UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE UNA SOLUCIÓN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)PARA FORTALECER LA CIBERSEGURIDAD BAJO EL ESTÁNDAR CIS EN LA EMPRESA STIERLIFT S.A., LIMA, 2025”

Trabajo de suficiencia profesional para optar al título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

George Leonard Tenorio Gonzales

Asesor:

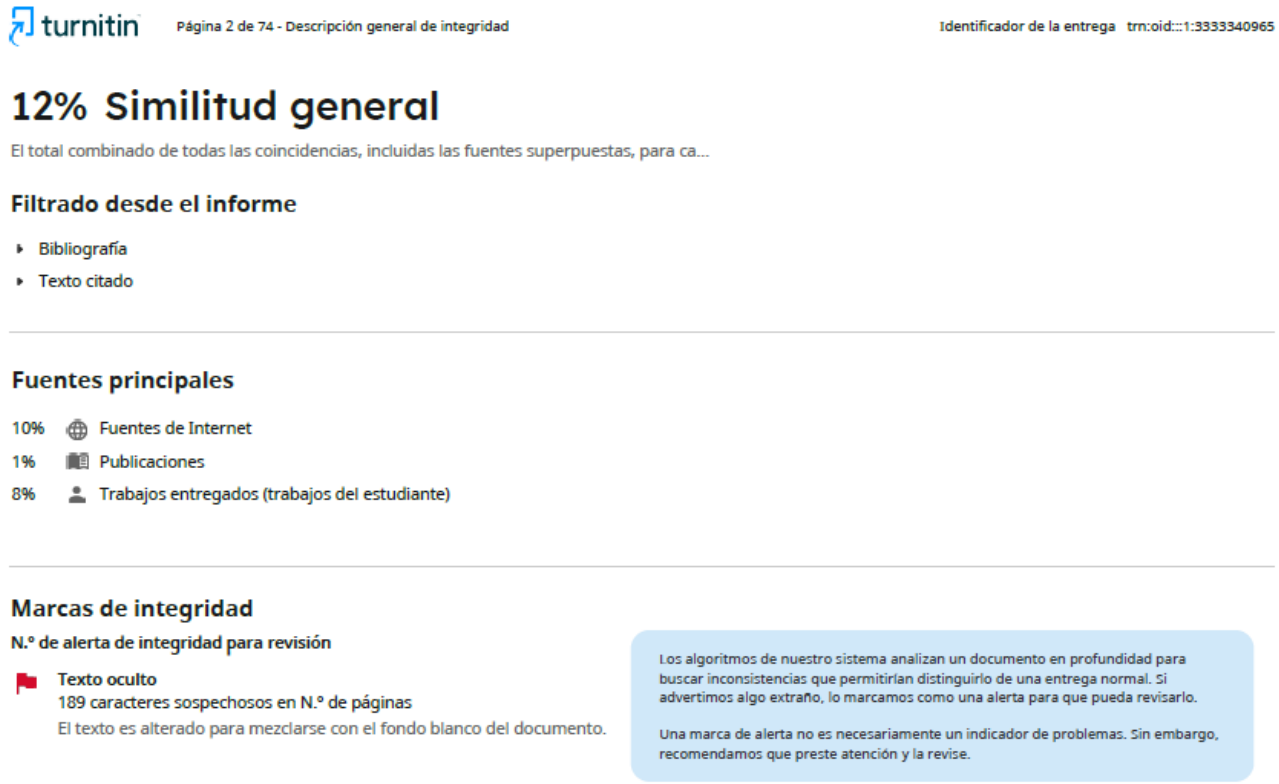
Mg. Luis Alfredo Romero Untiveros

Código ORCID 0000-0001-7050-5328

Lima - **Perú**

2025

Informe de Similitud



turnitin Página 2 de 74 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3333340965

12% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

10% Fuentes de Internet
1% Publicaciones
8% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Texto oculto
189 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dedicatoria

A mis hijos Sophie y Caleb, por su amor incondicional

y desmedido, los cuales nos han motivado

a superar cada desafío y alcanzar mis metas académicas.

Agradecimiento

Quisiera agradecer a Dios que siempre cuida de mí,

a mi esposa Joselyn y a toda mi familia por su

constante aliento y motivación.

También agradezco a la empresa Stierlift S.A. por la confianza

depositada en mí y el espacio para contribuir al crecimiento

tecnológico de la organización.

Tabla de contenidos

Informe de Similitud 2

Dedicatoria 3

Agradecimiento 4

Índice de tablas 6

Índice de Figuras 7

RESUMEN EJECUTIVO 8

CAPÍTULO I. INTRODUCCIÓN 9

CAPÍTULO II. MARCO TEÓRICO 19

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA 33

CAPÍTULO IV. RESULTADOS 55

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 63

REFERENCIAS 65

Índice de tablas

Tabla 1 Controles CIS por automatizar en Stierlift S.A. 20
Tabla 2 Seguimiento de controles CIS en Stierlift S.A. 25
Tabla 3 Aplicación del enfoque PMI en la implementación del SIEM 43
Tabla 4 Requisitos técnicos sugeridos por Wazuh 46
Tabla 5 Recursos de servidor SIEM instalado 47
Tabla 6 Errores y correcciones en la instalación de Wazuh 49
Tabla 7 Errores en la conexión entre los agentes y el manager 50
Tabla 8 Cronograma de implementación de Wazuh 53
Tabla 9 Cantidad de eventos por niveles de seguridad 60
Tabla 10 Listado de agentes con mayores alertas de Syscheck 61
Tabla 11 Top 5 de IPs origen con más intentos fallidos 62

Índice de Figuras

Figura 1 Logo de Stierlift S.A. 9
Figura 2 Transporte de carga especial 11
Figura 3 Transporte de parques eólicos 12
Figura 4 Organigrama de Stierlift S.A., junio 2025 13
Figura 5 Certificaciones de Stierlift S.A. 16
Figura 6 Marco de seguridad cibernética NIST (CSF) 2.0 21
Figura 7 Arquitectura Wazuh 29
Figura 8 Presentación de avance de la migración de cuentas para los comités de Gerencia 36
Figura 9 Diagrama de Gantt de migración de Tenant. 37
Figura 10 Proceso de entrada de mercancía 40
Figura 11 Costos y recursos indicados en el Business Case 45
Figura 12 Servidor Wazuh implementado 49
Figura 13 Configuración de syslog en Wazuh 51
Figura 14 Configuración en FortiGate 51
Figura 15 Listado de agentes instalados 52
Figura 16 Planner de proyecto de implementación del SIEM 54
Figura 17 Dashboard Wazuh de endpoint Windows 56
Figura 18 Detalle de un endpoint en dashboard de wazuh 57
Figura 19 Lista de aplicaciones instaladas de un equipo Windows 58
Figura 20 Recolección de logs del FortiGate 61
Figura 21 Confirmación del proveedor de inhabilitación de la VPN SSL-Web 62

RESUMEN EJECUTIVO

Este trabajo presenta la implementación de Wazuh como solución Security Information and Event Management (SIEM) de código abierto en Stierlift S.A., con el objetivo de centralizar el monitoreo de seguridad, detectar amenazas en tiempo real y garantizar el cumplimiento de controles de ciberseguridad alineados al estándar Center for Internet Security (CIS). La integración del firewall FortiGate con el SIEM Wazuh fortaleció la visibilidad y el monitoreo de eventos perimetrales, permitiendo la correlación de alertas críticas como intentos fallidos de autenticación SSL VPN, mientras que los controles CIS orientaron la priorización de acciones críticas, como la gestión de vulnerabilidades, el hardening de sistemas y la respuesta a incidentes.

Previo a la implementación, se desarrolló un Business Case que evaluó la viabilidad técnica-económica del proyecto, demostrando a la gerencia de Stierlift S.A. los beneficios tangibles de la plataforma: reducción de riesgos (ransomware, phishing, explotación de vulnerabilidades), optimización de recursos y cumplimiento normativo (CIS, NIST).

La solución se desplegó en una infraestructura compuesta por servidores críticos y endpoints, evidenciando que Wazuh no solo mejora la visibilidad de las amenazas, sino que también automatiza procesos de auditoría en entornos con limitaciones de presupuesto. Los resultados validaron su efectividad para fortalecer la postura de ciberseguridad y servir como base para futuras integraciones con otras aplicaciones.

Palabras claves: Ciberseguridad, Wazuh, SIEM, CIS, gestión de vulnerabilidades.

CAPÍTULO I. INTRODUCCIÓN

1.1. Antecedentes de la empresa

Stierlift S.A. es una compañía peruana fundada en 1938, con el objetivo de transportar en forma sólida y segura los proyectos más importantes para el país, para las industrias que mayor aporte hacen al desarrollo y al progreso de la nación. La empresa ha logrado liderar exitosamente la movilización de cargas especiales para los mayores proyectos del Perú, a través de complejos caminos y la especial geografía del país. Este liderazgo ha evolucionado en el tiempo, con el compromiso y calidad de su gente, sumando cada día una alta ingeniería de transporte, y teniendo siempre como máxima prioridad la seguridad en las operaciones y el respeto por el medioambiente.

Actualmente, forma parte del Grupo Kaptan, división logística de Ultramar, lo que le permite ampliar su alcance y optimizar recursos a través de sinergias corporativas (Ultramar, 2024).

Figura 1

Logo de Stierlift S.A.

Nota. Figura tomada de archivo interno de Stierlift S.A.

1.1.1. Sector, alcance y estructura organizacional

Stierlift S.A. opera en el sector de transporte especializado, ofreciendo servicios integrales que abarcan desde la planificación técnica hasta la ejecución de maniobras complejas. Entre sus principales servicios se incluyen:

- Transporte nacional e internacional de cargas especiales.
- Maniobras de izaje y montajes industriales.
- Estudios de rutas y evaluación estructural de puentes.
- Obras civiles asociadas al transporte especializado.
- Gestión de permisos y certificaciones técnicas.

La empresa cuenta con una flota de alta capacidad, que incluye grúas RT, AT, de orugas, heavy lift, grúas gantry de hasta 800 toneladas, tractocamiones Kenworth T800, unidades DAF XF105 y otros equipos especializados. Su equipo humano está conformado por ingenieros, técnicos y operadores certificados bajo estándares internacionales como Occupational Safety and Health Administration (OSHA) (Stierlift S.A., s.f.).

1.1.2. Clientes y sectores principales

Stierlift S.A. presta servicios a diversos sectores estratégicos para el desarrollo del país:

Minería: Transporte e izaje de maquinaria pesada, materiales peligrosos y equipos de gran volumen, incluyendo estudios de ruta y montaje.

Figura 2

Transporte de carga especial

Nota. Tomado de servicios/transporte, por **Stierlift S.A.**, s. f., https://stierlift.pe/servicios/transporte/

Industria: Participa en montaje y desmontaje, paradas de planta, mantenimiento de izaje e ingeniería.

Energías renovables: Logística para parques eólicos/fotovoltaicos, ingeniería de ruta y maniobras.

Oil & Gas: Servicios logísticos *onshore* y *offshore*, provisión de personal técnico y transporte especializado (Stierlift S.A., s.f.).

1.1.3. Recursos y certificaciones

La compañía dispone de infraestructura propia de ingeniería, talleres de mantenimiento, equipos de transporte e izaje de gran capacidad y personal técnico altamente calificado.

Además, Stierlift S.A cuenta con certificaciones ISO, sustentadas en su política de gestión integrada:

- ISO 9001 – Gestión de la calidad.
- ISO 14001 – Gestión ambiental.
- ISO 45001 – Seguridad y salud en el trabajo.
- ISO 39001 – Seguridad vial.

1.1.4. Estrategia de Sostenibilidad

Stierlift S.A. ha establecido una estrategia de sustentabilidad responsable de sus operaciones basada en cinco pilares: nuestras personas, confianza y transparencia, clientes y excelencia operacional, desarrollo social y cuidado del planeta, sobre los cuales se definen y actualizan metas anualmente, con el propósito de contribuir al desarrollo sostenible en sus tres dimensiones: económica, social y ambiental (Stierlift S.A., s.f.). De acuerdo con la Sociedad Nacional de Industrias (2024), las empresas logísticas que adoptan políticas de sostenibilidad mejoran su competitividad al cumplir con normativas internacionales y al alinearse con las expectativas de grandes clientes que exigen trazabilidad y reducción de huella de carbono.

Figura 3

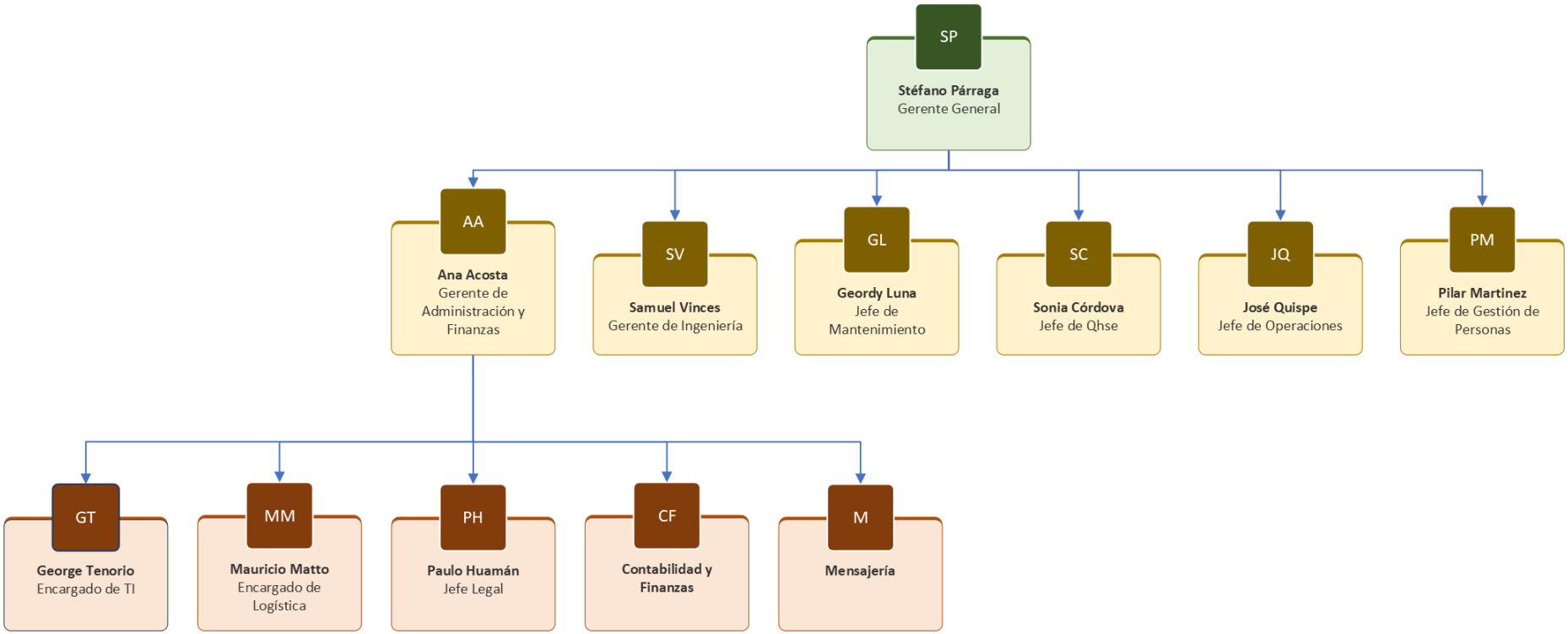
Transporte de parques eólicos

Nota. Tomado de servicios/transporte, por **Stierlift S.A.**, s. f., https://stierlift.pe/servicios/transporte/

1.2. Organigrama

Figura 4

Organigrama de Stierlift S.A., junio 2025



Nota. Elaboración propia a partir de información interna de la empresa.

1.3. Servicios principales

Stierlift S.A. es una empresa con más de 80 años de operación en el sector de transporte e izaje de cargas especiales, que aplica estándares técnicos y de seguridad establecidos por la normativa vigente. La organización desarrolla de forma continua nuevos servicios y procedimientos, orientados a su integración en la cadena de abastecimiento de diversas empresas del país. Su gestión se basa en la aplicación de criterios técnicos en ingeniería y seguridad.

La empresa busca mantener el liderazgo a través de un estándar superior en ingeniería, seguridad, compliance, y generar relaciones a largo plazo con nuestros clientes.

1.3.1. Transporte

Stierlift S.A. desarrolla ingeniería de carga, estudios de ruta, evaluaciones de puentes, reforzamientos y la ejecución de obras civiles requeridas para viabilizar el tránsito de cargas. La empresa cuenta con experiencia en el transporte de carga especial y en el manejo de diversos tipos de carga en general:

- Transporte regular y especial.
- Transporte nacional e internacional.
- Maniobras especiales.
- Estudios de ruta.
- Estudios de verificación estructural de puentes.
- Estudios de reforzamiento.
- Obras civiles.
- Gestión de permisos.
- Paradas de planta.

1.3.2. Izaje

Como parte del grupo Stierlift S.A., Grúas S.A. es especialista en ingeniería de izaje, proporcionando soluciones adaptadas a las necesidades de cada proyecto. Todas las actividades las planifican buscando garantizar una ejecución segura del trabajo, dentro de esta categoría, los servicios incluyen:

- Alquiler de equipos de izaje.
- Supervisión y dirección de maniobras.
- Planes de izaje,
- Montajes.
- Armado de equipos mineros (Palas, Camiones, etc.).
- Paradas de planta.

1.3.3. Maniobras

Cuando se presentan los escenarios más complejos de cargas, descargas, montajes, entre otras operaciones donde las soluciones con grúas no sean posibles, Stierlift S.A. tiene la capacidad de diseñar y desarrollar maniobras especiales hechas a la medida de cada necesidad.

- Diseño de ingeniería de maniobras.
- Montajes industriales.
- Elevación y deslizamiento.
- Carga y descarga de equipos complejos.

1.4. Certificaciones

Stierlift S.A. cuenta con 4 certificaciones importantes.

Figura 5

Certificaciones de Stierlift S.A.

Nota. Tomado de Política y certificaciones, por **Stierlift S.A.**, s. f., https://stierlift.pe/nosotros/politica-y-certificaciones/

1.4.1. ISO 9001: Sistemas de Gestión de la Calidad

Descripción

Esta norma establece los requisitos para un sistema de gestión de la calidad (SGC), asegurando que la empresa cumple con los estándares de satisfacción del cliente y mejora continua.

Estandarización de procesos

Optimiza operaciones de logística, mantenimiento de vehículos y atención al cliente.

Reducción de errores

Minimiza fallos en la entrega de carga y mejora la eficiencia operativa.

Mayor confianza de clientes

Demuestra compromiso con la calidad, facilitando contratos con grandes empresas.

1.4.2. ISO 14001: Sistemas de Gestión Ambiental

Descripción

Enfocada en la gestión ambiental, ayuda a las empresas a reducir su impacto ecológico mediante un enfoque sistemático.

Reducción de emisiones

Fomenta el uso eficiente de combustible y vehículos menos contaminantes.

Cumplimiento legal

Evita sanciones por normativas ambientales.

Imagen corporativa sostenible

Atrae clientes y socios comprometidos con el medio ambiente.

1.4.3. ISO 45001: Sistemas de Gestión de Seguridad y Salud en el Trabajo

Descripción

Establece estándares para prevenir riesgos laborales y proteger la salud de los trabajadores.

Menos accidentes

Implementa protocolos para conductores y operarios de carga.

Reducción de costos por siniestros

Disminuye indemnizaciones y pérdidas por accidentes.

Cultura de seguridad

Mejora el ambiente laboral y la productividad del personal.

1.4.4. ISO 39001: Sistemas de Gestión de Seguridad Vial

Descripción

Específica para empresas con flotas vehiculares, busca reducir muertes y lesiones graves en carreteras.

Menos accidentes viales

Implementa mejores prácticas en conducción y mantenimiento de vehículos.

Ahorro en seguros y multas

Reduce costos asociados a siniestros e infracciones.

Reputación de seguridad vial

Atrae clientes que valoran transportistas confiables.

CAPÍTULO II. MARCO TEÓRICO

2.1. Contexto Laboral

La empresa Stierlift S.A. contaba previamente con controles de ciberseguridad como revisión de activos desconocidos de la red, actualizaciones de parches de seguridad, control de cambios en archivos o sistemas sensibles, fundamentados en el marco del Center for Internet Security (CIS).

No obstante, los controles mencionados se aplicaban de forma manual mediante procedimientos documentados y configuraciones en el Active Directory (AD), lo que ocasionaba demoras en la búsqueda de vulnerabilidades conocidas (CVE), en las detecciones de configuraciones inseguras, en la identificación de cambios no autorizados en archivos críticos y en la correlación de eventos para identificar patrones de ataque.

Este escenario evidenció la necesidad de adoptar una solución centralizada que permitiera el monitoreo continuo, correlación de eventos y automatización de controles, garantizando el cumplimiento normativo y la eficiencia operativa. En este contexto, la organización optó por implementar Wazuh como plataforma SIEM. La correlación adecuada de logs permite mejorar la detección temprana y reducir la tasa de falsos positivos en entornos empresariales complejos (Mahmoud et al., 2022).

La implementación de Wazuh buscó automatizar controles prioritarios establecidos por los CIS Controls, entre ellos, inventario de activos, monitoreo continuo, gestión de vulnerabilidades y auditoría de registros. Estos objetivos se alinean con las mejores prácticas internacionales en materia de seguridad de la información (CIS, 2025; NIST, 2024).

Tabla 1

Controles CIS por automatizar en Stierlift S.A.

Control CIS	Acción Automatizada con Wazuh
CIS 1 y 2: Inventario de hardware y software	Escaneo semanal de activos, alerta por activos desconocidos
CIS 3: Gestión continua de vulnerabilidades	Escaneo con base en CVE y priorización de parches según criticidad.
CIS 5: Configuración segura para hardware y software	Monitoreo continuo de cambios no autorizados en sistemas críticos.
CIS 6: Recolección y auditoría de logs	Recolección y análisis centralizado de logs.
CIS 8: Protección de datos	File Integrity Monitoring (FIM) en archivos críticos.

*Nota***.** Estos controles se tomaron como prioridad para la implementación de Wazuh.

2.2. Concepto y evolución de la ciberseguridad

2.2.1. Concepto

La norma de la International Organization for Standardization (ISO) en ISO/IEC 27001, establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) basado en la identificación, evaluación y tratamiento de riesgos. La ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger redes, dispositivos, programas y datos frente a ataques, daños o accesos no autorizados. Su propósito principal es garantizar la confidencialidad, integridad y disponibilidad de la información para apoyar la continuidad del negocio y el cumplimiento normativo (ISO, 2022).

Según el National Institute of Standards (NIST), la ciberseguridad implica la implementación de controles de seguridad y privacidad para proteger los sistemas de información contra amenazas internas y externas (NIST, 2024).

Figura 6

Marco de seguridad cibernética NIST (CSF) 2.0

Nota. Tomado de "El Marco de Seguridad Cibernética (CSF) 2.0 del NIST" (NIST, 2024).

2.2.2. Evolución y tendencias

En la última década, la proliferación del trabajo remoto, el uso intensivo de la nube y la digitalización acelerada han transformado el panorama de la ciberseguridad. CIS Controls v8, lanzado en 2021, actualizó sus prácticas para entornos híbridos y cloud (CIS, 2021).

La ciberseguridad integra tecnología, procesos de gestión y factores humanos para reducir riesgos en entornos híbridos y distribuidos. La literatura reciente muestra que la superficie de ataque se acelera por la adopción acelerada de nube, IoT y arquitecturas distribuidas, lo que exige estrategias de defensa con múltiples capacidades de detección temprana y respuesta orquestada apoyadas en analítica avanzada como aprendizaje automático para priorización de alertas, detección de anomalías y automatización de contención (Admass et al., 2024).

Actualmente, se mantienen discrepancias entre parte teórica y las prácticas implementadas, especialmente en evaluación de políticas y en la integración de dimensiones humanas (conciencia, cultura y usabilidad) dentro de programas de seguridad en las empresas. También se observa un desplazamiento hacia enfoques "zero-trust", protección de datos por diseño y automatización guiada por evidencia, proponiéndose marcos que articulan amenazas emergentes con soluciones y agendas de investigación aplicada (Zaid & Garai, 2024).

La cooperación interorganizacional en materia de inteligencia de ciberseguridad ha emergido como una estrategia importante para mejorar la capacidad de recuperación ante amenazas complejas. Un análisis sistemático reciente identificó 35 factores influyentes en la adopción de prácticas de compartición de inteligencia, estructurados bajo el marco Tecnología, Organización y Entorno (TOE), y propuso un marco teórico que facilite la generalización de hallazgos y la interoperabilidad entre entidades (Kolini & Janczewski, 2022).

2.3. Estándares de ciberseguridad

2.3.1. CIS Controls

Los CIS Controls son un conjunto de mejores prácticas desarrolladas por el Center for Internet Security (CIS) para reducir el riesgo cibernético. Estos controles se organizan en categorías priorizadas, conocidas como controles críticos, que ayudan a las organizaciones a implementar medidas efectivas de protección. La versión 8, lanzada en 2021, reorganizó los controles en 18 grupos priorizados, incorporando conceptos de automatización y seguridad en la nube. Posteriormente, la versión 8.1 (2025) añadió un dominio de gobernanza, alineando las prácticas a marcos como el NIST CSF 2.0 y la ISO/IEC 27001:2022, consolidando la relación entre seguridad técnica y gestión estratégica (CIS, 2021; CIS, 2025).

Se han propuesto enfoques que emplean prompts y procedimientos basados en modelos de lenguaje de gran tamaño (LLMs) para hacer cumplir y validar salvaguardas de los CIS Controls, integrando técnicas como few-shot learning y chain-of-thought prompting para generar evidencias y reducir la dependencia de intervenciones manuales. Asimismo, la literatura relacionada sintetiza avances previos en el mapeo de requisitos a NIST/CIS, auditorías automatizadas con benchmarks y estudios empíricos sobre la efectividad de los controles. (Ahmed et al., 2024; Haverinen et al., 2024).

El núcleo de la propuesta de automatización de esta investigación se centra en el Control 6 del CIS Critical Security Controls v7.1: "Mantenimiento, Monitoreo y Análisis de Registros de Auditoría". Este control fue seleccionado debido a que constituye un elemento central para garantizar la visibilidad de la postura de seguridad y fortalecer la capacidad de respuesta preventiva en un entorno tecnológico. Si bien la

automatización se focalizará en este control, se reconoce su relación inherente con otros controles CIS esenciales, tales como el Control 1 (Inventario de Activos de Hardware), el Control 2 (Inventario de Activos de Software), el Control 5 (Gestión de Privilegios de Cuenta) y el Control 8 (Configuración de Auditoría y Gestión de Registros), los cuales serán analizados en sinergia para garantizar una implementación holística, junto con otros marcos normativos relevantes que se detallarán posteriormente.

El principio fundamental del Control CIS 6 parte de una idea sencilla pero significativa dado que toda acción realizada en un sistema de información deja un rastro. Estos rastros, conocidos como registros de auditoría o logs, capturan tanto las actividades de usuarios autorizados como, de manera crucial, las de potenciales atacantes.

Tabla 2

Seguimiento de controles CIS en Stierlift S.A.

Definición Controles CIS UMAR					
Control CIS			**Grupo de Implementación**		**Alternativas o Herramientas**
CIS Control 1: Inventario y control de activos hardware			**IG 1**		
Sub Control	**Control**	**Descripción**	**Requerido**	**Opcional**	**Descripción**
1.4	Mantener un inventario de activos detallado	Mantenga un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.	X		Planilla Excel, rvtool (Vmware) Herramienta Automatizada (Aranda, Intune, otros) Procedimiento.
1.5	Mantener la información del inventario de activo	Asegúrese que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.	X		Planilla Excel, rvtool (Vmware) Herramienta Automatizada (Aranda, Intune, otros)
1.6	Gestionar los activos no autorizados	Asegúrese de que los activos no autorizados se eliminen de la red, se pongan en cuarentena o el inventario se actualice oportunamente.	X		

Nota. Formato interno de control de los CIS, sólo se está mostrando el control CIS 1.

2.3.2. Estándares complementarios: NIST CSF 2.0 e ISO/IEC 27001:2022

El NIST CSF 2.0 es un marco de referencia flexible para la gestión de riesgos cibernéticos, actualizado para abarcar aspectos de gobernanza y adaptabilidad tecnológica: Gobernar, identificar, proteger, detectar, responder y recuperar (NIST, 2024).

Por su parte, la ISO/IEC 27001:2022 introduce 93 controles distribuidos en 4 grupos, incluyendo nuevos, como inteligencia de amenazas y enmascaramiento de datos (PECB, 2022; ISO, 2022).

2.4. Hardening

El hardening en entornos tecnológicos se define como "el proceso de eliminar un medio de ataque mediante la corrección de vulnerabilidades y la desactivación de servicios no esenciales". Esta práctica abarca la aplicación sistemática de parches, la configuración segura de servicios y el establecimiento de políticas que limiten puntos de exposición, con el objetivo primario de reducir la superficie de ataque de los sistemas. Su enfoque preventivo y estructurado lo convierte en un componente esencial de cualquier estrategia de protección, especialmente cuando se complementa con auditorías regulares y guías robustas de hardening (Kenfack et al., 2023).

2.5. Playbook

En el ámbito de la ciberseguridad, un playbook se define como un conjunto estructurado y predefinido de acciones, condiciones, flujos lógicos y puntos de respuesta ante incidentes, diseñado para automatizar o guiar la respuesta frente a escenarios específicos. Su propósito es capturar conocimiento operativo y garantizar consistencia y eficiencia en la gestión de incidentes. Estos playbooks son elementos esenciales en plataformas de Security Orchestration, Automation and Response

(SOAR), donde especifican los pasos automatizados como el enriquecimiento de datos, la contención de sistemas o la generación de alertas así como los puntos de decisión que requieren intervención humana (JumpCloud, 2025; Faisal Yahya, 2025).

2.6. Security Information and Event Management (SIEM)

Los sistemas Security Information and Event Management (SIEM) son plataformas centralizadas que integran tecnologías de recolección, correlación, normalización y análisis de datos de seguridad provenientes de fuentes heterogéneas (redes, endpoints, aplicaciones) para detectar amenazas en tiempo real, priorizar incidentes y automatizar respuestas. Su evolución reciente incorpora técnicas de inteligencia artificial (IA) y aprendizaje automático (ML) para mejorar la precisión en la identificación de patrones maliciosos, reducir falsos positivos y optimizar la gestión de vulnerabilidades en entornos complejos (Gavi & Kounde, 2024).

Existen diferencias entre soluciones SIEM propietarias, como Splunk o IBM QRadar, y las soluciones de código abierto, como Wazuh o el ELK Stack. Mientras que las herramientas propietarias ofrecen interfaces avanzadas como playbooks visuales (flujos de respuesta automatizada), integraciones listas para usar y soporte 24/7 con tiempos de respuesta garantizadas, las soluciones código abierto destacan por su flexibilidad y menor costo. Wazuh integra funcionalidades nativas de análisis de seguridad: detección de intrusos basada en host, detección y respuesta extendida y monitorización de log con herramientas como Elasticsearch y Kibana, lo que la hace atractiva para implementaciones de bajo presupuesto con altos requisitos técnicos.

Los sistemas de Security Information and Event Management (SIEM) ocupan un rol central en la detección y respuesta, al unificar recolección de registros, correlación de eventos, gestión de casos y cumplimiento. La efectividad del SIEM

reside en su automatización que ayuda a reducir los tiempos de respuesta y alivia la carga de los equipos de seguridad al priorizar alertas e incluso tomar medidas automatizadas contra amenazas conocidas (IBM, 2023).

2.7. Wazuh como solución SIEM

Wazuh es una plataforma de código abierto utilizada como sistema de gestión de eventos e información de seguridad (SIEM). Sus componentes son agentes, un administrador, un indexador, un panel de control, mecanismos de monitoreo de seguridad e integraciones con otras plataformas. La arquitectura se organiza en un servidor central encargado de la correlación de eventos y la gestión de alertas, agentes distribuidos para la recolección de datos desde los endpoints y módulos de análisis basados en reglas predefinidas y personalizadas (Wazuh, s. f.).

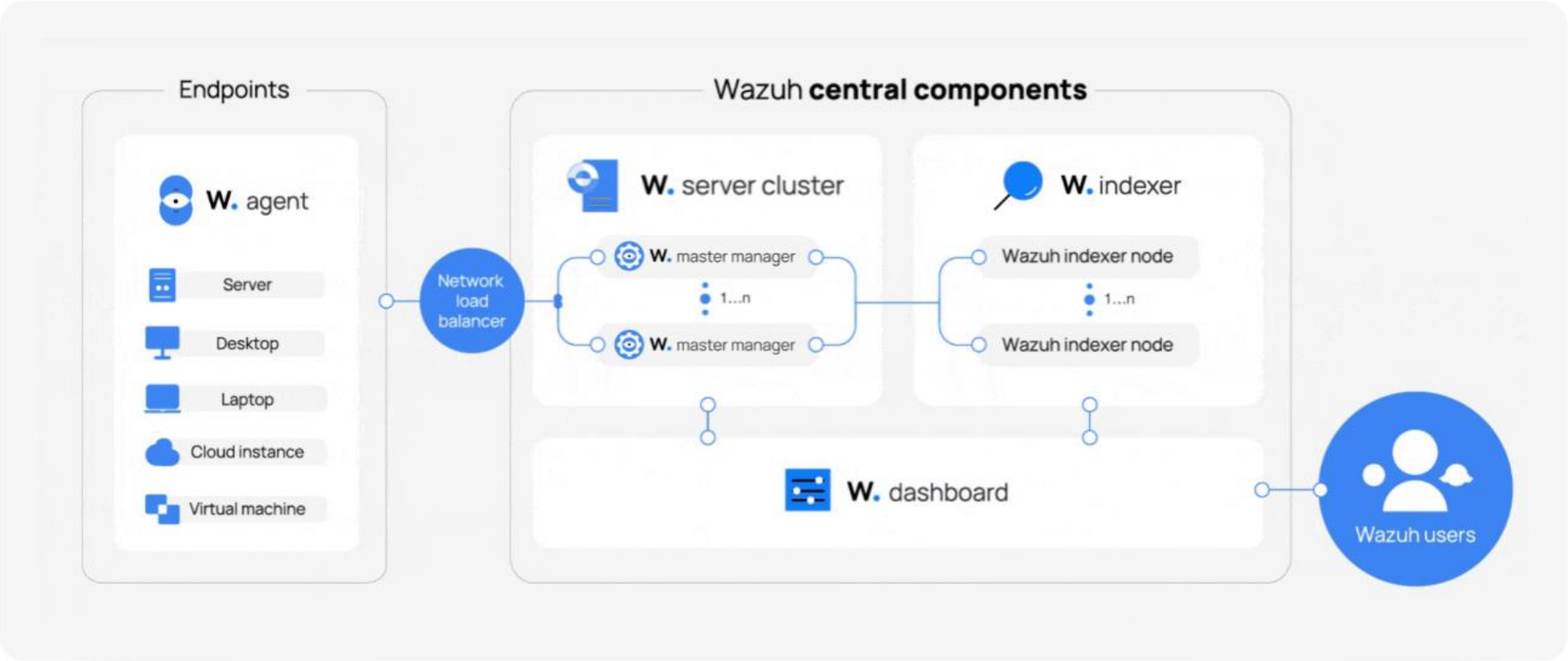
Entre sus funcionalidades más destacadas se encuentran:

- Detección de intrusiones mediante análisis de logs y monitoreo de integridad de archivos.
- Apoya el hardening automatizado conforme a las guías de seguridad del CIS pudiendo usar playbooks complementarios.

Además, Wazuh incorpora mecanismos para la aplicación de políticas de seguridad dinámicas, la generación de alertas en tiempo real y la construcción de paneles de visualización personalizables para la representación del estado de la seguridad en la infraestructura tecnológica.

Figura 7

Arquitectura Wazuh



Nota. La figura ha sido tomada de Wazuh Platform Overview (Wazuh, s. f.).

2.8. Integración de Wazuh con los CIS

En el contexto del presente proyecto, los controles CIS considerados son:

2.8.1. CIS Control 1 y 2: Inventario de hardware y software

Este control busca mantener una visibilidad completa sobre los activos tecnológicos. La implementación de escaneos semanales automatizados permite identificar nuevos dispositivos y software no autorizado en la red.

Wazuh permite la generación de alertas ante la detección de activos desconocidos o no autorizados, apoyando el control de accesos y la reducción de superficie de ataque.

2.8.2. CIS Control 3: Gestión continua de vulnerabilidades

Este control establece la necesidad de escanear regularmente los sistemas en busca de vulnerabilidades conocidas, evaluadas por su criticidad según el Common Vulnerability Scoring System (CVSS).

Wazuh integra o se complementa con escáneres de vulnerabilidades y bases de datos Common Vulnerabilities and Exposures (CVE) para identificar y priorizar vulnerabilidades, facilitando así un plan de remediación eficaz.

2.8.3. CIS Control 5: Configuración segura de hardware y software

Este control enfatiza la aplicación de políticas de hardening en sistemas operativos y aplicaciones críticas.

Wazuh facilita esta tarea mediante la supervisión continua de cambios en configuraciones importantes, notificando cualquier desviación respecto a una línea base definida, lo que permite identificar modificaciones maliciosas o errores de configuración.

2.8.4. CIS Control 6: Recolección y auditoría de logs

El control resalta la importancia de centralizar los logs de sistemas operativos, servidores y dispositivos de red para su análisis y correlación.

Wazuh permite recolectar y analizar registros de múltiples fuentes (Windows, Linux, firewalls, etc.), habilitando la detección temprana de comportamientos anómalos o eventos de seguridad.

2.8.5. CIS Control 8: Protección de datos

Este control se enfoca en la integridad y confidencialidad de los datos críticos. Wazuh incorpora el módulo de File Integrity Monitoring (FIM), el cual monitorea archivos sensibles en tiempo real, detecta accesos no autorizados, modificaciones o eliminaciones, brindando traza para análisis forense ante posibles incidentes. Estos controles son compatibles con Wazuh facilitando la automatización y auditoría de las medidas establecidas por los controles CIS.

2.9. Guía del Project Management Body of Knowledge (PMBOK)

El Project Management Institute (PMI) es una organización profesional sin fines de lucro fundada en 1969, que se ha consolidado como una autoridad global en la disciplina de la gestión de proyectos. Su misión es desarrollar estándares, certificaciones y buenas prácticas que faciliten la dirección eficaz de proyectos, fomentando la profesionalización del sector a través de la investigación y la educación. Además, el PMI es responsable de certificar a profesionales mediante credenciales reconocidas internacionalmente, como el Project Management Professional (PMP) y el Certified Associate in Project Management (CAPM) (Project Management Institute, 2021).

La Guía del PMBOK constituye el estándar más utilizado para la gestión de proyectos a nivel mundial, recopilando procesos, terminologías y mejores prácticas aceptadas universalmente. Esta guía organiza el marco metodológico en cinco grupos de

procesos inicio, planificación, ejecución, monitoreo y control y cierre, en áreas de conocimiento como integración, alcance, tiempo, costo, calidad, recursos, comunicaciones, riesgos, adquisiciones y gestión de interesados. La séptima edición del PMBOK introduce un enfoque más flexible que incorpora métodos predictivos, ágiles e híbridos, adaptándose a entornos complejos y dinámicos (Project Management Institute, 2021).

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

George Tenorio Gonzales es bachiller en Ingeniería de Sistemas Computacionales de la Universidad Privada del Norte, tiene actualmente 15 años de experiencia laboral en el área de Tecnologías de Información, trabajó en el 2010 como Analista de Sistemas en Expreso Internacional Ormeño, realizando mantenimiento y mejoras de la aplicación web de compra de pasajes terrestres y monitoreando los servidores de base de datos y aplicaciones. En el 2011 pasó a trabajar a Corporate Service Consulting S.A.C. como analista de Sistemas hasta junio del 2015, realizando procesos de inventarios físicos, como análisis y cruce de información, presentación de resultados de auditorías y reuniones de seguimiento de algunos proyectos. Desde Julio del 2015, asume la jefatura de Sistemas teniendo como responsabilidades principales las reuniones con clientes, gestión e implementación de proyectos de desarrollo de software, responsable de la integridad de la información, cálculo de costos de proyectos y elaboración de KPI´s.

En febrero de 2019 se le presentó una oportunidad laboral en Stierlift S.A., donde ingresó como Desarrollador de Tecnologías de Información, asumiendo funciones orientadas al desarrollo de aplicaciones de escritorio y web, mantenimiento de sistemas existentes y automatización de procesos para diversas áreas de la organización.

El proceso de selección incluyó dos entrevistas: la primera con el Gerente de Personas, Sr. Gino Gambini, y la segunda con la Gerente de Administración y Finanzas, Srta. Hasel Vásquez, quien posteriormente fue mi jefe directo. Durante el primer mes de incorporación, se enfocó en comprender el giro del negocio, las aplicaciones activas y sus respectivas integraciones. En el segundo mes, inició reuniones con los responsables de distintas áreas para relevar información sobre sus procesos internos y proponer

soluciones basadas en automatización.

Posteriormente, se produjeron cambios estructurales en el área de TI, lo cual derivó en su designación como Encargado del área de Tecnología e Información, incrementando sus responsabilidades y fortaleciendo sus compromisos con los objetivos estratégicos de la empresa.

3.1. Experiencia en Stierlift S.A.

3.1.1. Migración de GSuite a Office 365

En 2020, lideró el proceso de transformación digital dentro del área de TI, orientado a mejorar la gestión y disponibilidad de las herramientas corporativas. La primera iniciativa fue la migración del entorno de GSuite a Office 365, cuyo propósito fue centralizar la gestión de licencias de aplicaciones de escritorio (Word, Excel, PowerPoint, Outlook, entre otros) y optimizar la asignación de licencias de correo electrónico. Mientras que GSuite ofrecía un único tipo de licencia, Office 365 proporcionaba múltiples tipos, permitiendo una asignación más eficiente según el perfil de los colaboradores: conductores, asistentes, coordinadores, jefes y gerentes.

El objetivo del proyecto fue migrar las cuentas corporativas, garantizando la continuidad operativa, la integridad de la información y una adopción efectiva por parte de los usuarios finales. La ejecución se realizó bajo la metodología ágil SCRUM, facilitando una gestión iterativa y colaborativa con entregas incrementales distribuidas en tres hitos principales, además de un hito final destinado al cierre formal del proyecto.

Planificación y Ejecución del Proyecto

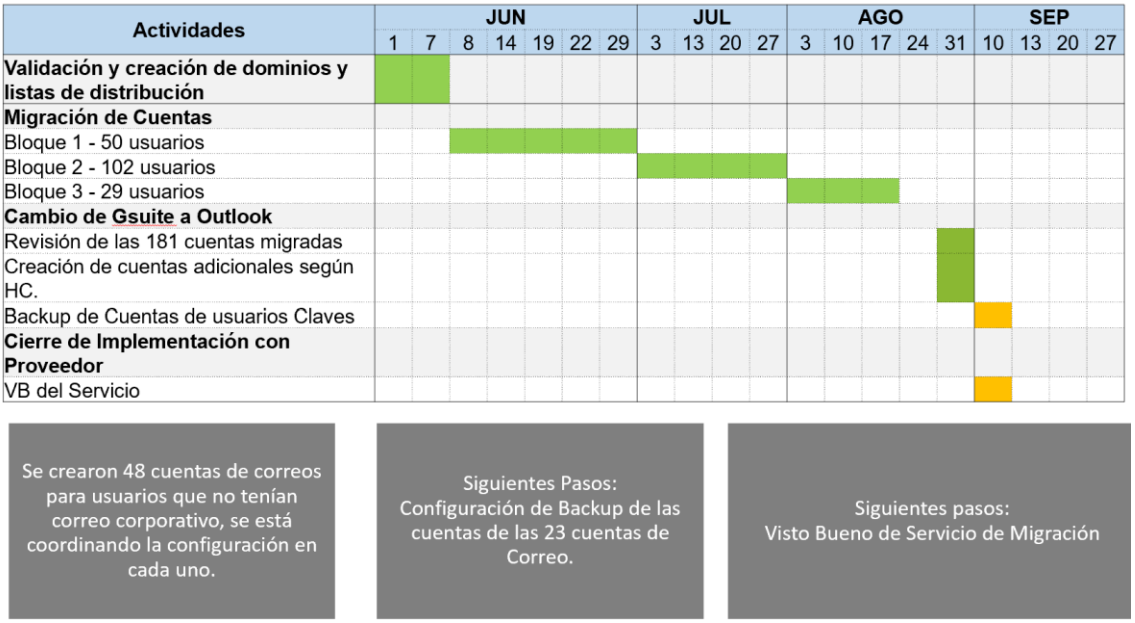
- **Migración de Cuentas (01/06/2020 – 29/08/2020)**
  - ✓ **Bloque 1:** 50 usuarios migrados y capacitados (junio).
  - ✓ **Bloque 2:** 102 usuarios migrados y capacitados (julio).
  - ✓ **Bloque 3:** 29 usuarios migrados y capacitados (agosto).

Cada bloque incluyó actividades de revisión técnica por parte del equipo de TI y sesiones de capacitación para usuarios finales.

- **Cambio de MX (31/08/2020 – 12/09/2020)**
  - ✓ Revisión de las 181 cuentas migradas.
  - ✓ Respaldo de cuentas de usuarios críticos.
  - ✓ Creación de cuentas adicionales conforme a requerimientos de Recursos Humanos.
- **Cierre de Implementación (06/09/2020 – 12/09/2020)**
  - ✓ Validación final del servicio, visto bueno (VB) del servicio y formalización del cierre del proyecto.

Figura 8

Presentación de avance de la migración de cuentas para los comités de Gerencia

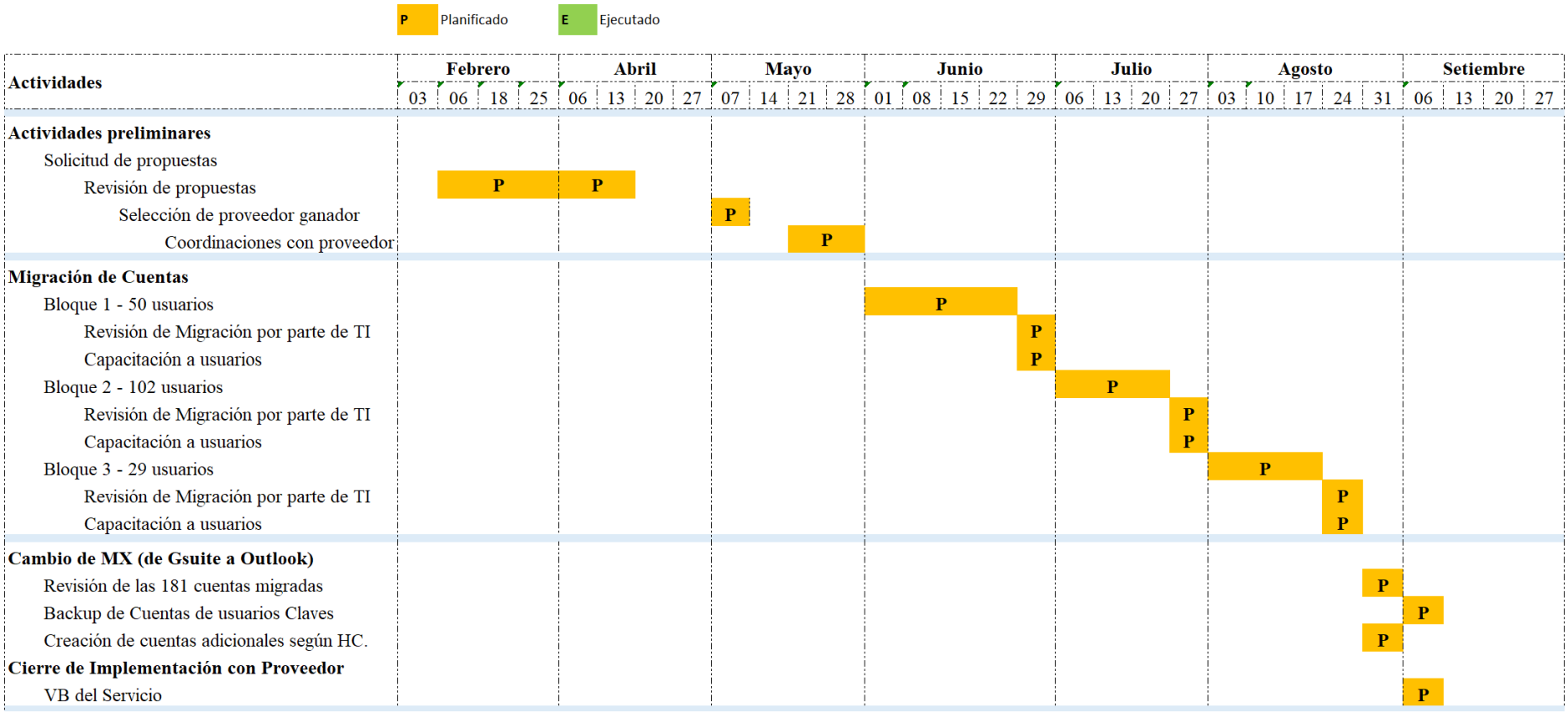


Nota. Elaboración propia a partir de información interna de la empresa.

El proyecto culminó con la migración del 100% de las cuentas planificadas, sin pérdidas de datos ni interrupciones críticas del servicio. Se logró capacitar efectivamente al personal en el uso de herramientas de Microsoft 365, consolidando la transición tecnológica. El cumplimiento de plazos, la adaptación continua a las necesidades emergentes y la participación de los usuarios fueron importantes para el éxito del proyecto. La adopción de SCRUM contribuyó significativamente a mitigar riesgos y optimizar la implementación.

Figura 9

Diagrama de Gantt de migración de Tenant.



Nota. Planificación de la migración de GSUITE a Office 365 en el año 2020.

3.1.2. MIGRACIÓN DE ERP CONTABLE-FINANCIERO

El año 2021 también estuvo a cargo como líder de sistemas y luego también como líder de proyecto dado que Stierlift S.A. tuvo la necesidad de poder integrar y centralizar los procesos más importantes de la empresa, para ello la Gerencia General solicitó la evaluación de un sistema de Planificación de Recursos Empresariales (ERP) contables/financieros que puedan cubrir con esta necesidad, se elaboró un Business Case para la justificación de este cambio de ERP.

El Business Case tuvo como objetivo principal justificar esta la implementación de un nuevo sistema ERP que permita integrar de manera centralizada y eficiente todos los procesos principales de Stierlift S.A., mejorando la trazabilidad de la información, reduciendo errores operativos y apoyando una gestión basada en datos en tiempo real. La empresa seguía en el proceso de transformación digital y ahora migraría de una estructura de sistemas descentralizada hacia una plataforma integrada que potenciaría la colaboración, agilizaría los flujos de trabajo y maximizaría la eficiencia operativa.

Dado que el ERP actual presentaba restricciones en funcionalidad, accesibilidad y soporte, lo cual afectaba la toma de decisiones, la eficiencia operativa y la seguridad de la información.

Se tenía como requerimientos del nuevo ERP:

- Integración total entre áreas: contable, financiera, logística, comercial, operativa y de RR.HH.
- Soporte para análisis por dimensiones (proyectos, centros de costo, operaciones).
- Acceso en la nube y desde dispositivos móviles (modelo SaaS).

- Automatización de procesos críticos como facturación electrónica, rendiciones, mantenimiento, compras.
- Capacidad de generar reportes de manera automática y en tiempo real.
- Conformidad con normativas locales y alineamiento con la casa matriz.

Para ello se analizaron tres ERPs:

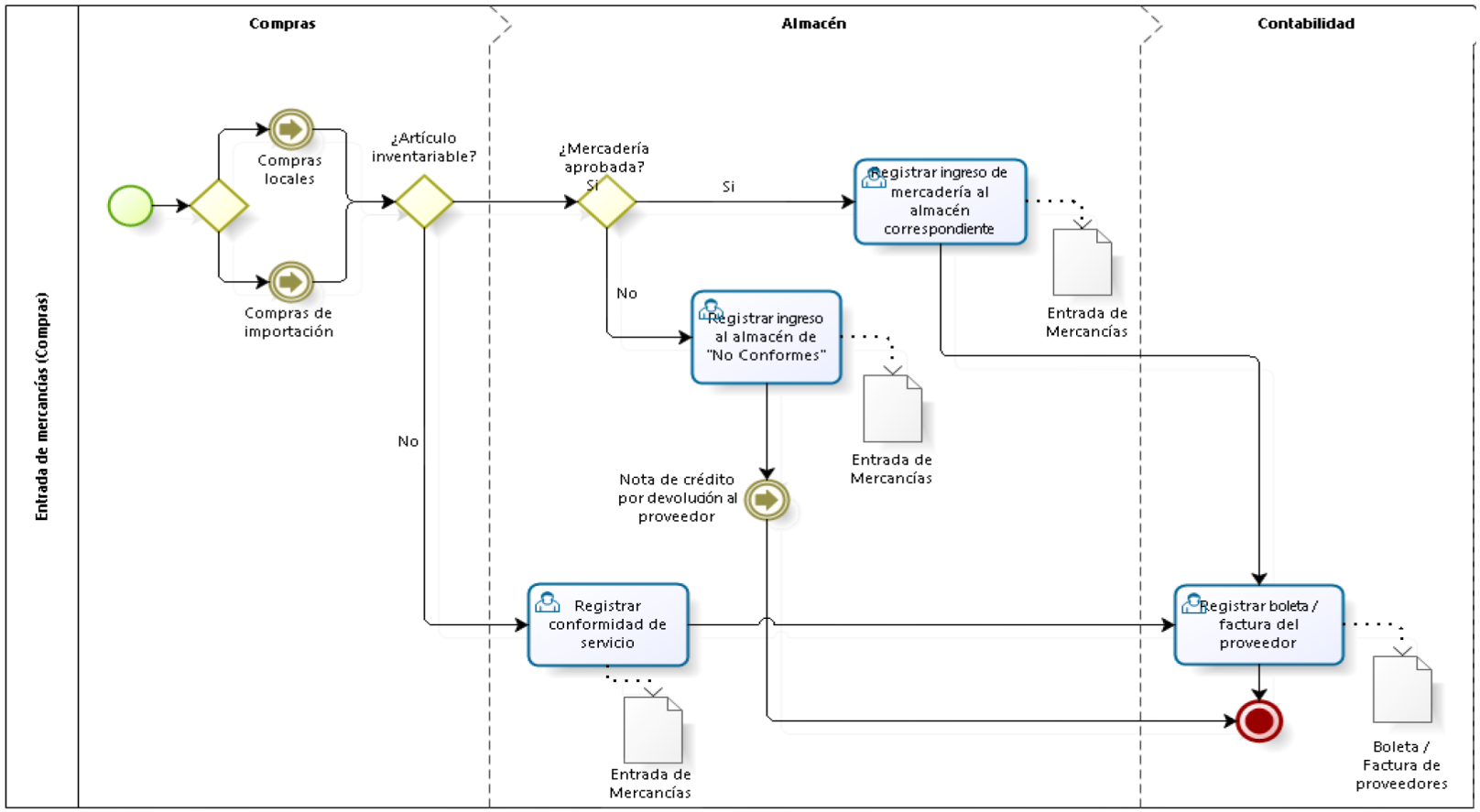
- SAP Business One
- Microsoft Dynamics 365 Business Central
- Ofisis ERP

La solución propuesta por el Business Case era migrar a SAP Business One, que cubre los requerimientos corporativos y locales, dado que ofrece integración nativa con módulos como logística, tesorería y planillas, y soporta reportería en tiempo real. El Business Case recomendó al proveedor que realizaría la implementación por su soporte post-implementación y también recomendó a una consultora externa para acompañar y asegurar el éxito del proyecto. Este proyecto inicio en enero del 2022 y culminó, con la puesta en producción, en julio 2022, se usó la metodología PMI con tiempos establecidos para cada hito.

El proveedor trabajó con Microsoft Project permitiendo una claridad en cada etapa de la implementación. Asimismo elaboraron un documento de diseño (blueprint) que funcionaba como un plan maestro detallado que alineó los procesos, la tecnología y stakeholders. El objetivo era definir alcances, metodología y requerimientos del sistema, para asegurar que todas las actividades sean ejecutadas en conocimiento de las partes.

Figura 10

Proceso de entrada de mercancía



Nota. Figura tomada del Blueprint, implementación de SAP Business One.

La implementación de SAP Business One se ejecutó conforme al cronograma establecido, cumpliendo integralmente con los objetivos planteados en el Business Case. Se logró integrar y automatizar los procesos críticos de la organización, incluyendo cotizaciones comerciales, operaciones de transporte, emisión de guías de transportistas, gestión de provisionales y control de proyectos, consolidando toda la información en una plataforma unificada.

Esto eliminó las brechas operativas del ERP anterior, como la poca trazabilidad por dimensiones (proyectos, centros de costos, márgenes) y los procesos manuales como la integración de las guías de remisión con las facturas para el área de Tesorería, la integración de las provisionales generadas con los pagos realizados en bancos alcanzando una mayor eficiencia en la generación de reportes, alineados a los estándares corporativos y normativas locales, esto permitió fortalecer la seguridad al migrar a una infraestructura en la nube, superando la dependencia de ese entonces.

La solución no solo cubrió los requerimientos funcionales y técnicos expuestos en el diagnóstico inicial, sino que también optimizó la toma de decisiones mediante datos en tiempo real, validando así la recomendación de adopción de SAP Business One y el trabajo conjunto con el proveedor.

3.2. IMPLEMENTACIÓN DE WAZUH COMO SOLUCIÓN SIEM

Esta implementación nace para fortalecer la capa de ciberseguridad de la empresa, automatizar algunos controles CIS manuales y ayudar al área de Tecnología de Información a monitorear en tiempo real los logs más severos que se pueden dar dentro de la red de la organización para responder rápidamente.

3.2.1. Objetivos

Principal

Proteger activos críticos y fortalecer el cumplimiento de CIS 1, 2, 3, 5, 6 y 8 mediante centralización de logs, correlación de eventos y monitoreo continuo.

Secundarios

- Visibilidad centralizada de logs de eventos.
- Identificar vulnerabilidades y configuraciones inseguras en los endpoints para priorizar su mitigación.

3.2.2. Diagnóstico Inicial

Situación actual

- Ausencia de visibilidad unificada en servidores y endpoints.
- Registro de eventos dispersos y no centralizados.
- Dependencia de herramientas sin integración ni automatización.

Mejoras identificadas

- Riesgo de ataques no detectados (ransomware, exfiltración).
- Cumplimiento normativo débil.
- Poca eficiencia en la detección y respuesta.

3.2.3. Enfoque y Metodología del Proyecto

El proyecto de implementación de Wazuh se desarrolló siguiendo las buenas prácticas establecidas en la guía del PMBOK enfocándose en sus cinco grupos de procesos de dirección de proyectos. Esta metodología permitió alinear la solución tecnológica con los objetivos estratégicos de Stierlift S.A., garantizar la gestión efectiva del alcance, tiempo, costos, calidad y riesgos, así como facilitar una adecuada comunicación con los interesados.

Tabla 3

Aplicación del enfoque PMI en la implementación del SIEM

Grupo de Procesos PMI	Actividades Aplicadas en el Proyecto
Inicio	– Elaboración de Business Case – Identificación de interesados
Planificación	– Aprobación del Business Case – Elaboración del cronograma – Identificación y análisis de riesgos
Ejecución	– Implementación del entorno de prueba (PoC) – Instalación y configuración de servidor Wazuh – Instalación de agentes en endpoints – Activación de módulos y controles
Monitoreo y Control	– Seguimiento del cronograma. – Verificación del cumplimiento técnico (logs, alertas, reportes). – Control de calidad de los resultados entregables.
Cierre	– Validación de entregables. – Documentación de lecciones aprendidas. – Informe final del proyecto.

3.2.4. Herramientas y tecnologías usadas en el proyecto

- **Plataforma**: Wazuh 4.11 (SIEM, XDR).
- **Software**: Ubuntu 24.04.
- **Integraciones**: CVE feed, FIM, herramientas de log, ModSecurity.
- **Recursos**: Servidor dedicado (16 CPU, 32GB RAM, 800SSD).

3.2.5. Implementación

Como en todos proyectos tecnológicos dentro de Stierlift S.A., se realiza un Business Case, el cual recomendó la implementación de Wazuh y la compra de un servidor según los requisitos técnicos para esta plataforma. Como se comentó, la implementación se basó en los 5 grupos del PMBOK cada uno en una fase:

3.2.5.1. Fase 1: Inicio

Diagnóstico y evaluación de riesgos

En esta fase inicial se realizó un levantamiento detallado de información sobre el estado actual de la ciberseguridad en la organización, identificando las principales brechas existentes, especialmente sobre la visibilidad centralizada de eventos, la automatización de controles y el cumplimiento normativo. Asimismo, se evaluaron los controles ya implementados a nivel documental y su automatización mediante herramientas tecnológicas.

Dado que Stierlift S.A. ya tenía implementado los controles CIS a nivel documental, esto facilitó la evaluación de automatización de los controles en especial el control CIS 6.

Se llevó a cabo un análisis comparativo entre soluciones SIEM comerciales y plataformas de código abierto, destacando a Wazuh como la alternativa más viable por su robustez técnica, bajo costo de implementación y alineamiento con estándares como CIS y otros como NIST e ISO 27001.

El business case recomendó la adopción de Wazuh como solución estratégica para fortalecer la postura de seguridad de la empresa, automatizar controles críticos y reducir significativamente los riesgos asociados a incidentes cibernéticos; asimismo y adquirir un equipo dedicado para esta plataforma; este Business Case se presentó a Gerencia de Administración y Finanzas, la cual dio el VB para la ejecución.

Figura 11

Costos y recursos indicados en el Business Case

$1,500 (infraestructura); implementación en 4-8 semanas con recursos internos.

Concepto	Detalle	Costo*
Infraestructura	Servidor para Wazuh (mínimo 8 núcleos, 16GB RAM, 500GB almacenamiento), más accesorios.	$1,500
Recursos Humanos	4 semanas para implementación y capacitación del equipo de TI/Security.	-
Mantenimiento	Actualizaciones periódicas y ajuste de reglas de detección.	-
Costos Totales	Bajo (solo costos de infraestructura y tiempo de implementación y mantenimiento físico del servidor).	$1,500

Nota. Figura tomada del Business Case elaborado para Stierlift S.A.

Este diagnóstico sirvió como base para definir las prioridades técnicas y estratégicas de la implementación de Wazuh, orientada a cubrir dichos vacíos de seguridad.

También se consideró las especificaciones técnicas que Wazuh sugiere para almacenar los logs por 90 días, la cantidad de procesador y la capacidad de memoria RAM para que funcione correctamente:

Tabla 4

Requisitos técnicos sugeridos por Wazuh

Agents	CPU	RAM	Storage (90 days)
1–25	4 vCPU	8 GiB	50 GB
25–50	8 vCPU	8 GiB	100 GB
50–100	8 vCPU	8 GiB	200 GB

Nota. Tomado de Wazuh Documentation, s. f.,

https://documentation.wazuh.com/current/quickstart.html

3.2.5.2. Fase 2: Planificación

Con base en el diagnóstico, se definieron las siguientes acciones:

- Instalación inicial en un entorno de prueba (PoC).
- Despliegue en servidores críticos.
- Activación gradual de los controles CIS prioritarios (1, 3, 5, 6 y 8).
- Capacitación técnica al equipo interno de TI.
- Escalamiento a toda la infraestructura tecnológica.

También se establecieron los recursos necesarios para el proyecto, entre ellos un servidor dedicado, 4 semanas de dedicación técnica del equipo interno de TI para la implementación del SIEM y un presupuesto base de $1,500 para infraestructura, sin recurrir a licencias comerciales. Este proyecto contempló una duración total estimada de 6 meses desde la elaboración del Business Case hasta la fase de cierre.

Tabla 5

Recursos de servidor SIEM instalado

Recurso	Valor
Plataforma	VMware Workstation Pro
Tipo de Red	Bridged (con IP estática)
IP Asignada	192.168.X.X
Sistema Operativo	Ubuntu Server 24.04.2 (64-bit)
Recursos asignados	32 GB RAM, 800 GB SSD, 16 Cores
Host LAN	Red local 192.168.X.0/24

Nota. El servidor fue virtualizado en VMware con recursos por arriba de las especificaciones mínimas.

3.2.5.3. Fase 3: Ejecución

En esta fase se ejecutaron las actividades previstas en la planificación:

- Se implementó una prueba de concepto para validar la compatibilidad del entorno con Wazuh.
- Se instaló el servidor Wazuh en una máquina con los recursos mínimos requeridos (16 núcleos, 32 GB RAM y 800 GB SSD de almacenamiento).
- Se configuró la recolección centralizada de logs desde sistemas Linux, Windows y firewalls.

Pasos técnicos para la implementación

Preparación del sistema operativo Ubuntu

Actualización del sistema:

sudo apt update && sudo apt upgrade -y

Instalación de paquetes base

sudo apt install curl vim net-tools unzip gnupg -y

Verificación de red y DNS

IP fija validada: *192.168.X.X*

Instalación de Wazuh All-in-One (Versión 4.11.0)

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh

chmod +x wazuh-install.sh

Ejecución de instalación todo-en-uno:

sudo ./wazuh-install.sh -a

Se instalaron correctamente

- ✓ Wazuh Manager
- ✓ Wazuh Indexer
- ✓ Wazuh Dashboard

Figura 12

Servidor Wazuh implementado

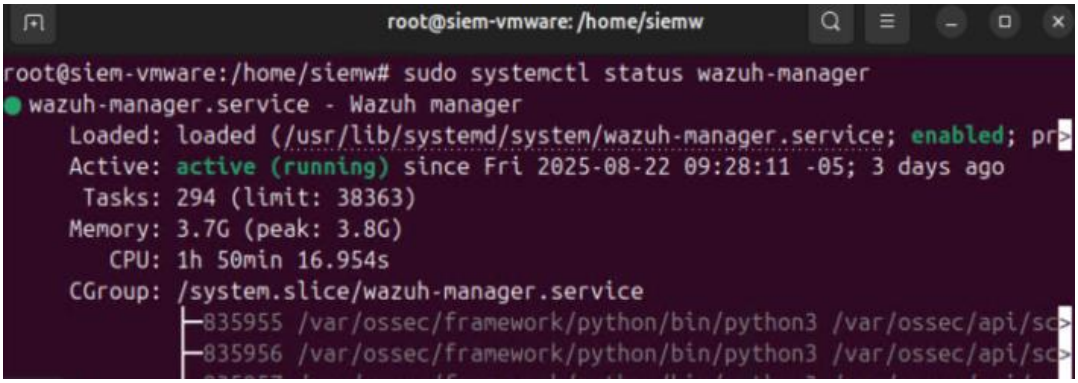


Tabla 6

Errores y correcciones en la instalación de Wazuh

Problema	**Solución Aplicada**
Uso incorrecto del parámetro --wazuh-version	Se corrigió usando -a (modo all-in-one)
Acceso HTTPS desde navegador externo fallaba	Se aceptó manualmente el certificado autofirmado
Acceso externo no funcionaba inicialmente	Confirmado UFW inactivo + puerto 8443 activo
Dashboard solo accesible desde la VM	Verificado modo Bridged, ping OK, puerto 8443 abierto

Capacitación y Fortalecimiento del Equipo

Se llevó a cabo una capacitación técnica intensiva dirigida al analista de sistemas que se encargará de realizar la instalación de los agentes en el resto de los equipos, enfocada en los siguientes temas:

- Generación de llaves para los agentes.
- Administración de la plataforma Wazuh.
- Interpretación de alertas y correlación de eventos.

- Gestión de reglas de detección y personalización de configuraciones.
- Generación de reportes para auditorías y cumplimiento normativo.

Instalación y configuración de agentes (Windows)

Agentes instalados manualmente en distintos equipos Windows (v4.11 y v4.12).

Agente con versión 4.12 no se conectaba:

Se detectó incompatibilidad por diferencia de versión. Se instaló agente 4.11 manualmente para garantizar compatibilidad.

Generación de claves para registrar agentes:

Desde la VM (Wazuh Manager):

/var/ossec/bin/manage_agents

Tabla 7

Errores en la conexión entre los agentes y el manager

Problema	**Solución**
Agente decía “Nunca conectado”	Se corrigió usando versión compatible y clave válida
Error en hostname o IP	Se usó IP correcta del manager en agent.conf
Servicio no iniciaba en Windows	Se reinició el servicio desde “Services”
Validación de conexión	
En Dashboard: agente pasó de “Nunca conectado” a “Activo”.	

Integración con FortiGate

La integración con FortiGate se realizó utilizando el protocolo *syslog* en el puerto 514, asegurando la transmisión constante de logs al servidor Wazuh. La decodificación de eventos FortiGate fue exitosa, identificando categorías como tráfico, IPs, autenticaciones y VPN. Este trabajo se hizo en coordinación con el proveedor de seguridad perimetral.

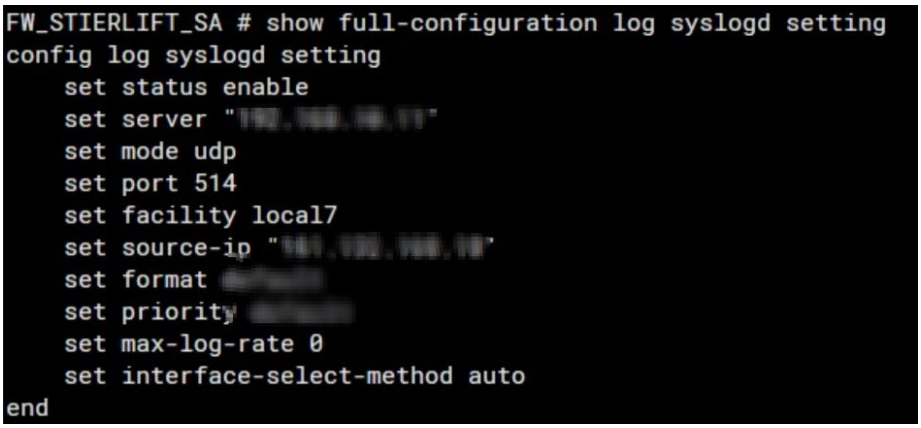
Figura 13

Configuración de syslog en Wazuh

Nota. Configuración realizada en el manager configuración de Wazuh

Figura 14

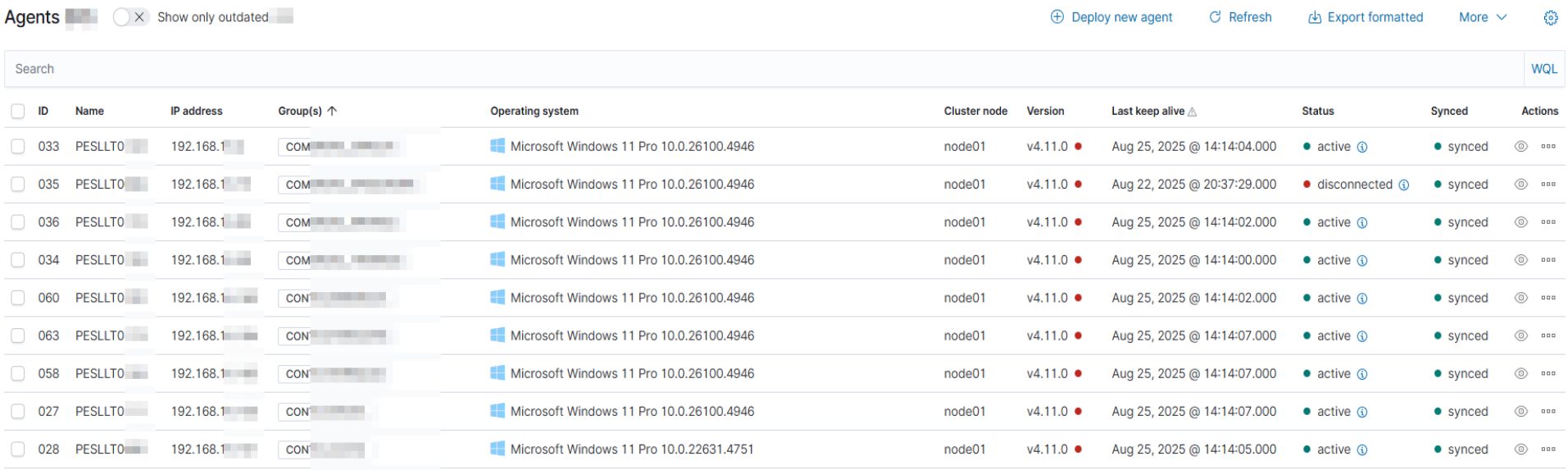
Configuración en FortiGate



Nota. Configuración realizada en el FortiGate del proveedor.

Figura 15

Listado de agentes instalados



Nota. Tomado de la vista de agentes del Wazuh manager.

3.2.5.4. Fase 4: Monitoreo y control

Durante esta fase se realizó un seguimiento continuo al avance del proyecto y la correcta ejecución de las actividades planificadas, asegurando el cumplimiento del cronograma, el alcance definido y la calidad del servicio. Para ello se empleó un diagrama de Gantt y la herramienta Microsoft Planner, lo que permitió controlar el progreso de cada tarea y detectar posibles desviaciones a tiempo.

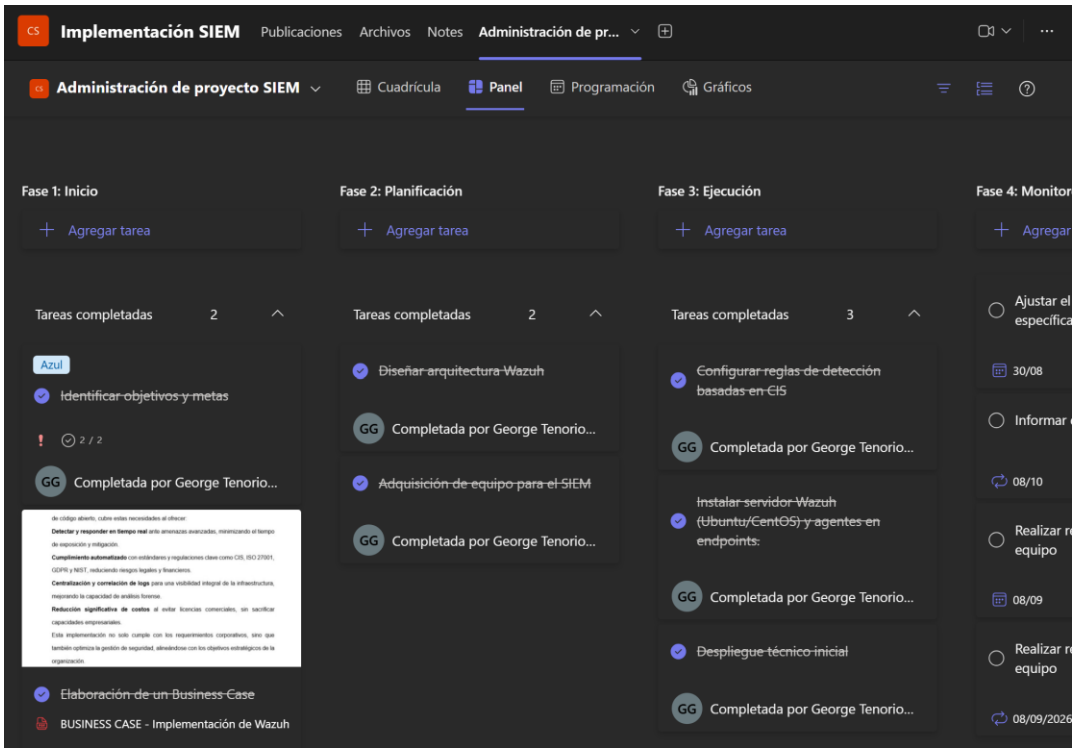
Tabla 8

Cronograma de implementación de Wazuh

Descripción del hito	Progreso	Días	Abril	Mayo	Junio	Julio	Agosto
Fase 1: Inicio							
Elaboración de Business Case	**100%**	28					
Identificación de interesados	**100%**	2					
Fase 2: Planificación							
Aprobación del Business Case	**100%**	1					
Elaboración del cronograma	**100%**	10					
Identificación y análisis de riesgos	**100%**	3					
Fase 3: Ejecución							
Implementación del entorno de prueba (PoC)	**100%**	3					
Instalación y configuración de servidor Wazuh	**100%**	3					
Instalación de agentes en endpoints	**100%**	24					
Activación de módulos y controles	**100%**	2					
Fase 4: Monitoreo y control							
Seguimiento del cronograma.	**100%**	30					
Verificación del cumplimiento técnico (logs, alertas, reportes).	**100%**	5					
Control de calidad de los resultados entregables.	**100%**	1					
Fase 5: Cierre							
Validación de entregables.	**100%**	2					
Documentación de lecciones aprendidas.	**100%**	2					
Informe final del proyecto.	**100%**	1					

Figura 16

Planner de proyecto de implementación del SIEM



CAPÍTULO IV. RESULTADOS

La implementación del SIEM Wazuh en un entorno de nodo único permitió consolidar todas las funciones críticas en una sola instancia, asegurando la centralización de eventos y la reducción de complejidad operativa.

El despliegue en Ubuntu 24.04.2, con recursos robustos (32 GB RAM, 16 vCPU, 800 GB SSD), brindó estabilidad para manejar la carga inicial sin saturaciones. Se alcanzó una integración efectiva con dispositivos endpoint (Windows) y FortiGate mediante Syslog, posibilitando la ingesta y correlación de eventos de firewall, IPs, webfilter y VPN, complementando la visibilidad de la red perimetral con la de los endpoints monitoreados.

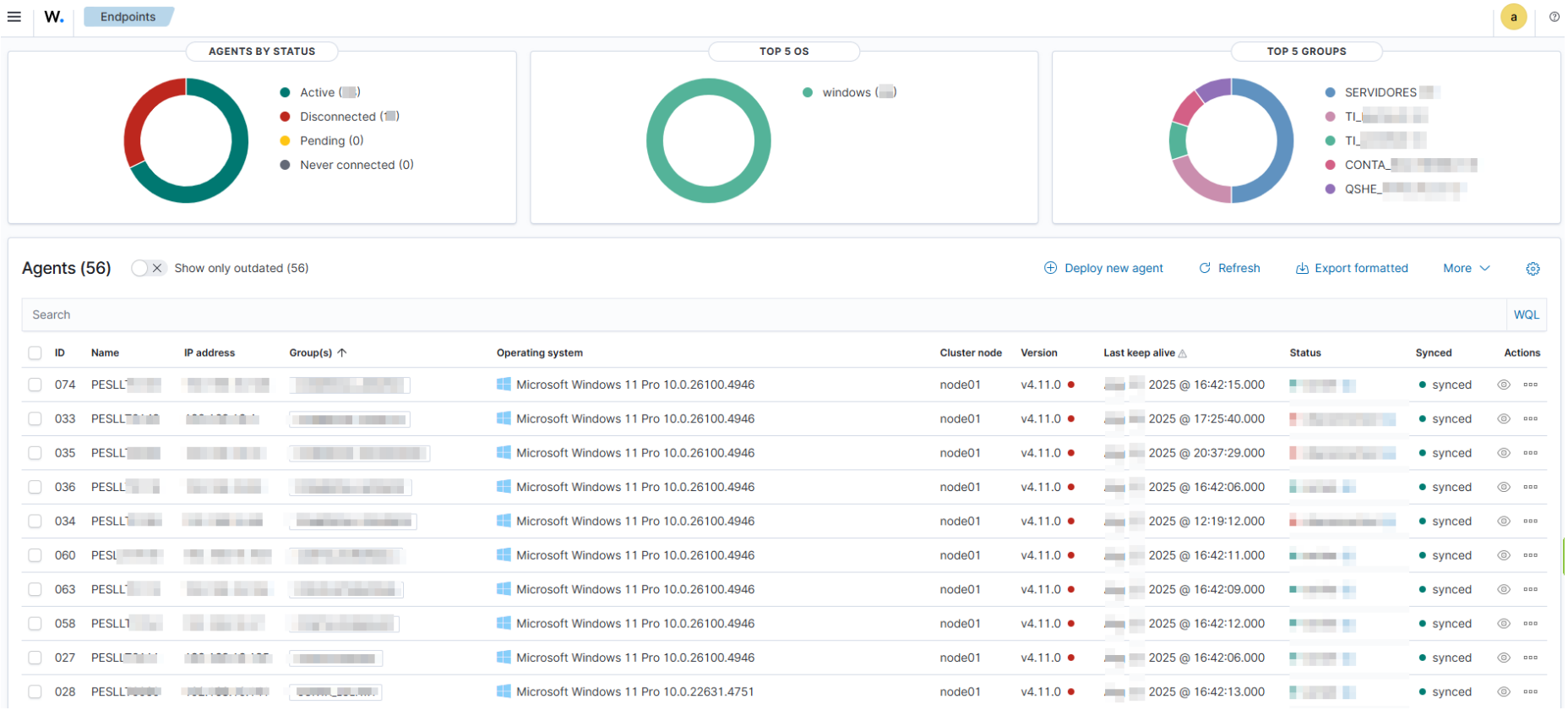
4.1. Cobertura de endpoints y agentes

Se logró la conexión y monitoreo de múltiples agentes Wazuh en Sistemas Operativos (SO) Windows, asegurando la recolección de logs, inventarios de aplicaciones y eventos críticos.

El tiempo promedio para el registro y activación de cada agente fue inferior a 5 minutos. La plataforma ofrece vistas detalladas del estado de los agentes, con indicadores de conectividad y actualizaciones, permitiendo una gestión proactiva.

Figura 17

Dashboard Wazuh de endpoint Windows

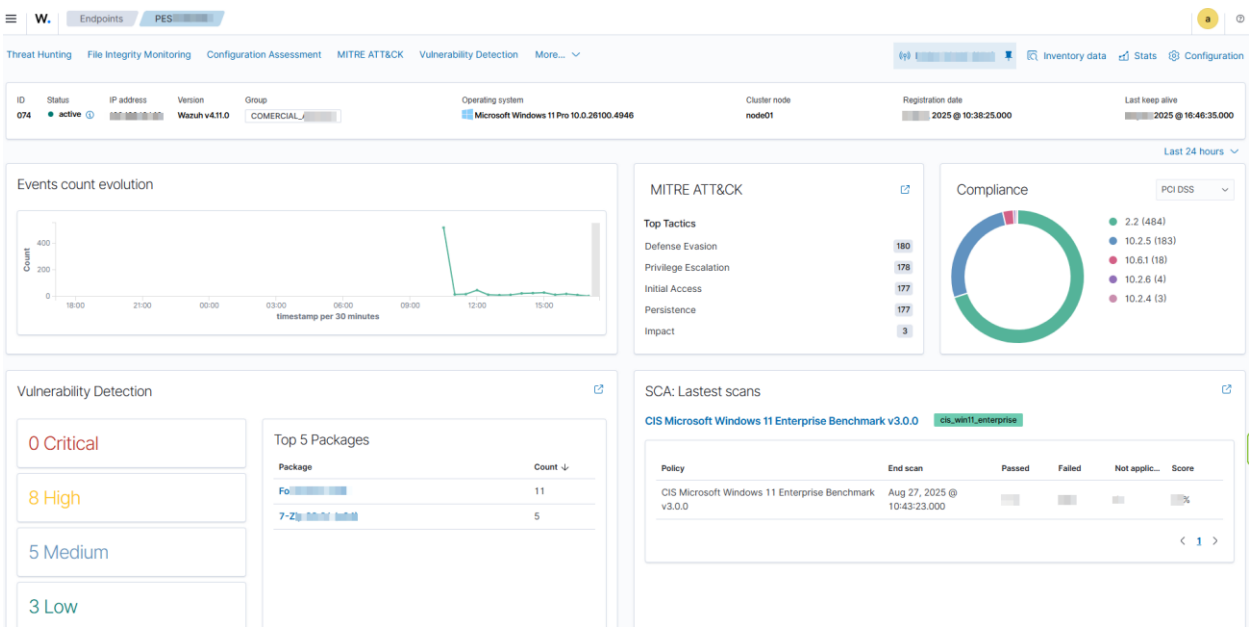


Nota. Tomado de wazuh-manager productivo TI Stierlift S.A. 2025.

Ahora se cuenta con un inventario completo de cada activo: IP, sistema operativo, memoria, CPU, arquitectura, inventario de aplicaciones instaladas, estado de puertos, conexiones e interfaces de red; asimismo, cumplimiento CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0, MITRE ATT&CK, detecciones de vulnerabilidades, permitiendo todo esto realizar un hardening automatizado.

Figura 18

Detalle de un endpoint en dashboard de wazuh



En la parte superior izquierda de la imagen, se observa la evolución de eventos, destacando un pico significativo alrededor de las 11:00 horas, esto debido a que es la primera vez que el agente se había configurado. En la sección MITRE ATT&CK se identifican tácticas asociadas a técnicas críticas como evasión de defensas, escalamiento de privilegios e intentos de acceso inicial, lo que sugiere posibles intentos de sesión. En cuanto a vulnerabilidades, no se reportan críticas, pero sí 8 de nivel alto, principalmente asociadas a FortiClient VPN y 7-Zip.

4.2. Resultados sobre los controles CIS

Los resultados que se presentan en este informe corresponden al estado de los sistemas monitoreados en un día específico del 2025, según los registros disponibles en el SIEM Wazuh en ese momento:

4.2.1. CIS 1 y 2

CIS 1: Se obtiene el inventario en tiempo real de los activos con los agentes conectados y desconectados. Ver figura 17.

CIS 2: Sobre el inventario de software, Wazuh mantiene todo el detalle por agente.

Figura 19

Lista de aplicaciones instaladas de un equipo Windows

Packages (78)

Search

Name	Architecture	Version	Vendor
7-Zip 24.09 (x64)	x86_64	24.09	Igor Pavlov
Adobe Acrobat (64-bit)	x86_64	25.001.20643	Adobe
Adobe Refresh Manager	i686	1.8.0	Adobe Systems Incorporated
AnyDesk	i686	ad 9.0.7	AnyDesk Software GmbH
Aplicaciones de Microsoft 365 para negocios - es-es	x86_64	16.0.19127.20154	Microsoft Corporation
Asistencia rápida	x86_64	2.0.36.0	Microsoft Corp.
Contactos	x86_64	10.2202.100.0	Microsoft Corporation
CrossDevice Files	x86_64	1.25072.52.0	Microsoft Windows
DefaultPackMSI	i686	4.6.2.0	Microsoft
EPSON L575 Series Printer Uninstall	x86_64		SEIKO EPSON Corporation

Rows per page: 10

Nota. Figura tomada del “Inventory Data software” de un agente específico.

4.2.2. CIS 3 – Gestión continua de vulnerabilidades (Vulnerability Detector)

Eventos del detector: 76 CVEs únicas

CVE-2022-40897, CVE-2023-27043, CVE-2024-28219, CVE-2024-34064, …, CVE-2025-53156, CVE-2025-53716, …, CVE-2025-8747

Hallazgo: Predominan vulnerabilidades High (72% de los eventos del detector), con 3 críticas. Esto orienta un backlog de parchado priorizado a alto/ crítico.

4.2.3. CIS 5 – Configuración segura (monitoreo de cambios en cuentas y grupos)

Conteo por EventID (gestión de identidad/grupos):

- **4625** (Logon Failed): **110**
- **4732** (Miembro agregado a grupo local habilitado para seguridad): **26**
- **4728** (Miembro agregado a grupo global habilitado para seguridad): **26**
- **4726** (Cuenta de usuario eliminada): **26**
- **4720** (Cuenta de usuario creada): **26**
- **4740** (Cuenta bloqueada): **1**

Hallazgo: Hubo 26 altas y 26 bajas de cuentas/miembros de grupo (eventos 4720/4726/4728/4732), lo que exige revisión de autorizaciones y tickets que los respalden. Los 110 fallos de inicio de sesión (4625) y 1 bloqueo (4740) sugieren intentos fallidos que conviene correlacionar con IPs/horarios.

4.2.4. CIS 6: Recolección y Auditoría de Logs

La centralización de registros fue uno de los resultados más significativos del proyecto, dado que se consolidaron en el SIEM 65,652 eventos provenientes de los 44 agentes y del firewall FortiGate, representando un volumen total de 7.2 GB de datos auditados.

La correlación en tiempo real permitió clasificar las alertas por severidad, obteniendo la siguiente distribución:

Tabla 9

Cantidad de eventos por niveles de seguridad

Nivel	Cantidad de eventos
3	41,248
4	1,894
5	13,288
6	4,541
7	759
8	47
9	3,956
10	1,080
12	23

De este total, el 62.8% correspondió a alertas de nivel 3, relacionadas principalmente con intentos de acceso no autorizado y fallos menores en autenticación, mientras que el 20.2% se concentró en nivel 5, asociado a configuraciones críticas. Se evidencia que los eventos de mayor severidad (niveles ≥9) representaron 7.6%, donde sobresalen registros provenientes del firewall FortiGate por intentos fallidos de acceso SSL VPN.

Esta integración permitió asegurar el cumplimiento del CIS Control 6, garantizando la recolección completa de logs, trazabilidad para auditorías y capacidad de respuesta inmediata ante incidentes.

4.2.5. CIS 8

Para el control CIS 8, el monitoreo de integridad de sistemas se realizó mediante el módulo S*yscheck* de Wazuh, generando un total de 25,605 alertas (100%). El alto volumen de alertas indica una cobertura integral de los endpoints, asegurando la detección continua de modificaciones, adiciones o eliminaciones de archivos críticos según la configuración de integridad, y proporcionando métricas precisas para auditoría y control de seguridad.

Tabla 10

Listado de agentes con mayores alertas de Syscheck

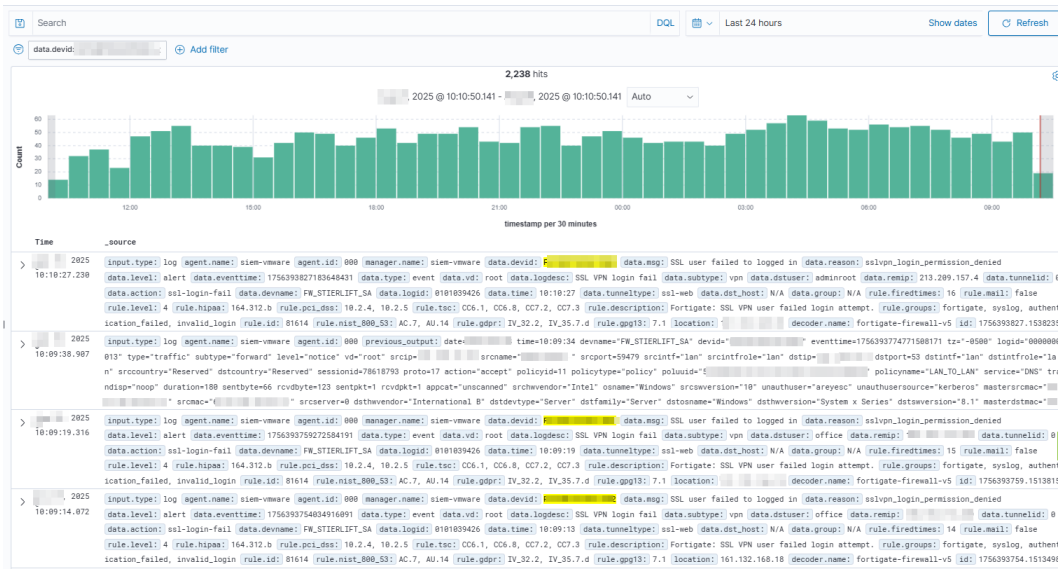
Agente	Alertas	% del total
ENDPOINT1	3,066	12.00%
ENDPOINT2	2,211	8.60%
ENDPOINT3	2,208	8.60%

4.3. Resultado de la integración con FortiGate

La integración del firewall FortiGate con el SIEM Wazuh se efectuó mediante el envío de logs en formato *syslog* al puerto designado, empleando el decodificador nativo *fortigate-firewall-v5* para normalizar los eventos.

Figura 20

Recolección de logs del FortiGate



Esta correlación no solo fortaleció la visibilidad del perímetro, sino que también facilitó la respuesta oportuna ante intentos de intrusión, permitiendo aplicar medidas correctivas en el sistema de acceso remoto.

Resultados de análisis de logs de FortiGate

Total de intentos SSL VPN fallidos: 997

read_alerts_by_date_local "$D" | jq -c 'select(.rule.groups[]? == "fortigate" and .data.action? == "ssl-login-fail")' | wc -l

Top 5 IPs origen con más intentos de acceso fallidos

read_alerts_by_date_local "$D" | jq -r 'select(.rule.groups[]? == "fortigate" and .data.action? == "ssl-login-fail") | .data.remip // "NA"' | sort | uniq -c | sort -nr | head -5

Tabla 11

Top 5 de IPs origen con más intentos fallidos

Top	Cantidad	IP
1	234	45.155.91.130
2	68	185.39.19.120
3	63	77.83.207.251
4	49	178.22.24.30
5	20	178.16.55.141

Una de las alertas encontradas fue la de “Fortigate: SSL VPN user failed login attempt”, la cual fue categorizada bajo el grupo *authentication_failed* e identificada con un nivel de severidad 4. Se comunicó inmediatamente al proveedor para que inhabilite dicho acceso dado que no era usado por Stierlift S.A.:

Figura 21

Confirmación del proveedor de inhabilitación de la VPN SSL-Web

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Stierlift S.A. presentaba una limitada visibilidad sobre la actividad de los activos críticos y la red, lo que dificultaba identificar intentos de acceso indebido y vulnerabilidades. La implementación de Wazuh permitió centralizar la recolección de eventos de agentes y del firewall FortiGate, generando una visión unificada del estado de seguridad y facilitando el cumplimiento de los controles CIS 1, 2, 3, 5, 8 y del CIS 6 principalmente.
- Inicialmente no se contaba con automatizaciones para detectar accesos no autorizados. Mediante la integración de los logs de FortiGate en Wazuh y la correlación de eventos, se identificaron intentos de conexión fallida vía SSL VPN, con evidencia de direcciones IP y usuarios objetivo. Esto demostró que la herramienta aportó capacidad de detección temprana de amenazas en concordancia con el CIS 5.
- La experiencia en Stierlift S.A. comprobó que, aún con limitaciones de infraestructura y alcance parcial de controles, la implementación de un SIEM como Wazuh proporciona un avance significativo en la postura de ciberseguridad, ofreciendo indicadores claros sobre accesos indebidos, vulnerabilidades críticas y evidencias alineadas a los controles de seguridad.

5.2. Recomendaciones

- Dado que el despliegue se realizó en un único nodo Wazuh, se recomienda evaluar la migración a un entorno distribuido (manager, indexer y dashboard separados) para soportar mayor volumen de agentes y mejorar la resiliencia ante fallos.

- El análisis mostró que existen vulnerabilidades con severidad “Critical” y “High” en diferentes agentes. Se recomienda establecer un ciclo de gestión de parches priorizando los activos más expuestos y usar Wazuh como sistema de alerta temprana para validar la efectividad de la remediación.
- Se recomienda implementar procedimientos guiados (playbooks) simplificados para la respuesta a incidentes de ocurrencia frecuente, como el bloqueo manual asistido de direcciones IP en FortiGate tras múltiples intentos de acceso fallido o la desactivación manual de cuentas de usuario con actividad sospechosa.
- Se recomienda integrar al SIEM herramientas de SOAR (Security Orchestration, Automation and Response), con el fin de enriquecer la detección de amenazas y automatizar la respuesta a incidentes, esto permitiría complementar la automatización de respuestas superando algunas restricciones actuales de Wazuh.

REFERENCIAS

Admass, S., Yang, Y., Chen, J., & Conran, A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 3, 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmed, M., Wei, J., & Al-Shaer, E. (2024). Prompting LLM to enforce and validate CIS Critical Security Control. En Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT 2024) (pp. 93–104). ACM. https://doi.org/10.1145/3649158.3657036

Center for Internet Security (CIS). (2021). CIS Critical Security Controls Version 7. Center for Internet Security. https://www.cisecurity.org/controls/v7-1

Center for Internet Security (CIS). (2025). CIS Critical Security Controls v8.1. Center for Internet Security. https://www.cisecurity.org/controls/v8

Faisal Yahya. (2025, abril). Security Orchestration, Automation, and Response (SOAR). Faisal Yahya's Blog. https://faisalyahya.com/threat-defense/security-orchestration-automation-and-response-soar

Gavi, K., & Kounde, M. (2024). Optimizing threat detection and incident response through AI-powered automation in SIEM systems. Journal of Cybersecurity and Privacy Research, 1(1), 1–15. https://www.researchgate.net/publication/387903611

Haverinen, H., Janhunen, T., Päivärinta, T., Lempinen, S., Kaartinen, S., & Merilä, S. (2024). Automating cybersecurity compliance in DevSecOps with open information model for security as code. En Proceedings of 4th Eclipse Security, AI, Architecture and Modelling Conference on Data Spaces (eSAAM 2024) (pp. 93–102). ACM. https://doi.org/10.1145/3685651.3686700

IBM. (2023). What is SIEM? IBM Think Topics. Recuperado el 26 de octubre de 2023, de https://www.ibm.com/think/topics/siem

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

JumpCloud. (2025, 14 de agosto). What is a SOAR Playbook? JumpCloud. https://jumpcloud.com/it-index/what-is-a-soar-playbook

Kenfack, P. D. B., et al. (2023). Strengthening the security of supervised networks by automating hardening mechanisms. Journal of Computer and Communications, 11(5), 109–125. https://doi.org/10.4236/jcc.2023.115009

Kolini, F., & Janczewski, L. J. (2022). Exploring incentives and challenges for cybersecurity intelligence sharing (CIS) across organizations: A systematic review. Communications of the Association for Information Systems, 50. https://doi.org/10.17705/1CAIS.05004

Mahmoud, M. M. E., Abdelhamid, A. A., ElGohary, R. E., & El-Nahas, M. (2022). Systematic literature review of security event correlation methods. IEEE Access, 10, 43387–43420.
https://doi.org/10.1109/ACCESS.2022.3168976

MITRE. (s. f.). *ATT&CK® framework*. https://attack.mitre.org

National Institute of Standards and Technology (NIST). (2024). El Marco de Seguridad Cibernética (CSF) 2.0 del NIST [NIST Cybersecurity White Papers (CSWP-29)] (versión en español). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

Occupational Safety and Health Administration (OSHA). (2023). *OSHA Standards*. https://www.osha.gov/laws-regs

PECB. (2022). ISO/IEC 27001 – What are the main changes in 2022? https://pecb.com/en/article/iso-iec-27001-what-are-the-main-changes-in-2022

Project Management Institute (PMI). (2021). A guide to the project management body of knowledge (PMBOK® Guide) (7.ª ed.). Project Management Institute.

Stierlift S.A. (s. f.). Historia y servicios. https://www.stierlift.com.pe

Ultramar. (2024). Informe corporativo anual. https://www.ultramar.com

Wazuh. (s. f.). Quickstart. Wazuh Documentation. https://documentation.wazuh.com/current/index.html

Zaid, T., & Garai, S. (2024). Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers. Blockchain in Healthcare Today, 7, e302. https://doi.org/10.30953/bhty.v7.302