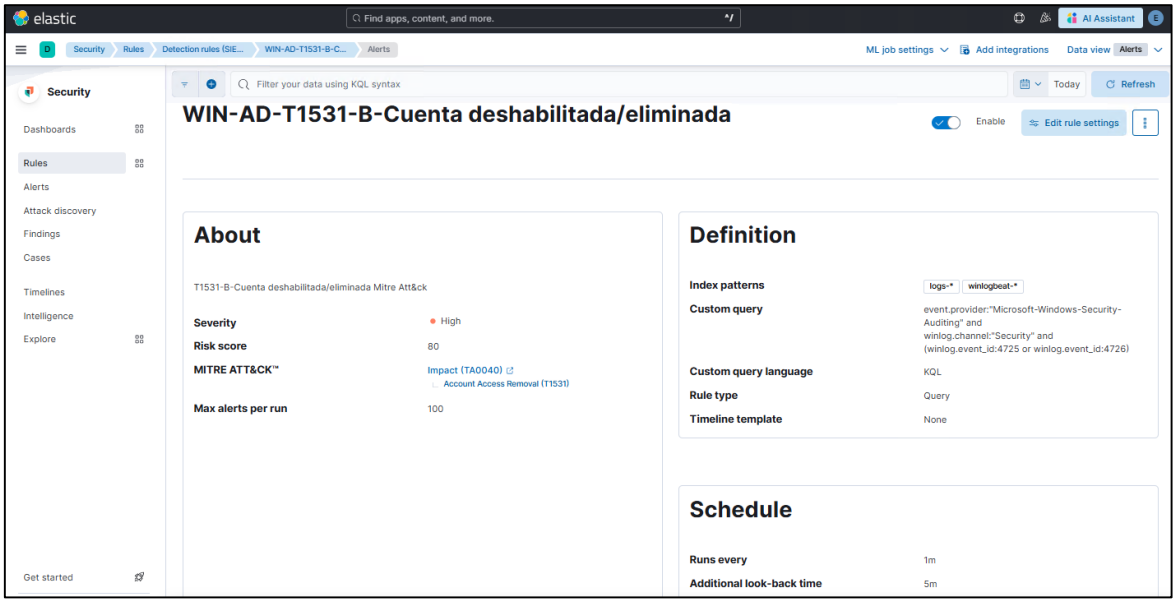
Lógica de detección:

La consulta KQL utilizada, permite filtrar los eventos relacionados con los eventos ID 4725 y 4726, asociados a la deshabilitación y eliminación de cuentas en Active Directory respectivamente, facilitando la detección de acciones que puedan afectar el acceso legítimo de usuarios dentro del entorno.

En la Figura 37 se muestra la configuración de la regla implementada en Kibana y los parámetros definidos para la detección de este tipo de eventos.

Figura 37

Caso de uso B cuentas deshabilitadas o eliminadas



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

c. Manipulación de credenciales (Cambio/Reset de contraseña)

Este caso de uso está orientado a detectar actividades relacionadas con la modificación directa de credenciales de cuentas de usuario dentro del Active Directory, incluyendo cambios de contraseña y restablecimientos realizados con éxito. Estas acciones, aunque pueden formar parte de procesos legítimos de administración, también pueden indicar actividad maliciosa cuando se ejecutan sin autorización o como parte de un intento de afectar la disponibilidad o integridad de cuentas. La regla permite supervisar eventos asociados a la manipulación de credenciales y fortalecer el monitoreo sobre acciones críticas dentro del entorno.

Configuración de la regla

Se configuró una regla en el SIEM en la plataforma Kibana, para supervisar los eventos de seguridad de Windows provenientes de Microsoft-Windows-Security-Auditing, recolectados mediante Winlogbeat. Para la detección de los eventos asociados a la administración de credenciales, se consideraron específicamente los identificadores 4723 (Intento de cambio de contraseña) y 4724 (Intento de reset de contraseña), filtrando únicamente aquellos eventos cuyo resultado sea exitoso (success). Así también, la regla

fue configurada con severidad High y un risk score de 75, ejecutándose cada 1 minuto con un período de retroceso adicional de 5 minutos, lo que permite una detección continua, oportuna y con adecuada tolerancia ante retrasos en la llegada de eventos. Esta detección permite identificar cuando un cambio o restablecimiento de credenciales se ha ejecutado de manera efectiva, lo que constituye un punto crítico para el análisis de posibles movimientos maliciosos o escaladas de privilegios dentro del entorno.

A continuación, se describe los parámetros configurados:

- Nombre de la regla: WIN-AD-T1531-C-Cambio/Reset de contraseña (success)
- KQL / Query: event.provider:"Microsoft-Windows-Security-Auditing" and winlog.channel:"Security" and (winlog.event_id:4723 or winlog.event_id:4724) and event.outcome:"success"

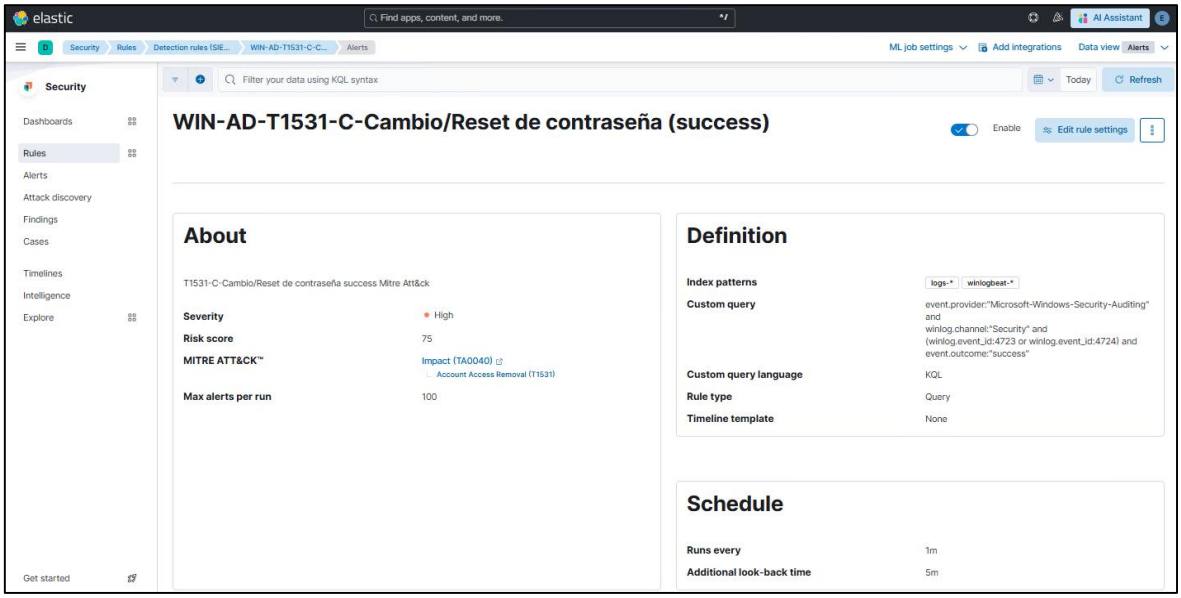
Lógica de detección:

La regla filtra específicamente los event ID 4723 y 4724, y además verifica que el campo event.outcome sea igual a success, garantizando que solo se alerten cambios de contraseña que se hayan completado de forma efectiva en Active Directory, facilitando la detección de actividades que puedan involucrar manipulación no autorizada de credenciales.

En la Figura 38, se muestra la configuración de la regla implementada en Kibana, incluyendo los patrones de índice utilizados y la consulta KQL que se indicó anteriormente, para la detección de estos eventos.

Figura 38

Caso de uso C Manipulación de credenciales (Cambio/Reset de contraseña)



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Variables de indicadores de logro del OE4

Para el logro correcto del objetivo específico señalado se han establecido las siguientes variables, las cuales serán usadas más adelante en la ejecución del plan de pruebas.

Variable 1: Tiempo de detección de incidentes

El Tiempo de Detección (TTD, Time to Detect) es una métrica clave en la gestión de eventos de seguridad, ya que mide cuánto tiempo tarda un sistema en detectar un incidente desde que ocurre. Para calcularlo, necesitas dos datos principales:

$$TTD = \ Hora\ de\ detección\ - Hora\ de\ inicio\ del\ evento$$

- Componentes de la fórmula:

Hora de inicio del evento: El momento en que ocurrió el incidente.

Hora de detección: El momento en que el sistema SIEM identificó el incidente.

A continuación, se muestra la formula del promedio del TTD

$$MTTD = \frac{\sum TTD\ de\ cada\ evento}{Número\ de\ eventos}$$

Ejemplo:

Se simula un ataque de tipo “Credential Dumping” (Técnica T1003 en MITRE ATT&CK).

- Hora de inicio del evento: 14:25:00
- Hora de detección por el SIEM: 14:26:30

Cálculo individual:

TTD = 14:26:30 - 14:25:00 = 1 minuto 30 segundos

Entonces para calcular el promedio vamos a asumir que, en un conjunto de 5 simulaciones de ataques similares, los TTD fueron: 90 s, 120 s, 100 s, 80 s, 110 s.

Por lo tanto, el cálculo del MTTD sería el siguiente:

$$MTTD = \frac{90 + 120 + 100 + 80 + 110}{5}$$

$$MTTD = 100\ segundos\ (1\ \text{minuto}\ 40\ segundos)$$

Esto significaría que el tiempo de detección promedio es de 1 minuto y 40 segundos.

3.1.5 Desarrollo de la Capacitación en SIEM y MITRE ATT&CK

El plan de capacitación propuesto contempla la implementación de una sesión formativa estructurada dirigida al personal del área de soporte de Tecnologías de la Información (TI), a los que previamente se les ha informado. Asimismo, se busca que esta capacitación genere una comprensión práctica y aplicable dentro del contexto operativo de la organización. En tal sentido, la metodología seleccionada será el método expositivo, caracterizado por la presentación clara y ordenada de los contenidos por parte del capacitador, favoreciendo la comprensión de los conceptos fundamentales mediante explicaciones teóricas y ejemplos prácticos.

Para esta sesión de capacitación se desarrolló un temario sobre los conceptos que se van a tratar en la sesión, los cuales se presentan seguidamente:

Tabla 12

Temario de Capacitación

TEMARIO	DETALLE
1. Introducción al SIEM	¿Qué es un SIEM? ¿Para qué sirve? Ejemplos
2. Componentes básicos de un SIEM Open Source	¿Qué herramientas componen un SIEM Open Source como ELK? ¿Qué son los logs y por qué son importantes? ¿Cómo llega los registros al SIEM?
3. Introducción al marco MITRE ATT&CK	¿Qué es MITRE ATT&CK? ¿Qué son tácticas y técnicas? Ejemplo de caso de uso
4. Rol del soporte TI frente al SIEM y ATT&CK	¿Cuál es su responsabilidad? Buenas prácticas
5. Cierre y preguntas	Resumen Ronda de preguntas

Como parte complementaria al presente material, se ha elaborado una presentación en formato PowerPoint, en la cual se desarrolla el temario propuesto que facilitan la comprensión de los conceptos tratados. Este documento tiene como finalidad servir de apoyo durante la exposición y está incluido como Anexo 1.

Con el objetivo de cuantificar la efectividad del programa formativo, el método de evaluación se fundamenta en un enfoque pre y post evaluación. Inicialmente, se administrará una evaluación para determinar el nivel de conocimiento actual de los participantes. Esta evaluación estará dividida en dos temas fundamentales: Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) y el marco MITRE ATT&CK. Dicho resultado permitirá establecer una línea base objetiva del dominio de estos conceptos por parte del personal. Para dicha evaluación de aprendizaje, se ha diseñado un cuestionario de opción múltiple, el cual se incluye en el Anexo 2.

Por otra parte, una vez finalizado el programa de formación, se aplicará nuevamente la evaluación con el propósito de medir el incremento en el conocimiento relacionado con SIEM y MITRE ATT&CK. Estos resultados obtenidos servirán como punto de referencia para medir la mejora en las competencias adquiridas post-capacitación. La comparación de los resultados de ambas evaluaciones permitirá calcular el porcentaje de mejora y, con ello, evaluar la efectividad del programa de capacitación en el fortalecimiento de las capacidades del personal en ciberseguridad.

Este procedimiento, apoyado en la metodología expositiva contribuirá a determinar el alcance real de la intervención formativa en el desarrollo profesional y la preparación del equipo ante desafíos de ciberseguridad.

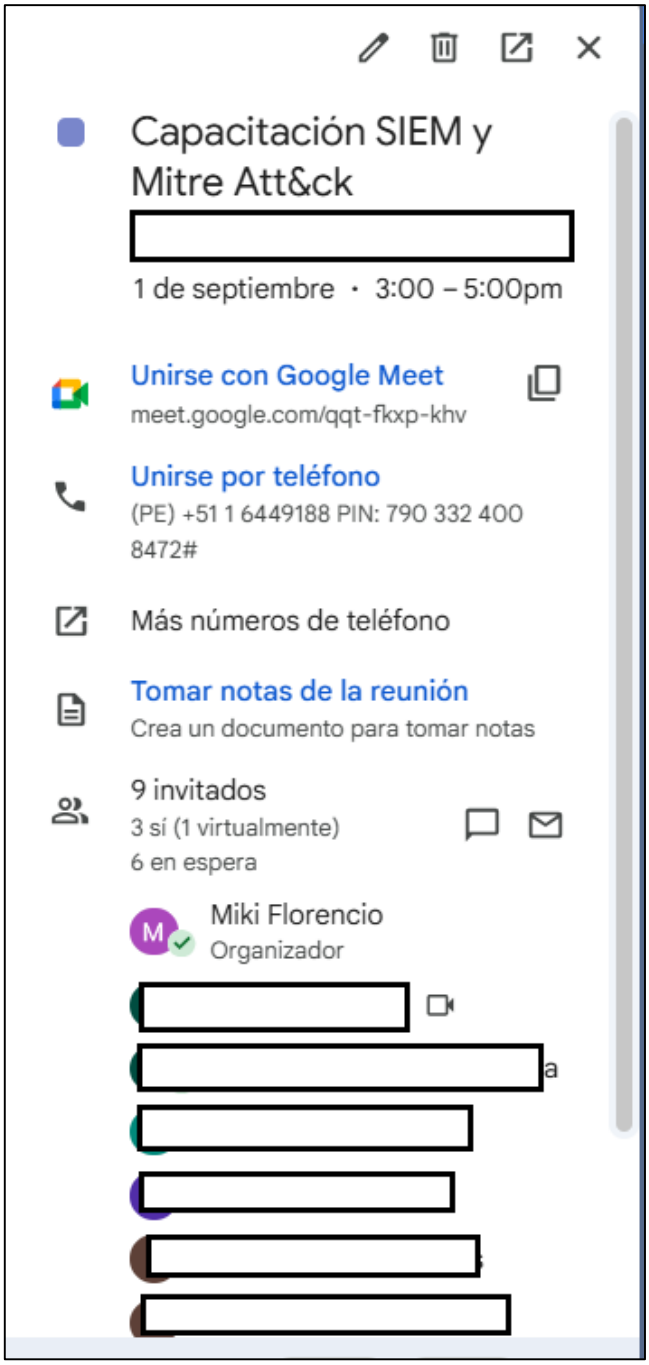
A continuación, se proyecta el desarrollo de la capacitación:

Preparación de la Capacitación:

Se envió un correo electrónico al personal de soporte TI, previo al desarrollo de la sesión, para participar en la capacitación, indicando la fecha, el contenido y el enlace de acceso a la reunión virtual. En la Figura 39, correspondiente muestra el correo de invitación remitido, evidenciando la convocatoria realizada al personal, se han ocultado los nombres de los participantes para preservar su confidencialidad.

Figura 39

Evidencia de reunión generada para la capacitación

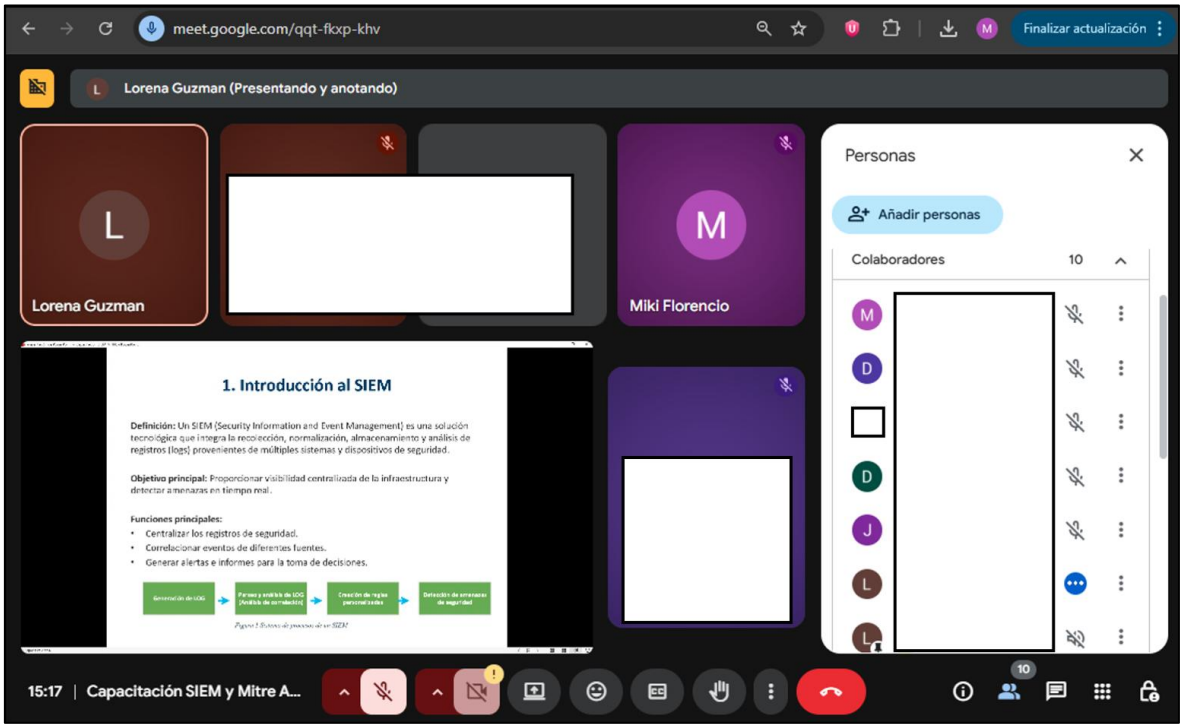


Ejecución de la Capacitación:

La capacitación se desarrolló mediante una sesión virtual sincrónica de dos horas, en la cual se expusieron los fundamentos del SIEM implementado, su arquitectura, las funciones principales y la relación operativa con las técnicas y tácticas del marco MITRE ATT&CK. En la Figura 40 se muestra la reunión realizada mediante Google Meet con la participación de los involucrados, se han ocultado los nombres de los participantes para preservar su confidencialidad.

Figura 40

Evidencia de Capacitación



Variables de indicadores de logro del OE5

Para este proceso de capacitación y el cumplimiento del objetivo específico señalado, se han definido dos variables fundamentales. Estas serán detalladas a continuación y aplicadas posteriormente durante la ejecución del plan de pruebas.

Variable 1: Capacitación del equipo de soporte TI

Esta variable mide el porcentaje de participación del equipo de soporte de TI en las sesiones de capacitación realizadas. Se puede expresar como la relación entre el número de asistentes y el total de convocados.

$$Tasa\ de\ Asistencia = \frac{Número\ de\ asistentes}{Número\ total\ de\ convocados} \times 100$$

Ejemplo:

Si se convoca a 5 miembros del equipo de soporte de TI para participar en una sesión de capacitación. Y el día de la capacitación, 3 personas asisten.

Al aplicar la fórmula tenemos los siguiente:

$$Tasa\ de\ Asistencia = \frac{3}{5} \times 100 = 60\ \%$$

Esto significaría que el 60% del equipo de soporte asistió a la capacitación.

Variable 2: Efectividad de la capacitación

Esta variable mide el nivel de mejora en el desempeño del personal de soporte de TI después de haber recibido una capacitación. Se utiliza la fórmula de mejora relativa al alcance máximo. Se calcula comparando los resultados obtenidos antes y después de la capacitación en evaluaciones.

$$Porcentaje\ de\ mejora = \left(\frac{NPC - NPRC}{20 - NPRC}\right) X\ 100$$

- Datos de medición:

NPC: Nota post-capacitación

NPRC: Nota pre-capacitación

Importante: Se considera que la nota máxima es 20 y la nota mínima es 0

Luego de calcular los datos de cada participante con la formula señalada se procederá con el promedio general del porcentaje de mejora.

Ejemplo:

Supongamos que antes de la capacitación, un miembro del equipo obtuvo una nota pre-capacitación (NPRC) de 10 en la evaluación. Después de la capacitación, en la misma evaluación adaptada, obtuvo una nota post-capacitación (NPC) de 16.

Al aplicar la fórmula tenemos los siguiente:

$$Porcentaje\ de\ mejora = \left(\frac{16-10}{20-10}\right) X\ 100$$

$$Porcentaje\ de\ mejora = \left(\frac{6}{10}\right) X\ 100$$

$$Porcentaje\ de\ mejora = \ 60\%$$

Esto significaría que la capacitación permitió una mejora del 60% en el desempeño del participante.

3.2 Validación del Proyecto

Esta sección se muestra el proceso mediante el cual se validaron los objetivos específicos del proyecto, a través de la planificación, ejecución y evaluación de planes de prueba estructurados. El propósito central de estas validaciones fue verificar que la solución implementada opere correctamente, muestre un desempeño adecuado y se alinee con los objetivos definidos en la investigación, asegurando que cada componente técnico y funcional responda a los requerimientos de detección, correlación y visualización de eventos de seguridad.

Para ello, los planes de prueba siguieron un enfoque sistemático estructurado en tres fases:

a. Definición y Alcance del Plan de Pruebas
b. Ejecución y Desarrollo del Plan de Pruebas
c. Análisis e Interpretación de los Resultados

Esta estructura garantiza que las actividades de validación técnica se desarrollen con rigor metodológico y permitan medir de forma objetiva la eficacia del sistema ante escenarios de incidentes de seguridad.

En ese contexto, las pruebas no se limitaron a verificar la correcta recepción, normalización y visualización de eventos dentro de la plataforma ELK Stack, sino que también evaluaron la eficacia de las reglas de correlación y alertas, así como el mapeo al marco MITRE ATT&CK, poniendo a prueba la capacidad del sistema para identificar tácticas y técnicas específicas mediante los casos de uso implementados. Finalmente, los resultados obtenidos constituyen evidencia objetiva del funcionamiento del SIEM propuesto y del cumplimiento de los objetivos específicos, conforme a los indicadores definidos en el capítulo 1.4.

3.2.1 Resultados del Plan de Prueba del Objetivo Específico N°1

3.2.1.1 Definición y Alcance del Plan de Pruebas

Tabla 13

Objetivo específico 1, Definición y Alcance del Plan de Pruebas

Objetivo Específico	Identificar los componentes críticos de infraestructura tecnológica de la empresa para el diseño del sistema SIEM mediante un listado técnico y una evaluación comparativa de al menos tres soluciones Open Source.		
I. Plan de Pruebas del Objetivo Específico			
Fecha de Ejecución	08/09/2025	**Versión**	v1
Patrocinador	Gerente de Sistemas		
Responsable del Plan de Pruebas	Coordinador de TI		
Objetivo del Plan de Pruebas	- Elaborar listado técnico de componentes críticos. - Evaluación comparativa documentada de soluciones SIEM Open Source.		
II. Detalle del Plan de Pruebas			
Alcance	El alcance comprende la elaboración de un documento detallado que identifica y describe los componentes tecnológicos críticos de la empresa. Además, se incluye la creación de un cuadro comparativo que analiza y evalúa las cuatro soluciones SIEM de código abierto más relevantes, especificando parámetros de evaluación.		

Duración del Plan de Pruebas	2 horas
Método de Prueba	Lista de Chequeo y Revisión Documental (Checklist Test): Se validará la identificación del 100 % de los componentes tecnológicos críticos mediante listas de verificación de la infraestructura. Asimismo, se revisará la consistencia del cuadro comparativo técnico de las cuatro soluciones SIEM.
Actividades a Ejecutar	1. Identificar los componentes y rol dentro de la arquitectura tecnológica. 2. Elaborar el listado técnico consolidado de la infraestructura crítica para la recolección de registros. 3. Seleccionar cuatro soluciones SIEM Open Source. 4. Construir un cuadro comparativo de las soluciones SIEM Open Source seleccionadas, según parámetros de investigación. 5. Puntuar cuadro comparativo de las soluciones SIEM, según criterios basados en investigación. 6. Documentar resultados y generar informe para la aprobación con la Gerencia de Sistemas.

3.2.1.2 Ejecución y Desarrollo del Plan de Pruebas

Tabla 14

Objetivo específico 1, Ejecución del Plan de Pruebas

III. Ejecución del Plan de Pruebas			
Escenario	Infraestructura de la empresa – Recupera Outsourcing		
Herramienta	Inventario de activos, hojas de cálculo, documentación técnica, fichas comparativas, lista de principales herramientas SIEM - Open Source.		
Criterios de Aceptación	**Detalle**	**Estado**	**Porcentaje**
	- Identificación del 100 % de los componentes críticos de infraestructura.	Realizado	100%

	- Elaboración de cuadro comparativo con puntuación técnica (compatibilidad, escalabilidad, soporte, comunidad, facilidad de integración).	Realizado	100%
Resultados	Realizado		100%
Participantes del Plan de Pruebas	**Puesto**	**Fecha**	
	Jefe de Infraestructura	08/09/2025	
	Coordinador de TI	08/09/2025	
	Analista de Ciberseguridad	08/09/2025	
Aceptado / Rechazado	ACEPTADO		

IV. Desarrollo del Plan de Pruebas

Considerando lo expuesto previamente sobre los componentes críticos de la empresa en la sección 3.1.1, se realizó la validación de su identificación mediante una lista de verificación de la infraestructura.

Por este motivo, se agrega el Anexo 3, el cual presenta la identificación de los componentes críticos de la infraestructura, debidamente validada y aprobada por la Gerencia de Sistemas.

Asimismo, se incluye el Anexo 4, donde se muestra la elaboración del cuadro comparativo de las soluciones SIEM Open Source, junto con su respectiva evaluación, donde se detalla la puntuación técnica asignada a cada alternativa conforme a los criterios definidos. Al igual que el anterior, este documento fue validado y aprobado por la Gerencia de Sistemas.

3.2.1.3 Análisis e Interpretación de los Resultados

En primer lugar, se identificó el 100 % de los componentes críticos de la infraestructura tecnológica de la empresa, mediante la elaboración de un inventario detallado y la verificación física de los activos. Como parte de este proceso, se identificaron 7 componentes, de los cuales se consideraron 4 componentes críticos, debido a que son administrados directamente por la empresa.

Asimismo, este proceso se documentó en un checklist acompañado de evidencia fotográfica, lo cual permitió validar la existencia, operatividad y relevancia de cada componente en la arquitectura tecnológica. Este resultado evidencia una visión clara de las fuentes que intervienen en el entorno de TI, requisito fundamental para la posterior integración de una solución SIEM.

En segundo lugar, se elaboró un cuadro comparativo de herramientas SIEM open source, evaluando cuatro alternativas: Wazuh, OSSIM, SIEMonster y ELK Stack. La comparación se realizó con base en una metodología de puntuación técnica que consideró aspectos de compatibilidad, escalabilidad, facilidad de implementación, capacidad de integración y soporte de la comunidad. Los puntajes obtenidos fueron: Wazuh (53 puntos), OSSIM (26 puntos), SIEMonster (43 puntos) y ELK Stack (54 puntos).

De acuerdo con el análisis, ELK Stack obtuvo la puntuación más alta (54 puntos), demostrando un mayor nivel de implementación y flexibilidad frente a los demás candidatos. Este resultado sustenta la selección de ELK Stack como la solución base para el diseño e implementación del sistema SIEM propuesto, dado su equilibrio entre rendimiento, escalabilidad, modularidad y compatibilidad con los entornos de red e infraestructura de la organización.

Por tanto, a partir de los resultados obtenidos, se determina que el objetivo específico 1 fue cumplido de manera satisfactoria, en concordancia con los parámetros establecidos en su descripción, los indicadores de logro y las métricas asociadas.

3.2.2 Resultado del Plan de Prueba del Objetivo Específico N°2

3.2.2.1 Definición y Alcance del Plan de Pruebas

Tabla 15

Objetivo específico 2, Definición y Alcance del Plan de Pruebas

Objetivo Específico	Diseñar un diagrama de arquitectura SIEM basada en una herramienta Open Source aprobado por la gerencia de sistemas, asegurando que permita la centralización y gestión de eventos de seguridad.		
I. Plan de Pruebas del Objetivo Específico			
Fecha de Ejecución	11/09/2025	**Versión**	v1
Patrocinador	Gerente de Sistemas		
Responsable del Plan de Pruebas	Coordinador de TI		
Objetivo del Plan de Pruebas	- Cumplimiento del plazo establecido en un tiempo menor o igual a 6 días hábiles para la elaboración y validación del diagrama de arquitectura. - Aprobación del diagrama de arquitectura SIEM por la gerencia de sistemas.		
II. Detalle del Plan de Pruebas			
Alcance	El diagrama debe reflejar con precisión los flujos de información y los componentes técnicos esenciales (ingesta, procesamiento, correlación y visualización de eventos) y garantizar la viabilidad de la centralización de logs desde las fuentes críticas definidas. También la validación se centrará en el diseño documentado y los principios básicos de una arquitectura SIEM ELK.		
Duración del Plan de Pruebas	3 horas		
Método de Prueba	Paseo de Revisión (Walkthrough Test) Se realiza una revisión guiada y participativa del diseño de arquitectura física y lógica del SIEM, asegurando que el flujo de logs y componentes esté correctamente representado. La gerencia y equipo TI evalúan la coherencia y completitud del diseño.		

Actividades a Ejecutar	1. Revisar los componentes críticos identificados de la infraestructura 2. Definir la arquitectura general de la solución SIEM propuesta. 3. Elaborar el diagrama de arquitectura SIEM basado en ELK Stack. 4. Incluir las rutas de flujo de datos desde las fuentes de logs hacia el servidor SIEM. 5. Incorporar en el diseño de arquitectura la alineación con el marco MITRE ATT&CK 6. Revisar la arquitectura con el equipo de TI y realizar los ajustes técnicos necesarios. 7. Presentar el diagrama final a la gerencia de sistemas para su aprobación formal. 8. Registrar observaciones y generar acta o documento de conformidad.

3.2.2.2 Ejecución y Desarrollo del Plan de Pruebas

Tabla 16

Objetivo específico 2, Ejecución del Plan de Pruebas

III. Ejecución del Plan de Pruebas			
Escenario	Infraestructura de la empresa – Recupera Outsourcing		
Herramienta	Inventario de componentes críticos, documentación técnica, fichas comparativas, solución SIEM seleccionada (ELK Stack).		
Criterios de Aceptación	**Detalle**	**Estado**	**Porcentaje**
	- El diagrama debe representar la infraestructura de la implementación del SIEM.	Realizado	100%
	- La arquitectura lógica debe representar el flujo de procesamiento de logs del SIEM.	Realizado	100%

	- Aprobación del diagrama de arquitectura por la gerencia de sistemas dentro de un plazo menor a 5 días hábiles desde su presentación.	Realizado	100%
Resultados	Realizado		100%
Participantes del Plan de Pruebas	**Puesto**	**Fecha**	
	Jefe de Infraestructura	11/09/2025	
	Coordinador de TI	11/09/2025	
Aceptado / Rechazado	ACEPTADO		

IV. Desarrollo del Plan de Pruebas

Con base en el diseño definido en la sección 3.1.2, se procedió a su validación mediante una revisión guiada de la arquitectura propuesta.

El resultado de este proceso se muestra en el Anexo 5, que documenta formalmente el diseño de arquitectura del SIEM basado en ELK Stack, con la respectiva revisión y aprobación de la Gerencia de Sistemas.

3.2.2.3 Análisis e Interpretación de los Resultados

En primer lugar, se elaboró el diagrama de arquitectura del SIEM ELK Stack, representando de manera clara y estructurada la infraestructura tecnológica de la empresa. Este documento incluye dos vistas complementarias:

La arquitectura física, donde se identifican los componentes principales del entorno implementado, entre ellos el servidor del SIEM y su distribución dentro de la red corporativa.

La arquitectura lógica, que muestra el flujo de procesamiento de logs provenientes de los dispositivos perimetrales y servidores críticos, integrando específicamente dos firewalls Fortinet, un servidor Active Directory y un servidor NAS.

Estos diagramas permitieron visualizar de forma integral la estructura de la solución SIEM, evidenciando la correcta planificación y el alineamiento con los requerimientos de la organización.

Dicho esto, se puede evidenciar que el diseño asegura la centralización y gestión de eventos de seguridad, mediante el SIEM propuesto. Además, la aprobación formal de la arquitectura SIEM por parte de la Gerencia de Sistemas confirma la viabilidad del diseño propuesto y avala la decisión de proceder con su implementación sobre la plataforma ELK Stack.

Asimismo, dicha aprobación se efectuó dentro del plazo establecido en el plan de pruebas, específicamente el documento fue elaborado el 16 de julio de 2025 y aprobado el 18 de julio de 2025, cumpliendo así con el criterio de validación y aceptación dentro de los cinco días hábiles previstos.

Por tanto, a partir de lo mencionado, se concluye que el objetivo específico 2 fue cumplido de manera satisfactoria.

3.2.3 Resultado del Plan Prueba del Objetivo Específico N°3

3.2.3.1 Definición y Alcance del Plan de Pruebas

Tabla 17

Objetivo específico 3, Definición y Alcance del Plan de Pruebas

Objetivo Específico	Desplegar un SIEM operativo que registre los logs de dos firewalls y dos servidores críticos, garantizando una disponibilidad ≥ 99.5 %.		
I. Plan de Pruebas del Objetivo Específico			
Fecha de Ejecución	12/09/2025	**Versión**	V1
Patrocinador	Gerente de Sistemas		
Responsable del Plan de Pruebas	Coordinador de TI		
Objetivo del Plan de Pruebas	- Validación de la integración del 100% de las fuentes (firewalls y servidores) en la plataforma SIEM. - Disponibilidad operativa del SIEM superior al 99,5 % durante el monitoreo.		

	- Capacidad de procesamiento de eventos del SIEM superior a 155 EPS (eventos por segundo).
II. Detalle del Plan de Pruebas	
Alcance	Verificar la implementación y operación del sistema SIEM en el entorno productivo. El alcance abarca la instalación del software base, la configuración inicial del sistema, y la integración de datos desde los 2 firewalls y 2 servidores.
Duración del Plan de Pruebas	5 horas
Método de Prueba	Prueba Funcional y de Rendimiento (Functional & Performance Test) Se prueba la integración técnica de los cuatro dispositivos (dos firewalls Fortinet, un servidor AD y un NAS QNAP), verificando conectividad, parseo y visualización de logs. Se mide disponibilidad y EPS constante.
Actividades a Ejecutar	1. Preparar el entorno de instalación del SIEM (máquina virtual con recursos asignados). 2. Instalar los servicios del SIEM (Elasticsearch, Logstash, Kibana, Filebeat) 3. Configurar la ingesta de logs mediante Syslog y Winlogbeat según cada dispositivo. 4. Integrar los dos firewalls Fortinet, el servidor Windows y el servidor NAS QNAP. 5. Verificar conectividad y flujo de logs en tiempo real hacia el SIEM. 6. Validar visualización de logs en Kibana. 7. Configurar políticas de retención y almacenamiento de eventos. 8. Medir la disponibilidad del SIEM durante el periodo de prueba (≥ 99.5%). 9. Calcular la tasa de procesamiento de eventos (EPS) promedio durante el monitoreo. 10. Mostrar resultados finales.

3.2.3.2 Ejecución y Desarrollo del Plan de Pruebas

Tabla 18

Objetivo específico 3, Ejecución del Plan de Pruebas

<table>
<tr><th colspan="5">III. Ejecución del Plan de Pruebas</th></tr>
<tr><td>Escenario</td><td colspan="4">Entorno productivo de la empresa donde se integrará fuentes reales de logs provenientes de dos firewalls Fortinet y dos servidores críticos. Se simulan condiciones normales de operación durante el monitoreo.</td></tr>
<tr><td>Herramienta</td><td colspan="4">Proxmox, QEMU, Recursos de infraestructura (CPU, RAM, almacenamiento)</td></tr>
<tr><td rowspan="4">Criterios de Aceptación</td><td>Detalle</td><td colspan="2">Estado</td><td>Porcentaje</td></tr>
<tr><td>- Integración exitosa del 100 % de las fuentes de logs.</td><td colspan="2">Realizado</td><td>100%</td></tr>
<tr><td>- Disponibilidad del SIEM ≥ 99.5 % durante el monitoreo.</td><td colspan="2">Realizado</td><td>100%</td></tr>
<tr><td>- Tasa de procesamiento ≥ 155 EPS constante.</td><td colspan="2">Realizado</td><td>100%</td></tr>
<tr><td>Resultados</td><td colspan="3">Realizado</td><td>100%</td></tr>
<tr><td rowspan="4">Participantes del Plan de Pruebas</td><td>Puesto</td><td colspan="3">Fecha</td></tr>
<tr><td>Jefe de Infraestructura</td><td colspan="3">12/09/2025</td></tr>
<tr><td>Coordinador de TI</td><td colspan="3">12/09/2025</td></tr>
<tr><td>Analista de Ciberseguridad</td><td colspan="3">12/09/2025</td></tr>
<tr><td>Aceptado / Rechazado</td><td colspan="4">ACEPTADO</td></tr>
</table>

IV. Desarrollo del Plan de Pruebas

Una vez implementado todos los servicios requeridos vistos en el punto 3.1.3.1 y 3.1.3.2; y además integrado las fuentes en el punto 3.1.3.3, en esta etapa del plan de pruebas se detallada las validaciones correspondientes a este objetivo.

Integración Exitosa

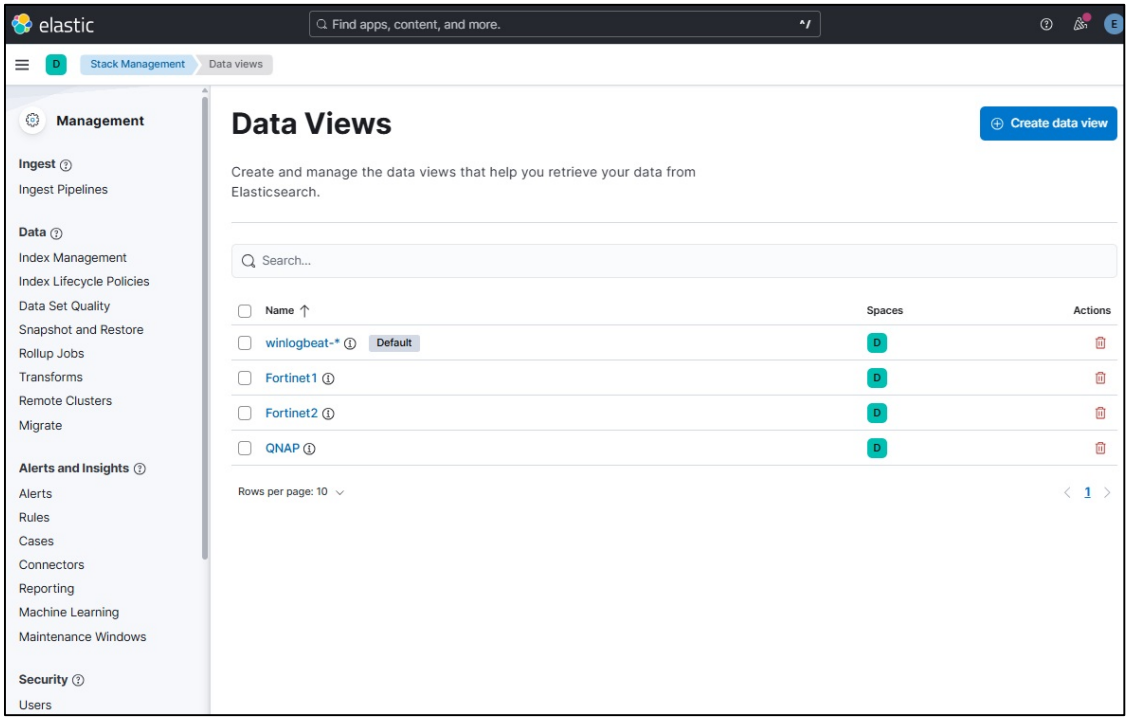
Se validó la correcta integración del 100 % de las fuentes de logs hacia la plataforma SIEM ELK Stack, confirmando la comunicación y recepción continua de eventos provenientes de los dos firewalls Fortinet, el servidor Active Directory y el servidor NAS QNAP.

En la siguiente Figura 41, se muestra la evidencia obtenida desde el módulo Data Views de Kibana, donde se visualizan las fuentes de logs integradas al SIEM. Se identifican cuatro dispositivos conectados: dos firewalls Fortinet, un servidor Windows y un servidor NAS QNAP.

a) **winlogbeat-*:** corresponde al servidor Windows Server 2019, donde se ejecuta el servicio de Active Directory.
b) **QNAP:** representa el servidor NAS, utilizado como almacenamiento compartido para las operaciones de la empresa.
c) **Fortinet1:** identifica el firewall principal de la red empresarial.
d) **Fortinet2:** corresponde al firewall secundario de la red empresarial.

Figura 41

Vista de Integración de Fuentes en SIEM ELK



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

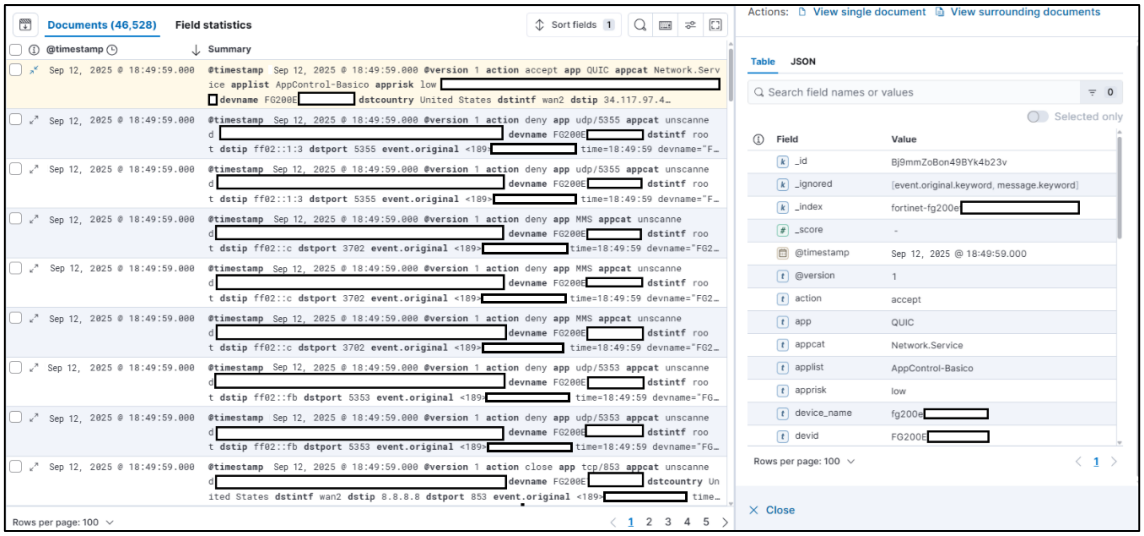
A continuación, se presentan las evidencias individuales de recepción de logs correspondientes a cada una de las fuentes integradas, con el propósito de mostrar el flujo de eventos y verificar la correcta comunicación entre las fuentes y el SIEM.

Fortinet Principal - Firewall 1

En la Figura 42, se muestra la interfaz del módulo Discover de Kibana, donde se visualiza el conjunto de eventos provenientes del Firewall 1 integrado al SIEM. En esta vista se aprecia un volumen significativo de registros (más de 46 mil eventos), evidenciando el envío continuo de logs desde el dispositivo Fortinet hacia la plataforma ELK Stack mediante el mecanismo de ingesta configurado para el procesamiento de eventos syslog.

Figura 42

Recepción de Logs Firewall 1



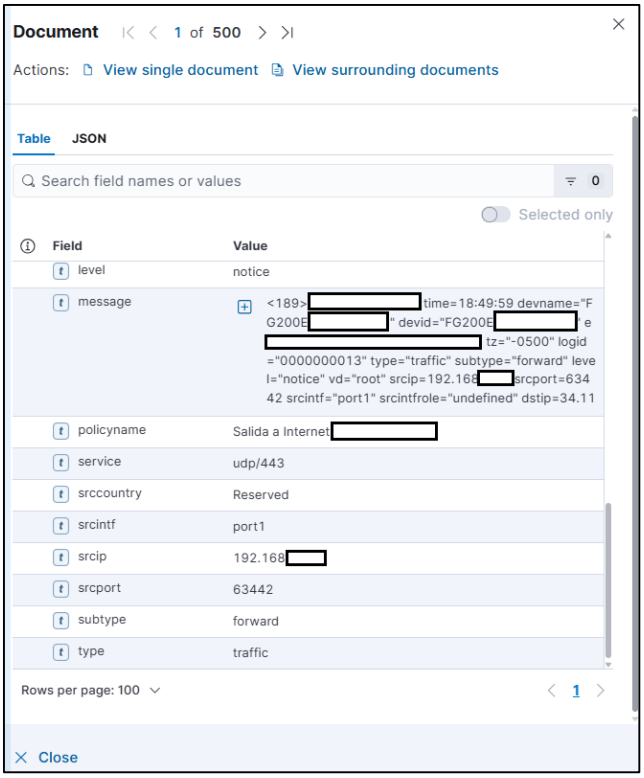
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

En la parte izquierda de la figura se observa la columna @timestamp, la cual permite validar la sincronización de cada evento generado por el firewall 1. A través de esta marca de tiempo, se evidencia el envío continuo de logs hacia el SIEM, reflejando tráfico de red y actividades propias del funcionamiento del firewall en tiempo real. Asimismo, es posible identificar campos relevantes como action, app, appcat, devname, dstip, dstport, event.original, característicos de los eventos generados por FortiOS. La presencia de estos campos confirma que el SIEM está capturando correctamente información asociada a la inspección de tráfico, aplicaciones detectadas, puertos utilizados y direcciones IP involucradas en las comunicaciones de red.

Dicho esto, en la Figura 43 se presenta la vista Table de un evento individual, donde se confirma la correcta extracción y normalización de los campos procesados por Logstash. En el campo message se conserva el log nativo enviado por el firewall, el cual contiene información relevante como el nombre del dispositivo(devname), identificador del equipo (devid), fecha de generación del evento, tipo de tráfico (traffic), subtipo (forward), así como los valores originales asociados a la comunicación de red.

Figura 43

Detalle de Recepción de Log Firewall 1



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Los campos desglosados en esta vista permiten verificar que el SIEM ha interpretado correctamente el formato syslog de Fortinet, extrayendo atributos fundamentales para el monitoreo y correlación de eventos, tales como:

- policyname, que indica la regla de firewall aplicada
- service, que representa el servicio/puerto detectado
- srcintf y dstintf, que identifican las interfaces del Firewall
- srcip y dstip, que representan las IPs de origen y destino de la comunicación
- action, que muestra si el tráfico fue permitido o denegado

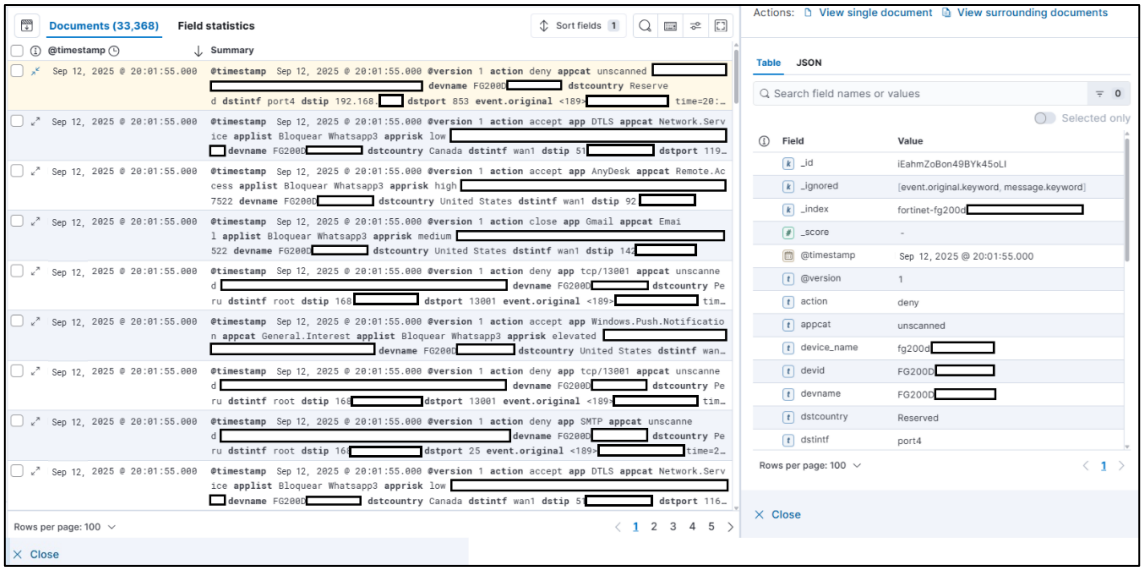
En conjunto, estas evidencias confirman que la integración del Firewall 1 fue realizada correctamente, garantizando la disponibilidad de información relevante para la inspección de tráfico, auditoría y correlación de eventos de seguridad.

Fortinet Secundario - Firewall 2

En la Figura 44, se muestra la interfaz del módulo Discover de Kibana, donde se visualiza los eventos provenientes del Firewall 2, el segundo dispositivo Fortinet integrado al SIEM. En esta vista se aprecia un volumen considerable de registros (más de 33 mil eventos), evidenciando la comunicación continua del firewall con la plataforma ELK Stack mediante el envío de logs en formato syslog.

Figura 44

Recepción de Logs Firewall 2



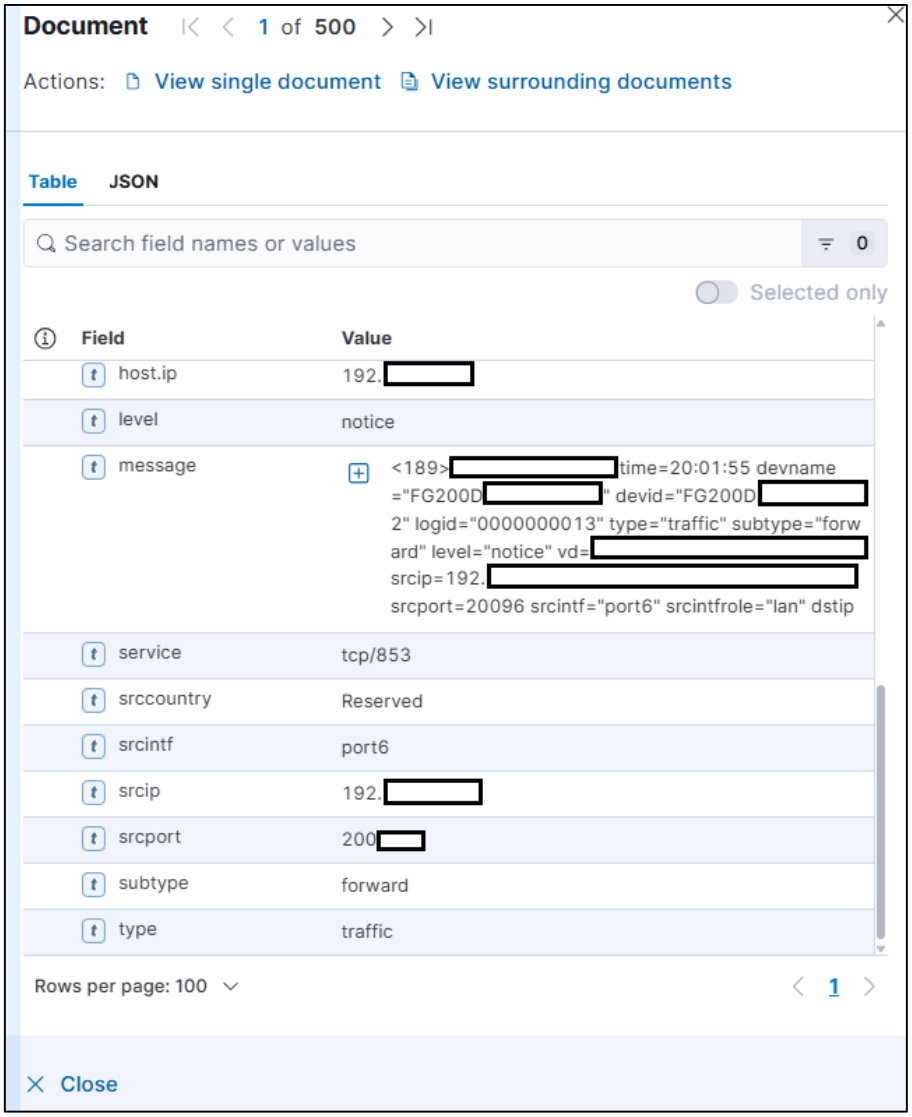
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

A través de la columna @timestamp se valida la sincronización temporal de los eventos recibidos, evidenciando un flujo continuo de información relacionada con el tráfico de red procesado por el Firewall 2. Asimismo, en el campo Summary se identifican campos relevantes como action, app, appcat, apprisk, dstip, dstport, dstcountry, dstintf y devname, correspondientes a eventos de tipo traffic con acciones accept y deny. Estos campos permiten identificar aplicaciones detectadas, niveles de riesgo, destinos de comunicación y políticas aplicadas por el firewall, confirmando que el SIEM está interpretando adecuadamente los eventos enviados por el dispositivo.

Dicho esto, en la Figura 45 se presenta la vista Table de un evento individual, donde se evidencia el detalle de la información procesada por el SIEM a partir del log original generado por Firewall 2. Como se visualiza, en el campo message conserva la estructura cruda enviada por el dispositivo, incluyendo información relevante como el identificador del dispositivo (devname), el tipo de evento (traffic), el subtipo (forward), el nivel de severidad(level), así como direcciones IP, puertos, y datos asociados a la sesión de red.

Figura 45

Detalle de Recepción de Log Firewall 2



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

En esta vista detallada se identifican atributos desglosados, tales como:

- host.ip, que representa el host origen de la comunicación.
- srcport y dstport, vinculados a la sesión establecida.
- subtype y type, utilizados para clasificar el evento según la lógica de FortiOS.

Estos campos permiten confirmar que el formato syslog generado por el Firewall 2 fue interpretado correctamente por el SIEM, facilitando las búsquedas y futuras reglas de correlación.

En conjunto, la evidencia presentada demuestra que la integración del Firewall 2 hacia el SIEM se realizó satisfactoriamente, garantizando la disponibilidad de información relevante para el análisis de eventos de seguridad en tiempo real.

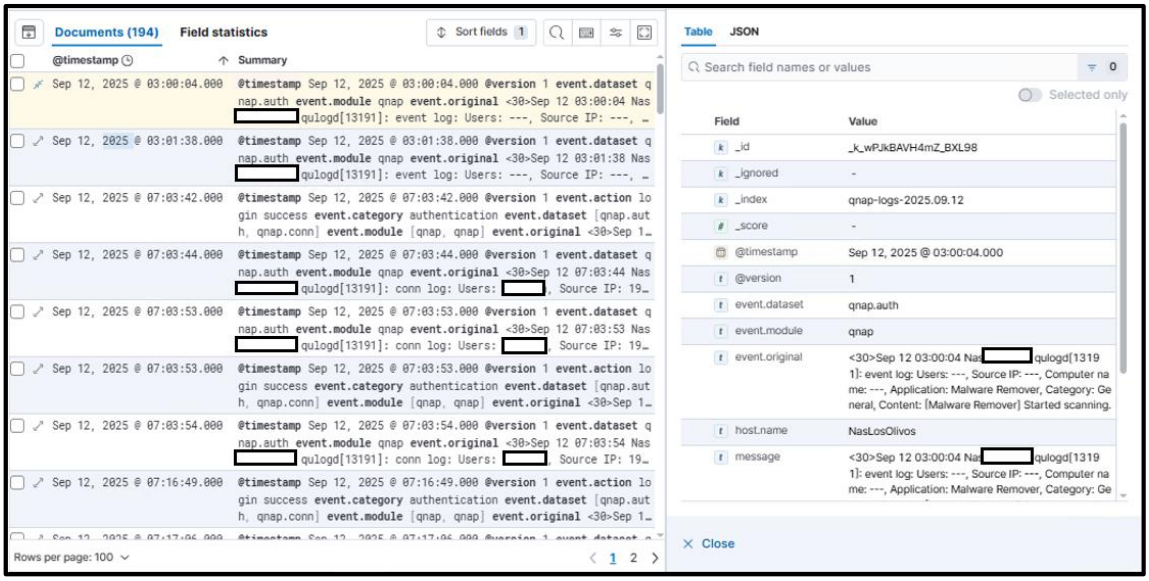
Servidor NAS QNAP

En la Figura 46, se observa la interfaz de Kibana dentro del módulo Discover, donde se visualizan de manera detallada los eventos recibidos desde el servidor NAS QNAP. Cada registro contiene el timestamp exacto de generación del evento, el cual permite validar la sincronización temporal entre la fuente y el SIEM. Asimismo, se aprecia la correcta clasificación del evento mediante los campos estándar del Elastic Common Schema (ECS), tales como event.dataset, event.module, event.original y message, confirmando que los registros han sido parseados, enriquecidos y normalizados adecuadamente.

Así también, en la parte derecha de la figura, la vista en formato Table evidencia que cada entrada de log incluye información propia del dispositivo, como el identificador del host (host.name: Nas***), el módulo correspondiente (event.module: qnap) y la categoría del evento (event.dataset: qnap.auth). Además, se aprecia el contenido original del log en el campo event.original, el cual conserva el mensaje nativo enviado por el dispositivo para fines de trazabilidad y auditoría.

Figura 46

Recepción de Logs Servidor NAS QNAP



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

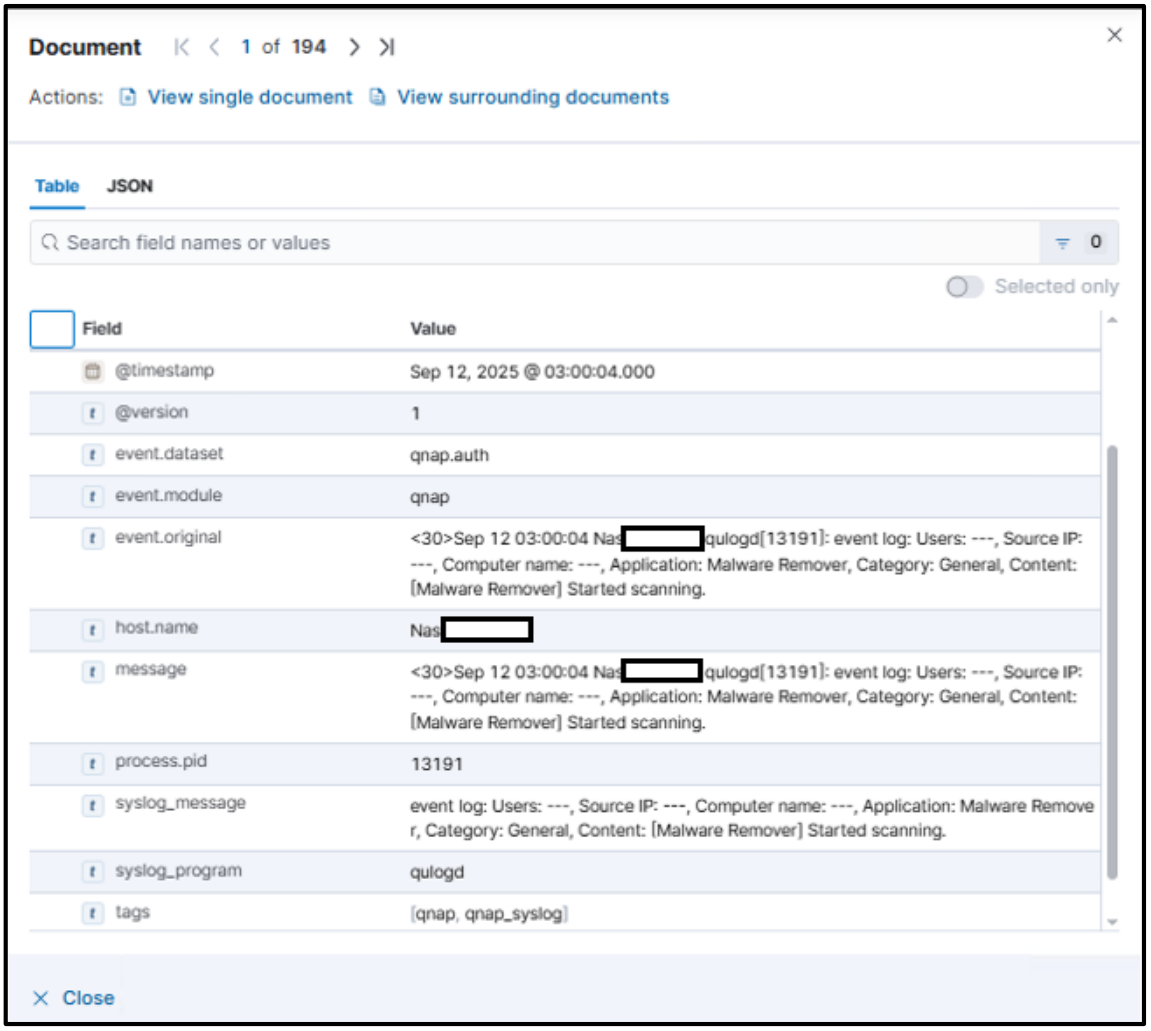
Por otro lado, en la Figura 47 se presenta la visualización detallada de un evento individual proveniente del servidor NAS QNAP dentro del módulo Discover de Kibana, utilizando el formato de vista Table. Este nivel de detalle permite observar cómo el SIEM procesa, clasifica y normaliza los registros enviados por el dispositivo, siguiendo los lineamientos del Elastic Common Schema (ECS).

Se aprecia el campo @timestamp, el cual refleja la fecha y hora exacta en que el evento fue generado por el QNAP, lo que permite validar la exactitud en el tiempo requerida para los procesos de correlación y análisis. Los campos event.dataset y event.module muestran que el log ha sido correctamente categorizado bajo los módulos qnap.auth y qnap, respectivamente, confirmando la identificación precisa del tipo de evento, en este caso asociado a autenticación y seguridad.

El campo host.name identifica al dispositivo de origen (Nas***), mientras que syslog_program y process.pid especifican el proceso responsable del registro (en este caso, qulogd), lo cual evidencia que la ingesta respeta la estructura nativa del servicio syslog del QNAP.

Figura 47

Detalle de Recepción de Log Servidor NAS QNAP



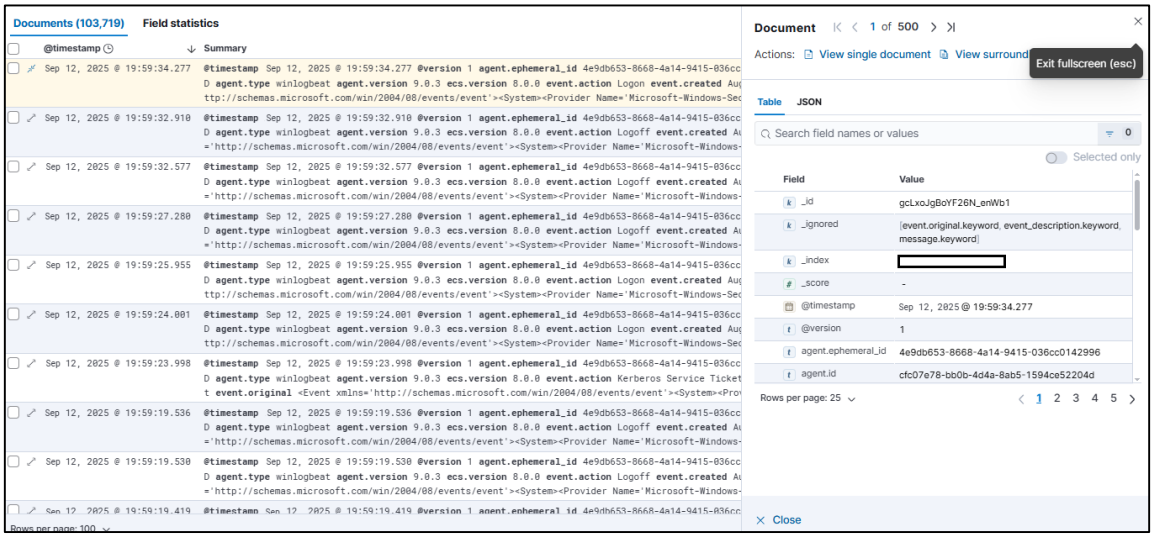
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Servidor Active Directory

En la Figura 48, se muestra la interfaz del módulo Discover de Kibana, donde se visualiza el conjunto de eventos provenientes del servidor Windows que desempeña el rol de Controlador de Dominio (Active Directory). En esta vista se aprecia un volumen significativo de registros (más de 100 mil eventos), lo cual evidencia una comunicación continua y estable entre el agente de ingesta (Winlogbeat) instalado en el servidor y el SIEM basado en ELK Stack.

Figura 48

Recepción de Logs Servidor Active Directory



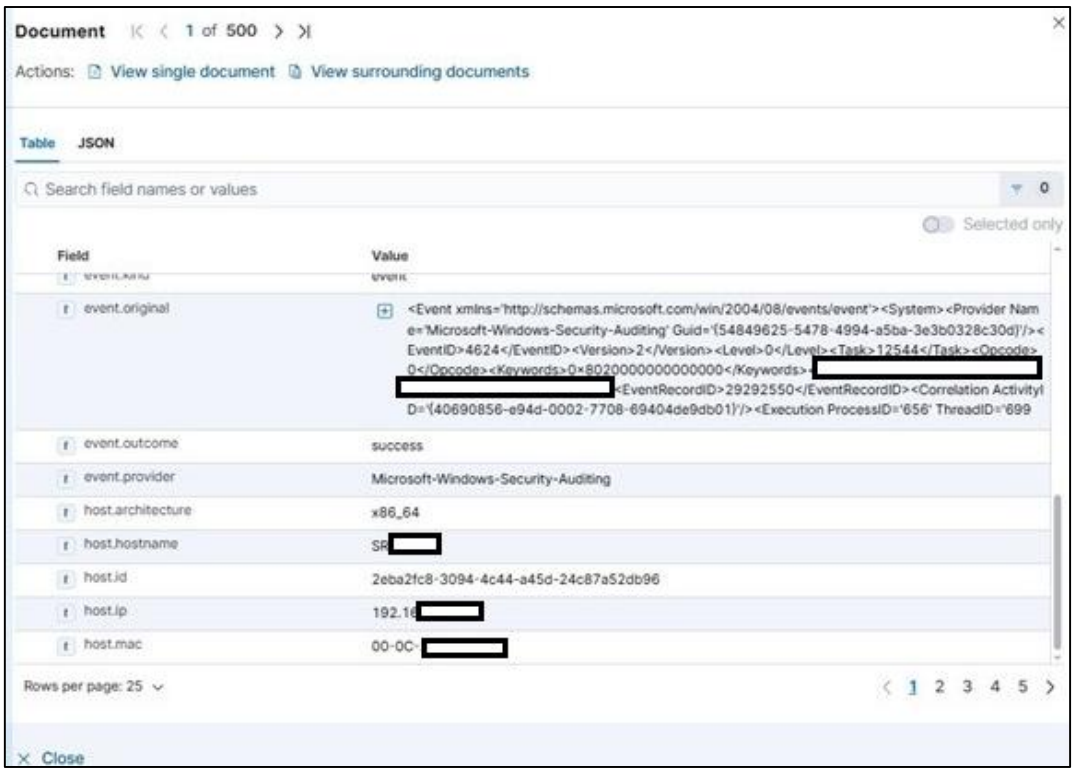
Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

En la parte izquierda de la figura se observa la columna de @timestamp, que permite verificar la sincronización temporal y la frecuencia de generación de eventos provenientes del servicio de autenticación y gestión de identidades de Windows. Los mensajes presentados en la sección de resumen muestran actividades típicas del Active Directory, tales como eventos de logon, logoff, auditorías de seguridad, y ejecución de procesos del propio dominio, reflejando que se están capturando correctamente los eventos críticos que intervienen en la administración de cuentas, sesiones y servicios de autenticación Kerberos.

Asimismo, en la Figura 49 se muestra la vista Table de un evento individual donde se confirma la correcta normalización bajo el esquema ECS. Se pueden apreciar el campo event.original que muestra detalles nativos del evento generado por los servicios de autenticación de Windows, preservando la información clave para auditoría y trazabilidad del dominio. Estos eventos incluyen información del Security Provider, el Event ID correspondiente y la descripción original proveniente de los logs del subsistema de seguridad de Microsoft.

Figura 49

Detalle de Recepción de Log Servidor Active Directory



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Una vez completada la validación de las integraciones, se procede a evaluar la disponibilidad del SIEM de manera detallada.

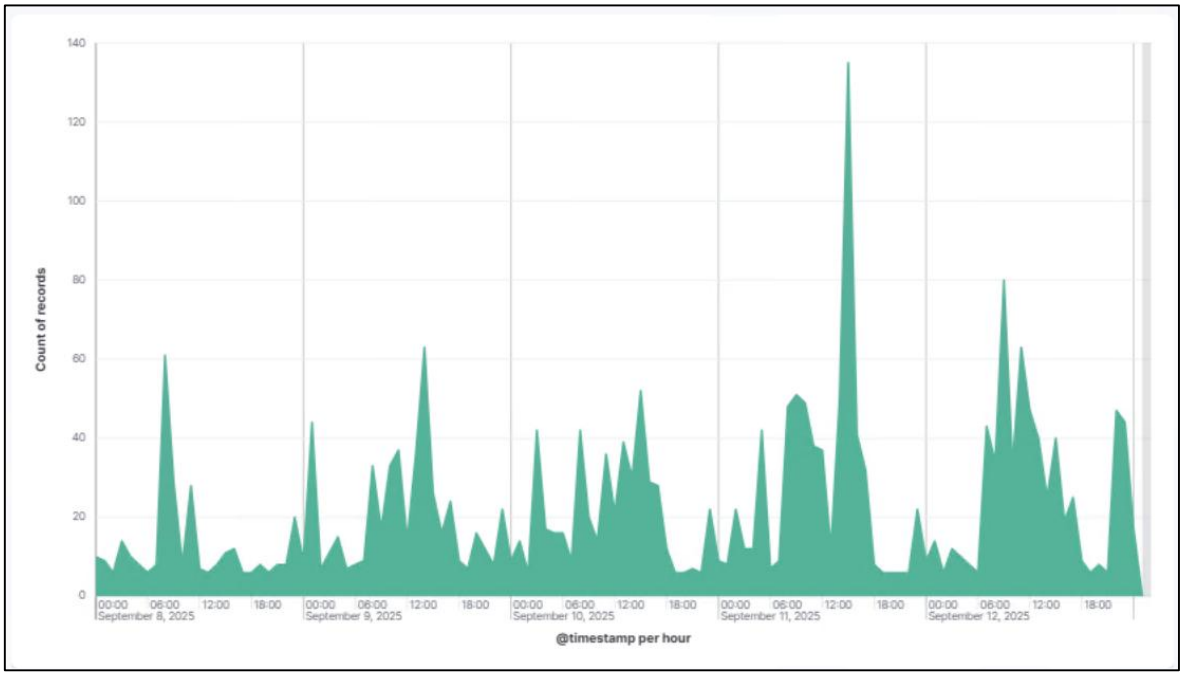
Disponibilidad del SIEM

Se llevó a cabo un monitoreo continuo de la plataforma SIEM durante un periodo equivalente a una semana laboral (cinco días), con el propósito de verificar su estabilidad operativa, así como la disponibilidad efectiva del servicio a lo largo del tiempo.

Por lo tanto, en la Figura 50, se muestra el comportamiento registrado, evidenciando una disponibilidad superior al 99.5 %, conforme al criterio establecido en el plan de pruebas.

Figura 50

Gráfica de Disponibilidad del SIEM



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Como se observa en la imagen, se evaluó la disponibilidad operativa del SIEM durante una semana laboral completa (cinco días), comprendida entre el 8 y el 12 de septiembre de 2025. La gráfica representa el count of records, es decir, la cantidad de paquetes de logs recibidos por hora dentro de dicho periodo de análisis. La continuidad en la recepción de estos registros, sin interrupciones ni vacíos temporales, evidencia que el sistema mantuvo un flujo constante de ingesta de datos.

Dicho esto, se procede con el cálculo de la variable del indicador de logro del objetivo específico mencionado en la sección 3.1.3.3.

Entonces si aplicamos la formula señalada para este criterio obtenemos lo siguiente:

Tiempo Operativo: 120 horas

Tiempo Total: 5 días × 24 horas = 120 horas

$$Disponibilidad = \frac{120\ horas}{120\ horas} \times 100 = 100\%$$

Este comportamiento confirma que el SIEM operó con una disponibilidad del 100 % durante el intervalo evaluado, garantizando la integridad del proceso de monitoreo y la confiabilidad del entorno.

Concluido esto se procede con el cálculo de la tasa de procesamiento de eventos.

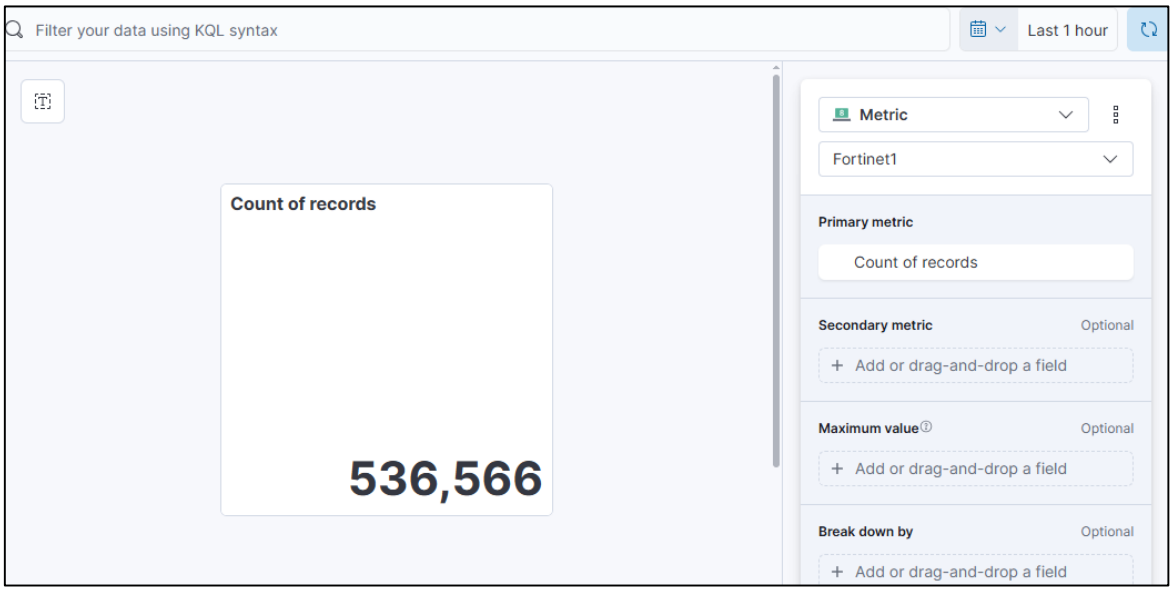
Capacidad de procesamiento de eventos del SIEM

Para ello, se analizó la tasa de eventos por segundo (EPS) generada por las cuatro fuentes integradas al SIEM. Como parte de esta evaluación, se realizó el recuento de registros procesados durante un periodo de una hora para cada uno de los equipos monitoreados.

En la siguiente figura se presentan los contadores de registros correspondientes al dispositivo Fortinet 1 durante el intervalo de tiempo de una hora.

Figura 51

Tasa De Procesamiento EPS (Events Per Second) – Firewall 1

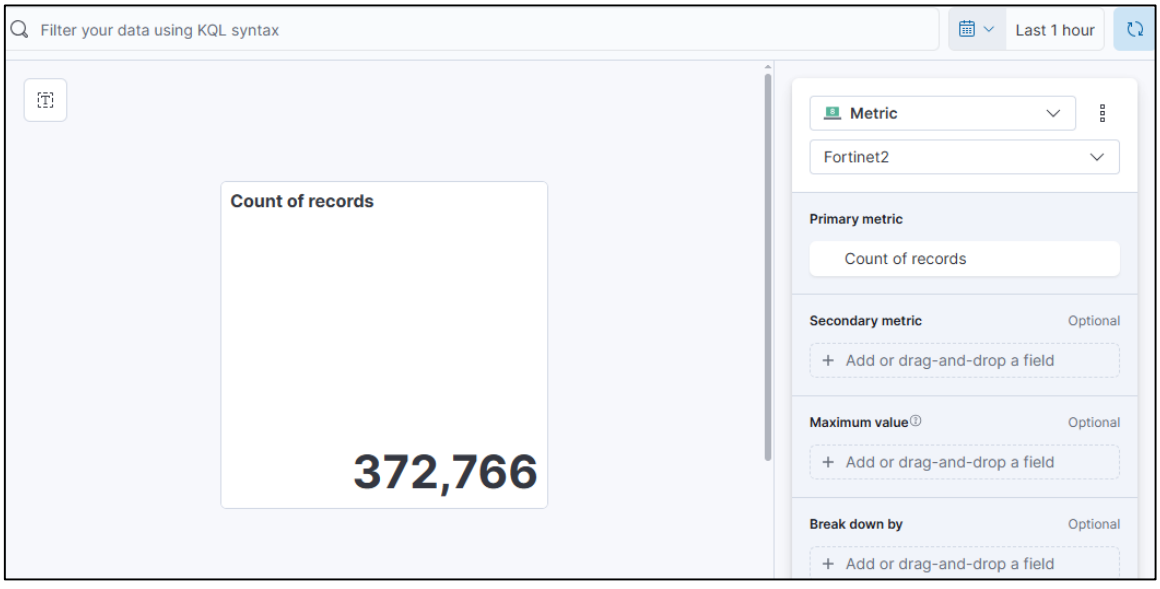


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Así también, se evidencia los contadores de los registros del Firewall 2, en un periodo de tiempo de una hora.

Figura 52

Tasa De Procesamiento EPS (Events Per Second) – Firewall 2

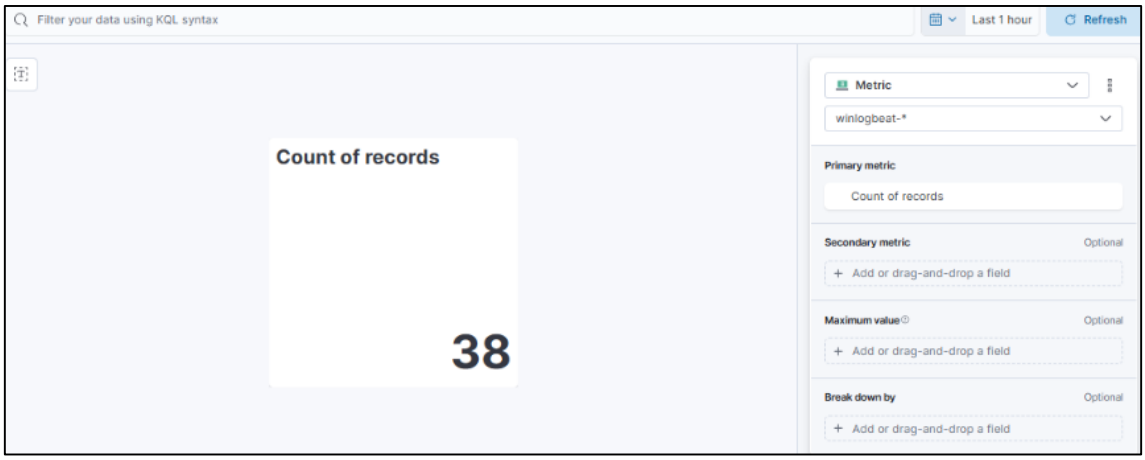


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

A continuación, se evidencia los contadores de los registros del AD (Windows Server) en un periodo de tiempo de una hora.

Figura 53

Tasa De Procesamiento EPS (Events Per Second) – Active Directory

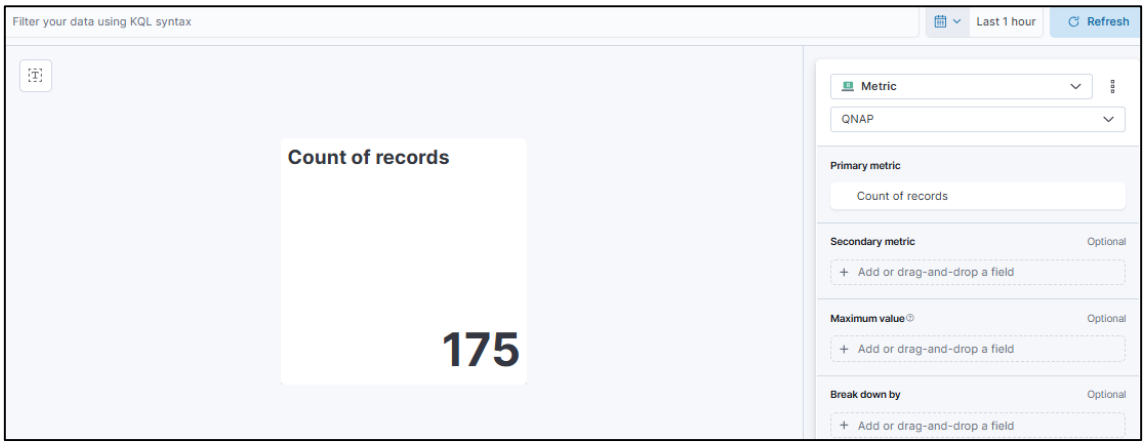


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Por último, se evidencia los contadores de los registros del QNAP en un periodo de tiempo de una hora.

Figura 54

Tasa De Procesamiento EPS (Events Per Second) – QNAP



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Es así que, considerando el periodo de una hora (3 600 segundos), el SIEM procesó un total de 909 545 eventos provenientes de los cuatro dispositivos integrados, es decir, la suma de los registros generados por los dos firewalls y los dos servidores.

Entonces usando la fórmula de la variable, tenemos:

- Total de eventos procesados = 909 454
- Total de segundos en una hora = 3600 s

$$EPS\ Promedio = \frac{909\ 454}{3600} = 253\ EPS$$

Este resultado indica que el SIEM soporta un promedio mayor o igual a 155 eventos por segundo.

3.2.3.3 Análisis e Interpretación de los Resultados

Los resultados obtenidos durante la ejecución del plan de pruebas permiten concluir que los criterios de aceptación establecidos para el Objetivo Específico 3 fueron cumplidos de manera satisfactoria. En primer lugar, se corroboró la integración del 100 % de las fuentes de logs mediante la verificación directa en Kibana, tanto en las vistas de Data View como en las representaciones gráficas del parseo individual de cada dispositivo integrado (dos firewalls y dos servidores). La correcta normalización y visualización de los campos provenientes de cada fuente evidenció que el SIEM fue capaz de recibir, procesar y estructurar adecuadamente todos los registros generados, cumpliendo con el criterio de integración total.

En relación con la disponibilidad del SIEM, el continuo monitoreo efectuado durante un periodo equivalente a una semana laboral (120 horas) mostró una ingesta estable y sostenida de eventos, sin interrupciones ni ausencia de datos. La persistencia en la llegada de registros permitió confirmar una disponibilidad operativa del 100 %, superando el umbral mínimo establecido de ≥ 99.5 %. Este resultado refleja una estabilidad adecuada de la plataforma y garantiza la continuidad del proceso de recolección y análisis de eventos.

Por último, respecto a la capacidad de procesamiento, se realizó un conteo del número total de eventos procesados por cada equipo en un periodo fijo de una hora. Aplicando la fórmula de cálculo del EPS (eventos por segundo), es decir, la división del total de

registros entre los 3600 segundos que conforman una hora, se obtuvo un valor promedio de 253 EPS. Este resultado supera ampliamente el criterio definido (≥ 155 EPS), lo cual demuestra que la infraestructura SIEM implementada posee la capacidad suficiente para procesar los volúmenes de datos requeridos en el entorno actual, manteniendo niveles adecuados de rendimiento.

En conjunto, estos resultados permiten confirmar que la solución SIEM basada en tecnologías Open Source fue integrada de manera correcta, opera con un nivel alto de disponibilidad y cuenta con un rendimiento óptimo para el procesamiento de eventos, logrando los objetivos planteados.

3.2.4 Resultado del Plan de Prueba del Objetivo Específico N°4

3.2.4.1 Definición y Alcance del Plan de Pruebas

Tabla 19

Objetivo específico 4, Definición y Alcance del Plan de Pruebas

Objetivo Específico	Desarrollar tres casos de uso basados en el marco MITRE ATT&CK para la detección de eventos de seguridad en un SIEM Open Source.		
I. Plan de Pruebas del Objetivo Específico			
Fecha de Ejecución	16/09/2025	**Versión**	V1
Patrocinador	Gerente de Sistemas		
Responsable del Plan de Pruebas	Coordinador de TI		
Objetivo del Plan de Pruebas	- Validar la creación de tres casos de uso en la plataforma SIEM, correlacionados con tácticas, técnicas y procedimientos (TTPs) del marco MITRE ATT&CK. - Número de alertas detectados igual o superior a tres. - Lograr un tiempo promedio de detección menor o igual a 5 minutos.		
II. Detalle del Plan de Pruebas			
Alcance	El alcance se centra en confirmar la capacidad de detección de la integración del marco MITRE ATT&CK en el SIEM mediante		

	la ejecución de pruebas funcionales basadas en tres casos de uso específicos, cada uno asociado a Tácticas y Técnicas (TTPs) del marco.
Duración del Plan de Pruebas	6h
Método de Prueba	Simulación Controlada (Simulation Test) Se ejecutan ataques controlados, para verificar que el SIEM detecte, clasifique y correlacione eventos con su técnica MITRE ATT&CK correspondiente.
Actividades a Ejecutar	1. Seleccionar las tres TTPs del marco MITRE ATT&CK: T1110.003 - Brute Force: Password Spraying, T1110.001 - Brute Force: Password Guessing, T1531 - Account Access Removal. 2. Diseñar los casos de uso correspondientes en el SIEM. 3. Configurar reglas de correlación en la plataforma Elastic SIEM. 4. Generar eventos simulados o reproducidos de logs reales en entornos controlados. 5. Verificar la detección automática de las alertas y la correlación con la TTP asociada. 6. Medir el tiempo medio de detección (TTD) desde la generación del evento hasta la alerta. 7. Mostrar resultados finales

3.2.4.2 Ejecución y Desarrollo del Plan de Pruebas

Tabla 20

Objetivo específico 4, Ejecución del Plan de Pruebas

III. Ejecución del Plan de Pruebas	
Escenario	Pruebas funcionales en el SIEM configurado, simulando comportamientos de ataque controlados que correspondan a técnicas del marco MITRE ATT&CK, con monitoreo continuo del sistema y registro de alertas generadas.

<table>
<tr><td>Herramienta</td><td colspan="3">CLI Ubuntu, documentación oficial Elastic, Elastic Security, MITRE ATT&CK Navigator (matriz y requisitos), Kibana Analytics Discover, Elastic Analitics Dashboards, MITRE ATT&CK Navigator</td></tr>
<tr><td rowspan="4">Criterios de Aceptación</td><td>Detalle</td><td>Estado</td><td>Porcentaje</td></tr>
<tr><td>- Creación exitosa de 3 casos de uso correlacionados con MITRE ATT&CK.</td><td>Realizado</td><td>100%</td></tr>
<tr><td>- Detección de 3 o más alertas, con trazabilidad completa hacia la TTP correspondiente del marco MITRE ATT&CK.</td><td>Realizado</td><td>100%</td></tr>
<tr><td>- Tiempo medio de detección (TTD) ≤ 5 minutos.</td><td>Realizado</td><td>100%</td></tr>
<tr><td>Resultados</td><td colspan="2">Realizado</td><td>100%</td></tr>
<tr><td rowspan="4">Participantes del Plan de Pruebas</td><td>Puesto</td><td colspan="2">Fecha</td></tr>
<tr><td>Jefe de Infraestructura</td><td colspan="2">16/09/2025 al 17/09/2025</td></tr>
<tr><td>Coordinador de TI</td><td colspan="2">16/09/2025 al 17/09/2025</td></tr>
<tr><td>Analista de Ciberseguridad</td><td colspan="2">16/09/2025 al 17/09/2025</td></tr>
<tr><td>Aceptado / Rechazado</td><td colspan="3">ACEPTADO</td></tr>
</table>

IV. Desarrollo del Plan de Pruebas

Con la implementación de los casos de uso descritos en los puntos 3.1.4.1, 3.1.4.2 y 3.1.4.3, esta etapa del plan de pruebas describe las validaciones llevadas a cabo para verificar su correcta integración en el sistema.

Creación exitosa de casos de uso

Tras configurar las reglas de detección en el SIEM, se procedió a validar que cada caso de uso definido en función del marco MITRE ATT&CK ha sido implementado de manera correcta. El objetivo de esta fase consistió en comprobar que las reglas se encontraran debidamente habilitadas y vinculadas a las tácticas y técnicas contempladas para el monitoreo de eventos de seguridad en la infraestructura analizada.

La Figura 55 presenta el listado de reglas configuradas en Kibana desde el módulo Rules, donde se evidencia la implementación de los casos de uso correspondientes a las fuentes Fortinet, Active Directory y NAS QNAP.

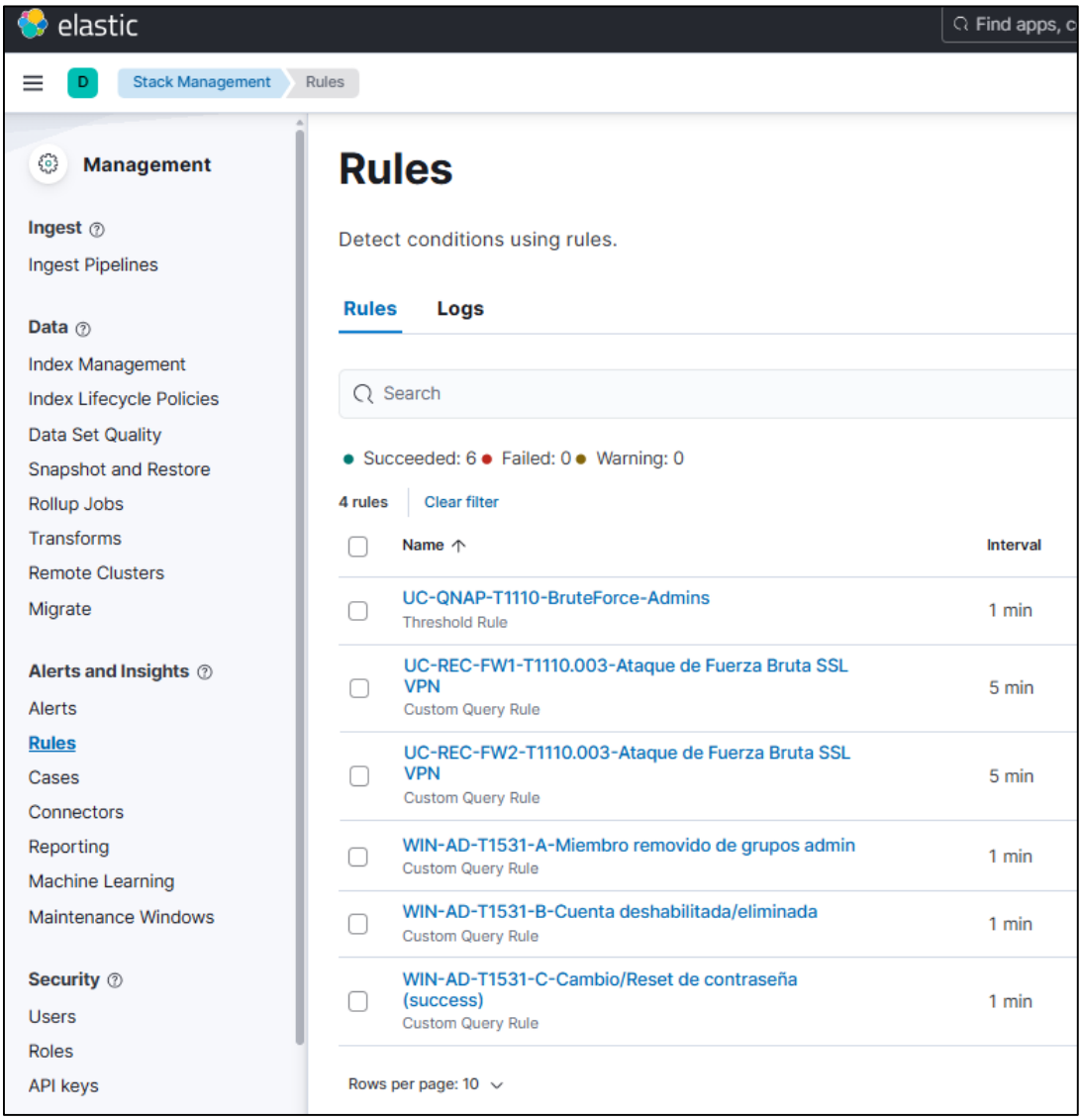
Entre las reglas registradas se encuentran:

- UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN,
- UC-REC-FW2-T1110.003 – Ataque de Fuerza Bruta SSL VPN,
- UC-QNAP-T1110-BruteForce-Admins,
- WIN-AD-T1531-A – Miembro removido de grupos admin,
- WIN-AD-T1531-B – Cuenta deshabilitada/eliminada y
- WIN-AD-T1531-C – Cambio/Reset de contraseña (éxito).

Cada una de estas reglas fue asociada a tácticas específicas del marco MITRE ATT&CK, como Credential Access e Impact.

Figura 55

Reglas de detección configuradas en el SIEM ELK Stack



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Como se aprecia en la figura, la totalidad de las reglas creadas en el SIEM guarda correspondencia directa con los casos de uso definidos en el punto 3.1.4, lo que confirma que la configuración se encuentra alineada con los objetivos de detección establecidos.

A partir de este punto, se presenta la ejecución de las simulaciones controladas realizadas para cada caso de uso implementado, detallando los eventos generados y las alertas registradas por el SIEM durante cada prueba.

Para el caso de uso 1: Detección de ataque de fuerza bruta SSL VPN

Táctica: Credential Access

Técnica (ID / Nombre): T1110.003 - Brute Force: Password Spraying

Detección de Caso de Uso:

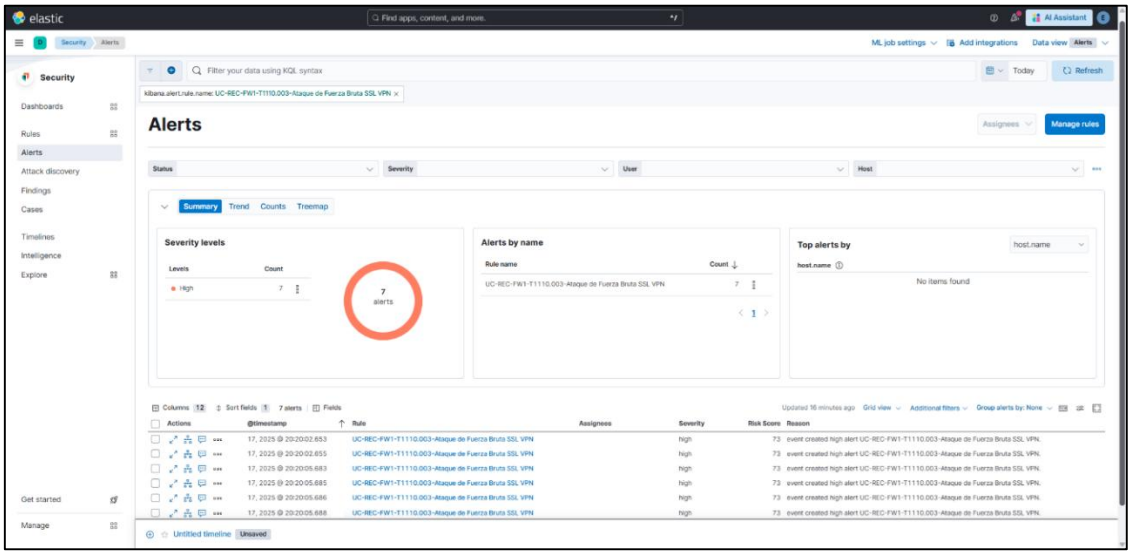
FIREWALL 1:

Nombre de la regla: UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN

En la Figura 56, se muestra el resultado de la simulación controlada de intentos fallidos de autenticación SSL VPN ejecutada hacia el Firewall 1. A medida que los accesos incorrectos fueron registrados, el SIEM correlacionó los eventos y generó 7 alertas de severidad alta, como se muestra en el panel principal. La visualización evidencia la repetición de intentos fallidos, el volumen total de alertas activadas por la regla y el comportamiento característico de un ataque de fuerza bruta tipo Password Spraying, confirmando que la lógica del caso de uso detecta correctamente la secuencia anómala de autenticaciones fallidas.

Figura 56

Detección de Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

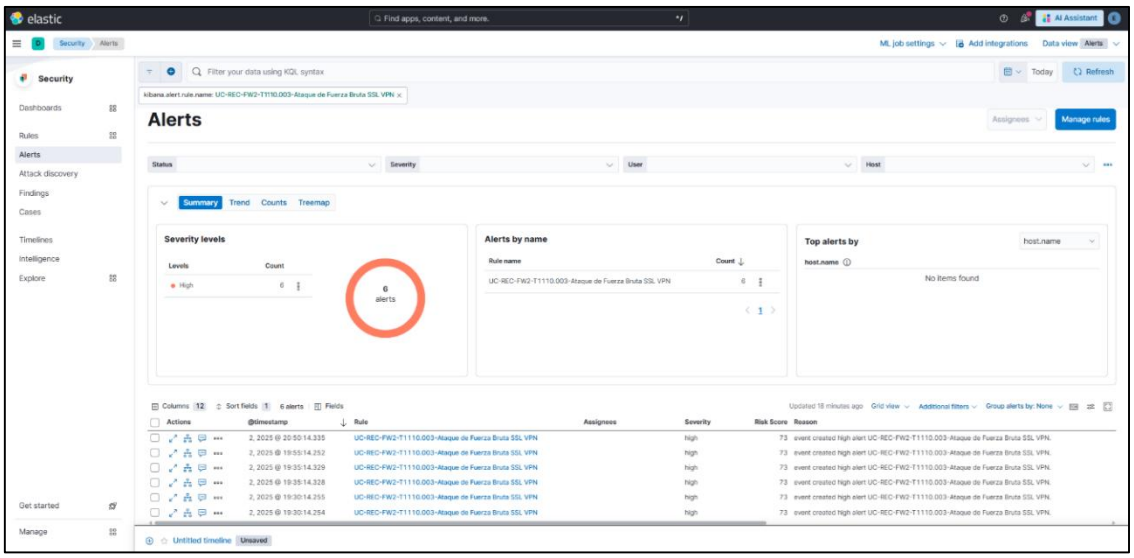
FIREWALL 2:

Nombre de la regla: UC-REC-FW2-T1110.003-Ataque de Fuerza Bruta SSL VPN

En la Figura 57, se muestra la ejecución del escenario de prueba sobre el firewall 2. Al igual que el caso anterior, los intentos fallidos de conexión SSL VPN fueron capturados y procesados por el SIEM, generando 6 alertas de severidad. El gráfico circular y el listado detallado de alertas en la parte inferior muestran la recurrencia de fallos y el volumen elevado de eventos relacionados con la regla. Esta evidencia confirma que el caso de uso opera consistentemente en ambos firewalls y que el SIEM es capaz de identificar, en tiempo real, patrones asociados a ataques de fuerza bruta en el servicio SSL VPN.

Figura 57

Detección de Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 2



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Una vez completadas estas validaciones para los firewalls, se procede a evaluar el siguiente criterio establecido.

Tiempo Medio de Detección MTTD:

FIREWALL 1:

Como se vio previamente, para este caso de uso se simuló un ataque de Fuerza Bruta SSL VPN (Técnica T1110.003 en MITRE ATT&CK) dirigido al Firewall 1, generando múltiples intentos fallidos de autenticación con el objetivo de evaluar el tiempo de

reacción del SIEM ante este tipo de eventos. De ahí que, para cada alerta se registró tanto la hora exacta en la que ocurrió el intento fallido como la hora en la que el SIEM emitió la correspondiente detección.

De esta manera, se muestra el listado de alertas generadas durante la prueba:

Tabla 21

TTD de alertas generadas por Caso de Uso de Ataque de Fuerza Bruta SSL VPN – Firewall 1

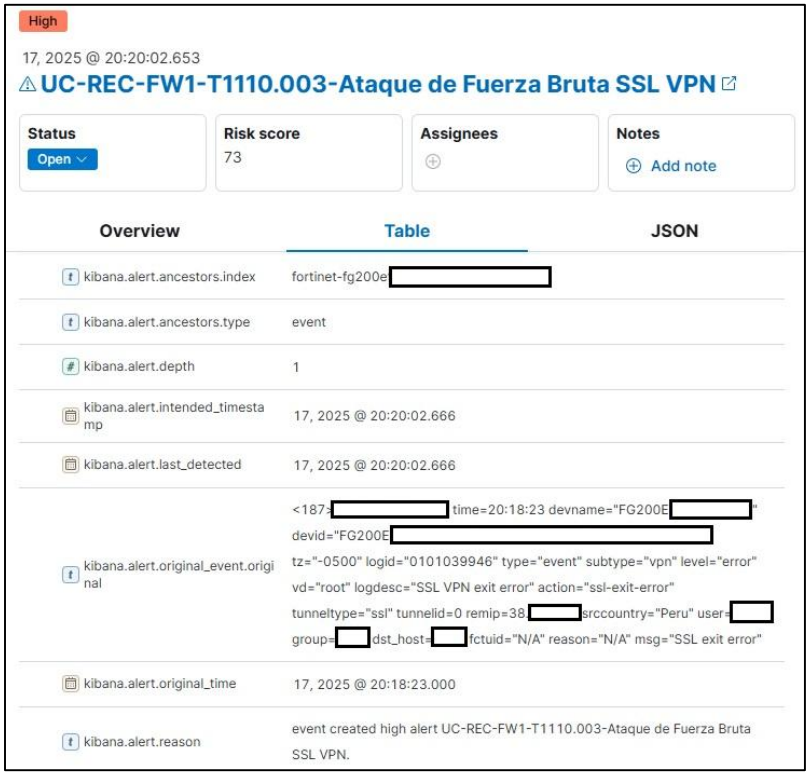
Alerta	Hora de inicio del evento (kibana.alert.original_time)	Hora de detección de la alerta (kibana.alert.last_detected)	TTD (segundos)
Alerta 1	20:18:23	20:20:02	99 s
Alerta 2	20:18:23	20:20:02	99 s
Alerta 3	20:18:31	20:20:05	94 s
Alerta 4	20:18:31	20:20:05	94 s
Alerta 5	20:19:01	20:20:05	64 s
Alerta 6	20:19:01	20:20:05	64 s
Alerta 7	20:19:35	20:20:08	33 s

Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

A continuación, en la Figura 58 se presenta una muestra representativa correspondiente a la Alerta 1, en la cual se visualizan los campos principales generados porel SIEM junto on el evento original recibido desde el firewall. Se incluye únicamente esta alerta como evidencia puntual, dado que las demás registradas durante la simulación presentan la misma estructura y nivel de detalle técnico.

Figura 58

Evidencia de alerta generada por el caso de uso UC-REC-FW1-T1110.003 – Ataque de Fuerza Bruta SSL VPN



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Una vez establecido lo anterior, se procede a calcular la variable definida en la sección 3.1.4, correspondiente al tiempo medio de detección.

Por lo tanto, el cálculo del Tiempo Medio de Detección (MTTD) fue el siguiente:

$$MTTD = \frac{99 + 99 + 94 + 94 + 64 + 64 + 33}{7}$$

$$MTTD = 78.14\ segundos \approx 1\ minuto\ y\ 18\ segundos$$

Es así como el Firewall 1 obtuvo un tiempo medio de detección de aproximadamente 1 minuto y 18 segundos, valor ampliamente inferior al criterio de aceptación establecido (TTD ≤ 5 minutos). En consecuencia, el caso de uso cumple satisfactoriamente con el objetivo de detección temprana frente a ataques de fuerza bruta en el servicio SSL VPN.

FIREWALL 2:

Como también se vio previamente, para este caso de uso se simuló un ataque de Fuerza Bruta SSL VPN (Técnica T1110.003 en MITRE ATT&CK) dirigido al Firewall 2, generando múltiples intentos fallidos de autenticación con el fin de validar el tiempo de reacción del SIEM ante este tipo de eventos. Es así que, para cada alerta se registró la hora exacta en la que ocurrió el intento fallido y la hora en la que el SIEM generó la detección correspondiente.

En consecuencia, se muestra el listado de las alertas generadas durante la prueba:

Tabla 22

Listado de alertas generadas de ataque de Fuerza Bruta SSL VPN – Firewall 2

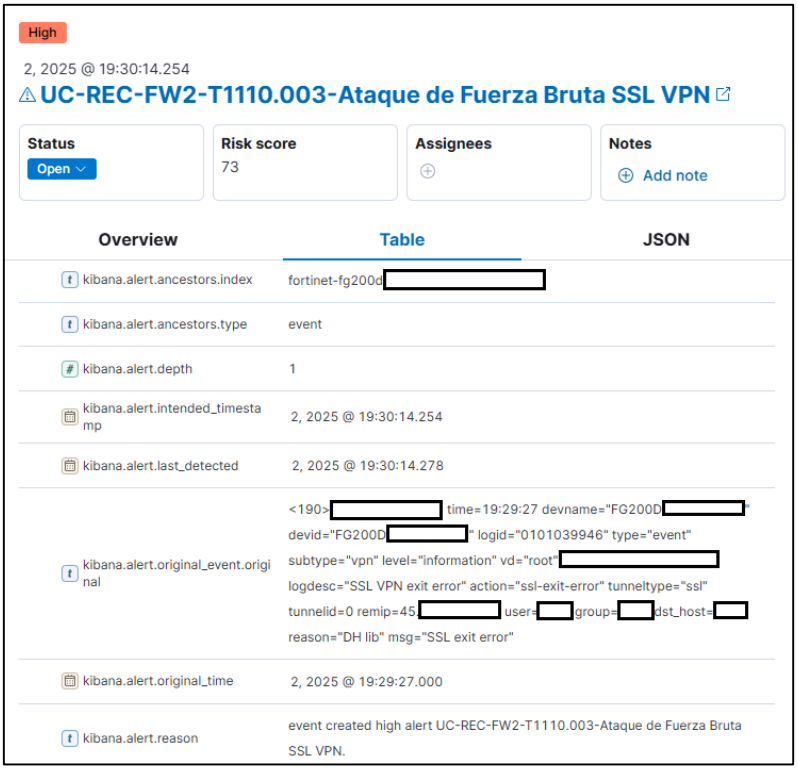
Alerta	**Hora de inicio del evento (kibana.alert.original_time)**	**Hora de detección de la alerta (kibana.alert.last_detected)**	**TTD (segundos)**
Alerta 1	19:29:27	19:30:14	47 s
Alerta 2	19:29:28	19:30:14	46 s
Alerta 3	19:30:49	19:35:14	256 s
Alerta 4	19:32:14	19:35:14	180s
Alerta 5	19:50:14	19:55:14	300s
Alerta 6	20:45:14	20:50:14	300s

Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

A continuación, se presenta en la Figura 59 una muestra representativa correspondiente a la Alerta 1, en la cual se visualizan los campos principales generados por el SIEM junto con el evento original recibido desde el firewall. Se incluye únicamente esta alerta como evidencia puntual, dado que las demás registradas durante la simulación presentan la misma estructura y nivel de detalle técnico.

Figura 59

Evidencia de alerta generada por el caso de uso UC-REC-FW2-T1110.003 – Ataque de Fuerza Bruta SSL VPN



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Una vez establecido lo anterior, se procede a calcular la variable definida en la sección

3.1.4, correspondiente al tiempo medio de detección.

Por lo tanto, el cálculo del Tiempo Medio de Detección (MTTD) es el siguiente:

$$MTTD = \frac{47 + 46 + 256 + 180 + 300 + 300}{6}$$

$$MTTD = 189.66\ segundos \approx 3\ minuto\ y\ 10\ segundos$$

De ahí que, el Firewall 2 obtuvo un tiempo medio de detección aproximadamente de 3 minutos y 10 segundos, valor que se encuentra muy por debajo del criterio de aceptación establecido (TTD $\leq$ 5 minutos). Por lo tanto, el caso de uso cumple satisfactoriamente con el objetivo de detección temprana para ataques de fuerza bruta SSL VPN.

Caso de uso 2: Detección de múltiples intentos fallidos de inicio de sesión por parte de administradores

Táctica: Credential Access

Técnica (ID / Nombre): T1110.001 - Brute Force: Password Guessing

Detección de Caso de Uso:

NAS QNAP

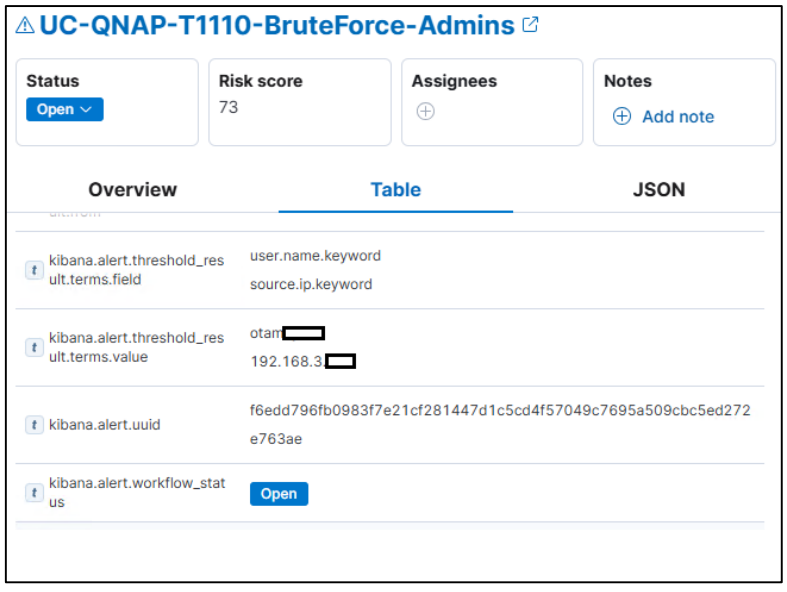
Nombre de la regla: UC-QNAP-T1110-BruteForce-Admins

Una vez establecida la regla de detección correspondiente al caso de uso, se procedió a ejecutar una simulación del ataque de fuerza bruta, específicamente del subtipo Password Guessing.

Para esta simulación se ha intentado acceder hacia el servidor Nas QNAP desde una computadora con IP 192.168.3.** con un usuario de privilegios administrativos el cual es otam***. Tal como se muestra en la siguiente figura.

Figura 60

Detección de Caso de Uso Múltiples intentos fallidos de inicio de sesión por parte de administradores

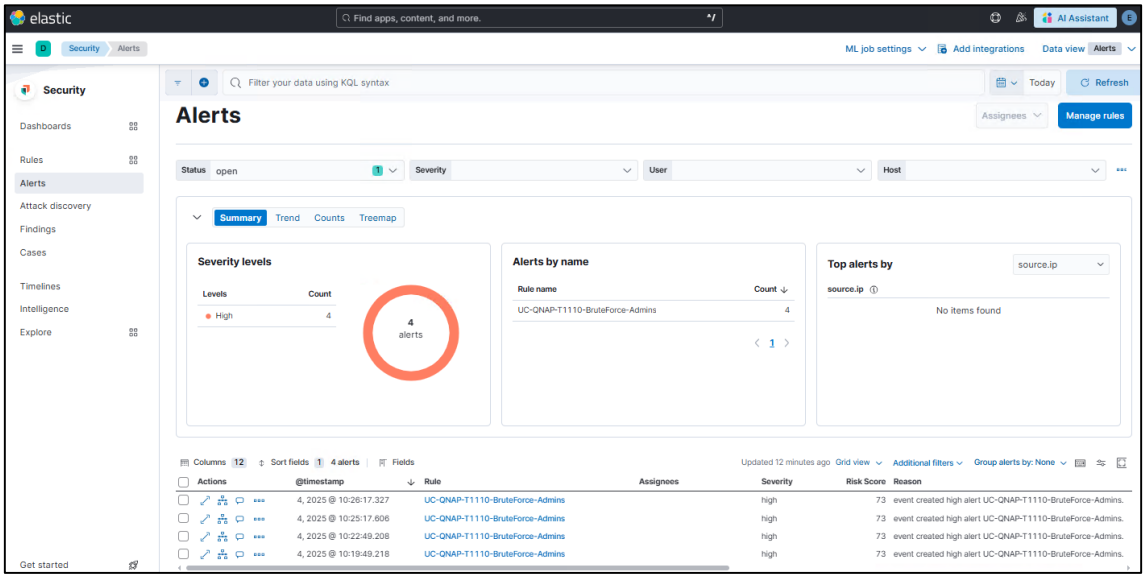


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Debido a esto, podemos ver en la figura a continuación las alertas del caso señalado.

Figura 61

Alertas de detección de Caso de Uso Múltiples intentos fallidos de inicio de sesión por parte de administradores



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Como se muestra en la imagen podemos visualizar cuatro alertas, es decir son los intentos de acceso al QNAP, esto ha demostrado que la regla funciona correctamente y por tanto nuestro caso de uso es adecuado y funcional y alineado en el marco MITRE ATT&CK.

Este caso detecta ataques de fuerza bruta contra cuentas privilegiadas del NAS QNAP. La regla evalúa intentos fallidos de autenticación normalizados a ECS (event.category: authentication, event.outcome: failure, user.name, source.ip) y genera alerta cuando, en una ventana de 2 minutos, se observan 2 o más fallos desde la misma IP contra el mismo usuario administrador. Esto se alinea al marco MITRE ATT&CK: Credential Access T1110 – Brute Force (enfoque password guessing). La alerta incluye campos clave para investigación (host, usuario, IP origen, protocolo) y está pensada para monitorear y contenciones manuales y bloqueo de origen si corresponde.

Una vez completadas estas validaciones, se procede a evaluar el siguiente criterio establecido.

Tiempo Medio de Detección MTTD:

En este caso, para el cálculo del promedio del TTD se ha considerado las alertas que forman parte del mismo escenario de prueba. Por ello, todos los tiempos de TTD obtenidos en las alertas se presentan en el cuadro siguiente.

Tabla 23

Listado de alertas generadas de ataques de Fuerza Bruta hacia las cuentas de administrador -QNAP

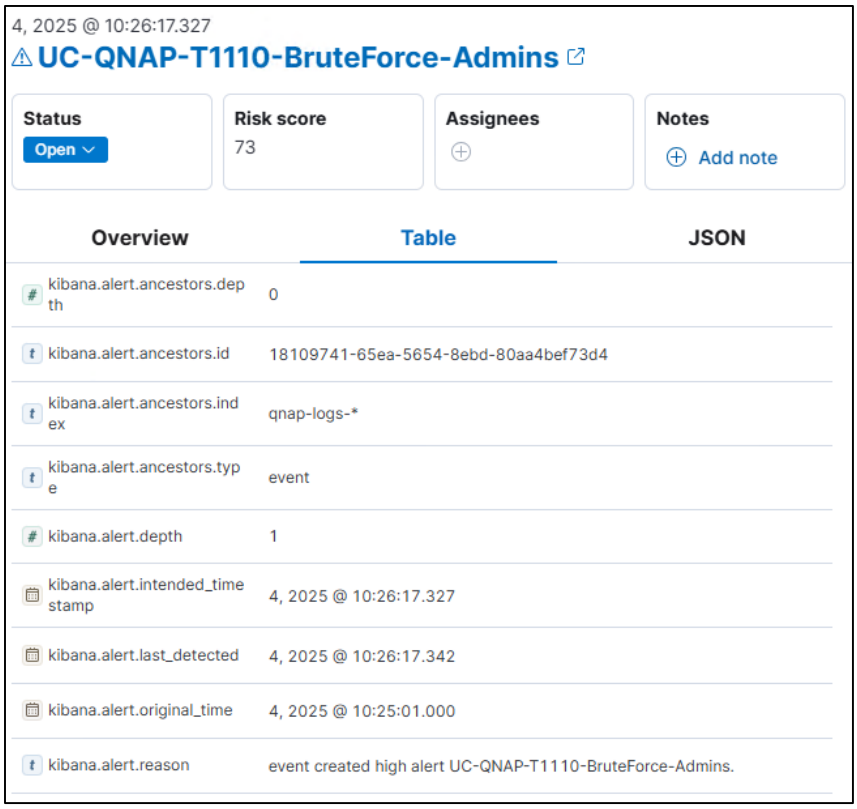
Alerta	Hora de inicio del evento (kibana.alert.original_time)	Hora de detección de la alerta (kibana.alert.last_detected)	TTD (segundos)
Alerta 1	10:25:01	10:26:17	76 s
Alerta 2	10:24:47	10:25:17	30 s
Alerta 3	10:20:47	10:22:49	122 s
Alerta 4	10:18:01	10:19:49	108 s

Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Enseguida, se presenta en la Figura 62 una muestra representativa correspondiente a la Alerta 1, en la cual se visualizan los campos principales generados por el SIEM junto con el evento original recibido desde el firewall. Se incluye únicamente esta alerta como evidencia puntual, dado que las demás registradas durante la simulación presentan la misma estructura y nivel de detalle técnico.

Figura 62

Evidencia de alerta 1 generada por el caso de uso UC-QNAP-T1110-BruteForce-Admins



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Una vez establecido lo anterior, se procede a calcular la variable definida en la sección 3.1.4, correspondiente al tiempo medio de detección.

Por lo tanto, el cálculo del MTTD sería el siguiente:

$$MTTD = \frac{76 + 30 + 122 + 108}{4}$$

$$MTTD = 84\ segundos$$

Esto significa que el tiempo de detección promedio para este caso de uso es de 84 segundos.

Para el caso de uso 3: Detección de Cuenta eliminada o modificada de un grupo administrador

Táctica: Impact

Técnica (ID / Nombre): T1531 – Account Access Removal

Detección de Caso de Uso:

ACTIVE DIRECTORY

A continuación, se evidencia las alertas luego de las simulaciones ejecutadas para cada caso.

a. Remoción de privilegios de grupos administrativos

Para este caso por políticas de la empresa solo se nos permitió usar un usuario de prueba, el cual fue agregado al grupo de administradores. Luego para realizar la simulación ese mismo usuario fue removido.

A continuación, la imagen muestra la descripción del evento, donde señala que se quitó un miembro de un grupo local de una cuenta de administrador.

Figura 63

Detección de Caso de Uso de Remoción de privilegios de grupos administrativos

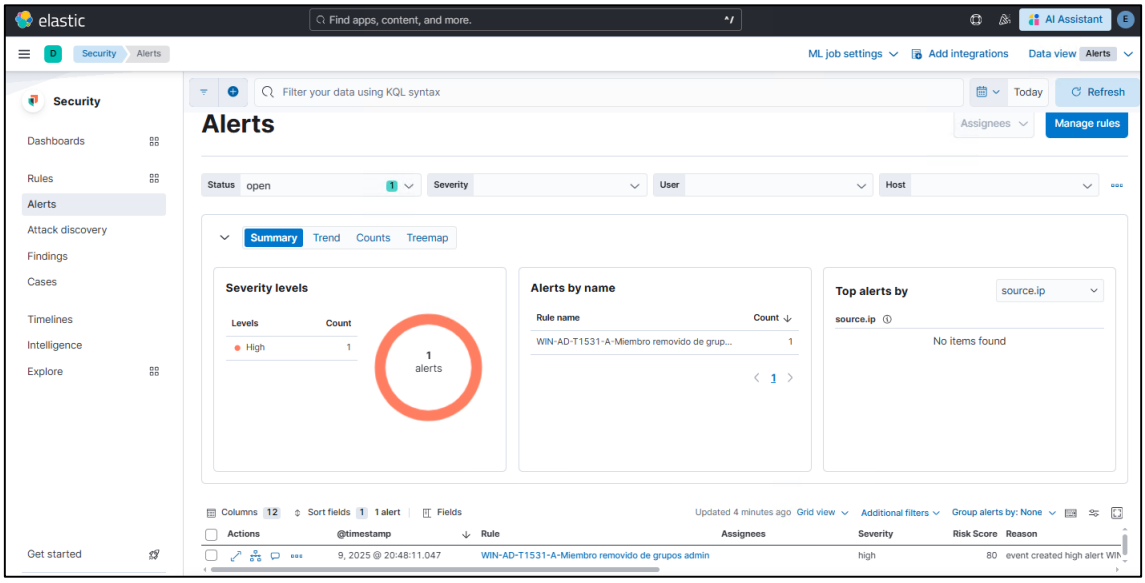


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Por otro lado, también se muestra la alerta señalada en la imagen a continuación:

Figura 64

Alertas de detección de Caso de Uso de Remoción de privilegios de grupos administrativos



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

La imagen muestra la visualización de una alerta en Kibana correspondiente a la ejecución del caso de uso. En la sección central se observa un panel resumen donde se indica que se ha generado una alerta clasificada con severidad “High”, lo cual refleja la criticidad del evento debido al impacto potencial que puede tener la modificación de usuarios en grupos de tipo administrador.

Este resultado valida que la regla configurada para la técnica funciona correctamente, detectando de manera efectiva cambios no autorizados o sospechosos en la composición de grupos administrativos, uno de los mecanismos más sensibles en la administración de cuentas privilegiadas.

b. Cuentas deshabilitadas o eliminadas

Para este subcaso la simulación consistió en eliminar tres usuarios pertenecientes al dominio de la empresa.

A continuación, se muestra una imagen de la descripción del evento de una de las alertas simuladas, como se observa la descripción indica que se eliminó una cuenta de usuario en el Active Directory.

Figura 65

Detección de Caso de Uso de cuentas deshabilitadas o eliminadas

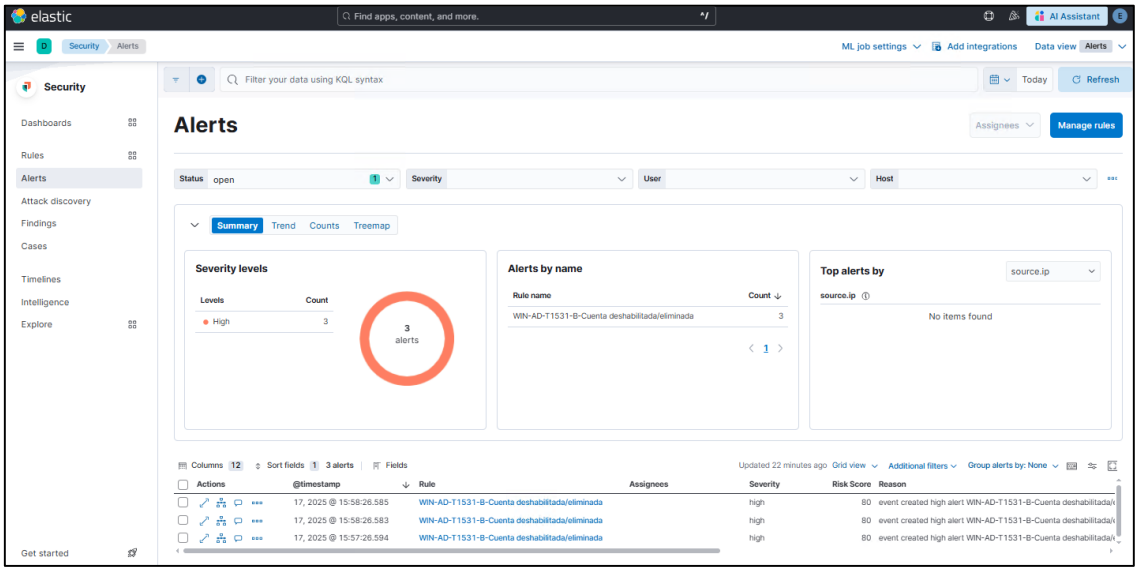


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Por otra parte, se presenta la evidencia de las alertas señaladas:

Figura 66

Alertas de detección de Caso de Uso de cuentas deshabilitadas o eliminadas



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

La imagen presenta el panel de alertas del SIEM en Kibana, donde se visualizan los resultados de la simulación correspondiente al Caso B – Cuenta deshabilitada/eliminada, asociado a la técnica T1531 – Account Access Removal. En el panel principal se observa que se han generado tres alertas con severidad “High”, lo que refleja la criticidad del evento al tratarse de acciones que afectan la disponibilidad y continuidad de cuentas de usuario dentro del Active Directory.

En la sección Alerts by name, se confirma que todas las alertas corresponden a la regla WIN-AD-T1531-B–Cuenta deshabilitada/eliminada, evidenciando que la lógica implementada para monitorear los eventos de seguridad identificados con el ID 4725 (cuenta deshabilitada) e ID 4726 (cuenta eliminada) se activó correctamente durante las pruebas.

c. Manipulación de credenciales (Cambio/Reset de contraseña)

Para esta regla, la simulación consistió en cambiar la contraseña de un usuario con el siguiente nombre: CLAR***, como se muestra en la figura a continuación.

Figura 67

Detección de Caso de Uso de manipulación de credenciales (Cambio/Reset de contraseña)

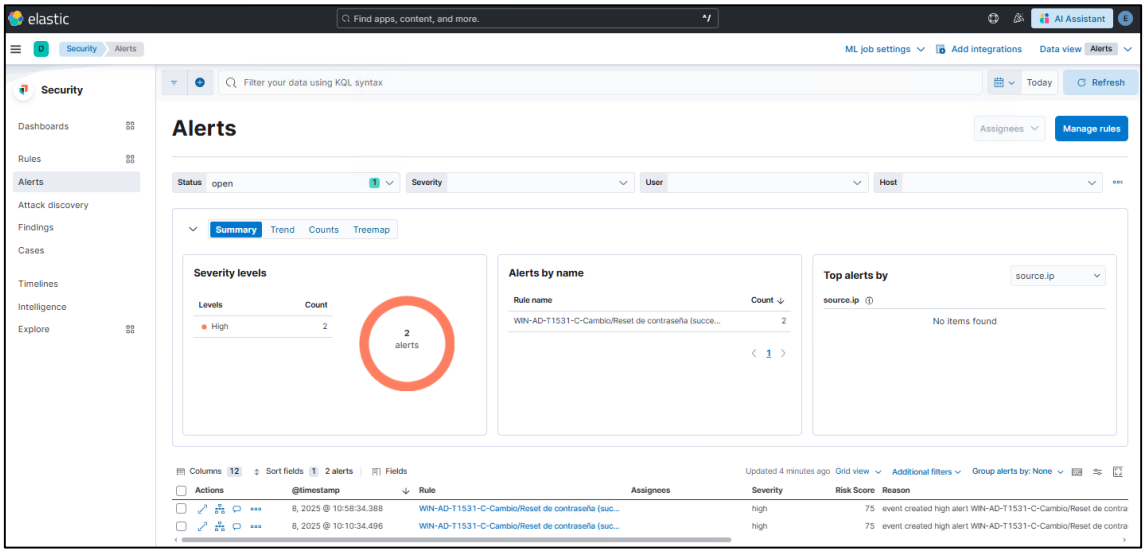


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Así también podemos ver en la imagen siguiente las alertas del caso señalado.

Figura 68

Alertas de detección de Caso de Uso de manipulación de credenciales (Cambio/Reset de contraseña)



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

La imagen muestra el panel de alertas del SIEM en Kibana, evidenciando los resultados de la simulación correspondiente al Caso C – Cambio/Reset de contraseña (success), asociado a la técnica T1531 – Account Access Removal del marco MITRE ATT&CK. En el panel principal, bajo la sección Severity levels, se observa que el sistema ha generado dos alertas clasificadas con severidad “High”, lo cual refleja la relevancia y criticidad de eventos que implican la modificación exitosa de credenciales de cuentas de usuario dentro del Active Directory.

En la sección Alerts by name, se confirma que ambas alertas corresponden a la regla WIN-AD-T1531-C–Cambio/Reset de contraseña (success), lo que demuestra que la lógica configurada para detectar eventos de los identificadores 4723 y 4724 con resultado exitoso se activó correctamente durante las pruebas.

Una vez completadas estas validaciones para todas las reglas del caso, se procede a evaluar el siguiente criterio establecido.

Tiempo Medio de Detección MTTD:

En este caso, para el cálculo del promedio del TTD se ha considerado que los tres casos (A, B y C) forman parte de un mismo escenario de prueba, ya que en conjunto permiten cubrir completamente la técnica T1531 – Account Access Removal del marco MITRE ATT&CK. Por ello, todos los tiempos de TTD obtenidos en las alertas descritas previamente se integran y se presentan en el cuadro siguiente.

Tabla 24

Listado de alertas generadas por los casos de uso que completan la técnica T1531 del marco Mitre ATT&CK

Alerta	Hora de inicio del evento (kibana.alert.original_time)	Hora de detección de la alerta (kibana.alert.last_detected)	TTD (segundos)
Alerta 1 - Caso A	20:46:46	20:48:11	85 s
Alerta 2 - Caso B	15:57:27	15:58:26	59 s
Alerta 3 - Caso B	15:56:49	15:58:26	97 s
Alerta 4 - Caso B	15:56:38	15:57:26	48 s
Alerta 5 - Caso C	10:09:31	10:10:34	63 s
Alerta 6 - Caso C	10:57:00	10:58:34	94 s

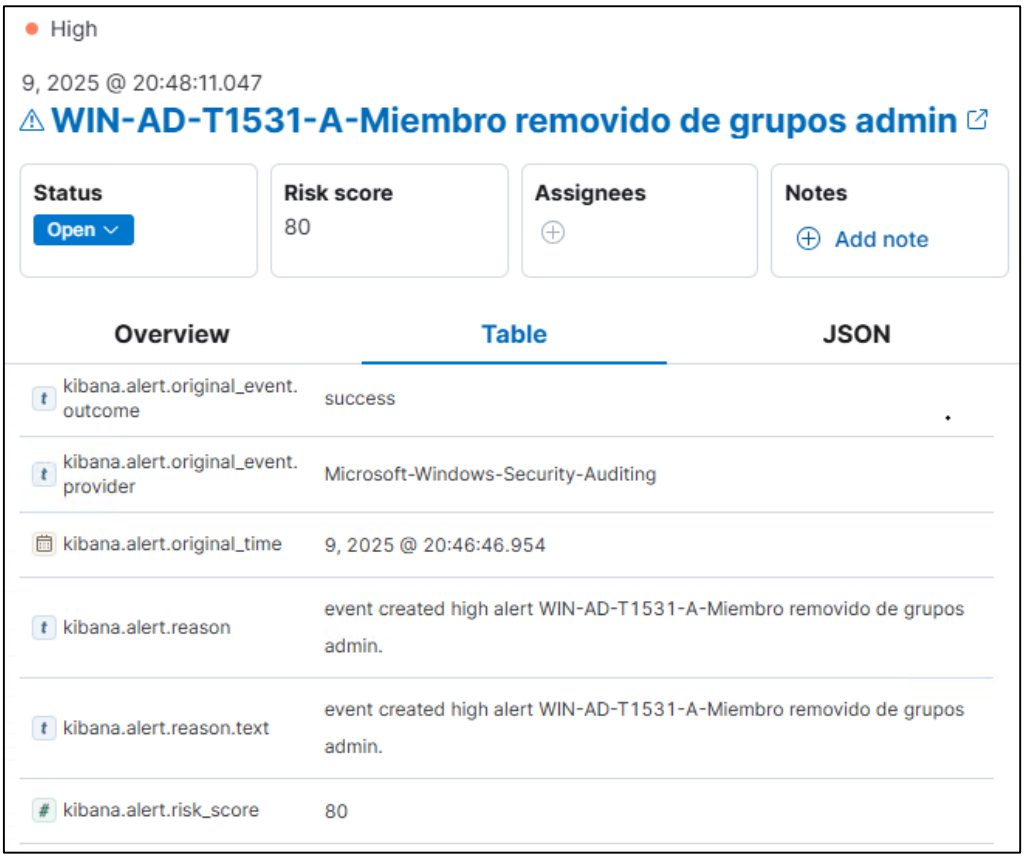
Nota. Elaboración propia con información extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

A continuación, se presenta en las siguientes figuras una muestra representativa correspondiente a los casos, en la cuales se visualizan los campos generados por el SIEM junto con el evento original recibido desde el Servidor Windows.

Alerta 1 - Caso A

Figura 69

Evidencia de Alerta 1 generada por el caso de uso A



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Alerta 2 - Caso B

Figura 70

Evidencia de Alerta 2 generada por el caso de uso B

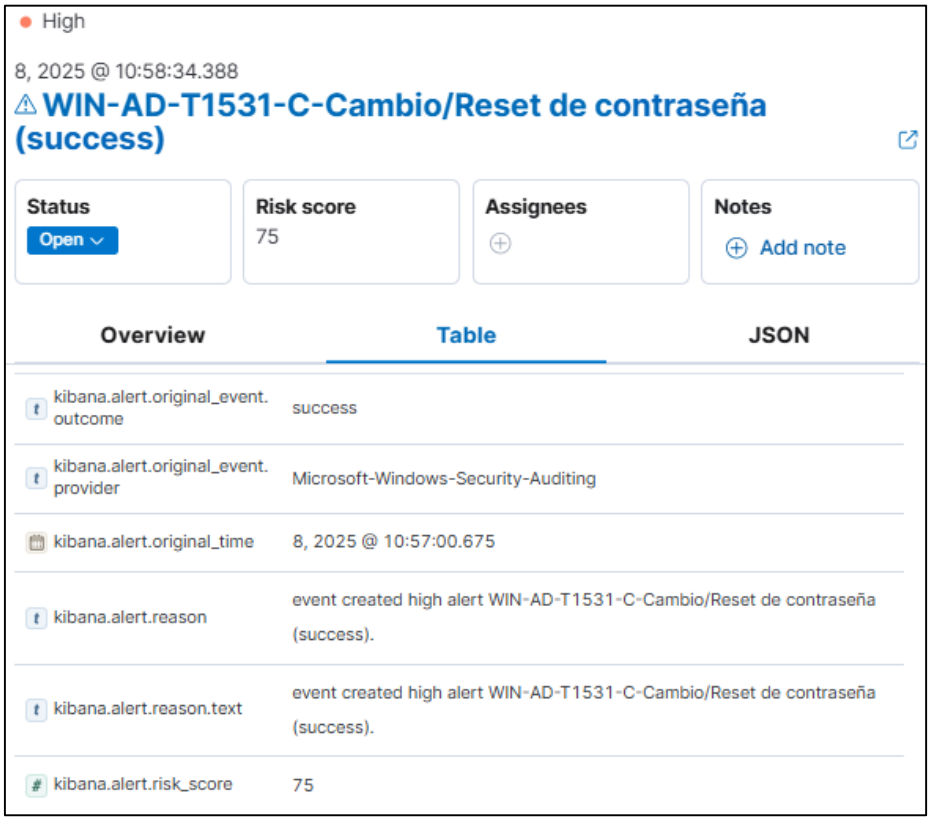


Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Alerta 6 - Caso C

Figura 71

Evidencia de Alerta 6 generada por el caso de uso C



Nota. La información fue extraída de una fuente privada, la misma que es consecuencia de la implementación realizada en la empresa de estudio. Por Recupera, 2025.

Todas ellas incluyen únicamente esta alerta como evidencia puntual, dado que las demás registradas durante la simulación presentan la misma estructura y nivel de detalle técnico.

Entonces para calcular el promedio de todas las simulaciones los TTD fueron: 85 s, 59 s, 97 s, 48 s, 63 s, 94 s respectivamente.

Por lo tanto, el cálculo del MTTD sería el siguiente:

$$MTTD = \frac{85 + 59 + 97 + 48 + 63 + 94}{6}$$

$$MTTD = 74\ segundos$$

Esto significa que el tiempo de detección promedio para el caso en general es de 74 segundos.

3.2.4.3 Análisis e Interpretación de los Resultados

Los resultados obtenidos durante la ejecución del plan de pruebas permiten confirmar que el Objetivo Específico 4 fue cumplido satisfactoriamente, al demostrarse la creación, detección y trazabilidad efectiva de los casos de uso construidos bajo el marco MITRE ATT&CK. En primera instancia, se verificó la creación exitosa de los tres casos de uso principales, cada uno asociado a una técnica o subtécnica del marco ATT&CK y alineado a las fuentes de datos integradas en el SIEM. Para la detección de ataques de fuerza bruta SSL VPN (T1110.003), se implementaron dos casos de uso independientes, uno por cada firewall, asegurando una correlación específica con los eventos generados por cada dispositivo. Del mismo modo, para identificar intentos reiterados de autenticación fallida por cuentas administrativas en el NAS QNAP, se configuró un caso orientado a la técnica T1110.001 (Password Guessing). Finalmente, para abordar la manipulación o eliminación de cuentas administrativas en el entorno Windows Server (Active Directory), se implementaron tres reglas vinculadas a la técnica T1531 (Account Access Removal), contemplando escenarios de des habilitación, eliminación y modificación de privilegios.

En relación con el segundo criterio de aceptación, se obtuvo evidencia suficiente de la detección de alertas asociadas a cada caso de uso, demostrando no solo su funcionamiento, sino también la trazabilidad completa hacia las TTP (tácticas, técnicas y procedimientos) correspondientes del marco MITRE ATT&CK. En total, se registraron 13 alertas asociadas a la técnica T1110.003, 4 alertas correspondientes a la técnica T1110.001 y 6 alertas relacionadas con la técnica T1531. Este conjunto de alertas permite confirmar que los casos de uso no solo se activaron correctamente ante los eventos simulados, sino que también reflejan fielmente los patrones de actividad maliciosa que describen las técnicas estudiadas, cumpliendo plenamente con el criterio de detección.

Por último, respecto al tercer criterio de aceptación, el análisis del Tiempo Medio de Detección (TTD) mostró resultados altamente favorables. El cálculo del MTTD para las alertas generadas por cada caso de uso evidenció tiempos consistentemente inferiores al umbral establecido de 5 minutos. En la totalidad de los eventos revisados, los tiempos de detección se mantuvieron por debajo de los 3 minutos y 11 segundos, lo cual representa un rendimiento superior al esperado. Este resultado demuestra que la solución SIEM implementada es capaz de identificar incidentes con rapidez, permitiendo una respuesta temprana ante potenciales compromisos de seguridad.

3.2.5 Resultado del Plan de Prueba del Objetivo Específico N°5

3.2.5.1 Definición y Alcance del Plan de Pruebas

Tabla 25

Objetivo específico 5, Definición y Alcance del Plan de Pruebas

Objetivo Específico	Capacitar al personal de soporte TI en el uso del SIEM y del marco MITRE ATT&CK para la gestión de eventos de seguridad, logrando una mejora del 40 % en las competencias adquiridas en los participantes.		
I. Plan de Pruebas del Objetivo Específico			
Fecha de ejecución	18/09/2025	**Versión**	V1
Patrocinador	Jefe de Infraestructura		
Responsable del Plan de Pruebas	Coordinador de TI		
Objetivo del Plan de Pruebas	- Equipo de soporte TI capacitado en SIEM y MITRE ATT&CK, con asistencia a la capacitación superior al 80% - Mejora en los resultados de pruebas post capacitación superior o igual al 40%.		
II. Detalle del Plan de Pruebas			
Alcance	- Capacitación del personal del área de Soporte de TI de la empresa. - Evaluación sobre temas expuestos. - Capacitación de manera online.		
Duración del Plan de Pruebas	2 horas		
Método de prueba	Prueba de Capacitación (Training Evaluation Test) Se aplica un modelo de evaluación tipo pre-test y post-test para medir el impacto del programa formativo en el conocimiento operativo del SIEM y comprensión del marco MITRE ATT&CK.		
Actividades a Ejecutar	1. Elaborar la presentación y el cuestionario de la capacitación. 2. Aplicar la evaluación diagnóstica (pretest) para medir el conocimiento inicial de los participantes		

	3. Ejecutar la sesión de la capacitación. 4. Aplicar la evaluación final (pos-test) para medir la mejora obtenida. 5. Registrar la asistencia y resultados de cada participante. 6. Consolidar y analizar los resultados del aprendizaje, verificando un porcentaje de mejora igual o superior al 40 %.

3.2.5.2 Ejecución y Desarrollo del Plan de Pruebas

Tabla 26

Objetivo específico 5, Ejecución del Plan de Pruebas

III. Ejecución del Plan de Pruebas			
Escenario	Ejecución del programa formativo en el entorno del área de soporte TI, empleando presentaciones en diapositivas y con el uso de herramientas de reuniones en línea.		
Herramienta	Gloogle Meet, diapositiva (Presentación SIEM-MITRE ATT&CK)		
Criterios de Aceptación	**Detalle**	**Estado**	**Porcentaje**
	- Asistencia ≥ 80 % del personal convocado.	Realizado	100%
	- Mejora ≥ 40 % en los resultados del pos-test respecto al pretest.	Realizado	100%
Resultados	Realizado		100%
Participantes del Plan de Pruebas	**Puesto**	**Fecha**	
	Jefe de Infraestructura	18/09/2025	
	Coordinador de TI	18/09/2025	
	Analista de Ciberseguridad	18/09/2025	
Aceptado / Rechazado	ACEPTADO		

IV. Desarrollo del Plan de Pruebas

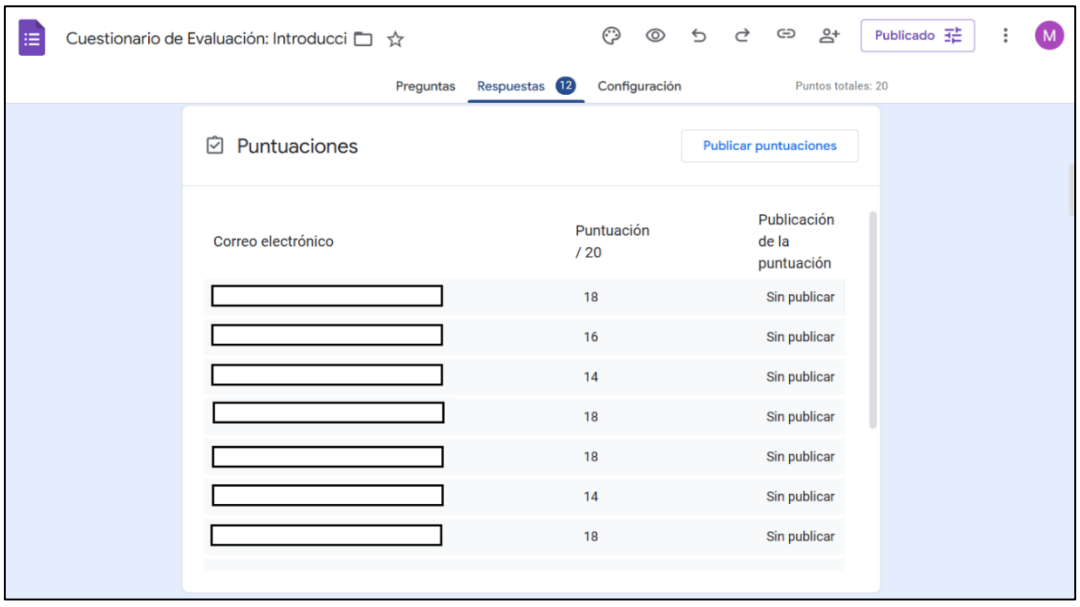
El presente plan de pruebas tiene como finalidad validar el cumplimiento del Objetivo 5, orientado a capacitar al personal de soporte TI en el uso del SIEM y del marco MITRE ATT&CK. Para ello, se midió el nivel de participación del personal convocado y la mejora en sus conocimientos mediante dos evaluaciones: un pre-test aplicado antes de la sesión y un post-test al finalizarla. Con estos datos se verificó si se alcanzaron los criterios de aceptación establecidos: asistencia mínima del 80 % y mejora igual o superior al 40 % entre ambas evaluaciones.

Evaluaciones Aplicadas:

Para evaluar la asimilación del contenido se aplicaron dos evaluaciones: un pre-test antes de iniciar la sesión y un post-test al finalizarla. Ambas evaluaciones permitieron comparar el nivel de conocimiento previo con el aprendizaje adquirido, particularmente en aspectos como el funcionamiento del SIEM, la lectura de logs y la identificación de tácticas y técnicas MITRE ATT&CK. En la Figura 72, muestra el registro de puntuaciones recopiladas a través del formulario en línea utilizado, reflejando las notas obtenidas por los asistentes tanto en el pre-test como en el post-test evidenciando la aplicación formal de ambas evaluaciones. Se han ocultado los correos electrónicos de los participantes para preservar la confidencialidad de la información.

Figura 72

Registro de Puntuaciones durante la Evaluación



Capacitación del equipo de soporte TI

La primera variable evaluada corresponde a la tasa de asistencia registrada durante la sesión de capacitación, cuyo propósito es determinar el nivel real de participación del personal convocado y verificar el cumplimiento del porcentaje mínimo requerido. La métrica utilizada para esta variable es el Porcentaje de asistencia a la capacitación. Para ello, se recopiló el registro formal de asistencia del equipo de soporte TI, el cual permitió identificar cuántos de los participantes convocados ingresaron efectivamente a la sesión realizada. A continuación, se presenta el cuadro con la relación de convocados y el registro de asistencia correspondiente:

Tabla 27

Listado de Asistencia de Capacitación

Participante	Asistió
Soporte 1	Si
Soporte 2	Si
Soporte 3	Si
Soporte 4	Si
Soporte 5	Si
Soporte 6	Si
Soporte 7	No

Con base en esta información se contabilizó un total de 7 personas convocadas, de las cuales 6 asistieron, y 1 no participó. Para calcular la tasa de participación se aplicó la fórmula señalada en la sección 3.1.5:

$$Tasa\ de\ Asistencia = \frac{6}{7} \times 100 = 85.71\%$$

Este resultado demuestra que la capacitación alcanzó una tasa de asistencia del 85.71 %, superando el porcentaje mínimo del 80 % requerido para validar la conformidad. Por tanto, se confirma que la participación del personal de soporte TI fue adecuada y cumplió con los criterios de aceptación establecidos para la actividad formativa.

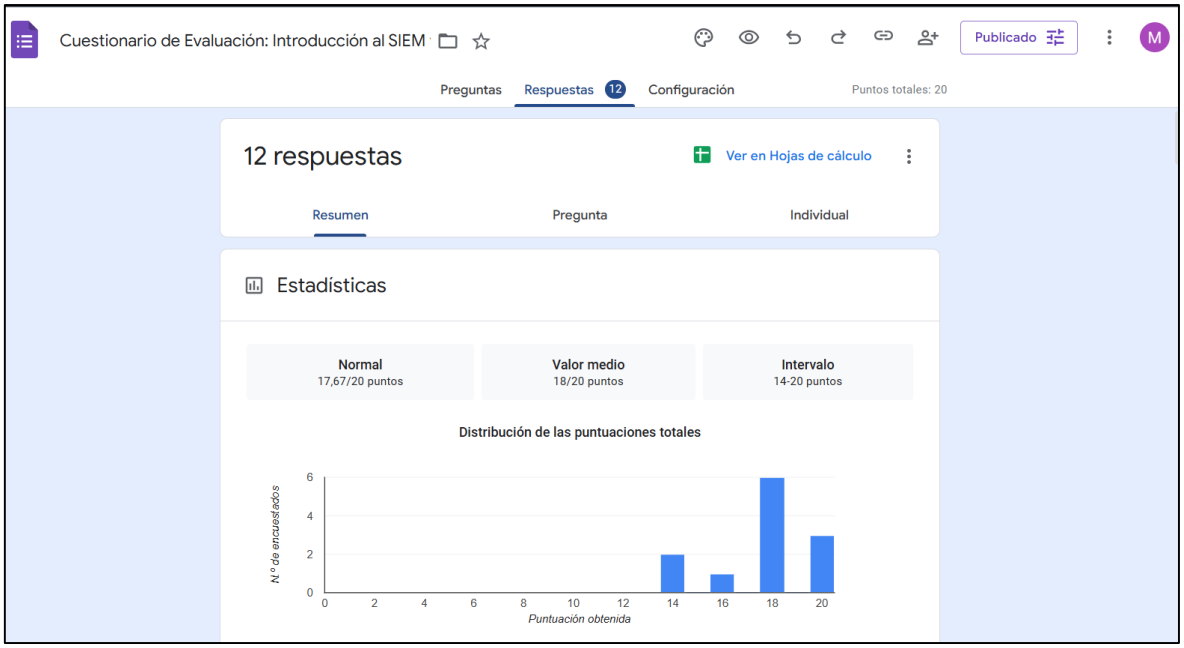
Efectividad de la capacitación

La segunda variable evaluada corresponde a la efectividad de la capacitación mediante el porcentaje de mejora obtenido por el personal de soporte TI tras recibir la capacitación, el cual permite medir el fortalecimiento de sus conocimientos y competencias. Para ello, se aplicaron dos evaluaciones: un pre-test previo al inicio de la sesión y un post-test al finalizarla, cuyos resultados permitieron comparar el nivel de desempeño antes y después de la capacitación.

En la siguiente imagen se muestra la evidencia de las respuestas pre-test y post-test del cuestionario aplicado a los participantes.

Figura 73

Evidencia de respuestas de cuestionario



En la siguiente tabla se presentan las notas obtenidas por cada participante convocado, así como las notas de ambas evaluaciones:

Tabla 28

Registro de Resultados del Pre-Test y Post-Test de los Participantes

Participante	Nota Pre-Test	Nota Post-Test
Soporte 1	16	18
Soporte 2	14	20
Soporte 3	18	20
Soporte 4	18	20
Soporte 5	14	18
Soporte 6	18	18
Soporte 7	-	-

Con base en estos resultados, el cálculo del porcentaje de mejora se realizó aplicando la siguiente fórmula establecida en la sección 3.1.5.

Cabe resaltar que se empleó esta fórmula de mejora relativa al alcance máximo para determinar la mejora obtenida entre el pre-test y el post-test. Esta métrica resulta más adecuada para el contexto de la capacitación desarrollada, la cual tuvo una duración de dos horas. Dado que, en sesiones de corta duración, el objetivo principal es reforzar conocimientos específicos más que generar incrementos porcentuales amplios, evaluar la mejora en función del margen real disponible hacia la nota máxima permite obtener un indicador más preciso y equitativo. A diferencia de la mejora porcentual simple que puede sobredimensionar el progreso de participantes con notas iniciales bajas y subvalorar a quienes partían de un nivel alto, la mejora relativa considera el potencial de mejora de cada individuo, mostrando qué proporción del espacio posible se logró cubrir en el breve periodo de capacitación.

A continuación, se presenta el cálculo aplicado a cada participante que asistió:

Tabla 29

Cálculo del Porcentaje de Mejora de los Participantes

Participante	Nota Pre-Test	Nota Post-Test	Resultado
Soporte 1	16	18	$= \left(\frac{18-16}{20-16}\right) X\ 100 = 50\%$
Soporte 2	14	20	$= \left(\frac{18-14}{20-14}\right) X\ 100 = 100\%$
Soporte 3	18	20	$= \left(\frac{20-18}{20-18}\right) X\ 100 = 100\%$
Soporte 4	18	20	$= \left(\frac{20-18}{20-18}\right) X\ 100 = 100\%$
Soporte 5	14	18	$= \left(\frac{18-14}{20-14}\right) X\ 100 = 66.67\%$
Soporte 6	18	18	$= \left(\frac{18-18}{20-18}\right) X\ 100 = 0\%$
Soporte 7	-	-	No aplica (no asistió y no rindió evaluaciones).

Una vez calculados los porcentajes individuales, se procedió a obtener el promedio general de mejora del grupo:

$$Promedio\ General\ de\ mejora = \frac{50 + \ 100 + 100 + 100 + 66.67 + 0}{6} = 69.44\%$$

El resultado demuestra que el personal participante alcanzó un promedio general de mejora del 69.44 %, superando ampliamente el umbral mínimo del 40 % establecido dentro de los criterios de aceptación. Cada participante con excepción de “Soporte 6”, cuyo resultado se mantuvo estable mostró incrementos significativos en su desempeño, confirmando que la capacitación tuvo un impacto positivo tanto a nivel individual como grupal.

3.2.5.3 Análisis e Interpretación de los Resultados

Los resultados obtenidos durante la ejecución del plan de pruebas del Objetivo Específico 5 permiten confirmar que los criterios de aceptación definidos para la capacitación del personal fueron cumplidos satisfactoriamente. En primer lugar, la asistencia a la sesión de capacitación fue verificada mediante los registros de participación generados por la plataforma Google Meet y complementados con la evaluación inicial aplicada en Google Forms. Se convocó a un total de siete integrantes del equipo de soporte TI, de los cuales seis asistieron efectivamente a la sesión. Es así que, al aplicar la fórmula establecida para calcular la tasa de asistencia, se obtuvo un valor de 85.71 %, superando el umbral mínimo del 80 % definido en los criterios de aceptación. Este resultado evidencia un adecuado nivel de participación del equipo y un interés significativo en la temática presentada.

En relación con el segundo criterio, referido a la mejora mínima del 40 % en el pos-test respecto al pre-test, los resultados de las evaluaciones aplicadas antes y después de la capacitación mostraron un progreso en el nivel de comprensión de los participantes. Para cada uno de los seis asistentes, se calculó la mejora relativa utilizando la fórmula definida previamente en el capítulo 3.1.5, lo que permitió obtener un porcentaje individual de incremento en el desempeño. Posteriormente, se calculó el promedio general de mejora, alcanzando un resultado de 69.44 %, valor superior al mínimo exigido.

Este incremento significativo refleja que los contenidos impartidos durante la capacitación fueron asimilados de manera efectiva, y que la metodología utilizada, combinando exposición teórica y evaluaciones, contribuyó positivamente al fortalecimiento de las competencias del personal de soporte TI en el conocimiento del SIEM y MITRE ATT&CK.

Con estos resultados se demuestra que la actividad formativa no solo alcanzó los niveles de participación esperados, sino que también generó un impacto positivo y medible en el conocimiento técnico de los participantes.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

a. Se identificaron los componentes críticos de la infraestructura tecnológica mediante un levantamiento detallado de los equipos que soportan la operación de la empresa, lo que permitió identificar las cuatro fuentes críticas de la empresa. Posteriormente, se aplicó una matriz comparativa a cuatro soluciones SIEM Open Source (Wazuh, OSSIM, SIEMonster y ELK Stack) evaluadas con base a una metodología de puntuación técnica. Como resultado, ELK Stack obtuvo la puntuación más alta (54 puntos), destacándose por su madurez, flexibilidad y abundancia de recursos, lo que lo establece como la solución base para el diseño del SIEM propuesto.

b. Se diseñó el diagrama de arquitectura SIEM basado en ELK Stack, describiendo el flujo de recolección, procesamiento y visualización de eventos, lo que permite la centralización de logs provenientes de los componentes críticos identificados y su gestión unificada desde un panel de control. El diagrama fue sometido a revisión por la gerencia de sistemas, obteniendo su aprobación formal al verificarse la coherencia entre la arquitectura propuesta y la infraestructura tecnológica real de la organización. Esto confirma la viabilidad técnica del diseño como base para la implementación del SIEM.

c. Se desplegó el SIEM operativo integrando las cuatro fuentes de logs definidas: dos firewalls y dos servidores críticos, logrando la centralización y monitoreo continuo de eventos de seguridad. Durante un período de prueba de 120 horas continuas (5 días laborales), el sistema registró una disponibilidad del 100 % y un rendimiento promedio de 253 EPS, superando los umbrales mínimos requeridos de $\geq$ 99.5 % y de 155 EPS. Estos resultados confirman la estabilidad operativa del SIEM y su capacidad para sostener el monitoreo de la infraestructura crítica de la organización.

d. Se desarrollaron tres casos de uso basados en el marco MITRE ATT&CK para la detección de eventos de seguridad: fuerza bruta SSL VPN (T1110.003 – Password Spraying), múltiples intentos fallidos de inicio de sesión administrativo (T1110.001 – Password Guessing) y eliminación o modificación de cuentas en grupos administradores (T1531 – Account Access Removal). Durante las pruebas, el SIEM registró 13 alertas para T1110.003, 4 alertas para T1110.001 y 6 alertas para T1531, superando el umbral mínimo de $\geq$ 3 alertas por caso de uso. El

Tiempo de Detección Promedio (MTTD) en su totalidad fue inferior a 3 minutos y 11 segundos, por debajo del criterio máximo establecido de ≤ 5 minutos, confirmando la precisión y capacidad de respuesta del SIEM ante eventos de seguridad reales.

e. Se capacitó a 6 de los 7 integrantes del área de TI convocados, alcanzando una asistencia del 85.71 %, superando el umbral mínimo requerido del ≥ 80 % del personal citado. La medición mediante pre-test y post-test evidenció una mejora del 69.44 % en las competencias adquiridas, superando en 29.44 puntos porcentuales el umbral mínimo requerido del 40 %. Estos resultados demuestran que el personal de soporte TI adquirió las capacidades necesarias para monitorear el SIEM e identificar eventos de seguridad bajo el marco MITRE ATT&CK.

4.2 Recomendaciones

a. Integrar herramienta SOAR para automatizar la respuesta a incidentes y reducir tiempos de reacción. Esta integración fortalecerá la capacidad del SIEM para ejecutar acciones inmediatas, mejorando la continuidad del servicio y la gestión de eventos críticos.
b. Integrar plataformas de inteligencia de amenazas (TIP – Threat Intelligence Platforms) para enriquecer la detección de amenazas mediante indicadores de compromiso (IOC) validados. Esta integración permitirá identificar conexiones, direcciones IP, dominios o archivos maliciosos asociados a amenazas conocidas, fortaleciendo los casos de uso implementados en el SIEM y alineados con el marco MITRE ATT&CK.
c. Extender la implementación del marco MITRE ATT&CK mediante nuevos casos de uso y reglas de correlación que permitan combinar múltiples alertas y eventos de seguridad para identificar amenazas más complejas y fortalecer las capacidades de detección del SIEM.
d. Implementar un sistema de monitoreo mediante dashboards de visualización en tiempo real orientado a correlacionar métricas operativas clave como EPS, disponibilidad y salud del sistema; con el propósito de prevenir la saturación de recursos, impedir la interrupción en la recepción de logs y evitar la caída del sistema SIEM.
e. Establecer una ruta formativa continua en entornos controlados que permita al personal de TI practicar la toma de decisiones ante incidentes en tiempo real, fortalecer sus competencias en el uso operativo del SIEM e incorporar temas clave de ISO 27001, complementándolo con evaluaciones periódicas.

5 REFERENCIAS

Abedin, I., Mukherjee, T., Kang, H.-E., Yoon, T.-H., Kim, H.-W., & Kundu, S. (2024). Unraveling the unknown: Adaptive spatial planning to enhance climate resilience for the endangered Swamp Grass-babbler (Laticilla cinerascens) with habitat connectivity and complexity approach. Heliyon, 10(9), e30273. https://doi.org/10.1016/j.heliyon.2024.e30273

Active Directory Domain Services overview. (s. f.). Microsoft.com. Recuperado el 23 de noviembre de 2025, de https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. IEEE Access: Practical Innovations, Open Solutions, 12, 1217–1234. https://doi.org/10.1109/access.2023.3344680

Alabdulhadi, S., & Al-Matouq, A. (2024). Efficient and standardized alarm rationalization for cybersecurity monitoring. IEEE Access: Practical Innovations, Open Solutions, 12, 166936–166944. https://doi.org/10.1109/access.2024.3492264

Ammi, M. (2023). Cyber Threat Hunting Case Study using MISP. Journal of Internet Services and Information Security, 13(2), 1–29. https://doi.org/10.58346/jisis.2023.i2.001

AT&T Cybersecurity. (s.f.-a). About USM Appliance components. Recuperado el 14 de septiembre de 2025, de https://cybersecurity.att.com/documentation/usm-appliance/intro/about-usm-components.htm

AT&T Cybersecurity. (s.f.-b). About USM Appliance system architecture and components. Recuperado el 14 de septiembre de 2025, de https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm

AT&T Cybersecurity. (s.f.-c). Using OTX in USM Appliance. Recuperado el 14 de septiembre de 2025, de https://cybersecurity.att.com/documentation/usm-appliance/otx/using-otx-in-usm.htm

AT&T Cybersecurity. (s.f.-d). What is OTX? Recuperado el 14 de septiembre de 2025, de https://cybersecurity.att.com/documentation/usm-appliance/otx/about-otx.htm

Bishop, J. L., & Verleger, M. A. (2013). The flipped classroom: A survey of the research. In ASEE Annual Conference & Exposition (pp. 1–18). American Society for Engineering Education.

Blanchard, P. N., & Thacker, J. W. (2019). Effective training: Systems, strategies, and practices (6th ed.). Pearson.

Bligh, D. A. (2000). What's the use of lectures? Jossey-Bass.

Cisco Systems NetFlow Services Export Version 9. (2004). Internet Engineering Task Force.

Coppolino, L., Nardone, R., Petruolo, A., & Romano, L. (2023). Building cyber-resilient smart grids with digital twins and data spaces. Applied Sciences (Basel, Switzerland), 13(24), 13060. https://doi.org/10.3390/app132413060

Coppolino, L., Sgaglione, L., D'Antonio, S., Magliulo, M., Romano, L., & Pacelli, R. (2022). Risk assessment driven use of advanced SIEM technology for cyber

protection of critical e-health processes. SN Computer Science, 3(1). https://doi.org/10.1007/s42979-021-00858-4

CS Group. (s. f.). Prelude SIEM. Recuperado el 14 de septiembre de 2025, de https://www.prelude-siem.org

Elastic. (s.f.-a). Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash. Recuperado el 16 de noviembre de 2025, de https://www.elastic.co/elastic-stack

Elastic. (s.f.-b). Elastic Common Schema (ECS): Normalizing your data with ECS. Recuperado el 16 de noviembre de 2025, de https://www.elastic.co/elasticsearch/common-schema

Elastic. (s.f.-c). Elastic Stack documentation. Recuperado el 23 de noviembre de 2025, de https://www.elastic.co/docs

Elastic. (s.f.-d). Elastic Stack features. Recuperado el 23 de noviembre de 2025, de https://www.elastic.co/es/elastic-stack/features

ESAN. (2024). Cómo debemos prepararnos ante el aumento de ciberataques en el Perú. Recuperado de https://www.esan.edu.pe/conexion-esan/

Folino, G., Otranto Godano, C., & Pisani, F. S. (2023). An ensemble-based framework for user behaviour anomaly detection and classification for cybersecurity. The Journal of Supercomputing. https://doi.org/10.1007/s11227-023-05049-x

Graham, C. R. (2013). Emerging practice and research in blended learning. In M. G. Moore (Ed.), Handbook of distance education (3rd ed., pp. 333–350). Routledge.

Graylog. (s. f.). What is Graylog? En Graylog Documentation. Recuperado el 14 de septiembre de 2025, de https://go2docs.graylog.org

Grupo Recupera. (2025). Nuestra organización. Recuperado de https://www.gruporecupera.com.pe/

Hadi, H. J., Ahmad, N., Aziz, K., Cao, Y., & Alshara, M. A. (2024). Cost-effective resilience: A comprehensive survey and tutorial on assessing open-source cybersecurity tools for multi-tiered defense. IEEE Access: Practical Innovations, Open Solutions, 12, 194053–194076. https://doi.org/10.1109/access.2024.3510533

Hazelcast. (2025). Data pipelines explained: Types, benefits, & real-world examples. Recuperado el 6 de junio de 2026, de https://hazelcast.com/foundations/event-driven-architecture/data-pipeline/

Herreid, C. F. (1994). Case studies in science-A novel method of science education. Journal of College Science Teaching, 23(4), 221–229.

Hines, M. (2018, May 7). 10 leading open source SIEM tools. Logz.Io. https://logz.io/blog/open-source-siem-tools/

Hmelo-Silver, C. E. (2004). Problem-based learning: What and how do students learn? Educational Psychology Review, 16(3), 235–266. https://doi.org/10.1023/B:EDPR.0000034022.16470.f3

Home. (2025, November 20). OpenSearch Documentation. https://opensearch.org/docs/latest

Horovits, D. (2023). The complete guide to the ELK Stack. Logz.io. https://logz.io/learn/complete-guide-elk-stack

Infobae. (2025). En 2025 aumentarán ciberataques en Perú: ¿cómo impactará en las empresas? Recuperado de https://www.infobae.com/peru/2025/01/04/

Internet Engineering Task Force. (2009). The Syslog Protocol (RFC 5424). IETF.

Internet Engineering Task Force. (s.f.). Network-Attached Storage (NAS) Definition. Recuperado de https://www.ietf.org/standards/nas-definition

Khairuddin, M. A., Mohd Isa, M. R., Mohd Shukran, M. A., Ismail, M. N., & Maskat, K. (2024). Detecting distributed denial-of-service (DDoS) attacks through the Log Consolidation Processing (LCP) framework. JOIV International Journal on Informatics Visualization, 8(3), 1064. https://doi.org/10.62527/joiv.8.3.2184

Kirkpatrick Partners. (2024, marzo 16). The Kirkpatrick Model of training evaluation. https://www.kirkpatrickpartners.com

LevelBlue. (s.f.). LevelBlue OSSIM. Recuperado el 23 de noviembre de 2025, de https://levelblue.com/products/ossim

Mahmoud, R.-V., Anagnostopoulos, M., Pastrana, S., & Pedersen, J. M. (2024). Redefining malware sandboxing: Enhancing analysis through sysmon and ELK integration. IEEE Access: Practical Innovations, Open Solutions, 12, 68624–68636. https://doi.org/10.1109/access.2024.3400167

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PloS One, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

MITRE Corporation. (s.f.-a). MITRE ATT&CK®. Recuperado el 23 de noviembre de 2025, de https://attack.mitre.org/

MITRE Corporation. (s.f.-b). MITRE ATT&CK® | MITRE. Recuperado el 23 de noviembre de 2025, de https://www.mitre.org/focus-areas/cybersecurity/mitre-attack

MITRE Corporation. (s.f.-c). Techniques – Enterprise. Recuperado el 23 de noviembre de 2025, de https://attack.mitre.org/techniques/enterprise/

MITRE Corporation. (s.f.-d). MITRE ATT&CK® enterprise matrix. Recuperado el 23 de noviembre de 2025, de https://attack.mitre.org/matrices/enterprise/

MITRE Corporation. (s.f.-e). ATT&CK Navigator [Herramienta web]. Recuperado el 23 de noviembre de 2025, de https://mitre-attack.github.io/attack-navigator/

Mohd Ariffin, M. A., Darus, M. Y., Haron, H., Kurniawan, A., Muliono, Y., & Pardomuan, C. R. (2022). Deployment of honeypot and SIEM tools for cyber security education model in UITM. International Journal of Emerging Technologies in Learning (iJET), 17(20), 149–172. https://doi.org/10.3991/ijet.v17i20.32901

Monib, W. K., Fakhreldein, M., & El-Sharkawy, M. (2024). Microlearning beyond boundaries: A systematic review and future directions. Heliyon, 10(8), e30273.

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning. Procedia Computer Science, 217, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

National Cyber Security Index. (s.f.). NCSI: Peru. Recuperado el 23 de noviembre de 2025, de https://ncsi.ega.ee/country/pe_2024/

National Institute of Standards and Technology. (2006). Guide to computer security log management (NIST Special Publication 800-92). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-92

National Institute of Standards and Technology. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations (NIST Special Publication 800-137). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-137

National Institute of Standards and Technology. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

National Institute of Standards and Technology. (2013). Glossary of key information security terms (NISTIR 7298 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.7298r2

Nezhmetdinov, R., Kotyrova, S., Nezhmetdinova, R., & Kovalev, I. (2023). Automating log analysis for industrial equipment maintenance using elastic stack. E3S Web of Conferences, 389, 01064. https://doi.org/10.1051/e3sconf/202338901064

Noe, R. A. (2020). Employee training and development (8th ed.). McGraw-Hill Education.

Park, J. S. (2024). Efficient analysis and detection of intelligent security threats in cloud environment. Journal of Internet Technology, 25(4), 629–635. https://doi.org/10.70003/160792642024072504013

Poat, M. D., Lauret, J., & Fedele, D. (2023). Flexible visualization of a 3rd party Intrusion Prevention (Security) tool: A use case with the ELK stack. Journal of Physics. Conference Series, 2438(1), 012040. https://doi.org/10.1088/1742-6596/2438/1/012040

Prince, M. (2004). Does active learning work? A review of the research. Journal of Engineering Education, 93(3), 223–231. https://doi.org/10.1002/j.2168-9830.2004.tb00809.x

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of local security event management system vs. Standard antivirus software. Applied Sciences (Basel, Switzerland), 12(3), 1076. https://doi.org/10.3390/app12031076

Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy. Karen A. Scarfone, Paul Hoffman. https://doi.org/10.6028/NIST.SP.800-41r1

Sheeraz, M., Durad, M. H., Paracha, M. A., Mohsin, S. M., Kazmi, S. N., & Maple, C. (2024). Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection. Sensors (Basel, Switzerland), 24(15), 4901. https://doi.org/10.3390/s24154901

Sheeraz, Paracha, Haque, Durad, Mohsin, Band, & Mosavi. (2023). Effective Security Monitoring using Efficient SIEM Architecture. Human-Centric Computing and Information Sciences, 13(0), 16–30. https://doi.org/10.22967/hcis.2023.13.023

Sim, D., Guo, H., & Zhou, L. (2023). A SIEM and multiple analysis software integrated malware detection approach. 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI).

Sitzmann, T. (2011). A meta-analytic examination of the instructional effectiveness of computer-based simulation games. Personnel Psychology, 64(2), 489–528. https://doi.org/10.1111/j.1744-6570.2011.01190.x

Sociedad Telecom. (2025). Kaspersky alerta que el Perú recibe más de 177,000 ataques de malware al día. Recuperado de https://sociedadtelecom.pe/

Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. (2013).

Stoleriu, R., Puncioiu, A., & Bica, I. (2021). Cyber attacks detection using open source ELK Stack. In 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1–6). IEEE. https://doi.org/10.1109/ECAI52376.2021.9515120

Universidad de Navarra. (s. f.). La clase expositiva: Nota técnica para profesores. Universidad de Navarra. https://www.unav.edu/

Valdivia, P. (2024, August 22). Perú se alza como un foco de ataques cibernéticos en Latinoamérica. El Comercio Perú. https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia/?ref=ecr

Vazão, A. P., Santos, L., Costa, R. L. de C., & Rabadão, C. (2023). Implementing and evaluating a GDPR-compliant open-source SIEM solution. Journal of Information Security and Applications, 75(103509), 103509. https://doi.org/10.1016/j.jisa.2023.103509

Wazuh. (s.f.-a). Architecture. Recuperado el 23 de noviembre de 2025, de https://documentation.wazuh.com/current/getting-started/architecture.html

Wazuh. (s.f.-b). Wazuh documentation. Recuperado el 23 de noviembre de 2025, de https://documentation.wazuh.com

Yeminyi. (2020, 22 de octubre). ELK Stack Architecture. Amy's blog. https://yeminyi.github.io/myblog/elk/2020/10/22/what-is-elk.html

Zenarmor. (s.f.). Best SIEM tools. Recuperado el 23 de noviembre de 2025, de https://www.zenarmor.com/docs/network-security-tutorials/best-siem-tools

6 ANEXOS

6.1 Anexo 1: Capacitación SIEM y Mitre Att&ck.

Capacitación en SIEM y MITRE ATT&CK

1. Introducción al SIEM

Definición: Un SIEM (Security Information and Event Management) es una solución tecnológica que integra la recolección, normalización, almacenamiento y análisis de registros (logs) provenientes de múltiples sistemas y dispositivos de seguridad.

Objetivo principal: Proporcionar visibilidad centralizada de la infraestructura y detectar amenazas en tiempo real.

Funciones principales:

- Centralizar los registros de seguridad.
- Correlacionar eventos de diferentes fuentes.
- Generar alertas e informes para la toma de decisiones.



Figura 1 Sistema de procesos de un SIEM

2. Componentes básicos de un SIEM Open Source (ELK)

¿Qué son los logs?

Los logs son registros cronológicos generados por sistemas operativos, aplicaciones y dispositivos de red, que documentan acciones de usuarios y procesos.

Importancia de los logs:

Evidencia en investigaciones de incidentes.

Fuente de datos para correlación de eventos.

Soporte para cumplimiento normativas.

ELK Stack:

Logstash: ingesta, transforma y normaliza los datos de distintas fuentes.

Elasticsearch: almacena datos de logs y permite búsquedas rápidas y escalables.

Kibana: interfaz gráfica para la consulta, visualización y construcción de dashboards.

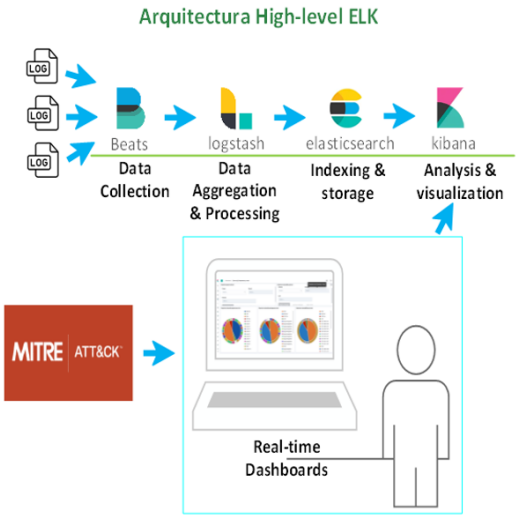


Figura 2 Arquitectura básica de un SIEM

3. Rol del soporte TI frente al SIEM

Responsabilidades:

- ✓ Monitorear que los sistemas críticos (Fuentes) sigan enviando eventos (LOG) al SIEM.
- ✓ Reportar al área de ciberseguridad incidentes o anomalías detectadas.
- ✓ Notificar al área de Ciberseguridad el correcto parseado de LOG.

Buenas prácticas:

- ✓ Evitar la eliminación manual de logs.



4. Introducción al marco MITRE ATT&CK

Definición:

MITRE ATT&CK es una base de conocimiento global que describe tácticas, técnicas y procedimientos (TTPs) utilizados por atacantes en escenarios reales.

Estructura:

Tácticas: metas estratégicas del adversario (ejemplo: Credential Access, Persistence, Exfiltration).

Técnicas: métodos concretos para cumplir la táctica (ejemplo: Brute Force – T1110, Phishing – T1566).

Aplicación en SIEM:

Permite mapear alertas y eventos a técnicas específicas.

Facilita la priorización de incidentes y la respuesta efectiva.

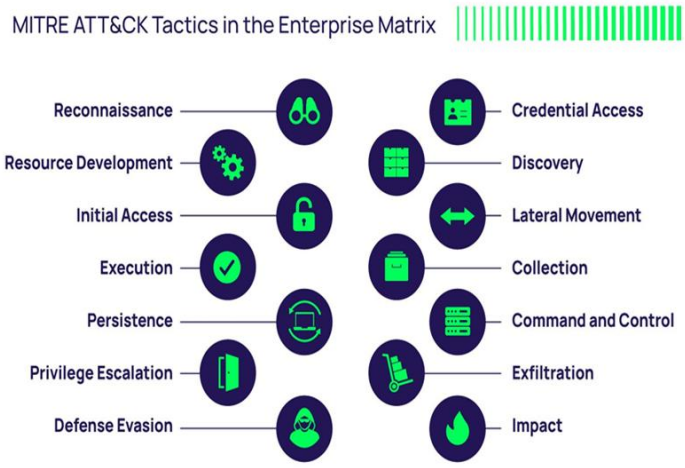


Figura 3 Mitre Att&ck Tactics en la matriz empresarial https://delinea.com/blog/what-is-the-mitre-attack-framework

5. Cierre y Preguntas

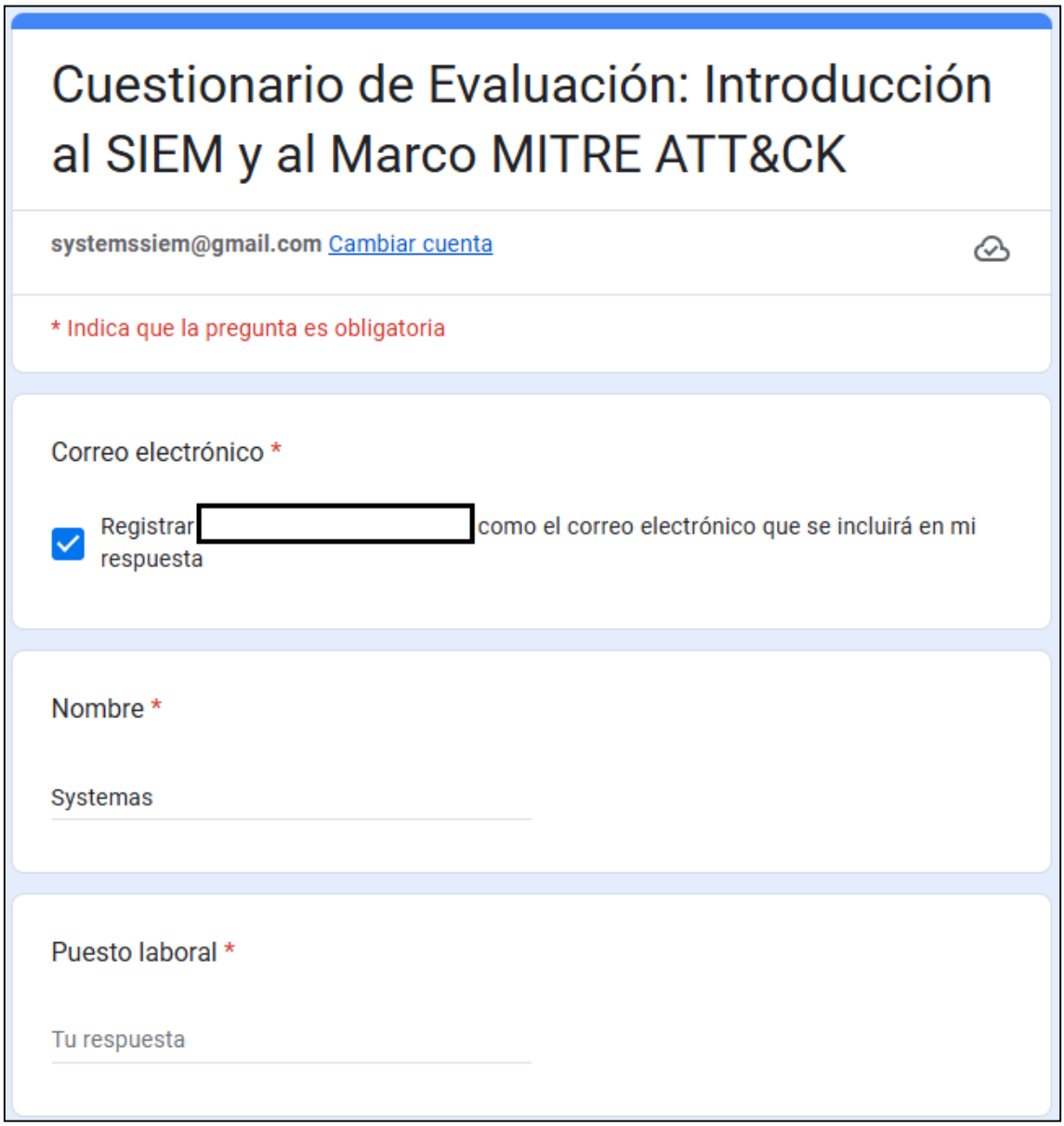
Conclusiones:

- El SIEM permite detección temprana de amenazas.
- MITRE ATT&CK clasifica tácticas y técnicas de atacantes.
- El rol del soporte TI es clave en la operación segura.

Preguntas y respuestas



6.2 Anexo 2: Cuestionario de Evaluación: Introducción al SIEM y al Marco MITRE ATT&CK



Cuestionario de Evaluación: Introducción al SIEM y al Marco MITRE ATT&CK

systemssiem@gmail.com Cambiar cuenta

* Indica que la pregunta es obligatoria

Correo electrónico *

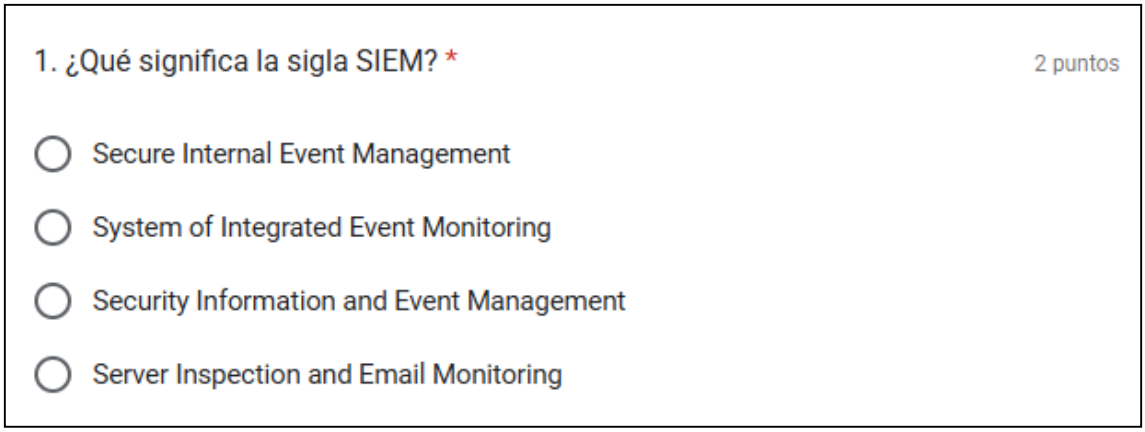
Registrar [redacted] como el correo electrónico que se incluirá en mi respuesta

Nombre *

Systemas

Puesto laboral *

Tu respuesta



1. ¿Qué significa la sigla SIEM? * 2 puntos

- Secure Internal Event Management
- System of Integrated Event Monitoring
- Security Information and Event Management
- Server Inspection and Email Monitoring

2. ¿Cuál es el principal objetivo de un SIEM? * 2 puntos

- ◯ Controlar el uso de internet en la organización
- ◯ Bloquear automáticamente a los usuarios sin permisos
- ◯ Centralizar y analizar registros para detectar amenazas
- ◯ Generar backups de servidores

3. ¿Qué tipo de información analiza un SIEM? * 2 puntos

- ◯ Correos electrónicos personales
- ◯ Logs generados por dispositivos y sistemas
- ◯ Documentos PDF compartidos en red
- ◯ Información bancaria de clientes

4. ¿Cuál de las siguientes herramientas pertenece al stack ELK? * 2 puntos

- ◯ Wireshark
- ◯ Logstash
- ◯ Nmap
- ◯ Nessus

5. ¿Qué función cumple Kibana en una solución SIEM? * 2 puntos

- ◯ Recolectar logs de red
- ◯ Visualizar y consultar la información recolectada
- ◯ Eliminar registros duplicados
- ◯ Realizar escaneos de puertos

6. ¿Qué es un log? * 2 puntos

- ◯ Una contraseña cifrada
- ◯ Un error de red
- ◯ Un archivo multimedia
- ◯ Un registro de eventos generado por un sistema

7. ¿Qué representa el marco MITRE ATT&CK? * 2 puntos

- ◯ Un antivirus gratuito
- ◯ Una guía de configuración de routers
- ◯ Una base de conocimiento de técnicas usadas por atacantes
- ◯ Un sistema de respaldo empresarial

8. En el marco MITRE ATT&CK, una táctica se refiere a: * 2 puntos

- ◯ Un tipo de sistema operativo
- ◯ Una herramienta de monitoreo
- ◯ El objetivo que persigue un adversario
- ◯ Un protocolo de red inseguro

9. ¿Cuál de los siguientes es un ejemplo de técnica en MITRE ATT&CK? * 2 puntos

- ◯ VPN empresarial
- ◯ Brute Force (fuerza bruta)
- ◯ IP pública
- ◯ DNS dinámico

10. ¿Qué responsabilidades debe tener el soporte TI en relación con el SIEM? * 2 puntos

- ◯ Apagar el servidor del SIEM al finalizar el turno
- ◯ Reiniciar los equipos sin verificar el estado de los agentes
- ◯ Monitorear que los sistemas críticos sigan enviando eventos (log)
- ◯ Eliminar logs antiguos manualmente

Respuestas del cuestionario:

1C	6D
2C	7C
3B	8C
4B	9B
5B	10C

6.3 Anexo 3: Identificación de Componentes Críticos de la Infraestructura

RECUPERA OUTSOURCING

IDENTIFICACIÓN DE COMPONENTES CRÍTICOS DE LA INFRAESTRUCTURA

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

TABLA DE CONTENIDO

Pág.

1. IDENTIFICACIÓN DE COMPONENTES CRÍTICOS DE LA INFRAESTRUCTURA 3
1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Componentes críticos 4
2. CONTROL DE CAMBIOS 6
3. REVISIONES Y APROBACIONES 6

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1. IDENTIFICACIÓN DE COMPONENTES CRÍTICOS DE LA INFRAESTRUCTURA

1.1. Antecedentes

La infraestructura tecnológica de la organización constituye el soporte principal de los servicios operativos y de seguridad. La identificación de sus componentes críticos es esencial para asegurar la continuidad del negocio y la protección de la información frente a incidentes o fallas.

1.2. Objetivos

Identificar los componentes críticos de la infraestructura tecnológica que incluya parámetros como el modelo y versión de cada dispositivo, su función específica dentro de la arquitectura tecnológica, ubicación física dentro de la organización y la asignación de responsabilidades o propietarios

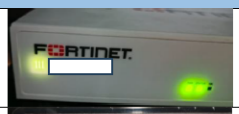
"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1.3. Componentes críticos

A continuación, se incluyen un checklist de los componentes críticos de la empresa.

Componente	Modelo/Versión	Función	Ubicación Física	Propietario	Validación
FortiGate	FG200E [redacted]	Firewall perimetral [redacted]	Rack2 Data center	La Empresa	
FortiGate	FG200D [redacted]	Firewall perimetral [redacted]	Rack2 Data center	La Empresa	
QNAP NAS	Modelo: [redacted] Version: [redacted] RAM: [redacted] CPU: [redacted]	Almacenamiento [redacted]	Rack1 Data center	La Empresa	
Servidor AD	Windows Server [redacted] CPU [redacted]	Almacenamiento [redacted]	Rxack1 Data center	La Empresa	
Router [redacted] (ISP 1)	Cisco [redacted]	Conectividad Internet	Rack2 Data center	Proveedor	

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

Componente	Modelo/Versión	Función	Ubicación Física	Propietario	Validación
Router [redacted] (ISP 2)	Fortinet [redacted]	Conectividad Internet	Rack2 Data center	Proveedor	
Router [redacted] RPV	Huawei [redacted]	Conectividad a la red [redacted]	Rack2 Data center	Proveedor	

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

2. CONTROL DE CAMBIOS

Versión N°	Fecha	Cambios Realizados
01	23/06/2025	Creación del documento
02	08/09/2025	Ejecución del Plan de Pruebas.

3. REVISIONES Y APROBACIONES

Cargo	E	R	A	Fecha de aprobación
Coordinador de TI	X			08/09/2025
Jefe de Infraestructura		X		
Gerente de Sistemas			X	

E: Elaborador
R: Revisor
A: Aprobador

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

6.4 Anexo 4: Evaluación de Soluciones SIEM Open Source



EVALUACIÓN DE SOLUCIONES SIEM OPEN SOURCE

TABLA DE CONTENIDO

Pág.

1. EVALUACIÓN DE SOLUCIONES SIEM OPEN SOURCE 3
1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Evaluación de Soluciones 3
2. CONTROL DE CAMBIOS 4
3. REVISIONES Y APROBACIONES 4

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1. EVALUACIÓN DE SOLUCIONES SIEM OPEN SOURCE

1.1. Antecedentes

Se evalúan diversas herramientas open source aplicables a los componentes del sistema SIEM (recolección, procesamiento, almacenamiento y visualización), con el fin de seleccionar aquellas que cumplan con los criterios de rendimiento, seguridad y facilidad de integración con la infraestructura tecnológica actual.

1.2. Objetivos

Determinar la idoneidad de los componentes open source que conforman el SIEM, considerando su estabilidad, soporte, vulnerabilidades y compatibilidad con los lineamientos técnicos de la organización.

1.3. Evaluación de Soluciones

Para la selección de una solución SIEM open source adecuada, se realizó un análisis comparativo de cuatro alternativas: Wazuh, OSSEM, SIEMonster y Elastic Security.

Tabla 1

Evaluación de Soluciones SIEM Open Source

N°	Parámetro	Puntuación			
		Wazuh	OSSIM	SIEMonster	ELK Stack
1	EPS	4	2	4	2
2	Reglas de correlación	4	2	4	2
3	Personalización de reglas	4	4	0	4
4	Integridad de los registros	4	2	4	4
5	Conservación de registros	4	2	4	4
6	Autenticación de usuarios	2	2	4	2
7	Control de acceso	4	4	4	4
8	Tolerancia a fallos	4	0	0	4
9	Visualización	4	2	4	4
10	Conformidad	4	0	4	4
11	Fuentes de datos personalizadas	2	2	0	2
12	Escalabilidad	2	0	0	2
13	Exploración de vulnerabilidades	2	2	2	0
14	Inteligencia sobre amenazas	1	1	2	2
15	Comunidad y apoyo	2	1	1	2
16	**Madurez de la solución Open Source**	**2**	**0**	**2**	**4**
17	**Flexibilidad para adaptarse a casos de uso personalizados**	**2**	**0**	**2**	**4**
18	**Abundancia de recursos de aprendizaje y documentación en línea**	**2**	**0**	**2**	**4**
	Puntuación SIEM	**53**	**26**	**43**	**54**

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

2. CONTROL DE CAMBIOS

Versión N°	Fecha	Cambios Realizados
01	10/07/2025	Creación del documento
02	08/09/2025	Ejecución del Plan de Pruebas.

3. REVISIONES Y APROBACIONES

Cargo	E	R	A	Fecha de aprobación
Coordinador de TI	X			08/09/2025
Jefe de Infraestructura		X		
Gerente de Operaciones Cloud y Servicios			X	

E: Elaborador
R: Revisor
A: Aprobado

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

6.5 Anexo 5: Diseño de Arquitectura SIEM ELK



RECUPERA OUTSOURCING	DISEÑO DE ARQUITECTURA SIEM ELK	**Código**: RE-TI-PS.03.2
		Versión: 02
		Página: Página **1** de **6**
		Clasificación: Uso Interno

RECUPERA OUTSOURCING

DISEÑO DE ARQUITECTURA SIEM ELK

TABLA DE CONTENIDO

Pág.

1. DISEÑO DE ARQUITECTURA SIEM ELK 3
1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Diseño de Arquitectura 3
1.3.1. Esquema General de la Solución SIEM (ELK) 4
1.3.2. Arquitectura Lógica 5
2. MÉTODO DE PRUEBA 6
3. CONTROL DE CAMBIOS 6
4. REVISIONES Y APROBACIONES 6

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1. DISEÑO DE ARQUITECTURA SIEM ELK

1.1. Antecedentes

Se propone el diseño de una arquitectura SIEM basada en ELK (Elasticsearch, Logstash y Kibana) para centralizar, procesar y analizar eventos de seguridad generados por diferentes sistemas y dispositivos de la organización.

1.2. Objetivos

Definir una arquitectura SIEM-ELK segura que permita la recolección, almacenamiento y visualización de logs, optimizando el monitoreo y la detección de incidentes de seguridad.

1.3. Diseño de Arquitectura

El diseño de la arquitectura se compone de la siguiente estructura:

- Esquema General de la Solución SIEM (ELK)
- Arquitectura Lógica

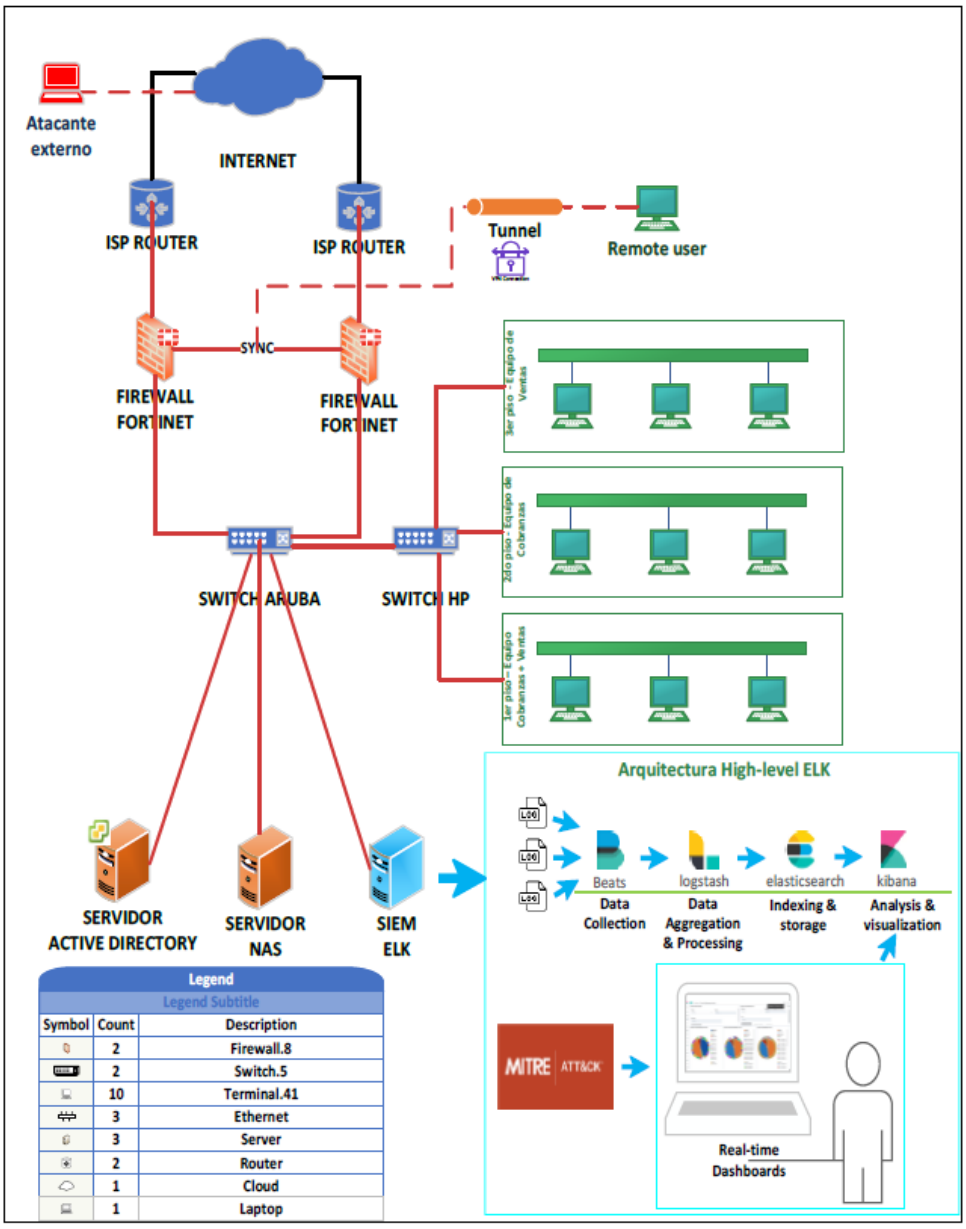
"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1.3.1. Esquema General de la Solución SIEM (ELK)

El esquema general describe la estructura integral del SIEM basado en ELK.

Figura 1

Diagrama de arquitectura



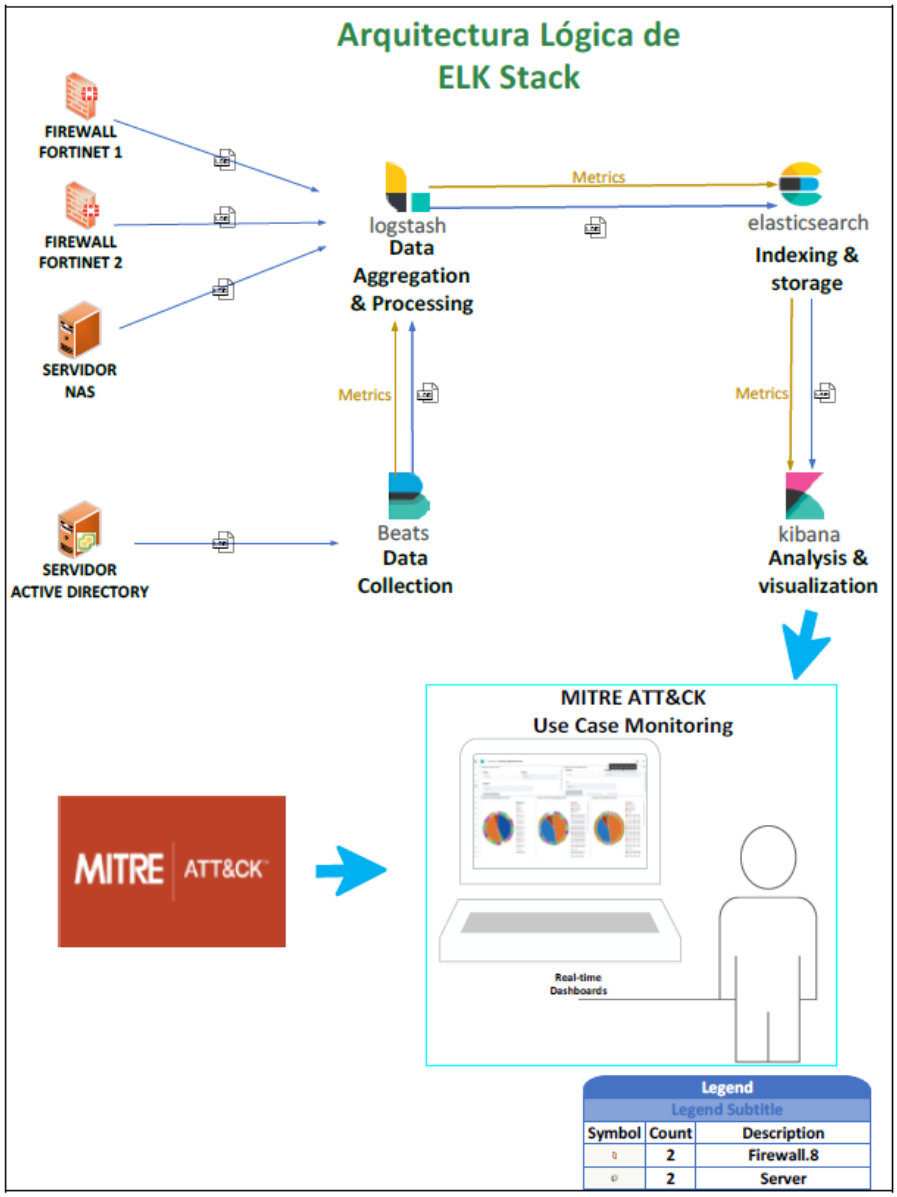
"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

1.3.2. Arquitectura Lógica

La arquitectura lógica define las capas funcionales que conforman el SIEM ELK, especificando la interacción entre los módulos de ingesta (Beats/Agents), procesamiento (Logstash), almacenamiento (Elasticsearch) y visualización (Kibana).

Figura 2

Arquitectura Lógica de ELK Stack



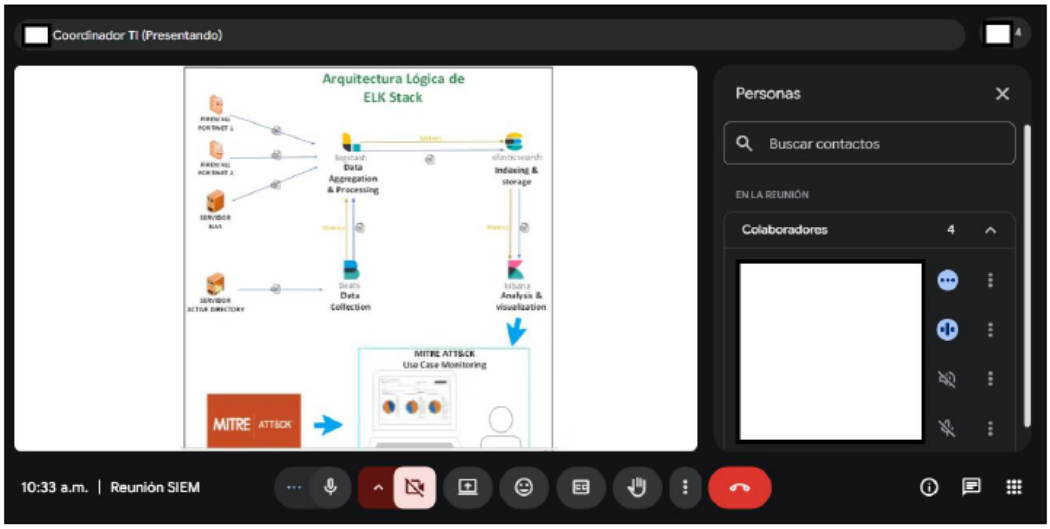
"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"

2. MÉTODO DE PRUEBA

Paseo de Revisión (Walkthrough Test)
A continuación, se muestra la revisión guiada en conjunto con las partes interesadas.

Figura 3

Evidencia del Paseo de Revisión



3. CONTROL DE CAMBIOS

Versión N°	Fecha	Cambios Realizados
01	16/07/2025	Creación del documento
02	11/09/2025	Ejecución del Plan de Pruebas

4. REVISIONES Y APROBACIONES

Cargo	E	R	A	Fecha de aprobación
Coordinador de TI	X			18/07/2025
Jefe de Infraestructura		X		
Gerente de Sistemas			X	

E: Elaborador
R: Revisor
A: Aprobado

"Este documento ha sido elaborado únicamente para el uso de la organización; por lo tanto, queda prohibida la modificación y/o reproducción sin la autorización previa del Grupo Recupera, la versión vigente se encuentra ubicada en el repositorio de Sistemas"